NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

NPTEL ETHICAL HACKING PREVIOUS YEAR ASSIGNMENT SOLUTION PDF (JAN-APR) 2023

Uploaded by Sudhanshu Sekhar Tripathy

Channel Link: -
https://www.youtube.com/@sudhanshusekhartripathy838/about

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment- Week 1

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

In which of the following penetration testing models, no information about the network is given to tester?

a. White box model.
b. Black box model.
c. Red box Model.
d. Gray box model.
e. None of these.

Correct Answer: b

Detail Solution: In the white box model, the tester has complete information about the network. In the black box model, the tester does not have any information about the network. Gray box model is somewhere in between, where the tester is only provided with partial information about the network. There is nothing called red box model.
Thus the correct option is (b).

QUESTION 2:

Which of the following statement(s) is/are true for a circuit switched network?

a. A communication link can be shared by more than one connection.
b. A communication link is dedicated to a connection and cannot be shared with other connections.
c. The packet transfer delay between a pair of nodes may depend on the prevailing network traffic.
d. The packet transfer delay between a pair of nodes is more or less constant during the entire period of the connection.
e. It is efficient for bursty traffic.

Correct Answer: b, d

Detail Solution: In a circuit switched network, a communication link remains dedicated to a connection; however, in a packet switched network, communication links may be shared by more than one connection. Also, in a packet switched network, packets between the same source and destination may follow different paths, and hence the packet transfer delay can vary with time; whereas in circuit switched network the link is dedicated so most of the time the delay remains constant. Circuit switched network is acceptable for voice communication but is very inefficient for high traffic like data streaming.

Thus true options are (b) and (d).

QUESTION 3:

A 1000 byte packet is sent over a 50 kilo-bits-per-second (Kbps) point-to-point link whose propagation delay is 10 msec. The packet will reach the destination after _____ msec. (Assume 1K = 1000)

Correct Answer: 160 to 170

Detail Solution: 50 x 1000 = 50,000 bits per second can be transferred through the link.

1 bit can be sent in = (1 / 50,000) sec

1000 bytes or 8,000 bits can be sent in 8,000 / 50,000 sec = 0.16 sec = 160 msec

Hence the packet will reach the destination after = 160 msec + 10 msec = 170 msec.

Thus the correct answer will be range 160-170.

QUESTION 4:

Which of the following statement(s) is/are true for virtual circuit based packet transfer approach?

a. It is a connection-oriented approach, where a route is established priori to transfer of packets.
b. In this approach, each packets follows distinct path.
c. The intermediate node can perform dynamic routing.
d. All the packets reach in order to the destination.
e. It is a true packet switched network.

Correct Answer: a, d

Detail Solution: Virtual circuit approach is a connection-oriented packet switching approach where a route is established before packet transmission starts. For a session the packets follows the same path, and then once the session is expired a new route is established. In virtual circuit, a virtual id is used which is used by intermediate node of the route such that the packet can be forwarded to the next node. This means that the Intermediate nodes can only forward the packet and cannot make dynamic routing decision. In virtual circuit all packets reach in order to the destination as packet follows the same path. It is not a true packet switched network as it uses a fixed path for transmitting data.

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

QUESTION 5:

Which of the following OSI layers is responsible for end-to-end reliable data transfer, with error recovery and flow control?

a. Session layer
b. Transport layer
c. Network layer
d. Datalink layer
e. Physical layer

Correct Answer: b

Detail Solution: The **physical layer** is responsible for actual transmission of signals over a communication medium. The **data-link layer** is responsible for transmitting data frames reliably over point-to-point links. The **network layer** is responsible for the switching or routing of packets from one node to the next on way to the final destination. The **transport layer** is a virtual host-to-host layer between the two end systems which is responsible for end-to-end reliable data transfer, with error recovery and flow control. The **session layer** manages connection sessions.

Thus the correct option is (b).

QUESTION 6:

Which of the following is/are false for TCP/IP model?

a. It allows cross-platform communications among heterogeneous networks.
b. It is a scalable client-server architecture which allows network modification without disrupting the current services.

c. It can also represent any other protocol stack other than the TCP/IP suite such as Bluetooth connection.
d. None of these.

Correct Answer: c

Detail Solution: TCP/IP is an open source scalable client-server based architecture used in computer network. It is used to bridge the gap between non-compatible (heterogeneous) networks. In TCP/IP based network a host/network can be added/removed without disturbing the current services/systems of the network. TCP/IP is not generic, and thus can only represent the protocol stacks defined in TCP/IP suite. It cannot represent any protocol that is not defined in TCP/IP such as Bluetooth connection.

Thus the false option is (c).

QUESTION 7:

Which of the following is true for the IP?

a. It uniquely identifies a network interface of a computer system.
b. It uniquely identifies a host in the network.
c. It indicates how many hardware ports are there in the computer system.
d. None of these.

Correct Answer: b

Detail Solution: IP uniquely identifies a host in the network.

Thus the true option is (b).

QUESTION 8:

How many bits are used for IP address (in IP version 4) and port number respectively?

a. 32, 8
b. 32, 16
c. 48, 8
d. 48, 16

Correct Answer: b

Detail Solution: 32 bits are used for IP address whereas 16 bits are used for port number.

Thus the correct option is (b).

QUESTION 9:

If a 2000 byte data message is sent using a TFTP, the corresponding Ethernet packet will be of size _____ bytes.

Correct Answer: 2050

Detail Solution: In TFTP protocol, along with the data, 18 bytes Ethernet header, 20 bytes of IP header, 8 bytes of UDP header and 4 bytes of TFTP header will be added.

Thus the effective size of Ethernet packet will be 2000 + 50 = 2050 bytes.

QUESTION 10:

If the IP header is 192 bits long, what will be the value (in decimal) of the "HLEN" field _____?

Correct Answer: 6

Detail Solution: The HLEN field contains the size of the IP header in multiples of 32 bits or 4 bytes. Here, size of the IP header = 192 bits = 6 x 32 bits. Hence, HLEN will contain 0110, which is the binary equivalent of the number 6.

Thus the correct answer will be 6.

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment- Week 2

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following is/are **false** for IP fragmentation?

a. It is a process that divides packets into smaller fragments.
b. Fragmentation is required due to intermediate networks with smaller maximum transmission unit (MTU).
c. Each fragmented packet is considered as separate IP packet.
d. IP fragmentation is typically done by layer-2 switches.
e. None of these.

Correct Answer: d

Detail Solution: IP fragmentation is necessary for data transmission, as every network has a unique limit for the size of datagrams that it can process, which is known as maximum transmission unit (MTU). In fragmentation, the packets are divided into smaller pieces and each piece is considered as separate IP packet. It is typically done by the routers in the network layer (or layer-3 switches).

Thus the correct option is (d).

QUESTION 2:

Consider the following statements:

(i) In transparent fragmentation, all fragmented packets are reassembled by an exit router.

(ii) In non-transparent fragmentation, all fragmented packets reassembled by host.

a. Only (i) is true.
b. Only (ii) is true.
c. Both (i) and (ii) are true.
d. Both (i) and (ii) are false.

