

X



(<https://swayam.gov.in>)



([https://swayam.gov.in/nc\\_details/NPTEL](https://swayam.gov.in/nc_details/NPTEL))

codingoclock@gmail.com ▾

NPTEL (<https://swayam.gov.in/explorer?ncCode=NPTEL>) » Ethical Hacking (course)

≡

If already  
registered, click  
to check your  
payment status

## Week 01: Assignment 01

The due date for submitting this assignment has passed.

Due on 2023-08-09, 23:59 IST.

### Course outline

How does an  
NPTEL  
online  
course  
work? ()

Week 0 ()

Week 1 ()

Lecture 01 :  
Introduction to  
Ethical  
Hacking (unit?  
unit=18&lesso  
n=19)

Lecture 02 :  
Basic  
Concepts of  
Networking  
(part-I) (unit?  
unit=18&lesso  
n=20)

Lecture 03 :  
Basic

Assignment submitted on 2023-07-21, 23:24 IST

1)

1 point

Which of the following point(s) is/are true for an ethical hacker?

- a. An ethical hacker intends to gain unauthorized access to a resource for financial gain or personal recognition.
- b. An ethical hacker defaces websites or crash backend servers for fun, reputation damage or to cause financial loss.
- c. An ethical hacker is not concerned with improving the organization's security posture.
- d. None of these.

- a
- b
- c
- d

Yes, the answer is correct.

Score: 1

Accepted Answers:

d

2)

1 point

Concepts of Networking (part-II) (unit? unit=18&lesson=n=21)

Lecture 04 : TCP/IP Protocol Stack (part-I) (unit? unit=18&lesson=n=22)

Lecture 05 : TCP/IP Protocol Stack (Part-II) (unit? unit=18&lesson=n=23)

Lecture Material of Week 1 (unit? unit=18&lesson=n=25)

Quiz: Week 01: Assignment 01 (assessment? name=168)

Week 1 Feedback Form (unit? unit=18&lesson=n=26)

Assignment 1 Solution (unit? unit=18&lesson=n=27)

Week 2 ()

Week 3 ()

Week 4 ()

Week 5 ()

Week 6 ()

Week 7 ()

Week 8 ()

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

- a. In the black box model, the tester has complete information about the network.
- b. In the white box model, the tester does not have any information about the network.
- c. In the gray box model, the tester has partial information about the network.
- d. None of these.

a  
 b  
 c  
 d

Yes, the answer is correct.  
Score: 1

Accepted Answers:

c

3)

**1 point**

Which of the following statement(s) is/are **false** for a packet 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. It is efficient for bursty traffic.
- d. The packet transfer delay between a pair of nodes may depend on the prevailing network traffic.

a  
 b  
 c  
 d

Yes, the answer is correct.  
Score: 1

Accepted Answers:

b

4)

**1 point**

Which of the following statement(s) is/are **true** for datagram-based packet transfer approach?

- a. It is a connection-less packet switching approach, where no route is established priori to transfer of packets.
- b. In this approach, each packet is transmitted as an independent entity.
- c. In this approach each intermediate node can perform dynamic routing.
- d. In this approach all the packets reach in order to the destination.

**Week 9 ()**

- a
- b
- c
- d

**Week 10 ()**

**Week 11 ()**

**Week 12 ()**

**DOWNLOAD VIDEOS ()**

**Text Transcripts ()**

**Books ()**

Yes, the answer is correct.

Score: 1

Accepted Answers:

- a
- b
- c

5)

**1 point**

What is the purpose of the port number in TCP/IP networks?

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

- a
- b
- c
- d
- e

Yes, the answer is correct.

Score: 1

Accepted Answers:

- c

6)

**1 point**

Which of the following is **not** a valid port numbers in TCP/IP?

- a. 21
- b. 80
- c. 443
- d. 8080
- e. 80800

- a
- b
- c
- d
- e

Yes, the answer is correct.

Score: 1

Accepted Answers:

e

7)

**1 point**

Which of the following functionality does Address Resolution Protocol (ARP) perform?

- a. Map IP addresses to hardware (MAC) addresses.
- b. Map hardware addresses (MAC) to IP addresses.
- c. Performs error control and correction.
- d. Breaks the packet into smaller packets, if required.

a

b

c

d

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

8)

**1 point**

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

- a. IP provides connectionless, unreliable delivery systems for packets.
- b. UDP provides connectionless, unreliable delivery systems for packets
- c. TCP provides connectionless, unreliable delivery systems for packets.
- d. None of these.

a

b

c

d

Yes, the answer is correct.

Score: 1

Accepted Answers:

c

9)

If the IP header is 96 bits long, what will be the value (in decimal) of the "HLEN" field \_\_\_\_\_?

3

Yes, the answer is correct.

Score: 1

Accepted Answers:

(Type: Numeric) 3

**1 point**

10)

The maximum size of data that can be accommodated in an IP datagram is \_\_\_\_\_ bytes.

65535

Yes, the answer is correct.

Score: 1

Accepted Answers:

(Type: Range) 65500,65535

**1 point**

X



(<https://swayam.gov.in>)



([https://swayam.gov.in/nc\\_details/NPTEL](https://swayam.gov.in/nc_details/NPTEL))

codingoclock@gmail.com ▾

NPTEL (<https://swayam.gov.in/explorer?ncCode=NPTEL>) » Ethical Hacking (course)

≡

If already  
registered, click  
to check your  
payment status

## Week 02: Assignment 2

The due date for submitting this assignment has passed.

Due on 2023-08-09, 23:59 IST.

Course  
outline

How does an  
NPTEL  
online  
course  
work? ()

Week 0 ()

Week 1 ()

Week 2 ()

Lecture 06 : IP  
addressing  
and routing  
(Part I) (unit?  
unit=29&lesso  
n=30)

Lecture 07 : IP  
addressing  
and routing  
(Part II) (unit?  
unit=29&lesso  
n=31)

Assignment submitted on 2023-07-29, 13:05 IST

1)

1 point

Why there is a need for fragmentation of IP packets?

- a. Fragmentation is necessary because every network has a unique limit for the maximum size of datagrams that it can process.
- b. Fragmentation is necessary for faster data transfer.
- c. Fragmentation is necessary for error-recovery and flow control.
- d. All of these.

- a
- b
- c
- d

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

2)

1 point

○ Lecture 08 :  
TCP and UDP  
(Part I) (unit?  
unit=29&lesso  
n=32)

○ Lecture 09 :  
TCP and UDP  
(Part II) (unit?  
unit=29&lesso  
n=33)

○ Lecture 10 : IP  
subnetting  
(unit?  
unit=29&lesso  
n=34)

● Lecture  
Material of  
Week 2 (unit?  
unit=29&lesso  
n=35)

● Quiz: Week  
02:  
Assignment 2  
(assessment?  
name=169)

○ Week 2  
Feedback  
Form (unit?  
unit=29&lesso  
n=36)

○ Assignment 2  
Solution (unit?  
unit=29&lesso  
n=37)

Week 3 ()

Week 4 ()

Week 5 ()

Week 6 ()

Week 7 ()

Week 8 ()

Week 9 ()

Week 10 ()

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

- In transparent fragmentation the subsequent networks are aware that the fragmentation had occurred.
- In transparent fragmentation, it is required to route all packet to the same exit router in a network.
- In non-transparent fragmentation, each fragment is treated as an independent packet.
- In non-transparent fragmentation, an exit router reassembles all fragmented packets.

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

b

c

3)

**1 point**

An IP packet arrives at the final destination with the M flag set as 1. Which of the following statement is true about the packet?

