QUESTION 938
Which one of the following is defined as the process of distributing incorrect Internet Protocol (IP) addresses/names with the intent of diverting traffic?

A. Network aliasing
B. Domain Name Server (DNS) poisoning
C. Reverse Address Resolution Protocol (ARP)
D. Port scanning

Correct Answer: B

QUESTION 939
A Packet containing a long string of NOP's followed by a command is usually indicative of what?

A. A syn scan
B. A half-port scan
C. A buffer overflow
D. A packet destined for the network's broadcast address

Correct Answer: C

QUESTION 940
You are running a packet sniffer on a network and see a packet with a long string of long string of "90 90 90 90...." in the middle of it traveling to an x86-based machine. This could be indicative of what?

A. Over-subscription of the traffic on a backbone.
B. A source quench packet.
C. A FIN scan.
D. A buffer overflow.

Correct Answer: D

QUESTION 941
Which of the following is true related to network sniffing?

A. Sniffers allow an attacker to monitor data passing across a network.
B. Sniffers alter the source address of a computer to disguise and exploit weak authentication methods.
C. Sniffers take over network connections
D. Sniffers send IP fragments to a system that overlap with each other.

Correct Answer: A

QUESTION 942
Which one of the following threats does NOT rely on packet size or large volumes of data?

A. SYN flood
B. Spam
C. Ping of death
D. Macro virus

Correct Answer: D

QUESTION 943
A TCP SYN Attack:

A. requires a synchronized effort by multiple attackers
B. takes advantage of the way a TCP session is established
C. may result in elevation of privileges
D. is not something system users would notice

Correct Answer: B

QUESTION 944
What attack is typically used for identifying the topology of the target network?

A. Spoofing
B. Brute force
C. Teardrop
D. Scanning

Correct Answer: D

QUESTION 945
Which one of the following is the reason for why hyperlink spoofing attacks are usually successful?

A. Most users requesting DNS name service do not follow hyperlinks.
B. The attack performs user authentication with audit logs.
C. The attack relies on modifications to server software.
D. Most users do not make a request to connect to a DNS names, they follow hyperlinks.

Correct Answer: D

QUESTION 946
Which of the following identifies the first phase of a Distributed Denial of Service attack?

A. Establishing communications between the handler and agent.
B. Disrupting the normal traffic to the host.
C. Disabling the router so it cannot filter traffic.
D. Compromising as many machines as possible.

Correct Answer: D

QUESTION 947
This type of vulnerability enables the intruder to re-route data traffic from a network device to a personal machine? This diversion enables the intruder to capture data traffic to and from the devices for analysis or modification, or to steal the password file from the server and gain access to user accounts.

A. Network Address Translation
B. Network Address Hijacking
C. Network Address Supernetting
D. Network Address Sniffing

Correct Answer: B

QUESTION 948
Which one of the following is an example of hyperlink spoofing?

A. Compromising a web server Domain Name Service reference.
B. Connecting the user to a different web server.
C. Executing Hypertext Transport Protocol Secure GET commands.
D. Starting the user's browser on a secured page.

Correct Answer: B

QUESTION 949
Why are packet filtering routers NOT effective against mail bomb attacks?

A. The bomb code is obscured by the message encoding algorithm.
B. Mail bombs are polymorphic and present no consistent signature to filter on.

C. Filters do not examine the data portion of a packet.
D. The bomb code is hidden in the header and appears as a normal routing information.

Correct Answer: C

QUESTION 950
Which one of the following correctly identifies the components of a Distributed Denial of Service Attack?

A. Node, server, hacker, destination.
B. Client, handler, agent, target.
C. Source, destination, client, server.
D. Attacker, proxy, handler, agent.

Correct Answer: B

QUESTION 951
Which one of the following attacks will pass through a network layer intrusion detection system undetected?

A. A teardrop attack.
B. A SYN flood attack.
C. A DNS spoofing attack.
D. A test.cgi attack.

Correct Answer: D

QUESTION 952
Which one of the following is a passive network attack?

A. Spoofing
B. Traffic Analysis
C. Playback
D. Masquerading

Correct Answer: B

QUESTION 953
Which one of the following can NOT typically be accomplished using a Man-in-the-middle attack?

A. DNS spoofing
B. Session hijacking
C. Denial of service flooding
D. Digital signature spoofing

Correct Answer: D

QUESTION 954
What is called an attach where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets?

A. SYN flood attack
B. Smurf attack
C. Ping of Dead Attack
D. Denial of Service (DOS) Attack

Correct Answer: B

QUESTION 955
Which type of attack involves the alteration of a packet at the IP level to convince a system that it is communicating with a known entity in order to gain access to a system?

A. TCP sequence number attack
B. IP spoofing attack
C. Piggybacking attack
D. Teardrop attack

Correct Answer: B

QUESTION 956
What attack takes advantage of operating system buffer overflows?

A. Spoofing
B. Brute force
C. DoS
D. Exhaustive