Correct Answer: c

Detail Solution: In transparent fragmentation, in every network that a packet passes through, all packets are routed through an exit router that assembles the fragmented packets. In this approach the subsequent network(s) have no information about fragmentation. Whereas in non-transparent fragmentation the packets can be transmitted through multiple routers as the reassembly is done by the destination host system.

Thus the correct option is (c).

QUESTION 3:

For reassembling the fragmented packets at the final destination, which of the following header field(s) is(are) used by IP?

a. Fragment offset.
b. Flags.
c. Header checksum.
d. HLEN.
e. Identification.

Correct Answer: a, b, e

Detail Solution: For fragment assembly, identification (ID), fragment offset and flag fields are used.

Thus true options are (a), (b) and (e).

QUESTION 4:

An IP packet arrives at a router with the first eight bits as 01001100. How many bytes are there in the OPTIONS field _____?

Correct Answer: 28

Detail Solution: The first four bits (0100) is the IP version, and the next four bits (1100 = 12) is the header length. The header length of 12 indicates 12 x 4 = 48 bytes of header. The basic IP header is 20 bytes long. Hence, the size of the OPTIONS field will be 48 – 20 = 28 bytes.

QUESTION 5:

In an IP packet, the value of HLEN is 6, and the value of the TOTAL LENGTH field is 1000 (one thousand). The number of data bytes in the packet will be _____.

Correct Answer: 976 to 1000

Detail Solution: Since HLEN = 6, the size of the IP header will be 6 x 4 = 24 bytes. The total size of the IP packet is given as 1000 bytes. Hence, the number of data bytes = 1000 – 24 = 976 bytes.

QUESTION 6:

Which of the following is/are **true** for IP addressing?

a. Each host connected to the Internet is defined by an IP address.
b. IP address consist of two parts: network number and host number.
c. When a packet is routed to the destination network, only the host number is used.
d. Class A address can have a maximum of 16,777,214 networks.
e. None of these.

Correct Answer: a, b

Detail Solution: Each host connected to the Internet is uniquely defined by IP address, where the IP address consists of network number and host number. When a packet is routed to the destination network, then only the network number is used. Class A address can have maximum of 127 networks and 16,777,214 hosts.

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

QUESTION 7:

Which of the following is/are **not** a feature of TCP?

a. Process to process communication.
b. Stream delivery service.
c. Connection-oriented service.
d. Unreliable service.
e. Full duplex communication.
f. None of these.

Correct Answer: d

Detail Solution: All given points except (d) are features of TCP. TCP provides reliable service.

Thus the correct option is (d).

QUESTION 8:

Which of the following statement(s) is/are **false** for flag bits in TCP header?

a. SYN=1 and ACK=1 represents a connection request message.
b. SYN=1 and ACK=0 represents a connection confirmation message.
c. RST bit is used to reject connection request.
d. PUSH bit is used to indicate end of a message
e. None of these.

Correct Answer: a, b

Detail Solution: In the TCP header, SYN=1 and ACK=0 represents connection request, whereas SYN=1 and ACK=1 represents connection confirmation. RST is used to reset/reject connection, and PUSH bit is used to indicate end of message.

Thus the false options are (a) and (b).

QUESTION 9:

What is the subnet address if the destination IP address is 144.16.34.124 and the subnet mask is 255.255.242.0?

a. 144.16.32.0
b. 144.16.34.0
c. 144.16.34.255
d. 144.16.242.0
e. 144.16.242.255

Correct Answer: b

Detail Solution: Let us express the two numbers in binary:

```
144.16.34.124 = 10010000 00010000 00100010 01111100
255.255.240.0 = 11111111 11111111 11110010 00000000
```

If we take bit-by-bit AND, we shall get the subnet address as

```
10010000 00010000 00100010 00000000 = 144.16.34.0
```

Thus the correct option is (b).

QUESTION 10:

An organization is allotted a block with beginning address as: 144.16.192.16/28 in CIDR notation. What will be the address range for that block?

a. 144.16.192.0 to 144.16.192.16
b. 144.16.192.0 to 144.16.192.255
c. 144.16.192.16 to 144.16.192.31
d. 144.16.192.16 to 144.16.192.32

Correct Answer: c

Detail Solution: First 28 bits in the IP address will denote network number. The range will be:

144.16.192.16 = 10010000 00010000 11000000 00010000

to

144.16.192.31 = 10010000 00010000 11000000 00011111

Thus the range given in option (c) is correct.

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment- Week 3

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

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

a. IP protocol uses connection-oriented routing.
b. IP protocol uses connection-less routing.
c. IP protocol is a host-to-host layer.
d. In connection-less routing, each packet is treated as an independent packet.
e. None of these.

Correct Answer: b, d

Detail Solution: IP protocol uses connection-less routing, where each packet is treated as independent packet. Also, IP is not a host-to-host layer.

Thus true options are (b) and (d).

QUESTION 2:

Which of the following is/are **false** for *direct and indirect packet delivery* option?

a. Direct delivery occurs when the destination host and deliverer are not present on same network.
b. Indirect delivery occurs when the destination host and deliverer are present on same network.
c. In direct delivery, hosts of same network can exchange packets without interference of router.
d. In direct delivery, an incoming packet to the router is forwarded to the destination host present in the network.
e. In an indirect delivery, the packet goes from router to router until it reaches the one connected to the same physical network as its final destination.
f. None of these.

Correct Answer: a, b

Detail Solution: Direct delivery occurs when the source and destination of the packet are located on the same physical network or when the delivery is between the last router and the destination host. If the destination host is not on the same network as the deliverer, the packet is delivered indirectly. In an indirect delivery, the packet goes from router to router until it reaches the one connected to the same physical network as its final destination.

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

QUESTION 3:

Which of the following routing flags can indicate route to a single host (and not to a network) in the routing table?

a. U
b. G
c. H
d. D
e. M

Correct Answer: c

Detail Solution: If the routing table entry indicates a host specific address, then it is specified by H flag.

Thus the correct option is (c).

QUESTION 4:

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

a. Autonomous systems are set of routers and networks managed by a single organization.
b. In exterior routing protocol, all the participating routers are present in the same autonomous system.
c. In interior routing protocol, the participating routers can be present in different autonomous systems.
d. None of these.

Correct Answer: b, c

Detail Solution: Autonomous Systems are set of routers and networks managed by a single organization. The interior routing protocols applies to a single autonomous system. All the routers inside the AS exchange messages using some standard protocol (e.g. RIP or OSPF) and update their routing tables. In an exterior routing protocol (like BGP), routers belonging to different AS's exchange messages.

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

QUESTION 5:

In Open Shortest Path First (OSPF) routing approach, which of the following packets is used to check if the neighbor router is up or not?

a. Link State Request.
b. Link Request Update.
c. Link State Acknowledgement.
d. Using TCP 3-way handshake protocol.
e. None of these.

Correct Answer: e

Detail Solution: In Open Shortest Path First (OSPF) routing approach, the "Hello" packet is used to check if a neighbor is up or not.

Thus, the correct option is (e).

QUESTION 6:

If a packet is to be delivered to all the hosts in a network, what kind of address should be used to specify the destination?

a. Unicast address.
b. Broadcast address.
c. Anycast address.
d. None of these.

