Vendor:EC-COUNCIL

Exam Code:312-50V7

Exam Name: Ethical Hacking and Countermeasures (CEHv7)

Version: Demo

QUESTION 1

Steve scans the network for SNMP enabled devices. Which port number Steve should scan?

A. 150

B. 161

C. 169

D. 69

Correct Answer: B

QUESTION 2

What statement is true regarding LM hashes?

A. LM hashes consist in 48 hexadecimal characters.

B. LM hashes are based on AES128 cryptographic standard.

C. Uppercase characters in the password are converted to lowercase.

D. LM hashes are not generated when the password length exceeds 15 characters.

Correct Answer: D

QUESTION 3

What two things will happen if a router receives an ICMP packet, which has a TTL value of 1, and the destination host is several hops away? (Select 2 answers)

A. The router will discard the packet

B. The router will decrement the TTL value and forward the packet to the next router on the path to the destination host

C. The router will send a time exceeded message to the source host

D. The router will increment the TTL value and forward the packet to the next router on the path to the destination host.

E. The router will send an ICMP Redirect Message to the source host

Correct Answer: AC

QUESTION 4

Company A and Company B have just merged and each has its own Public Key Infrastructure (PKI). What must the Certificate Authorities (CAs) establish so that the private PKIs for Company A and Company B trust one another and

each private PKI can validate digital certificates from the other company?

A. Poly key exchange

B. Cross certification

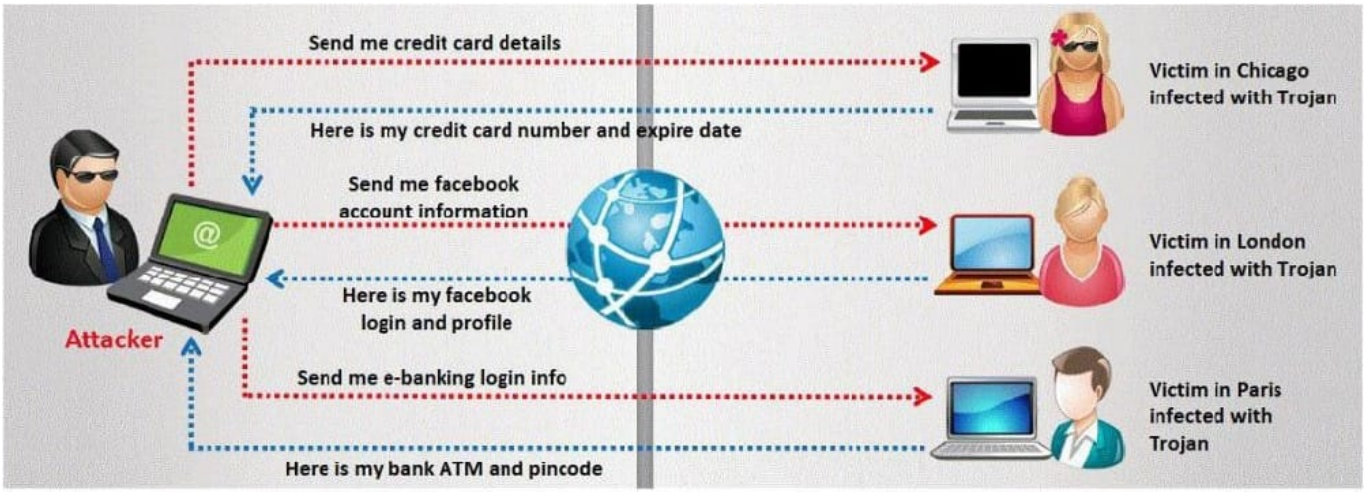
C. Poly key reference

D. Cross-site exchange

Correct Answer: B

QUESTION 5

A Trojan horse is a destructive program that masquerades as a benign application. The software initially appears to perform a desirable function for the user prior to installation and/or execution, but in addition to the expected function steals information or harms the system.



The challenge for an attacker is to send a convincing file attachment to the victim, which gets easily executed on the victim machine without raising any suspicion. Today\\'s end users are quite knowledgeable about malwares and viruses. Instead of sending games and fun executables, Hackers today are quite successful in spreading the Trojans using Rogue security software.

What is Rogue security software?

A. A flash file extension to Firefox that gets automatically installed when a victim visits rogue software disabling websites

B. A Fake AV program that claims to rid a computer of malware, but instead installs spyware or other malware onto the computer. This kind of software is known as rogue security software.

C. Rogue security software is based on social engineering technique in which the attackers lures victim to visit spear phishing websites

D. This software disables firewalls and establishes reverse connecting tunnel between the victim\\'s machine and that of the attacker

Correct Answer: B

QUESTION 6

Which tool can be used to silently copy files from USB devices?

