QUESTION 170
A penetration tester executed a vulnerability scan against a publicly accessible host and found a web server that is vulnerable to the DROWN attack. Assuming this web server is using the IP address 127.212.31.17, which of the following should the tester use to verify a false positive?

A. Openssl s_client -tls1_2 -connect 127.212.31.17:443
B. Openssl s_client -ss12 -connect 127.212.31.17:443
C. Openssl s_client -ss13 -connect 127.212.31.17:443
D. Openssl s_server -tls1_2 -connect 127.212.31.17:443

Answer: A

QUESTION 171
A penetration tester obtained access to an internal host of a given target. Which of the following is the BEST tool to retrieve the passwords of users of the machine exploiting a well-knows architecture flaw of the Windows OS?

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

Answer: A

QUESTION 172
Defining exactly what is to be tested and the results to be generated from the test will help prevent?

A. testing scope creep
B. scheduling conflicts
C. impact on production
D. disclosure of information.

Answer: A

QUESTION 173
A consultant is attempting to harvest credentials from unsecure network protocols in use by the organization. Which of the following commands should the consultant use?

A. Tcmpump
B. John
C. Hashcat

D. nc

Answer: A

QUESTION 174
An SMB server was discovered on the network, and the penetration tester wants to see if the server it vulnerable. Which of the following is a relevant approach to test this?

A. Null sessions
B. Xmas scan
C. ICMP flood
D. SYN flood

Answer: C

QUESTION 175
A penetration tester is reviewing a Zigbee Implementation for security issues. Which of the following device types is the tester MOST likely testing?

A. Router
B. loT
C. WAF
D. PoS

Answer: B

QUESTION 176
A vulnerability scan is run against a domain hosing a banking application that accepts connections over MTTPS and HTTP protocols Given the following results:

- SSU3 supported
- HSTS not enforced
- Application uses weak ciphers
- Vulnerable to clickjacking

Which of the following should be ranked with the HIGHEST risk?

A. SSLv3 supported
B. HSTS not enforced
C. Application uses week ophers
D. Vulnerable to clickjacking

Answer: B

QUESTION 177
A penetration tester discovers Heartbleed vulnerabilities in a target network Which of the following impacts would be a result of exploiting this vulnerability?

A. Code execution can be achieved on the affected systems
B. Man-in-the-middle attacks can be used to eavesdrop cookie contents.
C. The attacker can steal session IDs to impersonate other users
D. Public certificate contents can be used lo decrypt traffic

Answer: C

QUESTION 178
A system security engineer is preparing to conduct a security assessment of some new applications. The applications

were provided to the engineer as a set that contains only JAR files. Which of the following would be the MOST detailed method to gather information on the inner working of these applications?

A. Launch the applications and use dynamic software analysis tools, including fuzz testing
B. Use a static code analyzer on the JAR filet to look for code Quality deficiencies
C. Decompile the applications to approximate source code and then conduct a manual review
D. Review the details and extensions of the certificate used to digitally sign the code and the application

Answer: A

QUESTION 179
Which of the following can be used with John the Ripper to crack passwords?

A. Wordlists
B. Nmap
C. Meterpreter
D. PowerSploit

Answer: A

QUESTION 180
What elements should you be sure to remove from an exploited system before finalizing a penetration test?

A. User accounts created
B. Shells spawned
C. Any files left behind
D. Administrator account

Answer: ABC

QUESTION 181
When running an Nmap SYN scan, what will be the Nmap result if ports on the target device do not respond?

A. Open
B. Closed
C. Filtered
D. Listening

Answer: C

QUESTION 182
A company's corporate policies state that employees are able to scan any global network as long as it is done within working hours. Government laws prohibit unauthorized scanning. Which of the following should an employee abide by?

A. Company policies must be followed in this situation
B. Laws supersede corporate policies
C. Industry standards receding scanning should be followed
D. The employee must obtain written approval from the company's Chief Information Security Officer (CISO) prior to scanning

Answer: B