Correct Answer: b

Detail Solution: Unicast address is used if a packet is to be delivered to a specific host. Broadcast address is used if a packet has to be delivered to all the hosts within a network or

subnetwork. Anycast address is used if a packet has to be delivered to exactly one of the hosts in a network or subnetwork.

Thus, the correct option is (b).

QUESTION 7:

How many bits are used to represent IPv4 and IPv6 addresses respectively?

a. 4, 24
b. 24, 32
c. 32, 64
d. 32, 128
e. 255, 255

Correct Answer: d

Detail Solution: IPv4 address is represented with 32 bits, and that for IPv6 requires 128 bits.

Thus, correct option is (d).

QUESTION 8:

When an entire IPv6 packet is included as payload inside an IPv4 packet, it is called _____.

a. Encapsulation
b. Tunneling
c. Decapsulation
d. None of these

Correct Answer: b

Detail Answer: When entire IPv6 packets are encapsulated within IPv4 packets, it is called tunneling. The IPv6 packet gets transmitted as data over an IPv4 network.

Thus the correct option is (b).

QUESTION 9:

The size of base header in IPv6 datagram packet is _____ bytes.

Correct Answer: 40

Detail Answer: The base header size of IPv6 datagram packet is 40 bytes, which consists of 128+128 bit source and destination addresses, 8 bit hop limit, 8 bit for next header, 16 bit payload length, 4 bit version, 8 bit priority, and 20 bit flow label.

QUESTION 10:

Consider the following routing table in a router. On which interface will an IP packet with destination address 144.25.112.40 be forwarded?

Destination	Subnet Mask	Interface
144.25.0.0	255.255.0.0	Eth0
144.25.96.0	255.255.96.0	Eth1
144.25.64.0	255.255.192.0	Eth2
144.25.112.0	255.255.240.0	Eth3
Default	0.0.0.0	Def

a. Eth0
b. Eth1
c. Eth2
d. Eth3
e. Def

Correct Answer: d

Detail Solution:

Row 1: 144.25.112.40 AND 255.255.0.0 = 144.25.0.0 ➔ Matches with destination address

Row 2: 144.25.112.40 AND 255.255.96.0 = 144.25.96.0 ➔ No Match

Row 3: 144.25.112.40 AND 255.255.192.0 = 144.25.64.0 ➔ No Match

Row 4: 144.25.112.40 AND 255.255.240.0 = 144.25.112.0 ➔ Matches with destination address

Row 4 provides longest match, thus the packet will be forwarded to interface Eth3.

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

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*******

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment- Week 5

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 15 **Total mark: 15 x 0.8 = 12**

QUESTION 1:

Consider the following statements:

(i) The purpose of vulnerability scanning is to identify weakness of system/network in order to determine how a system can be exploited.

(ii) NMAP script can be useful for automated scanning. However, scripts can have specific requirement.

a. Only (i) is true.
b. Only (ii) is true.
c. Both (i) and (ii) are true.
d. Both (i) and (ii) are false.

Correct Answer: c

Detail Solution: The purpose of vulnerability scanning is to identify vulnerabilities and weaknesses of a system/network in order to determine how a system can be exploited. Typical tools that are used for scanning vulnerabilities in hosts and networks are NMAP, Nessus, Nexpose, MPSA, etc. NMAP scripts can be useful for automated scanning, however each script can have specific requirement, i.e. some specific ports should be open on the target system.

Thus the correct option is (c).

QUESTION 2:

Which of the following NMAP option runs some of the nmap scripts?

a. -A
b. -sC
c. -pn
d. -PE
e. –sL

Correct Answer: a, b

Detail Solution: -sC performs a script scan using the default set of scripts. It is equivalent to --script=default. –A option which is known as aggressive scan enables OS detection (-O), version scanning (-sV), script scanning (-sC) and traceroute (--traceroute).

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

QUESTION 3:

Which of the following NMAP scripts is used to preform DoS attack?

a. ssh-brute
b. smb-os-discovery
c. smb-brute
d. http-slowloris-check
e. None of these.

Correct Answer: e

Detail Solution: -ssh-brute is used to crack credential of ssh service; smb-brute is used to crack user credential; smb-os-discovery is used to identify the OS of the target system; http-slowloris-check script is used to check if the webserver is vulnerable to DoS attack without actually launching a DoS attack, http-Slowloris script is used to launch Slowloris attack.

Thus the correct options is (e).

QUESTION 4:

Which of the following tools/software **cannot** be used for scanning vulnerabilities?

a. Hypervisor
b. Nessus
c. Hydra
d. crunch
e. hascat
f. Nmap

Correct Answer: a, c, d, e

Detail Solution: The typical tools that are used for scanning vulnerabilities in hosts and networks are NMAP, Nessus, Nexpose, MPSA, etc.

Hypervisor is used to run virtual machines. Hydra is used for password cracking, crunch is used for making dictionary, hascat is used to generate has passwords.

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

QUESTION 5:

Which of the following tool/approach can be used for proxy preparation?

a. Web based proxy/Proxychains tools
b. By running NMAP vulnerability scanning scripts.
c. Macchanger tool
d. Hypervisor
e. Firewall

Correct Answer: a, c

Detail Solution: For proxy preparation, we can use web based proxy or Proxychains tools to change our IP. To change mac address we can use macchanger tool.

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

QUESTION 6:

Which of the following is **not** a password cracking approach?

a. Shoulder Surfing
b. Social Engineering
c. Dictionary Attack
d. Brute-Force attack
e. Rule Based Attack
f. None of these.

Correct Answer: f

Detail Solution: All of the approach can be used for password cracking. In Shoulder Surfing attacker spy at the user's keyboard or screen while he/she is logging in. In Social Engineering attack, attacker convince victim to reveal passwords. In Dictionary Attack a dictionary file is used that runs against user accounts. In Brute-Force Attack, attacker tries, every combination of characters until the password is broken. Rule-based Attack is used when the attacker gets some information about the password.

Thus the correct option is (f).

QUESTION 7:

Which of the following tools can be used to create a dictionary for dictionary based password attack?

a. Hydra

b. Crunch
c. Nessus
d. None of these.

Correct Answer: b

Detail Solution: To create a dictionary crunch tool can be used. Hydra is used for dictionary based password attack. Nessus is used for vulnerability scanning.

Thus the correct option is (b).

QUESTION 8:

Which of the following statement(s) is/are **true** for user enumeration?

a. Enumeration refers to collecting details of users and their privileges.
b. User enumeration refers to collecting username and passwords.
c. NMAP does not have any script for user enumeration.
d. Hydra and crunch tool can be used for user enumeration.

Correct Answer: a

Detail Solution: User enumeration refers to collecting details of user and there privilege. It can also give details for password rules, however it cannot generate password for respective users. For enumeration we can use tools such as enum4linux, rpcclient. We can also use an nmap scrip smb-enum-users for user enumeration. However, hydra and crunch is used for password cracking.

Thus the correct option is (a).

QUESTION 9:

Which of the following can be used for gaining same level privileges than existing one?

a. Vertical privilege escalation.
b. Horizontal privilege escalation.
c. Diagonal privilege escalation.
d. Triangular privilege escalation.
e. None of these.