A. USB Grabber

B. USB Dumper

C. USB Sniffer

D. USB Snoopy

Correct Answer: B

QUESTION 7

What are common signs that a system has been compromised or hacked? (Choose three.)

A. Increased amount of failed logon events

B. Patterns in time gaps in system and/or event logs

C. New user accounts created

D. Consistency in usage baselines

E. Partitions are encrypted

F. Server hard drives become fragmented

Correct Answer: ABC

QUESTION 8

Which types of detection methods are employed by Network Intrusion Detection Systems (NIDS)? (Choose two.)

A. Signature

B. Anomaly

C. Passive

D. Reactive

Correct Answer: AB

QUESTION 9

Peter extracts the SID list from Windows 2008 Server machine using the hacking tool "SIDExtracter". Here is the output

of the SIDs:

```
S-1-5-21-1125394485-807623933-549785860-100 John
S-1-5-21-1125394485-807623933-549785860-652 Rebecca
S-1-5-21-1125394485-807623933-549785860-412 Sheela
S-1-5-21-1125394485-807623933-549785860-999 Shawn
S-1-5-21-1125394485-807623933-549785860-777 Somia
S-1-5-21-1125394485-807623933-549785860-500 Chang
S-1-5-21-1125394485-807623933-549785860-555 Micah
```

From the above list identify the user account with System Administrator privileges?

A. John

B. Rebecca

C. Sheela

D. Shawn

E. Somia

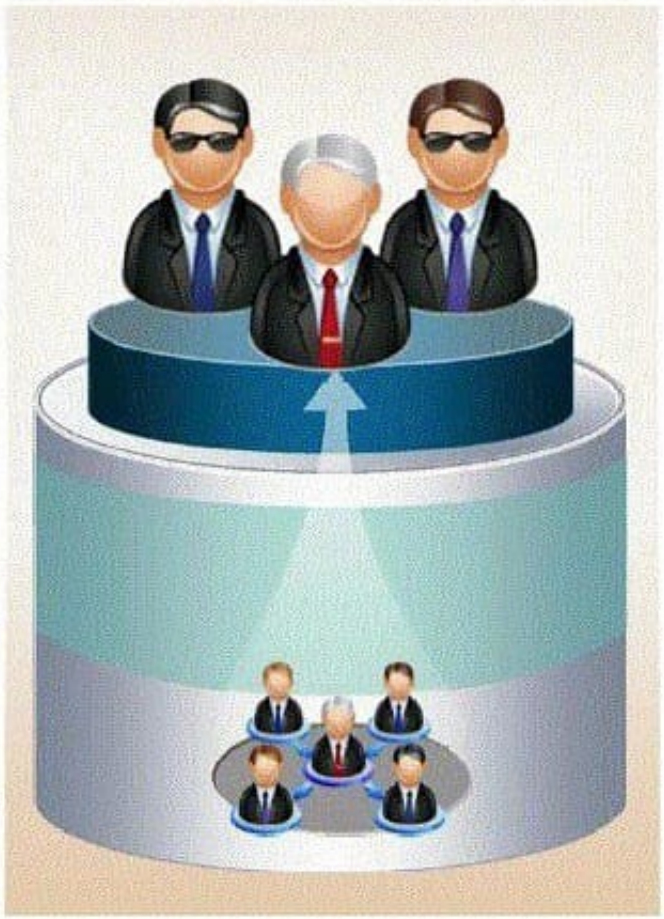
F. Chang

G. Micah

Correct Answer: F

QUESTION 10

If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.



How would you prevent such type of attacks?

A. It is impossible to block these attacks

B. Hire the people through third-party job agencies who will vet them for you

C. Conduct thorough background checks before you engage them

D. Investigate their social networking profiles

Correct Answer: C

QUESTION 11

Cyber Criminals have long employed the tactic of masking their true identity. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine, by "spoofing" the IP address of that machine.

How would you detect IP spoofing?

A. Check the IPID of the spoofed packet and compare it with TLC checksum. If the numbers match then it is spoofed packet

B. Probe a SYN Scan on the claimed host and look for a response SYN/FIN packet, if the connection completes then it is a spoofed packet

C. Turn on \\'Enable Spoofed IP Detection\\' in Wireshark, you will see a flag tick if the packet is spoofed

D. Sending a packet to the claimed host will result in a reply. If the TTL in the reply is not the same as the packet being checked then it is a spoofed packet

Correct Answer: D

QUESTION 12

An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?

A. Birthday attack

B. Plaintext attack

C. Meet in the middle attack

D. Chosen ciphertext attack

Correct Answer: D