- Prevents the fragmentation from taking place.
- The packet will be fragmented by the next router.
- The packet represents a fragment of a larger packet.
- None of these.

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

c

4)

**1 point**

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

- IP address is 32-bit quantity.
- IP address is typically expressed as dotted decimal notation where dots are used to separate each of the four octets of the address.
- IP address consists of three logical parts: network number, host number and port number.
- None of these.

[Week 11 \(\)](#)

[Week 12 \(\)](#)

[DOWNLOAD VIDEOS \(\)](#)

[Text Transcripts \(\)](#)

[Books \(\)](#)

- a
- b
- c
- d

Yes, the answer is correct.  
Score: 1

Accepted Answers:

c

5)

*1 point*

Which address classes do the IP addresses 144.16.75.12 and 10.10.85.120 belong to?

- a. Class C and Class A
- b. Class B and Class C
- c. Class B and Class A
- d. Class B and Class D

- a
- b
- c
- d

Yes, the answer is correct.  
Score: 1

Accepted Answers:

c

6)

*1 point*

Which of the following IP addresses represent broadcast address?

- a. 144.15.255.255
- b. 144.16.0.255
- c. 202.0.255.250
- d. 202.0.255.255

- a
- b
- c
- d

Yes, the answer is correct.  
Score: 1

Accepted Answers:

a

d

7)

The maximum number of hosts that are possible in a class C network is \_\_\_\_\_.

---

254

Yes, the answer is correct.

Score: 1

Accepted Answers:

(Type: Numeric) 254

**1 point**

8)

**1 point**

What is a TCP half-open connection in the context of connection establishment using 3-way handshake?

- a. The first transaction does not complete.
- b. The second transaction does not complete.
- c. The first transaction does not complete but the second transaction completes.
- d. The last transaction does not complete.
- e. None of these.

a  
 b  
 c  
 d  
 e

No, the answer is incorrect.

Score: 0

Accepted Answers:

d

9)

**1 point**

In the TCP header field, what do SYN=1 and ACK=0 represent?

- a. Connection request message.
- b. Connection confirmation message.
- c. Reject connection request.
- d. Reset connection request.

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

10)

**1 point**

What is the subnet address if the destination IP address is 144.16.75.105 and the subnet mask is 255.255.240.0?

- a. 144.16.32.0
- b. 144.16.75.0
- c. 144.16.16.0
- d. None of these

a

b

c

d

Yes, the answer is correct.

Score: 1

Accepted Answers:

*d*

X



(<https://swayam.gov.in>)



([https://swayam.gov.in/nc\\_details/NPTEL](https://swayam.gov.in/nc_details/NPTEL))

codingoclock@gmail.com ▾

NPTEL (<https://swayam.gov.in/explorer?ncCode=NPTEL>) » Ethical Hacking (course)

≡

If already  
registered, click  
to check your  
payment status

## Week 03: Assignment 03

The due date for submitting this assignment has passed.

Due on 2023-08-16, 23:59 IST.

Course  
outline

How does an  
NPTEL  
online  
course  
work? ()

Week 0 ()

Week 1 ()

Week 2 ()

Week 3 ()

Lecture 11 :  
Routing  
protocols (Part  
I) (unit?  
unit=38&lesso  
n=39)

Lecture 12 :  
Routing  
protocols (Part  
II) (unit?

Assignment submitted on 2023-08-06, 22:51 IST

1) 0 points

Consider the following statements:

- (i) In connection-oriented approach, network layer first makes a connection.  
(ii) IP protocol uses connection-oriented routing.

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

- a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 0

Accepted Answers:

a

2) 1 point

unit=38&lesson  
n=40)

○ Lecture 13 :  
Routing  
protocols (Part  
III) (unit?  
unit=38&lesson  
n=41)

○ Lecture 14 : IP  
version 6  
(unit?  
unit=38&lesson  
n=42)

○ Lecture 15 :  
Routing  
examples  
(unit?  
unit=38&lesson  
n=43)

● Lecture  
Material of  
Week 3 (unit?  
unit=38&lesson  
n=44)

● Quiz: Week  
03:  
Assignment  
03  
(assessment?  
name=170)

○ Week 3  
Feedback  
Form (unit?  
unit=38&lesson  
n=45)

○ Assignment 3  
Solution (unit?  
unit=38&lesson  
n=46)

**Week 4 ()**

**Week 5 ()**

**Week 6 ()**

**Week 7 ()**

**Week 8 ()**

Which of the following is/are **true** for default route?

- Default route is used when no specific address for next hop is available.
- In routing table default route is specified by an address 0.0.0.0.
- In routing table default route is specified by an address 255.255.255.255.
- In routing table default route is specified by an address 127.0.0.1.
- None of these.

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.

Score: 1

Accepted Answers:

a  
b

3)

**1 point**

Which of the following is/are **true** for static routing?

- In static routing routes are user defined.
- In static routing, routing table updates periodically depending on the network condition.
- Static routing is easy to configure.
- None of these.

a  
 b  
 c  
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

a

4)

**1 point**

**Week 9 ()**

**Week 10 ()**

**Week 11 ()**

**Week 12 ()**

**DOWNLOAD VIDEOS ()**

**Text Transcripts ()**

**Books ()**

Which of the following routing flags indicates that the router is up and running?

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

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

5)

**1 point**

Which of the following statement(s) is/are true for interior routing protocol?

- a. All the participating routers are present in the same autonomous system.
- b. The participating routers are present in different autonomous systems.
- c. Routers in different autonomous systems exchange messages to update their routing tables.
- d. Routers in the same autonomous system exchange messages to update their routing tables.

a  
 b  
 c  
 d

Partially Correct.

Score: 0.5

Accepted Answers:

a

d

6)

**1 point**

Which of the following statement(s) is/are **false** for Routing Information Protocol (RIP)?

- a. RIP is an example of interior routing protocol.
- b. RIP maintains timers to detect failed links.
- c. RIP converges faster for large networks.
- d. RIP consumes high bandwidth to update routes.
- e. None of these.

a  
 b  
 c  
 d  
 e

No, the answer is incorrect.

Score: 0

Accepted Answers:

c

7)

**1 point**

Which of the following is/are **false** for Border Gateway Protocol (BGP)?

- a. BGP allows routers belonging to different autonomous systems to exchange routing information.
- b. BGP uses TCP connection to send routing messages.
- c. BGP can also be used by routers within the same autonomous systems.
- d. BGP sends keepalive messages periodically to ensure that the connection between the BGP peers is alive.
- e. None of these.

a  
 b  
 c  
 d  
 e

No, the answer is incorrect.

Score: 0

Accepted Answers:

e

8)

**1 point**

If a packet is to be delivered to a specific host 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.

a  
 b  
 c  
 d

Yes, the answer is correct.  
Score: 1

Accepted Answers:  
a

9) **1 point**

Which of the following is **not true** for IPv6?

- a. It uses 32-bit IP addresses.
- b. IPv6 address does not have any defined classes.
- c. It uses 128-bit IP addresses.
- d. None of these.

a  
 b  
 c  
 d

Yes, the answer is correct.  
Score: 1

Accepted Answers:  
a

10) **1 point**

Consider the following routing table in a router. On which interface will an IP packet with destination address 161.44.64.120 be forwarded?