Correct Answer: b

Detail Solution: Vertical privilege escalation refers to gaining higher than existing privileges. Horizontal privilege escalation refers to acquiring the same level of privilege with the identity of some other user. There is nothing called diagonal/triangular privilege escalation.

Thus the correct option is (b).

QUESTION 10:

Which of the following approaches can be helpful to avoid privilege escalation attack?

a. Run user level application on least privileges.
b. Keep the software updated.
c. Regularly perform vulnerability scan.
d. Institute a strong password policy.
e. Avoid downloading files from untrusted/malicious websites.
f. Ignore unknown mails.

Correct Answer: a, b, c, d

Detail Solution: The approach given in option a, b, c, d can be useful for avoiding privilege escalation. The approach given in option e and f can be helpful against malware/social engineering attack.

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

QUESTION 11:

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

a. Malware are malicious software that damages or disables computer systems and gives limited or full control to the malware creator for the purpose of theft or fraud.
b. Malware can get inside systems through file sharing or fake programs.
c. Malware cannot replicate itself.
d. Malwares can alter, corrupt, modify or delete some data/files.
e. None of these.

Correct Answer: c

Detail Solution: Malware are malicious software that damages or disables computer systems and gives limited or full control to the malware creator for the purpose of theft or fraud. It can modify or delete data/files. Malware are usually get inside system using file sharing or by fake software. Some specific type of malwares such as virus and worms typically replicate themselves and get attached to other files.

The correct option is (c).

QUESTION 12:

Which of the following can be used as a countermeasure against malwares?

a. Use of firewall
b. Avoid downloading files from untrusted/malicious websites
c. Use of antivirus tools
d. Keep computer and software updated.
e. Ignoring unknown mails
f. All of these

Correct Answer: f

Detail Solution: All of the given approaches can be used as a countermeasure against Malwares.

QUESTION 13:

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

a. Sniffing is a process of monitoring and capturing all data packets passing through a given network.
b. The HTTPS packets are vulnerable to sniffing attack.
c. In passive sniffing ARP packets are used to flood the switch's CAM table.
d. None of these.

Correct Answer: b, c

Detail Solution: Sniffing is a process of monitoring and capturing all data packets passing through a given network. Sniffing is categorized into two types: active and passive. In passive sniffing, sniffing is done on a hub where traffic is sent to all device. Passive sniffing involves only monitoring. Active sniffing is used against switch-based network. In active sniffing first the switch CAM table is flooded with incorrect ARP entries. Mostly the unsecured protocols which shares data in plaintext are vulnerable to sniffing.

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

QUESTION 14:

Which of the following commands is used to delete an ARP entry in a system?

a. arp -l
b. arp -s
c. arp -i
d. arp –e
e. None of these

Correct Answer: e

Detail Solution: To access all information related to ARP, arp command is used, -a option is used to see all arp entries, -s option is used to create new arp entry, -i option is used to specify a particular network interface, -d option is used to delete an arp entry.

The correct option is (e).

QUESTION 15:

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

a. ARP spoofing involve construction of large number of forged ARP request/reply packets.

b. Using fake ARP messages, an attacker can divert all communications between two machines so that all traffic is exchanged via his/her PC.

c. In MAC attack, CAM table are flooded with fake MAC address and IP pairs.

d. MAC attack cannot change the behavior of the switch.

e. MAC attack can fill the CAM table of adjacent switches.

f. None of these.

Correct Answer: a, b, c, e

Detail Solution: ARP spoofing involve construction of large number of forged ARP request/reply packets. Using fake ARP messages, an attacker can divert all communications between two machines so that all traffic is exchanged via his/her PC. In MAC attack, CAM table are flooded with fake MAC address and IP pairs. MAC attack can change the behavior of switch to act like a hub and can also fill the CAM table of adjacent switch.

Thus the true options are (a), (b), (c) and (e).

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment- Week 6

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following statement is **true** for Masquerade attack?

a. In this attack, an attacker passively captures a transaction and its reply.
b. In this attack, some portion of message is altered on its way.
c. In this attack, an attacker prevents access of resource to its legitimate users.
d. In this attack, the attacker pretends as a legitimate entity.
e. In this attack, the attacker analyzes the network traffic.

Correct Answer: d

Detail Solution: Analyzing the network traffic refers to passive attack. Masquerade is an active attack, which can be categorized in 4 categories. In Masquerade, one entity (attacker) pretends to be a different entity (legitimate). Replay involve passive capture of a transaction and subsequent replay. In modification, some portion of a message is altered on its way. Denial of service prevents access to resources.

Thus the correct option is (d).

QUESTION 2:

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

a. In private key encryption, separate keys are used by sender and receiver.
b. In private key encryption, a single key is used by sender and receiver.
c. In public key encryption, separate keys are used by sender and receiver.
d. In public key encryption, a single key is used by sender and receiver.

Correct Answer: b, c

Detail Solution: Encryption is the most important concept for network security, typically two types of encryptions are used. Private key: where the sender and receiver uses same key for

encryption/decryption of the message. Public key: where a separate key is used for encryption and decryption of the message.

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

QUESTION 3:

Consider the following statement:
(i) In symmetric key cryptography, the security depends on secrecy of the key.
(ii) In symmetric key cryptography, the security depends on encryption/decryption algorithm.

a. Only (i) is true
b. Only (ii) is true
c. Both (i) and (ii) are true.
d. Both (i) and (ii) are false.

Correct Answer: a

Detail Solution: In symmetric key (private key) cryptography, the security of the data only depends on the secrecy of the key shared among sender and receiver, and not on the algorithm used for encryption and decryption.

Thus correct option is (a).

QUESTION 4:

25 parties want to exchange messages securely. The number of distinct key required by a symmetric key encryption algorithm and public key encryption technique like RSA will be _____ and _____ respectively.

a. 25 and 50
b. 50 and 50
c. 100 and 50
d. 300 and 25
e. 300 and 50

Correct Answer: e

Detail Solution: In symmetric encryption, every pair of communicating parties must have a separate key. For N parties, the number of keys will be ${}^{N}C_2$. For N = 25, ${}^{25}C_2 = 25 \times 24 / 2 = 300$.

In public-key or asymmetric encryption, every party is in possession of two keys, a public key and a private key. For N parties, the number of keys will be 2N. For N = 25, the number of distinct keys required will be 2 x 25 = 50.

Thus the correct option is (e).

QUESTION 5:

How will be the plaintext for the cipher text "LETTY CEIV" encrypted using a substitution cipher approach, where each letter is replaced by the k-th next letter. (Assumption: (i) the alphabets are wrapped around, i.e. Z is followed by A, (ii) each alphabets (A to Z) is assigned a number (1 to 26), (iii) the value of secrete key k is 4).

a. HAPPY YEAR
b. HAPPU YAER
c. HAPPY YEAR
d. None of this

Correct Answer: b

Detail Solution: k=4 indicates that for encryption, each letter is replaced by its 4^{th} following letter. If we decrypt the message we will get the plain text as HAPPU YAER.

Thus the correct option is (b).

QUESTION 6:

In data encryption standard (DES), longer plain text are processed in _____ bit blocks.

