QUESTION 142

File extensions provide information regarding the underlying server technology. Attackers can use this information to search vulnerabilities and launch attacks. How would you disable file extensions in Apache servers?

A. Use disable-eXchange
B. Use mod_negotiation
C. Use Stop_Files
D. Use Lib_exchanges

Correct Answer: B

QUESTION 143

Bob has a good understanding of cryptography, having worked with it for many years. Cryptography is used to secure data from specific threats, but it does not secure the application from coding errors. It can provide data privacy; integrity and enable strong authentication but it cannot mitigate programming errors. What is a good example of a programming error that Bob can use to explain to the management how encryption will not address all their security concerns?

A. Bob can explain that using a weak key management technique is a form of programming error.
B. Bob can explain that using passwords to derive cryptographic keys is a form of a programming error.
C. Bob can explain that a buffer overflow is an example of programming error and it is a common mistake associated with poor programming technique.
D. Bob can explain that a random number generator can be used to derive cryptographic keys but it uses a weak seed value and this is a form of a programming error.

Correct Answer: C

QUESTION 144

Finding tools to run dictionary and brute forcing attacks against FTP and Web servers is an easy task for hackers. They use tools such as arhontus or brutus to break into remote servers.

```
CEH# ./rpa
Remote Password Assassin V 1.0
Roses Labs / w00w00
Usage: ./rpa <host> (options)
Options:
-l : Login file to use.
-s : Use the same login.
-c : Password file to use.
-r : Attack FlowPoint Router.
-t : Attack Telnet Port.
-f : Attack FTP Port.
-p : Attack POP Port.
CEH# ./rpa 10.0.0.34 -t -f -c passwords.txt -s linksys
```

A command such as this, will attack a given 10.0.0.34 FTP and Telnet servers simultaneously with a list of passwords and a single login name linksys. Many FTP-specific password-guessing tools are also available from major security sites. What defensive measures will you take to protect your network from these attacks?

A. Never leave a default password.
B. Never use a password that can be found in a dictionary.
C. Never use a password related to your hobbies, pets, relatives, or date of birth.
D. Use a word that has more than 21 characters from a dictionary as the password.
E. Never use a password related to the hostname, domain name, or anything else that can be found with whois.

Correct Answer: ABCE

QUESTION 145
One of the most common and the best way of cracking RSA encryption is to begin to derive the two prime numbers, which are used in the RSA PKI mathematical process. If the two numbers p and q are discovered through a _____ process, then the private key can be derived.

A. Factorization
B. Prime Detection
C. Hashing
D. Brute-forcing

Correct Answer: A

QUESTION 146
Data is sent over the network as clear text (unencrypted) when Basic Authentication is configured on Web Servers.

A. true

B. false

Correct Answer: A

QUESTION 147

NetBIOS over TCP/IP allows files and/or printers to be shared over the network. You are trying to intercept the traffic from a victim machine to a corporate network printer. You are attempting to hijack the printer network connection from your laptop by sniffing the wire. Which port does SMB over TCP/IP use?

A. 443
B. 139
C. 179
D. 445

Correct Answer: D

QUESTION 148

One of the ways to map a targeted network for live hosts is by sending an ICMP ECHO request to the broadcast or the network address. The request would be broadcasted to all hosts on the targeted network. The live hosts will send an ICMP ECHO Reply to the attacker's source IP address. You send a ping request to the broadcast address 192.168.5.255.

```
[root@ceh/root]# ping -b 192.168.5.255
WARNING: pinging broadcast address
PING 192.168.5.255 (192.168.5.255) from 192.168.5.1 : 56(84) bytes of
data.
64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=4.1 ms
64 bytes from 192.168.5.5: icmp_seq=0 ttl=255 time=5.7 ms
```

There are 40 computers up and running on the target network. Only 13 hosts send a reply while others do not. Why?

A. Windows machines will not generate an answer (ICMP ECHO Reply) to an ICMP ECHO request aimed at the broadcast address or at the network address.
B. Linux machines will not generate an answer (ICMP ECHO Reply) to an ICMP ECHO request aimed at the broadcast address or at the network address.
C. You should send a ping request with this command ping 192.168.5.0-255.
D. You cannot ping a broadcast address. The above scenario is wrong.

Correct Answer: A

QUESTION 149

Charlie is the network administrator for his company. Charlie just received a new Cisco router and wants to test its capabilities out and to see if it might be susceptible to a DoS attack resulting in its locking up. The IP address of the Cisco switch is 172.16.0.45. What command can Charlie use to attempt this task?

A. Charlie can use the command ping -l 56550 172.16.0.45 -t.
B. Charlie can try using the command ping 56550 172.16.0.45.
C. By using the command ping 172.16.0.45 Charlie would be able to lockup the router.
D. He could use the command ping -4 56550 172.16.0.45.

Correct Answer: A

QUESTION 150

What type of encryption does WPA2 use?

A. DES 64 bit
B. AES-CCMP 128 bit
C. MD5 48 bit
D. SHA 160 bit

Correct Answer: B

QUESTION 151

Attackers send an ACK probe packet with random sequence number, no response means port is filtered (Stateful firewall is present) and RST response means the port is not filtered. What type of Port Scanning is this?

A. RST flag scanning
B. FIN flag scanning
C. SYN flag scanning
D. ACK flag scanning

Correct Answer: D

QUESTION 152

What is the command used to create a binary log file using tcpdump?

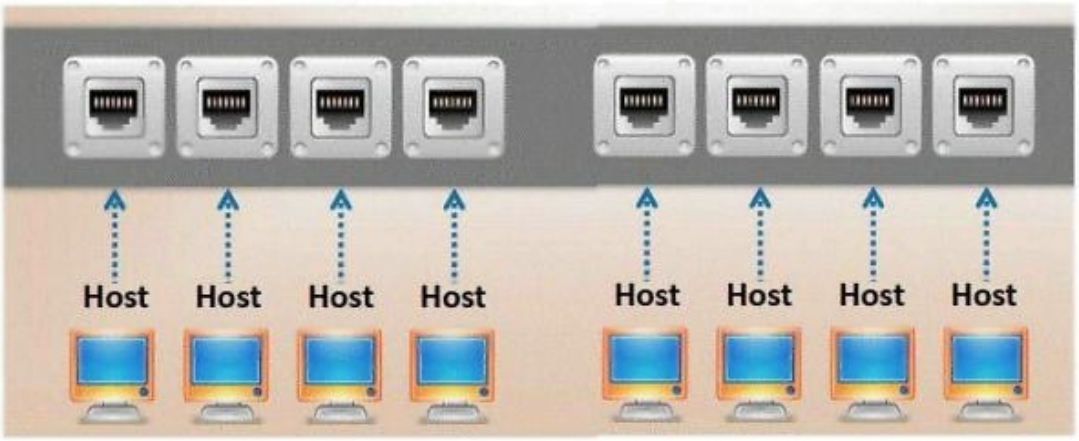
A. tcpdump -w ./log
B. tcpdump -r log
C. tcpdump -vde logtcpdump -vde log

D. tcpdump -l /var/log/

Correct Answer: A

QUESTION 153

Which port, when configured on a switch receives a copy of every packet that passes through it?



A. R-DUPE Port
B. MIRROR port
C. SPAN port
D. PORTMON

Correct Answer: C

QUESTION 154

What is the IV key size used in WPA2?

A. 32
B. 24
C. 16
D. 48
E. 128

Correct Answer: D