Destination	Subnet Mask	Interface
161.44.0.0	255.255.0.0	a
161.44.64.0	255.255.224.0	b
161.44.68.0	255.255.255.0	c
161.44.68.64	255.255.255.224	d
Default	0.0.0.0	e

- a. Interface a
- b. Interface b
- c. Interface c
- d. Interface d
- e. Interface e

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.  
Score: 1

Accepted Answers:  
*b*

X



(<https://swayam.gov.in>)



([https://swayam.gov.in/nc\\_details/NPTEL](https://swayam.gov.in/nc_details/NPTEL))

codingoclock@gmail.com ▾

NPTEL (<https://swayam.gov.in/explorer?ncCode=NPTEL>) » Ethical Hacking (course)

≡

If already  
registered, click  
to check your  
payment status

## Week 04: Assignment 04

The due date for submitting this assignment has passed.

Due on 2023-08-23, 23:59 IST.

Course  
outline

How does an  
NPTEL  
online  
course  
work? ()

Week 0 ()

Week 1 ()

Week 2 ()

Week 3 ()

Week 4 ()

Lecture 16 :  
Software  
Installation  
and Network  
Setup (unit?  
unit=47&lesso  
n=48)

Lecture 17 :  
Information

Assignment submitted on 2023-08-13, 23:27 IST

1)

1 point

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.

a

b

c

d

No, the answer is incorrect.

Score: 0

Accepted Answers:

a

c

2)

1 point

Gathering  
(Part 1) (unit?  
unit=47&lesso  
n=49)

Lecture 18 :  
Information  
Gathering  
(Part 2) (unit?  
unit=47&lesso  
n=50)

Lecture 19 :  
Port Scanning  
Using NMAP  
(unit?  
unit=47&lesso  
n=51)

Lecture 20 :  
Other  
Features of  
NMAP (unit?  
unit=47&lesso  
n=52)

Lecture  
Material of  
Week 4 (unit?  
unit=47&lesso  
n=53)

Quiz: Week  
04:  
Assignment  
04  
(assessment?  
name=172)

Feedback for  
Week 4 (unit?  
unit=47&lesso  
n=54)

Assignment 4  
Solution (unit?  
unit=47&lesso  
n=55)

Week 5 ()

Week 6 ()

Week 7 ()

Week 8 ()

Week 9 ()

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.

a  
 b  
 c  
 d

Partially Correct.  
Score: 0.5

Accepted Answers:

a  
d

3)

**1 point**

Which of the following can be used for active reconnaissance.

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

a  
 b  
 c  
 d  
 e  
 f

No, the answer is incorrect.  
Score: 0

Accepted Answers:

c  
d  
e

4)

**1 point**

**Week 10 ()**

**Week 11 ()**

**Week 12 ()**

**DOWNLOAD VIDEOS ()**

**Text Transcripts ()**

**Books ()**

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.

a  
 b  
 c  
 d  
 e  
 f

Yes, the answer is correct.

Score: 1

Accepted Answers:

f

5)

**1 point**

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

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

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

d

6)

**1 point**

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.

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

7)

**1 point**

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

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

8)

**1 point**

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

- a. -PE
- b. -PP
- c. -PM
- d. -PU

a

- b
- c
- d

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

9)

**1 point**

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

- a
- b
- c
- d

Yes, the answer is correct.

Score: 1

Accepted Answers:

d

10)

**1 point**

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.

- a
- b
- c
- d

Yes, the answer is correct.

Score: 1

Accepted Answers:

b

11)

**1 point**

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.

a  
 b  
 c  
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

a  
b

12) Can the use of firewall prevent port/host scanning? **1 point**

- a. True
- b. False

a  
 b

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

13)

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

1000

Yes, the answer is correct.

Score: 1

Accepted Answers:

(Type: Numeric) 1000

**1 point**

14)

**1 point**

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.

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.  
Score: 1

Accepted Answers:

d

15)

**1 point**

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

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.  
Score: 1

Accepted Answers:

c

X



(<https://swayam.gov.in>)



([https://swayam.gov.in/nc\\_details/NPTEL](https://swayam.gov.in/nc_details/NPTEL))

codingoclock@gmail.com ▾

NPTEL (<https://swayam.gov.in/explorer?ncCode=NPTEL>) » Ethical Hacking (course)

≡

If already  
registered, click  
to check your  
payment status

## Week 5: Assignment 5

The due date for submitting this assignment has passed.

Due on 2023-08-30, 23:59 IST.

Course  
outline

How does an  
NPTEL  
online  
course  
work? ()

Week 0 ()

Week 1 ()

Week 2 ()

Week 3 ()

Week 4 ()

Week 5 ()

Lecture 21 :  
Vulnerability  
Scanning  
using NMAP  
(unit?  
unit=56&lesso  
n=57)

Assignment submitted on 2023-08-22, 01:23 IST

1)

1 point

Which of the following tools can be used for scanning vulnerabilities?

- a. Hypervisor
- b. Nessus
- c. Hydra
- d. Nmap
- e. Crunch

- a
- b
- c
- d
- e

Yes, the answer is correct.

Score: 1

Accepted Answers:

- b
- d

<input type="checkbox"/> Lecture 22 : Security Scanning and Proxy Preparation (unit? unit=56&lesso n=58)	<p>2) NMAP scripts can be used for:</p> <ul style="list-style-type: none"> <li>a. Vulnerability scanning</li> <li>b. Backdoor detection.</li> <li>c. Port detection.</li> <li>d. Password attack.</li> <li>e. None of these.</li> </ul>	<b>1 point</b>
<input type="checkbox"/> Lecture 23 : System Hacking (unit? unit=56&lesso n=59)	<input checked="" type="checkbox"/> a <input checked="" type="checkbox"/> b <input checked="" type="checkbox"/> c <input type="checkbox"/> d <input type="checkbox"/> e	Partially Correct. Score: 0.75
<input type="checkbox"/> Lecture 24 : Malware, Trojans, Virus and Worms (unit? unit=56&lesso n=60)	Accepted Answers: a b c d	<b>1 point</b>
<input type="checkbox"/> Lecture 25 : Miscellaneous Attacks (unit? unit=56&lesso n=61)	a b c d	3)
<input checked="" type="checkbox"/> Week 5 Lecture Material (unit? unit=56&lesso n=62)	<p>Which of the following NMAP scripts is used to identify the OS of a target system?</p> <ul style="list-style-type: none"> <li>a. smb-os-brute</li> <li>b. smb-os-discovery</li> <li>c. http-os-check</li> <li>d. None of these.</li> </ul>	<b>1 point</b>
<input checked="" type="checkbox"/> Quiz: Week 5: <b>Assignment 5</b> (assessment? name=176)	<input type="radio"/> a <input type="radio"/> b <input type="radio"/> c <input checked="" type="radio"/> d	No, the answer is incorrect. Score: 0
<input type="checkbox"/> Feedback for Week 5 (unit? unit=56&lesso n=64)	Accepted Answers: b	<b>1 point</b>
<input type="checkbox"/> Assignment 5 Solution (unit? unit=56&lesso n=63)	4)	<b>1 point</b>
<b>Week 6 ()</b>		
<b>Week 7 ()</b>		
<b>Week 8 ()</b>		
<b>Week 9 ()</b>		

**Week 10 ()**

**Week 11 ()**

**Week 12 ()**

**DOWNLOAD VIDEOS ()**

**Text Transcripts ()**

**Books ()**

Which of the following scripts can be used to detect if a target system is vulnerable to DoS attack?

- a. http-methos
- b. http-brute
- c. http-dos-check
- d. http-slowloris-check
- e. ftp-anon

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.