Correct Answer: 64

Detail Solution: In the DES algorithm, the key size is 56 bits, plaintext length is 64-bit. It is a block cipher; thus if the plain text are longer, then it is processed in 64-bit blocks.

QUESTION 7:

The effective key lengths used in AES encryption algorithms can be:

a. 64 bit
b. 128 bit
c. 192 bit
d. 256 bit
e. 512 bit

Correct Answer: b, c, d

Detail Solution: In AES the block length is limited to 128 bit, however the key length can be 128, 192 or 256 bit.

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

QUESTION 8:

For decryption using public-key cryptography _____ is used.

a. Receiver's public key
b. Receiver's private key
c. Sender's public key
d. Sender's private key

Correct Answer: b

Detail Solution: If a sender A wants to carry out encryption on a message and send it to receiver B using public-key cryptography, A will encrypt the given message using B's public key, so that it can be correctly decrypted by the receiver B using B's private key.

Thus the correct option is (b).

QUESTION 9:

Which of the following statement(s) is/are **true**.

a. The security of RSA algorithm is dependent on prime factorization problem.
b. RSA algorithm is vulnerable to man-in-the middle attack.
c. Diffie-Hellman approach can be used for encryption/decryption of message.
d. Symmetric encryption approaches are faster than asymmetric encryption.
e. None of these.

Correct Answer: a, d

Detail solution: The security of the RSA algorithm depends on the complexity of factoring the product of two large prime numbers. It is not vulnerable to man-in the middle attack. Diffie-Hellman is used to exchange keys rather than encryption/decryption applications. Symmetric encryption/decryption is much faster than asymmetric encryption/decryption.

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

QUESTION 10:

Which of the following techniques **cannot** be used for message authentication?

a. Conventional encryption approach such as private key.
b. MD4
c. SHA-256
d. SHA-0
e. RIPEMD-128

Correct Answer: d

Detail Solution: For message authentication, conventional encryption approach, MD2, MD4, MD5, SHA-1, SHA-256, SHA-384, SHA512, RIPEMD-128 and RIPEMD-160 can be used. There is nothing called SHA-0.

Hence, the correct option is (d).

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

Course Name: ETHICAL HACKING

Assignment- Week 7

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Consider a hash function H that generates hash values h1 and h2, when fed with messages m1 and m2 respectively. Which of the following options can **never be true**?

a. h1 and h2 are equal, but m1 and m2 are unequal.

b. m1 and m2 are equal, but h1 and h2 are unequal.

c. None of these.

Correct Answer: b

Detail Solution: A hash function maps a given message m to generate some particular hash value h. Two different messages m1 and m2 can, however, generate the same hash value, which is called collision. The same message always generates the same hash value. The correct option is (b).

QUESTION 2:

What is meant by collision in the context of hashing?

a. More than one different message can generate the same hash value.

b. After encryption, the ciphertexts corresponding to two or more plaintexts are the same.

c. The hash function generates the all zero string as the hash value.

d. None of these.

Correct Answer: a

Detail Solution: In a hash function, collision refers to the situation where more than one different message generate the same hash value. It has nothing to do with encryption. The correct option is (a).

QUESTION 3:

A message M is fed to a hash function HASH to generate the hash value H:

H = HASH (M)

Which of the following statements is **true**?

a. The number of bits in H is much larger than the number of bits in M.
b. The number of bits in H and M are almost equal.
c. The number of bits in M is much larger than the number of bits in H.
d. None of these.

Correct Answer: c

Detail Solution: A hash function maps a very large number to a relatively much smaller number. The correct option is (c).

QUESTION 4:

What of the following does not correspond to the first preimage resistance in the context of hash functions?

a. It is difficult to find a message M such that HASH(M) = H, except for a few hash values H.
b. Given a message M1, it is difficult to find another message M2 such that HASH(M1) = HASH(M2).
c. It is difficult to find two messages M1 and M2 such that HASH(M1) and HASH(M2) and unequal.
d. None of these.

Correct Answer: b, c

Detail Solution: This follows from the definition of the desirable properties of a hash function. First preimage resistance refers to the condition that we are given a hash value H, and are trying to find out some message M such that HASH(M) = H. This should be difficult to do. The correct options are (b) and (c).

QUESTION 5:

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

a. Hashing realizes a one-to-one mapping.

b. Encryption realizes a one-to-one mapping.
c. Hashing realizes a many-to-one mapping.
d. Encryption realizes a many-to-one mapping.

Correct Answer: b, c

Detail Solution: A hash function by definition realizes a many-to-one mapping, where more than one message can get mapped to the same hash function. In contrast, encryption realizes a one-to-one function, where a given plaintext maps to a unique ciphertext, and vice versa. The correct options are (b) and (c).

QUESTION 6:

Which of the following are hash functions?

a. MD5
b. Triple-DES
c. SHA-1
d. AES

Correct Answer: a, c

Detail Solution: MD5 and SHA-1 are examples of hash function, while Triple-DES and AES are examples of symmetric key encryption algorithm. The correct options are (a) and (c).

QUESTION 7:

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

a. Computing a hash function is faster than computing symmetric-key encryption.
b. Computing public-key encryption is slower than computing symmetric-key encryption.
c. Computing public-key encryption is slower than computing hash function.
d. Both public-key and symmetric-key encryption take approximately the same time.

Correct Answer: a, b, c

Detail Solution: Public-key encryption is the slowest, while hash function computation is the fastest. Hence, the correct options are (a), (b) and (c).

QUESTION 8:

What are the block size and key size of the DES algorithm?

a. 64 bits, 56 bits
b. 56 bits, 64 bits
c. 64 bits, 64 bits
d. 64 bits, 128 bits

Correct Answer: a

Detail Solution: In the DES algorithm, the block size is 64 bits and the key size is 56 bits. The correct option is (a).

QUESTION 9:

What kinds of algorithms are typically used in the computation of digital signature?

a. Cryptographic hash function.
b. Symmetric-key encryption.
c. Biometric authentication.
d. All of these

Correct Answer: a

Detail Solution: Digital signature is the electronic equivalent of pen-and-paper signature, and typically uses a combination of hashing and public-key cryptography. A hash function is first computed on the given message, and the hash value is encrypted using public-key cryptography, with the sender's private key. It does not reply on biometric authentication. The correct option is (a).

QUESTION 10:

The SSL record protocol is responsible for

a. High-speed data transmission
b. Data authentication
c. Non repudiation
d. None of these

Correct Answer: d

Detail Solution: The SSL Record protocol uses a combination of various cryptographic techniques to provide secure data transmission over a network. It ensures data encryption and also data integrity (using a hash function). However, it does not provide authentication service or non-repudiation guarantee. The correct option is (d).

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment- Week 8

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following are examples of steganography?

a. Hiding some text information within an image file.
b. Hiding some text information within an audio clip.
c. Hiding some secret information within an executable file.
d. Encrypting an image file so that only the intended recipient can view it.

Correct Answer: a, b, c

Detail Solution: Steganography refers to a set of methods where some information is hidden within some other file (like image, audio, video, executable, etc.). It does not involve encryption for secure access. The correct options are (a), (b) and (c).

