NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Ethical Hacking

Assignment- Week 4

TYPE OF QUESTION: MCQ/MSQ

Number of questions: 15 **Total mark: 15 x 1 = 15**

QUESTION 1:

Which of the following statement(s) is/are **true** for NAT networking mode?

a. In NAT mode, the virtual machines cannot access each other.
b. NAT mode does not allow access of internet to the installed virtual machines.
c. In NAT mode, the hypervisor allocate same IP address to all virtual machines.
d. All of these.

Correct Answer: a, c

Detailed Solution:

By default, virtual box uses NAT mode. In this mode internet access is allowed; however, each system gets the same IP, and thus the virtual machines cannot access each other in this mode.

Thus the correct options are (a) and (c).

QUESTION 2:

Which of the following statement(s) is/are **true** about "Passive Reconnaissance"?

a. Information about the target is collected indirectly.
b. Information about the target is collected directly.
c. There is a chance of detection.
d. There is no chance of detection.

Correct Answer: a, d

Detailed Solution: Reconnaissance is the process of gathering information about a target network or system. In passive reconnaissance, we collect information about a target indirectly, e.g., web search. As the attacker and victim does not communicate directly, there is no a chance of detection.

Thus the true options are (a) and (d).

QUESTION 3:

Which of the following can be used for active reconnaissance.

a. Whois
b. Archive.org
c. NMAP
d. Nessus
e. Metasploit
f. Hydra

Correct Answer: c, d, e

Detailed Solution: Whois and archive are used for passive reconnaissance. NMAP, Nessus and Metasploit are used in active reconnaissance as they directly communicate with the target system. Hydra is a tool used for password cracking.

The correct options are (c), (d) and (e).

QUESTION 4:

Which of the following information **cannot** be retrieved using active reconnaissance?

a. Live host in a network.
b. Open ports.
c. Services running in the systems.
d. Operating system of the target system.
e. Vulnerabilities of target machine/application.
f. None of these.

Correct Answer: f

Detailed Solution: In active reconnaissance scanning tool performs major role, it can be used for identification of live host, active ports, services, operating system and vulnerabilities of the target system.

The correct option is (f).

QUESTION 5:

Which of the following tools **cannot** be used for DNS enumeration?

a. host
b. dnsenum
c. dig
d. None of these

Correct Answer: d

Detailed Solution: For DNS enumeration various tools can be used such as host, dnsenum, dig, nslookup, nmap, dnsrecon, etc.

The correct option is (d).

QUESTION 6:

What is the main objective of host discovery?

a. Identification of live hosts.
b. Identification of services running in the target system.
c. Identification of version of the services running in the target system.
d. Identification of the operating system of the target systems.
e. Identification of open ports.

Correct Answer: a

Detailed Solution: The main objective of host discovery is to identify the live hosts in the network or network infrastructure.

The correct option is (a).

QUESTION 7:

Which of the following options is used to trace the details of the sent/received packets?

a. --packet-trace
b. --reason
c. --disable-arp-ping
d. None of these

Correct Answer: a

Detailed Solution: To get the details of the packets used for scanning, --packet-trace option can be used. – reason option is used to get the reason of the report (why the port/system is up/down). – disable-arp-ping is used to disable arp table check.

The correct option is (a).

QUESTION 8:

Which of the following options can be used to perform ICMP ECHO sweep?

a. –PE
b. –PP
c. –PM
d. –PU

Correct Answer: a

Detailed Solution: In ICMP ECHO sweep, the attacker sends out an ICMP ECHO request packet (ICMP type 8) to the target. If it receives an ICMP ECHO reply packet, it assumes that the target is alive. To perform ICMP ECHO sweep scan –PE option is used.

Thus the correct option is (a).

QUESTION 9:

The establishment of a TCP connection involves a negotiation called 3-way handshake. What type of message the client sends to the server in order to begin this negotiation?

a. RST
b. ACK
c. SYN-ACK
d. SYN

Correct Answer: d

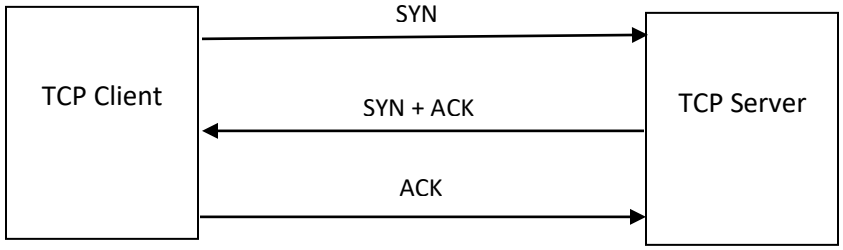
Detailed Solution: TCP connection establishment involves a 3-way handshake.

Step 1 (SYN): In the first step, client wants to establish a connection with server, so it sends a segment with SYN that informs server that client is likely to start communication and with what sequence number it starts the segments.

Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement (ACK) signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments with.

Step 3 (ACK): In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start actual data transfer.

The correct option is (d).



QUESTION 10:

How does port scanning using TCP Connect works?

a. It creates a half-open connection during TCP connection establishment, and decides whether the port is open or not.
b. It completes the 3-way handshake in TCP connection establishment, and decides whether the port is open.
c. It does not use 3-way handshake.
d. None of these.

Correct Answer: b

Detailed Solution: In TCP Connect, the attacker tries to complete a TCP connection with the target by using 3-way handshake. If successful, it concludes that the given port is open.

The correct option is (b).

QUESTION 11:

In port scanning using TCP SYN scan, how are the open and closed ports identified?

a. An attacker sends a SYN packet to a port, if it receives an SYN-ACK (SA) then the port is reported as open.
b. An attacker sends a SYN packet to a port, if it receives an RST (RA) then the port is reported as closed.
c. An attacker sends an ACK packet to a port, if it receives an RST then the port is reported as open.
d. An attacker sends an ACK packet to a port, if it receives an RST then the port is reported as closed.

Correct Answer: a, b

Detailed Solution: In TCP SYN scan open and closed ports are identified by sending SYN request to various ports of the target system. If a SYN-ACK packet is received for a port then the port is reported as open, whereas if it receives a RST (RA) packet then the port is reported as closed. ACK packets are not used in TCP SYN scan.

The correct options are (a) and (b).

QUESTION 12:

Can the use of firewall prevent port/host scanning?

a. True
b. False

Correct Answer: a

Detailed Solution: Use of firewalls (inbuilt as well as software firewall) can protect you to prevent port/host scanning. We have already done demonstration for this.

The correct option is (a).

QUESTION 13:

By default how many ports are scanned in NMAP for a target system _____?

Correct Answer: 1000

Detailed Solution: By default nmap scans for top 1000 ports.

QUESTION 14:

If we does not want to carry out port scanning then which of the following options can be used with NMAP?

a. -F
b. -p-
c. -Pn
d. -sn
e. We cannot disable port scanning.

Correct Answer: d

Detail Solution: The –sn options tells nmap not to carry out a port scan after host discovery, and only provide a list of the available hosts that respond to the scan. Basically, only a ping scan is performed.

Thus, the correct option is (d).

QUESTION 15:

Which of the following options can be used for OS and Version detection?

a. –sn
b. -Pn
c. -A
d. –sT
e. None of these

Correct Answer: c

Detailed Solution: For OS and version detection –O and –sV option is used. However scanning with option –A, which is known as aggressive scan, performs various type of scanning such as port scanning, host scanning, OS and version detection, vulnerabilities, etc.

The correct option is (c).

********END*******