Score: 1

Accepted Answers:

*d*

5)

**1 point**

Assume that we want to connect to a target system (10.0.0.1) through ssh service, the username and password are "user" and "pwd" respectively. Which of the following commands can be used to create a ssh connection?

- a. ssh 10.0.0.1 -p pwd
- b. ssh 10.0.0.1 -l pwd -p user
- c. ssh 10.0.0.1 user pwd
- d. None of these

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

*d*

6)

**1 point**

The necessary parameters required to generate word list using crunch tool is:

- a. Minimum length of the word list.
- b. Maximum length of the word list.
- c. File name where the word list will be stored.
- d. No parameters are required to generate a word list.

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

a  
b

7)

**1 point**

Which of the following tools can be used to perform password attack?

- a. Hydra
- b. Archive.org
- c. Netcraft
- d. Whois
- e. None of these.

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

8)

**1 point**

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

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

- a
- b
- c
- d
- e

Yes, the answer is correct.  
Score: 1

Accepted Answers:

a

9)

**1 point**

Which of the following approaches can be used to extract information about all users in a target system?

- a. Use of nmap script smb-enum-user
- b. Hydra tool
- c. Crunch tool
- d. Enum4linux

- a
- b
- c
- d

Partially Correct.  
Score: 0.5

Accepted Answers:

a

d

10)

**1 point**

In an attack using the remote administrative tool, which part of the tool needs to be placed in target system?

- a. Client
- b. Server

- a
- b

Yes, the answer is correct.  
Score: 1

Accepted Answers:

b

11)

**1 point**

To upload any file in the target system which is connected through FTP connection which of the following command can be used?

- a. put
- b. get
- c. upload
- d. download

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

12) Which of the following can self-replicate itself? **1 point**

- a. Trojan
- b. Virus
- c. Ransomware
- d. All of these

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

b

13) How a malware can get inside into a system? **1 point**

- a. Removable devices
- b. Attachments
- c. Fake Programs
- d. Untrusted sites and freeware software.

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

- a
- b
- c
- d

14)

**1 point**

The major loophole of ARP is that "a host can send unlimited number of ARP requests", and this can be used for ARP spoofing / ARP poisoning.

- a. True
- b. False

a  
 b

Yes, the answer is correct.

Score: 1

Accepted Answers:

- a

15)

**1 point**

Which of the following commands is used to see all arp entries in a system?

- a. arp -a
- b. arp -s
- c. arp -i
- d. arp -d

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

- a

X



(<https://swayam.gov.in>)



([https://swayam.gov.in/nc\\_details/NPTEL](https://swayam.gov.in/nc_details/NPTEL))

codingoclock@gmail.com ▾

NPTEL (<https://swayam.gov.in/explorer?ncCode=NPTEL>) » Ethical Hacking (course)

≡

If already  
registered, click  
to check your  
payment status

Course  
outline

How does an  
NPTEL  
online  
course  
work? ()

Week 0 ()

Week 1 ()

Week 2 ()

Week 3 ()

Week 4 ()

Week 5 ()

Week 6 ()

Lecture 26 :  
Basic  
concepts of  
cryptography  
(unit?)

## Week 06: Assignment 06

The due date for submitting this assignment has passed.

**Due on 2023-09-06, 23:59 IST.**

As per our records you have not submitted this assignment.

1)

*1 point*

Which of the following is not an example of active security attack?

- a. Masquerade
- b. Replay
- c. Traffic analysis
- d. Modification
- e. Denial of Service.

- a
- b
- c
- d
- e

No, the answer is incorrect.

Score: 0

Accepted Answers:

c

2)

*1 point*

unit=65&lesso  
n=66)

Lecture 27 :  
Private-key  
cryptography  
(Part I) (unit?  
unit=65&lesso  
n=67)

Lecture 28 :  
Private-key  
cryptography  
(Part II) (unit?  
unit=65&lesso  
n=68)

Lecture 29 :  
Public-key  
cryptography  
(Part I) (unit?  
unit=65&lesso  
n=69)

Lecture 30 :  
Public-key  
cryptography  
(Part II) (unit?  
unit=65&lesso  
n=70)

Lecture  
Material of  
Week 6 (unit?  
unit=65&lesso  
n=71)

Quiz: Week  
06:  
Assignment  
06  
(assessment?  
name=177)

Feedback for  
Week 6 (unit?  
unit=65&lesso  
n=72)

Assignment 6  
Solution (unit?  
unit=65&lesso  
n=73)

Week 7 ()

Week 8 ()

Consider the following statements:

- (i) In symmetric key cryptography, single shared key is used by sender and receiver.
- (ii) In Asymmetric key cryptography, separate keys are used by sender and receiver.

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

- a
- b
- c
- d

No, the answer is incorrect.

Score: 0

Accepted Answers:

c

3)

15 parties want to exchange messages securely using a symmetric key encryption algorithm.

The number of distinct key values required will be \_\_\_\_\_.

No, the answer is incorrect.

Score: 0

Accepted Answers:

(Type: Numeric) 105

1 point

4)

1 point

Consider a mono-alphabetic cipher with the following key value:

(A B C D I J K L E F G H M N O P U V W X Q R S T Y Z)

What will be the encrypted form of the message "W I N D O W" ?

- a. W E N D H W
- b. S K N G H S
- c. S E N D O S
- d. None of these.

- a
- b
- c
- d

[Week 9 \(\)](#)

[Week 10 \(\)](#)

[Week 11 \(\)](#)

[Week 12 \(\)](#)

[DOWNLOAD VIDEOS \(\)](#)

[Text Transcripts \(\)](#)

[Books \(\)](#)

No, the answer is incorrect.

Score: 0

Accepted Answers:

c

5) How many AES rounds are required for 192-bit key size? **1 point**

- a. 10
- b. 11
- c. 12
- d. 14

a

b

c

d

No, the answer is incorrect.

Score: 0

Accepted Answers:

c

6) What is the key length in data encryption standard (DES)? **1 point**

- a. 56
- b. 64
- c. 128
- d. 192

a

b

c

d

No, the answer is incorrect.

Score: 0

Accepted Answers:

a

7)

100 parties want to exchange messages securely using some public key encryption technique like RSA. The number of distinct key values required will be \_\_\_\_\_.

No, the answer is incorrect.

Score: 0

Accepted Answers:

(Type: Numeric) 200

**1 point**

8) In Digital signature sender signs a message with its: **1 point**

- a. Private key
- b. Public key

a  
 b

No, the answer is incorrect.

Score: 0

Accepted Answers:

a

9) **1 point**

On which difficult mathematical problem does the security of RSA algorithm depend on?

- a. Discrete logarithm problem.
- b. Testing whether a given number if prime or not.
- c. Prime factorization problem.
- d. The RSA threshold detection.
- e. All of these.

a  
 b  
 c  
 d  
 e

No, the answer is incorrect.

Score: 0

Accepted Answers:

c

10) **1 point**

Which of the following statement(s) is/are **true** for Diffie-Hellman Key Exchange algorithm?

- a. It allows group of users to agree on secret key over insecure channel.
- b. The security of the algorithm depends on prime factorization problem.
- c. The algorithm is vulnerable to man-in-the-middle attack.
- d. It does not require any prior communication between sender and receiver.
- e. All of these.

a  
 b  
 c

d

e

No, the answer is incorrect.

Score: 0

Accepted Answers:

a

c

d

X



(<https://swayam.gov.in>)



([https://swayam.gov.in/nc\\_details/NPTEL](https://swayam.gov.in/nc_details/NPTEL))

codingoclock@gmail.com ▾

NPTEL (<https://swayam.gov.in/explorer?ncCode=NPTEL>) » Ethical Hacking (course)

≡

If already  
registered, click  
to check your  
payment status

## Week 07: Assignment 07

The due date for submitting this assignment has passed.