QUESTION 2:

Which of the following statements correctly represents the term steganography?

a. Encrypting some information such that it will not be legible to an unauthorized person.
b. A low-cost alternative to encryption and decryption.
c. Secure way of communicating without sharing any key.
d. None of these.

Correct Answer: d

Detail Solution: Steganography refers to a set of methods where some information is hidden within some other file (like image, audio, video, etc.). It does not concern encryption or decryption, and also secure communication. The correct option is (d).

QUESTION 3:

Which of the following correspond to behavioral biometrics?

a. Biometrics that relate to human behavior.
b. Biometrics that relate to human body.
c. Biometrics that rely on the use of a powerful computer system.
d. None of these

Correct Answer: a

Detail Solution: Behavioral biometrics refers to biometrics that relate to human behavior, like signature (hand and finger movement) and Gait (walking style). However, fingerprint, Iris scan and Retina scan are properties of the human body and not dependent on the behavior. It does not rely on computing power. Hence, the correct option is (a).

QUESTION 4:

Consider a gray-level image of size 1000 x 1000, where each pixel is stored in 8-bits (representing a gray scale). How many bits of information can be hidden in the image by using LSB steganography technique? Assume 1K = 1000, and 1M = 1,000,000.

a. 100 Kbits
b. 500 Kbits
c. 1 Mbits
d. None of these.

Correct Answer: c

Detail Solution: Each pixel consists 1 byte, and hence 1 bit of information can be stored in each pixel. The number of bits of hidden information that can be stored in the whole image will be:

1000 x 1000 x 1 bits = 1,000,000 bits = 1 Mbits

The correct answer is (c).

QUESTION 5:

What is denial-of-service attack?

a. An attack on a system whereby stored files get modified or deleted.
b. An attack that destroys users information from a system.
c. An attack that destroys the stored password information in a system.
d. None of these.

Correct Answer: d

Detail Solution: In a denial-of-service attack, some service running on a victim machine is rendered inaccessible from legitimate users of the service. The correct option is (d).

QUESTION 6:

Which of the following attacks refer to the situation where an attacker gains entry into the victim machine (or spoofs the IP address) and then sends a ping request to a broadcast address?

a. SYN flooding attack.
b. Smurf denial-of-service attack.
c. DNS spoofing attack.
d. None of these.

Correct Answer: b

Detail Solution: In the Smurf DoS attack, the victim gains entry into the victim machine (or spoofs the IP address) and then sends a ping request to a broadcast address. A large number of ping response packets are received, which can overload the victim. The correct option is (b).

QUESTION 7:

Which of the following attacks rely on some vulnerability in the TCP connection establishment phase?

a. SYN flooding attack.
b. DNS spoofing attack.
c. Smurf DoS attack.
d. None of these.

Correct Answer: a

Detail Solution: The SYN flooding attack tries to exploit a weakness in the TCP connection establishment phase. The attacker floods the victim machine with a large number of TCP connection requests, each of which is left as half-open (i.e. the third packet in 3-way handshake is not sent). Each connection request will take up some resources on the victim machine (e.g. port number, buffer space, etc.), and ultimately genuine requests will not get processed.

The correct option is (a).

QUESTION 8:

Which of the following is/are true for Botnet?

a. A Botnet refers to a host connected to the Internet that is under control of the attacker.
b. A Botnet host runs a number of bots that are repetitive code segments with some malicious intent.
c. It relies on IP spoofing to mount attacks.
d. All of these.

Correct Answer: a, b

Detail Solution: Many of the network-based attacks (DoS and DDoS in particular) are based on so-called Botnets. A Botnet refers to a host connected to the Internet that is under the control of the attacker. The Botnet host runs a number of "bots" that are repetitive code segments with some malicious intent, typically used to mount an attack. It does not spread from one machine to another.

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

QUESTION 9:

Which of the following is true for iterative name resolution?

a. A host may have to send multiple DNS requests to several DNS servers.
b. A host sends a single DNS request to its next higher-level DNS server.
c. Name resolution happens iteratively within the host itself without sending any DNS request messages.
d. None of these.

Correct Answer: a

Detail Solution: The DNS server receives a DNS request from a host containing a domain name, and it returns the corresponding IP address. In iterative name resolution, in response to a DNS request, the DNS server sends back a response specifying the next DNS server to send the query. In this way, the host may have to send a number of DNS requests before it gets resolved. In recursive name resolution, the host sends a DNS request to the next higher level DNS server. The DNS server in turn recursively forwards the request to its next higher-level DNS server, and so on, until the request gets resolved. The final reply gets back to the host. Here, the host sends a single DNS request.

Thus, option (a) is true.

QUESTION 10:

What is the full form of PGP?

a. Packet Group Protocol
b. Port Group Protocol
c. Pretty Good Privacy
d. All of these.

Correct Answer: c

Detail Solution: PGP stands for Pretty Good Privacy. The correct option is (c).

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment Solution- Week 9

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following statement(s) is/are true for sniffing?

a. It is a process of analyzing network activity by capturing network traffic.
b. It is a process of finding the vulnerability in a network.
c. It is a process used for user enumeration.
d. None of these.

Correct Answer: a

Detail Solution: Sniffing is a process of analyzing network activity by capturing network traffic. Using a sniffing tool we can capture network data and display them in a readable format; we can capture network log for forensics and evidence.

Thus the correct option is (a).

QUESTION 2 :

Consider the following statements.
(i) Burp suite is a popular tool used for sniffing.
(ii) Using Burp suite we can perform password attack on web applications.

a. Only (i) is true.
b. Only (ii) is true.
c. Both (i) and (ii) are true.
d. Both (i) and (ii) are false.

Correct Answer: c

Detail Solution: Burp suite is a tool that can be used for sniffing. With the help of payload option available in intruder module, we can also perform password attack on web applications.

The correct option is (c).

QUESTION 3:

What is the purpose of repeater module available in burp suite?

a. It is used to mount password attack.
b. It is used for manipulating and reissuing packets and to analyze their response.
c. It is used for creating dictionary.
d. None of these.

Correct Answer: b

Detail Solution: Repeater module is used for manipulation and reissuing packets, it analyzes the response of manipulated packet.

The correct option is (b).

QUESTION 4:

Which of the following approach(es) cannot protect against sniffing?

a. Restrict physical access to the network media.
b. Permanently add the MAC address of gateway to ARP cache.
c. Use encryption to protect confidential information.
d. Use dynamic IP address and ARP entries.
e. None of these.

Correct Answer: d

Detail Solution: To protect against sniffing following countermeasures can be used:

(a) Restrict the physical access to the network media to ensure that a packet sniffer cannot be installed; (b) Use encryption to protect confidential information; (c) Permanently add the MAC address of the gateway to the ARP cache; (d) Use static IP addresses and static ARP tables to prevent attackers from adding spoofed ARP entries for their machines to the network; (e) Turn off network identification broadcasts, and if possible, restrict the network to authorized users in order to protect the network from being discovered with sniffing tools; (f) Use the IPv6 instead of the IPv4 protocol; (g) Use encrypted sessions such as Secure Shell (ssh) instead of Telnet; (h) Use Secure Copy (scp) instead of a file transfer protocol (ftp); (i) Use Secure Socket Layer (SSL) for email connections.

