QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

Mile2

MK0-201

CPTS - Certified Pen Testing Specialist

D. IP Poisoning

Answer: C

QUESTION: 234
When a network switch receives a very large quantity of random MAC addresses which would overfill the Content Addressable Memory (CAM) table, how will the switch react?

A. It will drop packets until the tables are cleared and then will resume normal processing
B. It will drop the oldest entries in the CAM table to make room for the new packets and will continue working normally
C. It will revert to being a HUB and will broadcast all traffic on each of the ports
D. It is impossible to flood the MAC tables because of their very large size

Answer: C

QUESTION: 235
Jhezza has just arrived at her office and she is checking her stock portfolio as she does every day.She connects to her broker web site and decides to buy some stocks that are highly recommended. She makes use of her special Portfolio Credit Card because she wishes to collect travel points.This is the only online site where Jhezza uses this specific card. Jhezza always ensures there is a secure connection established by looking at the lock icon at the bottom of her browser window.A few weeks later, Jhezza realized that someone has compromised her credit card number and has been doing fraudulent transactions online, the first of which is on the same day she used it to buy stocks from her office.How did the card number get compromised?

A. By a Man in the middle attack
B. By someone who read her emails
C. By someone who was able to perform a FTP server spoofing
D. By a Meet in the middle attack, which compromises encryption

Answer: A

QUESTION: 236
You have just attempted to perform DNS poisoning on the local network DNS server and did not succeed; you decide to launch an attack against routing tables instead.Which of the following would NOT be an effective way of attempting to manipulate the routing table on the local network or through its gateway?

A. By using a source route attack
B. By using ICMP redirect messages
C. By advertising bogus OSDF routes
D. By advertising bogus RIP routes

Answer: C

QUESTION: 237
This technique consists of using social skills to trick someone into revealing information they should not usually release to unauthorized users. What do we call this technique or type of attack?

A. Shoulder Surfing
B. Eavesdropping
C. Social Engineering
D. Social Coining

Answer: C

QUESTION: 238
To uniquely identify an active session, TCPIP protocol will make use of the client IP address and port as well as the destination IP address and port.How are these four elements matched together called?

A. Client-Server Pair
B. Socket
C. Session Identifier
D. Server-Client Pair

Answer: B

QUESTION: 239
An attacker must create a spoofed/crafted packet in order to hijack a session.Which of the following would have to be present within the spoofed packet?

A. The client IP address
B. The client MAC address
C. The client port number
D. The sequence numbers

Answer: B

QUESTION: 240
You have been reading a series of papers on connection hijacking. However, there were contradictions as to which Operating System would be more vulnerable and which one has predictable sequence number generation.Which of the following tools could be used to help you

in evaluating sequence number predictability? Choose two from the list below.

A. nmap
B. hping
C. Senna
D. SeqNum

Answer: A, B

QUESTION: 241
Traditional firewalls have serious limitations where the data payload is not being inspected. These firewalls usually tend to work within the lower layer of the OSI model.What layer does traditional firewall monitor?

A. Layers 2 to 4
B. Layers 2 to 5
C. Layers 2 to 6
D. Layers 1 to 4

Answer: A

QUESTION: 242
Which of the following techniques would be effective to get around some of the blocking rules on certain firewalls?The same technique could be used to avoid detection by Intrusion Detection Systems (IDS) in some cases.

A. Injection
B. Spoofing
C. Fragmentation
D. Diffusion

Answer: C

QUESTION: 243
Intrusion Detection Systems have multiple ways to decode the information. Which of the following definitions would best describe Protocol Anomaly Detection within an Intrusion Detection System (IDS) engine?

A. Interprets the attack as the victim would for greater accuracy
B. Identifies attacks that are based on condition, not patterns
C. Compares traffic to RFC standards and reports deviations
D. Identifies traffic that breaks policy or is not normal for network

Answer: C

QUESTION: 244
One of the challenges when doing large scale security tests is the time required.If you have to scan a class B network it might take you a very long time. Scanrand is a tool that has been optimized to scan a large number of hosts in very little time. It was reported that it was used to scan about 8300 web servers in less than 4 seconds. How does scanrand achieve such an impressive benchmark?

A. It does not maintain any state
B. It makes use of multiple Network Interface Cards (NIC)
C. It has a probabilistic algorithm that can predict if a port is open or not
D. It does not attempt to use UDP due to the overhead involved

Answer: A

QUESTION: 245
On a Linux system, which of the following files would contain the list of user accounts, their shell, and their home directories?

A. useradd
B. shadow
C. passwd
D. group

Answer: C

QUESTION: 246
Pen testing is another area of security where acronyms and expressions abound.What does the term rooting refers to?

A. Getting access to the root directory
B. Getting administrator access on a Linux system
C. Getting administrator access on a Windows system
D. Planting a worm that will develop and grow within the system

Answer: B

QUESTION: 247
One of your clients has been the victim of a brute force attack against their SSH server.They ask you what could be done to protect their Linux servers. You propose the use of IPTables (the built

in kernel firewall) to limit connection attempts to protect their servers. You agree with your client to limit connections to the SSH port to a maximum of only three trials per minutes considering there is only one administrator who has a valid need to connect remotely onto this port.If the threshold of three connections is exceeded, the attacker will have to wait for another 60 seconds before it will resume allowing connections again.Which of the following IPTables entry would meet your clients needs?

A. iptables -A INPUT -p tcp --dport 23 -m state --state NEW -m recent --update --seconds 60 --hitcount 4 --rttl --name SSH -j DROP

B. iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 60 --hitcount 3 --rttl --name SSH -j DROP

C. iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 60 --hitcount 4 --rttl --name SSH -j DROP

D. iptables -A OUTPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 60 --hitcount 4 --rttl --name SSH -j DROP

Answer: C