Due on 2023-09-13, 23:59 IST.

Course  
outline

How does an  
NPTEL  
online  
course  
work? ()

Week 0 ()

Week 1 ()

Week 2 ()

Week 3 ()

Week 4 ()

Week 5 ()

Week 6 ()

Week 7 ()

Lecture 31 :  
Cryptographic  
hash functions

Assignment submitted on 2023-09-07, 21:42 IST

1)

1 point

Which of the following is/are true for Unkeyed hash function (Modification Detection Code)?

- a. Unkeyed hash function is used to preserve integrity of message.
- b. Unkeyed hash function is used to authenticate source of message.
- c. Unkeyed hash function produces an output that depends only on the input data.
- d. None of these.

a

b

c

d

Partially Correct.

Score: 0.5

Accepted Answers:

a

c

2)

1 point

(Part I) (unit?  
unit=74&lesson  
n=75)

○ Lecture 32 :  
Cryptographic  
hash functions  
(Part II) (unit?  
unit=74&lesson  
n=76)

○ Lecture 33 :  
Digital  
signature and  
certificate  
(unit?  
unit=74&lesson  
n=77)

○ Lecture 34 :  
Applications  
(Part I) (unit?  
unit=74&lesson  
n=78)

○ Lecture 35 :  
Applications  
(Part II) (unit?  
unit=74&lesson  
n=79)

● Lecture  
Material of  
Week 7 (unit?  
unit=74&lesson  
n=80)

● Quiz: Week  
07:  
Assignment  
07  
(assessment?  
name=178)

○ Feedback for  
Week 7 (unit?  
unit=74&lesson  
n=82)

○ Assignment 7  
Solution (unit?  
unit=74&lesson  
n=81)

Week 8 ()

Week 9 ()

Two messages M1 and M2 are fed to a hash function HASH to generate the hash values:

$$H1 = \text{HASH}(M1)$$

$$H2 = \text{HASH}(M2)$$

When do we say there is a collision?

- a.  $H1 = H2$ .
- b.  $M1 = M2$ .
- c.  $H1 = \text{HASH}(H2)$ .
- d. None of these.

a

b

c

d

Yes, the answer is correct.  
Score: 1

Accepted Answers:

a

3)

**1 point**

Which of the following corresponds to second preimage resistance in the context of hash  
functions?

- a. Except of few hash values H, it should be difficult to find a message M1 such that  
 $\text{HASH}(M1) = H$ .
- b. Given a message M1, it should be difficult to find another message M2 such that  
 $\text{HASH}(M1) = \text{HASH}(M2)$ .
- c. It should be difficult to find two messages M1 and M2 such that  $\text{HASH}(M1) =$   
 $\text{HASH}(M2)$ .
- d. None of these.

a

b

c

d

Yes, the answer is correct.  
Score: 1

Accepted Answers:

b

4)

**1 point**

[Week 10 \(\)](#)

[Week 11 \(\)](#)

[Week 12 \(\)](#)

[DOWNLOAD VIDEOS \(\)](#)

[Text Transcripts \(\)](#)

[Books \(\)](#)

What is the message digest length of MD5 and SHA-1 hash functions?

- a. 32-bit, 64-bit.
- b. 64-bit, 128-bit.
- c. 128-bit, 160-bit.
- d. 128-bit, 256-bit.
- e. None of these.

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.

Score: 1

Accepted Answers:

c

5) Which of the following is/are not hash functions?

*1 point*

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

a  
 b  
 c  
 d

Partially Correct.

Score: 0.5

Accepted Answers:

b

d

6)

*1 point*

Hash functions are faster than symmetric and public key encryption?

- a. True
- b. False

a  
 b

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

7)

**1 point**

Which of the following is/are **false** for digital signature?

- a. Digital signature is legally equivalent to hand-written signature.
- b. In digital signature, signer uses his public key to sign.
- c. Anybody having access to the signer's public key can verify the signature.
- d. None of these.

a

b

c

d

Yes, the answer is correct.

Score: 1

Accepted Answers:

b

8)

**1 point**

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

- a. Secure Socket Layer (SSL) provides security to the data transferred between web browser and server.
- b. SSL can be used for any network service running over TCP/IP.
- c. SSL Handshake Protocol provides mutual authentication.
- d. None of these.

a

b

c

d

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

b

c

9)

**1 point**

Which of the following statement(s) is/are **true** for SSL Alert Protocol?

- a. If the first byte is 1 then it indicates that this alert has no impact on the connection between sender and receiver.
- b. If the first byte is 1 then the SSL connection is terminated.
- c. If the first byte is 2 then it indicates that this alert has no impact on the connection between sender and receiver.
- d. If the first byte is 2 then the SSL connection is terminated.

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

a  
d

10)

**1 point**

Consider the following statements:

- (i) SSL is designed to establish secure connection between two hosts.
  - (ii) s-HTTP is designed to send individual messages securely.
- a. Only (i) is true
  - b. Only (ii) is true
  - c. Both (i) and (ii) are true
  - d. Both (i) and (ii) are false.

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

c

X



(<https://swayam.gov.in>)



([https://swayam.gov.in/nc\\_details/NPTEL](https://swayam.gov.in/nc_details/NPTEL))

codingoclock@gmail.com ▾

NPTEL (<https://swayam.gov.in/explorer?ncCode=NPTEL>) » Ethical Hacking (course)

≡

If already  
registered, click  
to check your  
payment status

Course  
outline

How does an  
NPTEL  
online  
course  
work? ()

Week 0 ()

Week 1 ()

Week 2 ()

Week 3 ()

Week 4 ()

Week 5 ()

Week 6 ()

Week 7 ()

Week 8 ()

## Week 08: Assignment 08

The due date for submitting this assignment has passed.

**Due on 2023-09-20, 23:59 IST.**

As per our records you have not submitted this assignment.

1)

*1 point*

Consider the following statements:

- (i) Steganography refers to a set of methods to hide some secret information in an audio/image/executable files.  
(ii) Steganography and digital watermarking share same operational and functional behaviors.

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

- a  
 b  
 c  
 d

No, the answer is incorrect.  
Score: 0

Accepted Answers:

c

2)

Lecture 36 :  
Steganography (unit?  
unit=83&lesson  
n=84)

Lecture 37 :  
Biometrics (unit?  
unit=83&lesson  
n=85)

Lecture 38 :  
Network Based Attacks (Part I) (unit?  
unit=83&lesson  
n=86)

Lecture 39 :  
Network Based Attacks (Part II) (unit?  
unit=83&lesson  
n=87)

Lecture 40 :  
DNS and Email Security (unit?  
unit=83&lesson  
n=88)

Lecture Material of Week 8 (unit?  
unit=83&lesson  
n=89)

Quiz: Week 08:  
Assignment 08  
(assessment?  
name=179)

Feedback for Week 8 (unit?  
unit=83&lesson  
n=90)

Assignment 8 Solution (unit?  
unit=83&lesson  
n=91)

**Week 9 ()**

Consider a gray-level image of size 2000 x 2000, where each pixel is stored in 24-bits (containing red, green, and blue components as 8-bit each. How many bytes of information can be hidden in the image by using LSB steganography technique? (*Assume that only the least significant bit in each 8-bit color component is modified.*)

No, the answer is incorrect.  
Score: 0

Accepted Answers:  
(Type: Numeric) 1500000

**1 point**

3)

**1 point**

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

- a. Biometrics refers to an automated method for hiding information in a media like audio, video, image etc.
- b. Biometrics refers to embedding copyright, ownership, license and similar information in a medium such as audio, video, image etc.
- c. Biometrics refers to an automated method for recognizing individuals based on measurable biological and behavioral characteristics.
- d. None of these.