However if we use dynamic IP address and ARP entries then an attacker can mount arpspoof attack and can change the NIC of the system in promiscuous mode.

The correct option is (d).

QUESTION 5:

Which of the following is/are example(s) of human-based social engineering attack?

a. Impersonation
b. Piggybacking
c. Shoulder surfing
d. Pop-up windows
e. Chain letters
f. phishing

Correct Answer: a, b, c

Detail Solution: The options (a), (b) and (c) are example of human-based social engineering attacks, while d, e and f are examples of computer-based social engineering attack.

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

QUESTION 6:

Which of the following tools can be used for social engineering attack?

a. Dnsenum
b. Hydra
c. Crunch
d. SEToolkit
e. Arpspoof

Correct Answer: d

Detail Solution: Social Engineering Toolkit (SEToolkit) is used to perform social engineering attacks. Whereas Dnsenum is used for user enumeration; Hydra and Crunch are used for password attack; arpspoof tool is used for arpspoofing.

The correct option is (d).

QUESTION 7:

Which of the following protocols is/are not vulnerable to sniffing attack?

a. HTTP
b. Telnet
c. SSH
d. SSL

Correct Answer: c, d

Detail Solution: SSH and SSL exchange data over secure channel, HTTP, Telnet, rlogin and FTP protocols exchange data in plain text (unsecured form), thus it is vulnerable to sniffing attack.

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

QUESTION 8:

Which of the following can be used as a countermeasure for DoS/DDoS attack?

a. Replicate servers to provide additional failsafe protection.
b. Increase bandwidth on critical connections.
c. Secure the infrastructure using approaches such as anti-spam, content filtering, anti-trojan, firewalls, and load balancing.
d. Shut down all services until the attack has subsided.
e. None of this.

Correct Answer: a, b, c, d

Detail Solution: All measures given in option (a) to (d) can be used to protect against DoS/DDoS attacks.

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

QUESTION 9:

Which of the following tool/approach cannot be used to perform DoS attack?

a. Hping3 tool
b. “http-slowloris” nmap script
c. LOIC tool
d. Hydra and Crunch.

Correct Answer: d

Detail Solution: We can perform DoS attack using Slowloris script, Hping tool as well as using LOIC tool. Hydra and Crunch tool are used for password cracking.

The correct option is (d).

QUESTION 10:

For mounting DoS attack using hping3 tool how many packets will be send per second if we use --faster option?

a. 10
b. 100
c. 1000
d. 10000

Correct Answer: b

Detail Solution: -- faster option allows the sending 100 packets in a second.

The correct option is (b).

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment- Week 10

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following is/are true for black box testing kind of attack?

a. It is an invasive type of attack.
b. It is a non-invasive type of attack.
c. The attacker has information about the implementation details.
d. It relies on weakness of implementation

Correct Answer: b

Detail Solution: In black box testing, the attacker sends an input to the circuit and receives an output. Based on the input/output behavior, the attacker decides what kind of algorithm is used inside. It is a non-invasive type of attack.

The correct option is (b).

QUESTION 2:

What are the typical countermeasures to prevent hardware-based attacks?

a. We obfuscate data in registers and buses.
b. We add preventive measures against side-channel attacks.
c. We provide authentication using physical unclonable functions.
d. We use a very secure cryptographic algorithm.

Correct Answer: a, b, c

Detail Solution: All of (a), (b) and (c) constitute countermeasures for the prevention of hardware-based attacks. Use of a secure cryptographic algorithm cannot prevent hardware-based attacks.

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

QUESTION 3:

Which of the following statement(s) is/are true for side channel attacks?

a. They exploit some weakness in the algorithm.
b. They exploit some weakness in the implementation of the algorithm.
c. They require physical access to the device.
d. They only require the set of inputs/outputs to the algorithm.

Correct Answer: b, c

Detail Solution: Side-channel attacks basically exploit weaknesses in the implementation (hardware or software) of an algorithm. It requires physical access to the device for measurement of some parameter. They are not dependent on the weaknesses of the algorithm. Moreover, they do not rely on applying inputs and observing the outputs only.

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

QUESTION 4:

Which of the following side channel(s) is/are typically exploited in side-channel attacks?

a. Electromagnetic emissions.
b. Time taken to execute an algorithm.
c. The time and space complexities of an algorithm.
d. Power consumed during computation.
e. All of these.

Correct Answer: a, b, d

Detail Solution: Timing analysis, power analysis, and EM emission analysis are very common in mounting side-channel attacks. It does not rely on the time or space complexity of the algorithm.

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

QUESTION 5:

For modular exponentiation computation of x^{17}, how many squaring and multiplication operations would be required?

a. 4 and 4.
b. 4 and 2.

c. 3 and 2.
d. 3 and 1.
e. None of these.

Correct Answer: e

Detail Solution: The binary representation of 17 is 10001.

Thus, $x^{17} = x^{16} * x^1 = (x^8)^2 * x^1 = ((x^4)^2)^2 * x^1 = (((x^2)^2)^2)^2 * x^1$

This computation requires 4 squaring and 1 multiplication operations.

The correct option is (e).

QUESTION 6:

What does power analysis do?

a. It measures variation in power consumption during a computation.
b. It attacks the power supply and feeds power to the circuit.
c. It relies on the use of a hardware Trojan in the circuit.
d. All of these.

Correct Answer: a

Detail Solution: Power analysis attack relies on measuring the variations in power consumption during execution of an algorithm. It neither tries to attack the power supply, nor it uses a hardware Trojan.

The correct option is (a).

QUESTION 7:

Which of the following strategies can help to prevent power analysis attacks?

a. The computation times in the different branches of conditional statements must be unequal.
b. The computation times in the different branches of conditional statements must be the same.
c. We can use a random noise generator in the circuit.
d. We obfuscate the scan chains in the circuit.

Correct Answer: b, c

Detail Solution: Power analysis attack can be prevented by making all the branches in conditional statements symmetric with respect to computation. It can also be prevented by using a random noise generator. It does not depend on the scan chains in the circuit.

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

QUESTION 8:

What is the meaning of PUF?

a. Perfect Universal Function
b. Physically Unclonable Function
c. Polynomially Unclonable Function
d. None of these.

Correct Answer: b

Detail Solution: The full form of PUF is Physically Unclonable Function.

The correct option is (b).

QUESTION 9:

Which of the following is/are true for hardware Trojan?

a. It incurs small hardware overhead.
b. It is stealthy and usually difficult to detect.
c. It relies on a number of malicious nodes to mount attacks.
d. It is used to reduce power consumption.

Correct Answer: a, b

Detail Solution: A hardware Trojan incurs small hardware overhead, and is difficult to detect. It does not lead to reduction in power consumption. Also, it is not used to mount attacks.

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

QUESTION 10:

What are some of the software-based countermeasures to prevent timing-based side-channel attack?

a. Use a structured programming language for implementation.

b. Mask the data representation.
c. Introduce redundant computations as required.
d. All of these.

Correct Answer: b, c

Detail Solution: To prevent timing attacks, we can use masking and also introduce redundant computations to make all the branches of conditional statements symmetrical.

