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 0.8 = 12**

---

**QUESTION 1:**

Which of the following statement(s) is/are **false**?

a. Hypervisor allows one host system to support multiple virtual machines by sharing the resources.
b. Hypervisor allows one host system to support multiple virtual machines; however, it does not allow resource sharing.
c. Kali-linux is a Debian-based Linux distribution that has collection of tools that are useful for penetration testing.
d. Kali-linux is a hack-proof secured operating system.
e. None of these.

**Correct Answer: b, d**

**Detailed Solution:** Hypervisor or Virtual Machine Monitor is a software tool that allows the creation and running of one or more virtual machines (VMs) on a computer system, each system can use the resources of main system (host system) such as memory, network interface, storage etc. This is very essential for security practice. Kali Linux is a specific Linux distribution based on Debian. It consists of a large collection of tools for carrying out penetration testing, security research, computer forensics, etc. No systems can be considered as hack-proof.

Thus the correct options are (b) and (d).

---

**QUESTION 2:**

Which of the following statement(s) is/are **true** about “Active Reconnaissance”?

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

**Correct Answer: b, c**

**Detailed Solution:** Reconnaissance is the process of gathering information about a target network or system. In active reconnaissance, we collect information about a target directly by communication with the target system. As the attacker and victim communicate directly, thus there is a chance of detection.

Thus the true options are (b) and (c).

---

**QUESTION 3:**

Which of the following is **not** an information source over the internet for an attackers?

a. Whois
b. YouTube
c. Archive.org
d. Netcraft
e. Hydra

**Correct Answer: b, e**

**Detailed Solution:** YouTube is just a video streaming platform, and not an information source for attacker. Hydra is a tool to generate permutation of words used for password cracking. All other tools can be used as an information source by attackers.

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

---

**QUESTION 4:**

Which of the following data **cannot** be retrieved about the target system/website using Whois database lookup?

a. Registration details.
b. Name servers.
c. IP address.
d. History of the website.
e. None of these.

**Correct Answer: d**

**Detailed Solution:** Using Whois database lookup we can retrieve various useful information about the target system, such as IP address, registration details, mail id, contact, name servers, domain owner, etc. However, we cannot retrieve history of the website. To check complete history of the website, archive.org can be used.

Thus the correct option is (d).

---

**QUESTION 5:**

Which of the following search operators can narrow down the search results to a site that has the targeted search term in the URL?

a. inurl
b. intitle
c. site
d. exclude
e. double quote (“”)
f. filetype

**Correct Answer: a**

**Detailed Solution:** The “inurl” search operator is used to search all websites that contain the given term as a part of its url.

Thus the correct option is (a).

---

**QUESTION 6:**

Which of the following information can be retrieved using DNS/Mail server enumeration?

a. Usernames
b. Computer names
c. Operating system
d. Open ports
e. IP address of system
f. Size of the network

**Correct Answer: a, b, e, f**

**Detailed Solution:** Using DNS and mail server enumeration we can extract information such as usernames, computer names, IP addresses, it can also reveal the size of the network. However, it cannot identify OS and open ports.

The correct option are (a), (b), (e), and (f).

---

**QUESTION 7:**

Which of the following statement(s) is/are **true** for host discovery using ICMP ECHO and ICMP non-ECHO sweep?

a. In ICMP sweep, the attacker sends out an ICMP ECHO request packet to the target, and waits for an ICMP ECHO reply response.
b. In Non-Echo ICMP sweep, the attacker sends out an ICMP ECHO request packet to the target, and waits for an ICMP ECHO reply response.
c. In ICMP sweep, if the attacker does not receive an ICMP ECHO reply then the host is considered as down.
d. In ICMP sweep, if the attacker does not receive an ICMP ECHO reply then the host is considered as live.
e. In Non-Echo ICMP sweep, if the attacker dose not receive an ICMP ECHO reply then the host is considered as down.

**Correct Answer: a, c**

**Detailed Solution:** In ICMP 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. In Non-Echo ICMP sweep, ICMP time stamp and ICMP mask request packet are used.

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

---

**QUESTION 8:**

Which of the following option(s) is/are used for host discovery using TCP and UDP sweep respectively?

a. PE, PP
b. PE, PM
c. PS, PA
d. PS, PU
e. PA, PU

**Correct Answer: d, e**

**Detailed Solution:** PE option is used for ICMP Echo sweep. PM and PP options are used for ICMP Non-Echo sweep. PS and PA option are used for TCP sweep and PU is used for UDP sweep.

Thus correct options are (d) and (e).

---

**QUESTION 9:**

Which of the following information is retrieved by port scanning?

a. Information about the operating system running on the target system.
b. The services running on the target system.
c. The IP address of the target system.

d. None of these.

**Correct Answer: b**

**Detailed Solution:** Port generally specifies the services running on the systems, thus by port scanning we can identify the services running on any target system.

The correct option is (b).

---

**QUESTION 10:**

What kind of packet is received if the target port is closed/filtered in TCP connect/SYN scan?

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

**Correct Answer: e**

**Detailed Solution:**

To begin connection, SYN packet is used, if the port is open then the attacker receives SYN/ACK packet. If the port is closed/filtered then a RST/ACK packet is received. RST is used to close the connection.

The correct option is (e).

---

**QUESTION 11:**

Which of the following option(s) is/are used for OS and Version detection respectively?

a. sn, PE
b. Pn, sP
c. O, -sV
d. sT, PP
e. None of these.

**Correct Answer: c**

**Detailed Solution:** for OS and version detection -O and -sV option is used. OS and version can also be scanned using only –A option 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).

---

**QUESTION 12:**

How many ports are scanned in NMAP for a target system if we use –F option _____?

**Correct Answer: 100**

**Detailed Solution:** -F option limits the port scanning to top 100 ports.

---

**QUESTION 13:**

Which of the following NMAP scanning option(s) is/are correct with respect to port scanning?

a. –F
b. -p20
c. -p20-100
d. -p20::100
e. -p20, 22, 28, 80
f. All of these.

**Correct Answer: a, b, c, e**

**Detailed Solution:** By default NMAP scans for 1000 ports (without any option). If we want to restrict this, we can directly give the specific port numbers that need to be scanned (as given in option b) or we can give range of ports (as given in option c). We can give option F that scans top 100 ports. We can also separate some ports using comma (as given in option e), there is one more port scanning option that is (-p-), which scans all ports (0 to 65535). However, option (d) is incorrect, to specify range of ports "–"symbol is used.

The correct options are (a), (b), (c) and (e).

---

**QUESTION 14:**

If we want to disable host discovery in port scanning, then which of the following options can be used?

a. -F
b. -p-
c. -Pn
d. -sn
e. We cannot disable host discovery.

**Correct Answer**: c

**Detail Solution**: The –Pn options tells nmap not to carry out host discovery and consider all host as up and start port scanning.

Thus the correct option is (c).

---

## QUESTION 15:

Which of the following can be used to reconnaissance countermeasures?

a. Do not release critical info in public.
b. Encrypt password and sensitive information.
c. Restrict zone transfer.
d. Examine logs periodically.
e. Use firewalls.
f. All of these.

**Correct Answer**: f

**Detail Solution**: All of the given options can be used for reconnaissance countermeasures.

---

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