- a  
 b  
 c  
 d

No, the answer is incorrect.  
Score: 0

Accepted Answers:

c

4)

**1 point**

Which of the following is/are example(s) of behaviour biometric?

- a. Retina scan
- b. Fingerprint recognition
- c. Facial recognition
- d. None of these

- a  
 b  
 c  
 d

No, the answer is incorrect.

**Week 10 ()**

**Week 11 ()**

**Week 12 ()**

**DOWNLOAD VIDEOS ()**

**Text Transcripts ()**

**Books ()**

Score: 0

Accepted Answers:

*d*

5)

**1 point**

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

- a. For authentication application, a user template is compared against all possible templates stored in the database.
- b. For verification application, a user template is compared against a specific single template stored in the database.
- c. Biometric systems can provide 100% accuracy in security applications.
- d. None of these.

a  
 b  
 c  
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

*d*

6)

**1 point**

Which of the following attacks rely on the accumulation of TCP half-open connections on the server?

- a. Ping of death attack.
- b. SYN flooding attack.
- c. Smurf attack.
- d. None of these.

a  
 b  
 c  
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

*b*

7)

**1 point**

In which of the following denial-of-service attacks, the attacker attempts to crash/freeze target computer/service by sending oversized packet in simple ping command?

- a. SYN flooding attack.
- b. Smurf attack.
- c. Ping-of-death.
- d. None of these.

a  
 b  
 c  
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

c

8)

**1 point**

Which of the following statement(s) is/are true for HTTP Flood attack?

- a. It is a type of Distributed-Denial-of-Service (DDoS) attack.
- b. It overwhelms a target server by accumulating large number of TCP half-open connections.
- c. It overwhelms a target server using oversized ping packets.
- d. It overwhelms a target server with HTTP request.
- e. None of these.

a  
 b  
 c  
 d  
 e

No, the answer is incorrect.

Score: 0

Accepted Answers:

a

d

9)

**1 point**

Which of the following approach can be used to mitigate HTTP flood attack?

- a. Use captcha test.
- b. Use JavaScript computational challenge.
- c. Use web application firewall.
- d. Block ping requests.
- e. Block TCP connections.
- f. None of these.

a  
 b  
 c  
 d  
 e  
 f

No, the answer is incorrect.

Score: 0

Accepted Answers:

a  
b  
c

10)

**1 point**

Which of the following is true for recursive 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 recursively within the host itself.
- d. All of these.

a  
 b  
 c  
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

b

X



(<https://swayam.gov.in>)



([https://swayam.gov.in/nc\\_details/NPTEL](https://swayam.gov.in/nc_details/NPTEL))

codingoclock@gmail.com ▾

NPTEL (<https://swayam.gov.in/explorer?ncCode=NPTEL>) » Ethical Hacking (course)

≡

If already  
registered, click  
to check your  
payment status

## Week 09: Assignment 09

The due date for submitting this assignment has passed.

Due on 2023-09-27, 23:59 IST.

Course  
outline

How does an  
NPTEL  
online  
course  
work? ()

Week 0 ()

Week 1 ()

Week 2 ()

Week 3 ()

Week 4 ()

Week 5 ()

Week 6 ()

Week 7 ()

Week 8 ()

Assignment submitted on 2023-09-17, 22:26 IST

1)

1 point

In promiscuous mode, a network device, such as an adapter on a host system, can intercept and read all traffic on the network segment to which the adapter is connected.

- a. True
- b. False

a

b

Yes, the answer is correct.  
Score: 1

Accepted Answers:

a

2)

1 point

**Week 9 ()**

○ Lecture 41 :  
Packet Sniffing  
(Part 1) (unit?  
unit=92&lesso  
n=93)

○ Lecture 42 :  
Packet Sniffing  
(Part 2) (unit?  
unit=92&lesso  
n=94)

○ Lecture 43 :  
Packet Sniffing  
(Part 3) (unit?  
unit=92&lesso  
n=95)

○ Lecture 44 :  
Social  
Engineering  
Attack (unit?  
unit=92&lesso  
n=96)

○ Lecture 45 :  
Denial of  
Service Attack  
(unit?  
unit=92&lesso  
n=97)

○ Week 9  
Lecture  
Material (unit?  
unit=92&lesso  
n=99)

● Quiz: Week  
09:  
Assignment  
09  
(assessment?  
name=180)

○ Feedback for  
Week 9 (unit?  
unit=92&lesso  
n=100)

○ Assignment 9  
Solution (unit?  
unit=92&lesso  
n=101)

**Week 10 ()**

Which of the following commands can be used to put the NIC of a machine to promiscuous mode? (Assumption: Machine IP - 192.168.43.48, IP of default gateway - 192.168.43.141, the machine is connected with eth0 interface).

- a. arpspoof 192.168.43.48
- b. arpspoof 192.168.43.141
- c. arpspoof -i eth0 192.168.43.48
- d. arpspoof -i eth0 192.168.43.141

a  
 b  
 c  
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

d

3)

**1 point**

In Wireshark, to filter all the packets used by an IP address 23.36.4.106, which of the following filter option/command can be used?

- a. 23.36.4.106
- b. ip == 23.36.4.106
- c. ip.addr == 23.36.4.106
- d. ip.address = 23.36.4.106
- e. None of these.

a  
 b  
 c  
 d  
 e

No, the answer is incorrect.

Score: 0

Accepted Answers:

c

4)

**1 point**

[Week 11 \(\)](#)

[Week 12 \(\)](#)

[DOWNLOAD VIDEOS \(\)](#)

[Text Transcripts \(\)](#)

[Books \(\)](#)

A simple packet analyzer tool such as Wireshark can capture login credential of a user if the login page is using the following Protocol:

- a. HTTP
- b. SSH
- c. HTTPS
- d. SSL
- e. None of these.

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

5)

**1 point**

How to detect whether network sniffing is probably going on in a network?

- a. By checking the ARP entry.
- b. By conducting TCP stealth scan on all the machines in the network.
- c. By using a script that checks whether any of the machines has the network card configured in the promiscuous mode.
- d. None of these.

a  
 b  
 c  
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

a

c

6)

**0 points**

What is the purpose of scanner 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. It is used for automotive crawling web applications.
- e. None of these.

a  
 b  
 c  
 d  
 e

No, the answer is incorrect.

Score: 0

Accepted Answers:

e

7)

**1 point**

In Burp suite which of the following module is used to intercept, inspect and modify raw traffic?

- a. Spider
- b. Scanner
- c. Intruder
- d. Proxy
- e. None of these.

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.

Score: 1

Accepted Answers:

d

8)

**1 point**

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

- a. Impersonation
- b. Tailgating
- c. Shoulder surfing
- d. Chain letters
- e. phishing

a  
 b  
 c  
 d  
 e

No, the answer is incorrect.

Score: 0

Accepted Answers:

d  
e

9)

**1 point**

How does Slowloris attack work?

- a. It sends a single large ping packet to victim system.
- b. It sends multiple HTTP requests to the victim system but never completes the request.
- c. It sends large number ARP packet to the victim system.
- d. None of these.

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

b

10)

**1 point**

Which of the following tools can be used to mount DoS attack?