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

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

NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

Course Name: ETHICAL HACKING

Assignment Solution- Week 11

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which of the following Metasploit module(s) can be used to establish communication channel between Metasploit framework and target system?

a. Exploit
b. Payload
c. Auxiliary
d. Encoder
e. msfvenum

Correct Answer: b

Detail Solution: Encoder module is used to encode the payloads. Exploit module is used to take advantage of System/Application bugs. Payload module is used to establish communication channel between Metasploit framework and target system. Auxiliary module is used to perform brute force attack, DoS attack, host and port scanning, vulnerability scanning, etc.

The correct option is (b).

QUESTION 2:

Which of the following command is used to launch Metasploit framework?

a. msfconsole
b. msfvenum
c. Metasploit
d. None of these.

Correct Answer: a

Detail Solution: The msfconsole command is used to launch Metasploit framework.

The correct option is (a).

QUESTION 3:

In Metasploit to check the compatible target (OS) for any exploit, which of the following command (option) is used?

a. Show targets
b. Set payloads
c. Set targets
d. Show payloads
e. None of these.

Correct Answer: a

Detail Solution: To check the compatible operating systems for any exploits we can use "show targets" command, similarly to check compatible payload we can use "show payloads" option.

The correct option is (a).

QUESTION 4:

We can execute basic commands and tools inside Metasploit console.

a. True
b. False

Correct Answer: a

Detail Solution: The very interesting feature of Metasploit framework is that we can use all commands and tools such as nmap, inside the Metasploit framework.

The correct option is (a).

QUESTION 5:

Which of the following commands can be used to get user account details in Metasploit framework?

a. getsystem
b. hashdump
c. getuser
d. msfvenum

Correct Answer: b

Detail Solution: getsystem is used to escalate privilege and get administrative login, hashdump is used to get user account details, msfvenum is used for creating payloads. There is no command called getuser.

The correct option is (b).

QUESTION 6:

Which of the following types of attacks are possible on a webservers/web applications?

a. Denial-of-Services
b. Cross-Site-Scripting
c. SQL Injection
d. Session Hijacking
e. None of these.

Correct Answer: a, b, c, d

Detail Solution: In webserver various type of attacks are possible, the most common of which are: SQL Injection Attacks; Session Hijacking; Buffer Overflow Attacks; Cross-Site Scripting (XSS) Attacks; Denial-of-Service (DoS).

The correct options are (a), (b), (c), (d).

QUESTION 7:

Which of the following tools uses brute-force attack to extract existing and hidden page of a webserver?

a. Dirb
b. SQL MAP
c. Hydra
d. Crunch
e. None of these

Correct Answer: a

Detail Solution: To scan a webserver tools like dirb, dnsenum is used, we also use nmap script http-enum for the same purpose. Dirb tool performs brute-force attack to find out existing and

hidden webpages and directories. To automate sql injection attack, SQL MAP tool can be used. Hydra and Crunch are used for password cracking.

The correct option is (a).

QUESTION 8:

If any web page is vulnerable to error based sql injection, then which of the following is true?

a. It will print error message for incorrect user input.
b. It will not print anything for incorrect user input.

Correct Answer: a

Detail Solution: If the webpage is vulnerable to error-based sql injection, then it will generate an error message for incorrect user input.

The correct option is (a).

QUESTION 9:

Which of the following SQLMAP options is used to list all users along with hashed password?

a. - - users
b. - - passwords
c. - - user-pass
d. - - user-privileges

Correct Answer: b

Detail Solution: --passwords option is used to list all users with their hashed password.

The correct option is (b).

QUESTION 10:

Consider the following statements related to stored Cross-Site-Scripting attack.
(i) It is stored in the database of web application.
(ii) It affects only a single client of the web application.

a. Only (i) is true
b. Only (ii) is true.

c. Both (i) and (ii) are true.
d. Both (i) and (ii) are false.

Correct Answer: a

Detail Solution: Stored XSS are stored in database of web application and can affect all users; however, reflected XSS is limited to a single client.

The correct option is (a).

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

Course Name: ETHICAL HACKING

Assignment- Week 12

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

With help of NMAP tool:

a. We can determine which host are alive.
b. We can determine the services running on any target system.
c. We can determine the OS of the target systems.
d. We can create a dictionary.
e. We can identify the vulnerabilities of the target system.

Correct Answer: a, b, c, e

Detail Solution: NMAP can perform all of the above operations (except option d). NMAP can perform password attack; however, it uses the default dictionary available in the system. For creating dictionary, secondary tools such as crunch is used.

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

QUESTION 2:

In ICMP (ECHO) sweep scan, a scanner sends an ICMP type-8 packet and receives a ICMP type-0 packet from target. What does it indicates?

a. Target is alive/up.
b. Target is down.

Correct Answer: a

Detail Solution: If the sender receives ICMP type-0 packet, this indicates that the target is up. The correct option is (a).

QUESTION 3:

Which of the following NMAP options can be used for TCP sweep scan?

a. –PE
b. –PP
c. –PM
d. None of these.

Correct Answer: d

Detail Solution: TCP sweep is carried out using the –PS, –PU option in NMAP. It is also done by some default options such as –sT, -p, -Pn.

The correct option is (d).

QUESTION 4:

Which of the following sweep scans are automatically done when we use –sn option.

a. ICMP Echo
b. ICMP Non-Echo
c. TCP Sweep
d. UDP Sweep

Correct Answer: a, b, c

Detail Solution: All type of sweep options are used with –sn option except UDP sweep.

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

QUESTION 5:

The number of host (IP) scanned by NMAP command “nmap –sL 192.168.62.48-58” will be _____.

Correct Answer: 11

Detail Solution: The given command will scan all hosts with IP addresses 192.168.62.48 to 192.168.62.58 (including both the IPs).

Thus, a total of 11 IP addresses will be scanned.

QUESTION 6:

Which of the following NMAP options treats all hosts as online (skip host discovery)?

a. –sL
b. –sP
c. –PO
d. –sU
e. –Pn

Correct Answer: e

Detail Solution: -sL is used to list all IPs for scan; -sP is used for only determining if the host is online; -PO is used for IP protocol ping; -sU is used for UDP scan; -Pn is used to skip host discovery and treats all host as online

The correct option is (e).

QUESTION 7:

How many ports will be scanned using NMAP command “nmap --top-ports 5 Target_IP”?

a. 5
b. 100
c. 1000
d. 65535

Correct Answer: a

Detail Solution: --top-ports option is used to scan top ports, 5 represents that top 5 ports will be scanned by this NMAP command.

Thus correct option is (a).

QUESTION 8:

In NMAP by default _____ number of ports are scanned.

Correct Answer: 1000

Detail Solution: By default NMAP scans for top 1000 ports.

QUESTION 9:

In NMAP scan, a filtered port indicates that either the firewall or any other filter software is blocking nmap requests.

a. True.
b. False

Correct Answer: a

Detail Solution: An Open port indicates that some service are running on the port and nmap can identify this, a filtered port indicates that nmap cannot access that as some filtering software is blocking nmap request.

Thus, the correct option is (a).

QUESTION 10:

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

a. –PE
b. –PP
c. –sV
d. –O

Correct Answer: c, d

Detail Solution: For OS detection –O option is used, whereas for services and version detection –sV option is used.

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

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