A. A buffer overflow exploit.
B. A chained exploit.
C. A SQL injection exploit.
D. A denial of service exploit.

Correct Answer: B

QUESTION 461

When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?

A. The key entered is a symmetric key used to encrypt the wireless data.
B. The key entered is a hash that is used to prove the integrity of the wireless data.
C. The key entered is based on the Diffie-Hellman method.
D. The key is an RSA key used to encrypt the wireless data.

Correct Answer: A

QUESTION 462

Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
B. The root CA stores the user's hash value for safekeeping.
C. The CA is the trusted root that issues certificates.
D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

Correct Answer: C

QUESTION 463

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?

TCP port 21 - no response TCP port 22 - no response TCP port 23 - Time-to-live exceeded

A. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host.
B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server.
C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not

blocked at the firewall.

D. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error.

Correct Answer: C

QUESTION 464

A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company’s internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

A. SSL
B. Mutual authentication
C. IPSec
D. Static IP addresses

Correct Answer: C

QUESTION 465

What results will the following command yield?

'NMAP -sS -O -p 123-153 192.168.100.3'

A. A stealth scan, opening port 123 and 153.
B. A stealth scan, checking open ports 123 to 153.
C. A stealth scan, checking all open ports excluding ports 123 to 153.
D. A stealth scan, determine operating system, and scanning ports 123 to 153.

Correct Answer: D

QUESTION 466

Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

A. Teardrop
B. SYN flood
C. Smurf attack
D. Ping of death

Correct Answer: A

QUESTION 467

Which of the following are advantages of adopting a Single Sign On (SSO) system? (Choose two.)

A. A reduction in password fatigue for users because they do not need to know multiple passwords when accessing multiple applications.
B. A reduction in network and application monitoring since all recording will be completed at the SSO system.
C. A reduction in system administration overhead since any user login problems can be resolved at the SSO system.
D. A reduction in overall risk to the system since network and application attacks can only happen at the SSO point.

Correct Answer: AC

QUESTION 468

An ethical hacker for a large security research firm performs penetration tests, vulnerability tests, and risk assessments. A friend recently started a company and asks the hacker to perform a penetration test and vulnerability assessment of the new company as a favor. What should the hacker's next step be before starting work on this job?

A. Start by foot printing the network and mapping out a plan of attack.
B. Ask the employer for authorization to perform the work outside the company.
C. Begin the reconnaissance phase with passive information gathering and then move into active information gathering.
D. Use social engineering techniques on the friend's employees to help identify areas that may be susceptible to attack.

Correct Answer: B

QUESTION 469

A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the corporate network. What tool should the analyst use to perform a Blackjacking attack?

A. Paros Proxy
B. BBProxy
C. BBCrack
D. Blooover

Correct Answer: B

QUESTION 470

ICMP ping and ping sweeps are used to check for active systems and to check

A. if ICMP ping traverses a firewall
B. the route that the ICMP ping took
C. the location of the switchport in relation to the ICMP ping
D. the number of hops an ICMP ping takes to reach a destination

Correct Answer: A

QUESTION 471

A hacker searches in Google for filetype:pcf to find Cisco VPN config files. Those files may contain connectivity passwords that can be decoded with which of the following?

A. Cupp
B. Nessus
C. Cain and Abel
D. John The Ripper Pro

Correct Answer: C

QUESTION 472

Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

A. They are written in Java.
B. They send alerts to security monitors.
C. They use the same packet analysis engine.
D. They use the same packet capture utility.

Correct Answer: D

QUESTION 473

A pentester gains access to a Windows application server and needs to determine the settings of the built-in Windows firewall. Which command would be used?

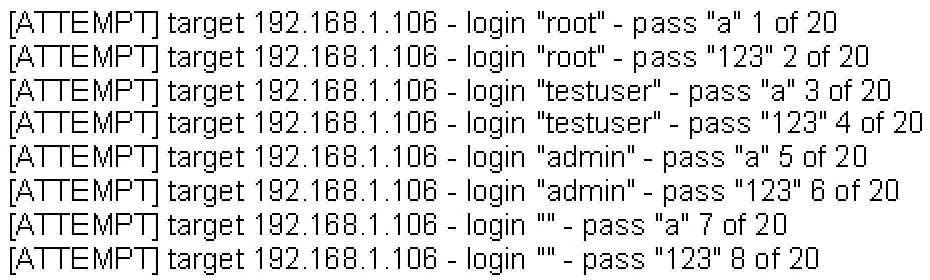
A. Netsh firewall show config
B. WMIC firewall show config
C. Net firewall show config

D. Ipconfig firewall show config

Correct Answer: A

QUESTION 474

The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106:



```
[ATTEMPT] target 192.168.1.106 - login "root" - pass "a" 1 of 20
[ATTEMPT] target 192.168.1.106 - login "root" - pass "123" 2 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "a" 3 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "123" 4 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "a" 5 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "123" 6 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "a" 7 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "123" 8 of 20
```

What is most likely taking place?

A. Ping sweep of the 192.168.1.106 network.

B. Remote service brute force attempt.

C. Port scan of 192.168.1.106.

D. Denial of service attack on 192.168.1.106.

Correct Answer: B

QUESTION 475

A tester is attempting to capture and analyze the traffic on a given network and realizes that the network has several switches. What could be used to successfully sniff the traffic on this switched network? (Choose three.)

A. ARP spoofing

B. MAC duplication

C. MAC flooding

D. SYN flood

E. Reverse smurf attack

F. ARP broadcasting

Correct Answer: ABC

QUESTION 476

A newly discovered flaw in a software application would be considered which kind of security vulnerability?