- a. LOIC tool.
- b. Hping3.
- c. Hydra.
- d. Crunch.
- e. None of these.

a

b

c

d

e

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

b

X



(<https://swayam.gov.in>)



([https://swayam.gov.in/nc\\_details/NPTEL](https://swayam.gov.in/nc_details/NPTEL))

codingoclock@gmail.com ▾

NPTEL (<https://swayam.gov.in/explorer?ncCode=NPTEL>) » Ethical Hacking (course)

≡

If already  
registered, click  
to check your  
payment status

## Week 10: Assignment 10

The due date for submitting this assignment has passed.

Due on 2023-10-04, 23:59 IST.

Course  
outline

How does an  
NPTEL  
online  
course  
work? ()

Week 0 ()

Week 1 ()

Week 2 ()

Week 3 ()

Week 4 ()

Week 5 ()

Week 6 ()

Week 7 ()

Week 8 ()

Assignment submitted on 2023-09-27, 20:18 IST

1)

1 point

Which of the following are examples of hardware-based attacks?

- a. Side-channel attack.
- b. Physical probing.
- c. Denial of service stack.
- d. SQL injection attack

a

b

c

d

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

b

2)

1 point

**Week 9 ()****Week 10 ()**

○ Lecture 46 :  
Elements of  
Hardware  
Security (unit?  
unit=102&less  
on=103)

○ Lecture 47 :  
Side Channel  
Attacks (Part I)  
(unit?  
unit=102&less  
on=104)

○ Lecture 48 :  
Side Channel  
Attacks (Part  
II) (unit?  
unit=102&less  
on=105)

○ Lecture 49 :  
Physical  
Unclonable  
Function (unit?  
unit=102&less  
on=106)

○ Lecture 50 :  
Hardware  
Trojan (unit?  
unit=102&less  
on=107)

○ Lecture  
Material of  
Week 10  
(unit?  
unit=102&less  
on=108)

● Quiz: Week  
10:  
Assignment  
10  
(assessment?  
name=181)

○ Feedback for  
Week 10  
(unit?  
unit=102&less  
on=109)

For modular exponentiation computation of  $x^{25}$ , how many squaring and multiplication operations would be required?

- a. 4 and 4.
- b. 4 and 2.
- c. 3 and 4.
- d. 5 and 2.
- e. 5 and 3.

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.  
Score: 1

Accepted Answers:

b

3)

**1 point**

Which of the following is/are true for side-channel attacks?

- a. They exploit weakness in cryptographic algorithm.
- b. They exploit weakness in algorithm implementation.
- c. They do not require physical access to the device.
- d. It is used to encrypted ciphertexts for a number of given plaintext messages.

a  
 b  
 c  
 d

Yes, the answer is correct.  
Score: 1

Accepted Answers:

b

4)

**1 point**

○ Assignment 10  
Solution (unit?  
unit=102&less  
on=110)

**Week 11 ()**

**Week 12 ()**

**DOWNLOAD  
VIDEOS ()**

**Text  
Transcripts  
()**

**Books ()**

Which of the following is/are true for simple power analysis?

- a. In this analysis attacker directly uses power consumption to learn bits of secret key.
- b. Using this analysis we can identify features like rounds of DES/AES, multiply in RSA exponentiation.
- c. In this analysis the waveform is partitioned into two sets according to selected bits.
- d. It relies on the use of a hardware Trojan in the circuit.
- e. None of these.

a

b

c

d

e

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

b

5) 1 point

Which of the following strategies can be used to prevent timing analysis attack?

- a. Make the computation independent of the input.
- b. Package the chip in a temper proof casing.
- c. Use highly secured cryptographic algorithm.
- d. None of these.

a

b

c

d

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

6) 1 point

Which of the following is **not** a desirable property of PUF?

- a. Given a PUF, it is hard to construct a procedure PUF', where PUF  $\neq$  PUF', and  $\text{PUF}'(x) = \text{PUF}(x)$  for all x.
- b. Given only y and corresponding PUF instance, it is hard to find x such that  $\text{PUF}(x) = y$ .
- c. Given PUF and x, it should be easy to evaluate  $y = \text{PUF}(x)$
- d. None of these.

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

*d*

7) PUF can be used for:

**1 point**

- a. Security Primitive
- b. Identification
- c. Private/Public key pair generation.
- d. None of these.

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

*a*

*b*

*c*

8)

Number of possible paths in 8-bit arbiter PUF will be \_\_\_\_\_.

256

Yes, the answer is correct.

Score: 1

Accepted Answers:

(Type: Numeric) 256

**1 point**

9) Consider the following statements: **1 point**

- (i) Hardware Trojans are small modifications in the circuit.
- (ii) It is used to reduce power consumption of a circuit.

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

a  
 b  
 c  
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

a

10) **1 point**

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

- a. It performs tasks for which it are designed or programmed.
- b. It can replicate itself.
- c. It does nothing harmful to the user's computer system.
- d. None of these.

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

X



(<https://swayam.gov.in>)



([https://swayam.gov.in/nc\\_details/NPTEL](https://swayam.gov.in/nc_details/NPTEL))

codingoclock@gmail.com ▾

NPTEL (<https://swayam.gov.in/explorer?ncCode=NPTEL>) » Ethical Hacking (course)

≡

If already  
registered, click  
to check your  
payment status

## Week 11: Assignment 11

The due date for submitting this assignment has passed.

Due on 2023-10-11, 23:59 IST.

Course  
outline

How does an  
NPTEL  
online  
course  
work? ()

Week 0 ()

Week 1 ()

Week 2 ()

Week 3 ()

Week 4 ()

Week 5 ()

Week 6 ()

Week 7 ()

Week 8 ()

Assignment submitted on 2023-10-01, 16:57 IST

1)

1 point

Which of the following is used to take advantage of system/application bugs?

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

- a
- b
- c
- d
- e

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

2)

1 point

**Week 9 ()****Week 10 ()****Week 11 ()**

○ Lecture 51 :  
Web  
Application  
Vulnerability  
Scanning  
(unit?  
unit=111&less  
on=112)

○ Lecture 52 :  
Part 1 : SQL  
Injection  
Authentication  
Bypass (unit?  
unit=111&less  
on=113)

○ Lecture 52 :  
Part 2: SQL  
Injection Error  
Based (unit?  
unit=111&less  
on=114)

○ Lecture 52 :  
Part 3 : SQL  
Injection Error  
Based from  
Web  
Application  
(unit?  
unit=111&less  
on=115)

○ Lecture 53 :  
SQLMAP  
(unit?  
unit=111&less  
on=116)

○ Lecture 54 :  
Cross Site  
Scripting (unit?  
unit=111&less  
on=117)

○ Lecture 55 :  
File Upload  
Vulnerability  
(unit?

Which of the following statement is **true** for meterpreter payload?

- a. Meterpreter payload is used to perform brute force attack.
- b. Meterpreter payload provides an interactive shell to the attacker from which attacker can explore the target machine and can execute codes.
- c. Meterpreter payload is used to launch Metasploit framework.
- d. Meterpreter payload is used to bypass the anti-virus installed in target system.
- e. None of these.

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.

Score: 1

Accepted Answers:

b

3)

**1 point**

Which of the following module is used to create new payloads.

- a. Msfconsole
- b. Encoders
- c. Exploit
- d. None of these

a  
 b  
 c  
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

d

4)

**1 point**

In Metasploit, to check various parameters that need to be set for an exploit, which of the following commands is used?

- a. Show parameters
- b. Show options
- c. Set parameters
- d. Set options
- e. None of these

a  
 b  
 c

unit=111&less  
on=118)

- d  
 e

Yes, the answer is correct.

