QUESTION 132
Which of the following commands will allow a penetration tester to permit a shell script to be executed by the file owner?

A. `chmod u+x script.sh`
B. `chmod u+e script.sh`
C. `chmod o+e script.sh`
D. `chmod o+x script.sh`

Answer: A
Explanation:
https://newbedev.com/chmod-u-x-versus-chmod-x

QUESTION 133
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

QUESTION 134
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 over time.

Answer: A
Explanation:
https://attack.mitre.org/

QUESTION 135
A penetration tester discovered a vulnerability that provides the ability to upload to a path via discovery traversal. Some of the files that were discovered through this vulnerability are:

```
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/newbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/rmbm.pl
https://xx.xx.xx.x/vpn/../vpns/portal/scripts/picktheme.pl
https://xx.xx.xx.x/vpn/../vpns/cfg/smb.conf
```

Which of the following is the BEST method to help an attacker gain internal access to the affected machine?

A. Edit the discovered file with one line of code for remote callback.
B. Download .pl files and look for usernames and passwords.
C. Edit the smb.conf file and upload it to the server.
D. Download the smb.conf file and look at configurations.

Answer: C

QUESTION 136
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: B

QUESTION 137
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

QUESTION 138
Which of the following is the MOST common vulnerability associated with IoT devices that are directly connected to the Internet?

A. Unsupported operating systems
B. Susceptibility to DDoS attacks
C. Inability to network
D. The existence of default passwords

Answer: A

QUESTION 139
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

QUESTION 140
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

QUESTION 141
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

QUESTION 142
A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees' phone numbers on the company's website, the tester has learned the complete phone catalog was published there a few months ago.
In which of the following places should the penetration tester look FIRST for the employees' numbers?

A. Web archive
B. GitHub
C. File metadata
D. Underground forums

Answer: A

QUESTION 143
A penetration tester completed a vulnerability scan against a web server and identified a single but severe vulnerability.
Which of the following is the BEST way to ensure this is a true positive?

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

Answer: B

QUESTION 144
A company's Chief Executive Officer has created a secondary home office and is concerned that the WiFi service being used is vulnerable to an attack. A penetration tester is hired to test the security of the WiFi's router.
Which of the following is MOST vulnerable to a brute-force attack?

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

Answer: A
Explanation:
https://us-cert.cisa.gov/ncas/alerts/TA12-006A

QUESTION 145
A penetration tester ran the following commands on a Windows server:

```
schtasks
echo net user svsaccount password /add >> batchjopb3.bat
echo net localgroup Administrators svsaccount /add >> batchjopb3.bat
net user svsaccount
runas /user:svsaccount mimikatz
```

Which of the following should the tester do AFTER delivering the final report?

A. Delete the scheduled batch job.
B. Close the reverse shell connection.
C. Downgrade the `svsaccount` permissions.
D. Remove the tester-created credentials.

Answer: C

QUESTION 146
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

QUESTION 147
The following line-numbered Python code snippet is being used in reconnaissance:

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

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

A. Line 01
B. Line 02
C. Line 07
D. Line 08
E. Line 12

Answer: A

QUESTION 148
A consulting company is completing the ROE during scoping.
Which of the following should be included in the ROE?

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

Answer: B

QUESTION 149
A new client hired a penetration-testing company for a month-long contract for various security assessments against the client’s new service. The client is expecting to make the new service publicly available shortly after the assessment is complete and is planning to fix any findings, except for critical issues, after the service is made public. The client

wants a simple report structure and does not want to receive daily findings.
Which of the following is most important for the penetration tester to define FIRST?

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

Answer: A

QUESTION 150
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

QUESTION 151
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. OWASP ZAP
D. Empire

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

QUESTION 152
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