Score: 1

Accepted Answers:

b

5)

**1 point**

To create a payload (backdoor), which of the following is required?

- a. Name of the payload
- b. IP of the target system
- c. IP of an attacker system
- d. Port of target system
- e. Port of an attacker system.

- a  
 b  
 c  
 d  
 e

No, the answer is incorrect.

Score: 0

Accepted Answers:

a  
c  
e

6)

**1 point**

Which of the following tools/approach can be used to extract existing and hidden pages of a webserver?

- a. Dirb
- b. NMAP scan using "http-enum" script
- c. Hydra
- d. Crunch

- a  
 b  
 c  
 d

Partially Correct.

Score: 0.5

Accepted Answers:

a  
b

7)

**1 point**

Consider the table “USERS” consist of 3 column u\_id, u\_name and pass as given below:

u_id	u_name	Pass
1	NPTEL	nptel1234
2	IIT_KGP	kgp1234
3	Eth_Hack	eth4321

Which of the following SQL queries are malicious with respect to the above table?

- a. SELECT \* from USERS;
- b. SELECT \* from USERS where u\_id = "5"
- c. SELECT \* from USERS where u\_name = "any"
- d. SELECT \* from USERS where u\_name = "any" or 1=1

a  
 b  
 c  
 d

Yes, the answer is correct.

Score: 1

Accepted Answers:

*d*

8)

**1 point**

Which of the following statement(s) is/are true for sql injection attack?

- a. If a webpage is vulnerable to blind sql injection then it will print error message for an incorrect user input.
- b. If a webpage is vulnerable to blind sql injection then it will not print anything for an incorrect user input.
- c. If a webpage is vulnerable to error-based sql injection then it will print error message for an incorrect user input.
- d. If a webpage is vulnerable to error-based sql injection then it will not print anything for an incorrect user input.

a  
 b  
 c  
 d

No, the answer is incorrect.

Score: 0

Accepted Answers:

*b*  
*c*

9)

**1 point**

Which of the following tools is used to automate sql injection attacks?

- a. Hydra
- b. Metasploit
- c. SQL MAP
- d. NMAP

a  
 b  
 c  
 d

Yes, the answer is correct.  
Score: 1

Accepted Answers:

c

10)

*1 point*

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

- a. It affects all users of that web application.
- b. It affects only a single client of the web application.
- c. It is stored in the database of web application.
- d. None of these.

a  
 b  
 c  
 d

No, the answer is incorrect.  
Score: 0

Accepted Answers:

b

X



(<https://swayam.gov.in>)



([https://swayam.gov.in/nc\\_details/NPTEL](https://swayam.gov.in/nc_details/NPTEL))

codingoclock@gmail.com ▾

NPTEL (<https://swayam.gov.in/explorer?ncCode=NPTEL>) » Ethical Hacking (course)

≡

If already  
registered, click  
to check your  
payment status

## Week 12: Assignment 12

The due date for submitting this assignment has passed.

Due on 2023-10-18, 23:59 IST.

Course  
outline

How does an  
NPTEL  
online  
course  
work? ()

Week 0 ()

Week 1 ()

Week 2 ()

Week 3 ()

Week 4 ()

Week 5 ()

Week 6 ()

Week 7 ()

Week 8 ()

Assignment submitted on 2023-10-08, 17:54 IST

1)

1 point

Which of the following options can be used for host discovery using NMAP?

- a. -PE
- b. -PC
- c. -PM
- d. -PP

- a
- b
- c
- d

No, the answer is incorrect.

Score: 0

Accepted Answers:

- a
- c
- d

2)

1 point

**Week 9 ()**

Which of the following packets will be received in response form a target if an attacker sends out an ICMP ECHO request (Type 8) packet (Assume that the target is live).

- a. ICMP Echo Request (Type 8)
- b. ICMP Echo Reply (Type 0)
- c. ICMP Timestamp reply (Type 14)
- d. ICMP Address mask reply (Type 18)

a

b

c

d

Yes, the answer is correct.

Score: 1

Accepted Answers:

b

3)

**0 points**

In TCP sweep scan, a scanner sends a "S" packet (Synchronization) and receives a "RA" packet (Reset) from target. What does it indicates?

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

a

b

No, the answer is incorrect.

Score: 0

Accepted Answers:

b

4)

**1 point**

To see why NMAP is reporting any port as open or close (or a host as up or down) which of the following options is used?

- a. --disable-arp-ping
- b. --packet-trace
- c. --show-reason
- d. --reason

a

b

c

d

No, the answer is incorrect.

Score: 0

Accepted Answers:

d

5)

**1 point**

**Week 10 ()**

**Week 11 ()**

**Week 12 ()**

Lecture 56 :  
The NMAP  
Tool: A Relook  
(Part I) (unit?  
unit=122&less  
on=123)

Lecture 57 :  
The NMAP  
Tool: A Relook  
(Part II) (unit?  
unit=122&less  
on=124)

Lecture 58 :  
The NMAP  
Tool: A Relook  
(Part III) (unit?  
unit=122&less  
on=125)

Lecture 59 :  
Network  
Analysis using  
Wireshark  
(unit?  
unit=122&less  
on=126)

Lecture 60 :  
Summarization  
of the Course  
(unit?  
unit=122&less  
on=127)

Lecture  
Material of  
Week 12  
(unit?  
unit=122&less  
on=128)

**Quiz: Week  
12:  
Assignment  
12  
(assessment?  
name=183)**

Feedback for Week 12  
(unit?  
unit=122&less  
on=129)

Assignment 12 Solution (unit?  
unit=122&less  
on=130)

**DOWNLOAD VIDEOS ()**

**Text Transcripts ()**

**Books ()**

Which of the following scanning options uses all type of sweep operations (except UDP sweep)?

- a. -sn
- b. -PE
- c. -PP
- d. None of these

a  
 b  
 c  
 d

No, the answer is incorrect.  
Score: 0

Accepted Answers:

a

6)

**1 point**

Which of the following NMAP scans completes 3-way handshake?

- a. ICMP Echo Sweep Scan
- b. ICMP Non-Echo Sweep Scan
- c. TCP Connect Scan
- d. TCP Stealth Scan

a  
 b  
 c  
 d

Yes, the answer is correct.  
Score: 1

Accepted Answers:

c

7)

In NMAP, \_\_\_\_\_ number of ports are scanned when we use -F option.

100

Yes, the answer is correct.  
Score: 1

Accepted Answers:

(Type: Numeric) 100

**1 point**

8)

**1 point**

Which of the following NMAP option is used for OS detection?

- a. -sL
- b. -sP
- c. -PO
- d. -sU
- e. None of these.

a  
 b  
 c  
 d  
 e

Yes, the answer is correct.

Score: 1

Accepted Answers:

e

9)

*1 point*

Which of the following protocols are vulnerable to sniffing attack?

- a. HTTP
- b. HTTPS
- c. SSL
- d. SSH
- e. FTP

a  
 b  
 c  
 d  
 e

No, the answer is incorrect.

Score: 0

Accepted Answers:

a

e

10)

*1 point*

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

- a. While running network analyzer tool such as sniffer, it is necessary to enable promiscuous mode.
- b. In promiscuous mode the sniffer can read all traffic on the network segment to which the NIC is connected.
- c. We do not require root privilege to set the NIC to promiscuous mode.
- d. All of these.

a

b

c

d

Yes, the answer is correct.

Score: 1

Accepted Answers:

a

b

