NPTEL » Ethical Hacking

Final Revision On Ethical Hacking (July-Dec)-2023 Batch

Frequently Asked Questions Regarding NPTEL Ethical Hacking Each Year.

Q.1 Which of the following model the tester has partial information about the network?

a. Black box model

b. White box model

c. Gray box model

d. None of these.

Ans: C

Solutions: 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.

2. Which address classes do the IP addresses 118.16.75.12 and 191.10.85.120 belong to?

a. Class A and Class B

b. Class B and Class B

c. Class C and Class A

d. Class B and Class A

Ans: a

Solution:

Class Address Range Application

IP Class A:- 0 to 127 Used for large number of hosts.

IP Class B: - 128 to 191 Used for medium size network.

IP Class C: - 192 to 223 Used for local area network.

IP Class D: - 224 to 239 Reserve for multi-tasking.

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

Ans- 65535 bytes

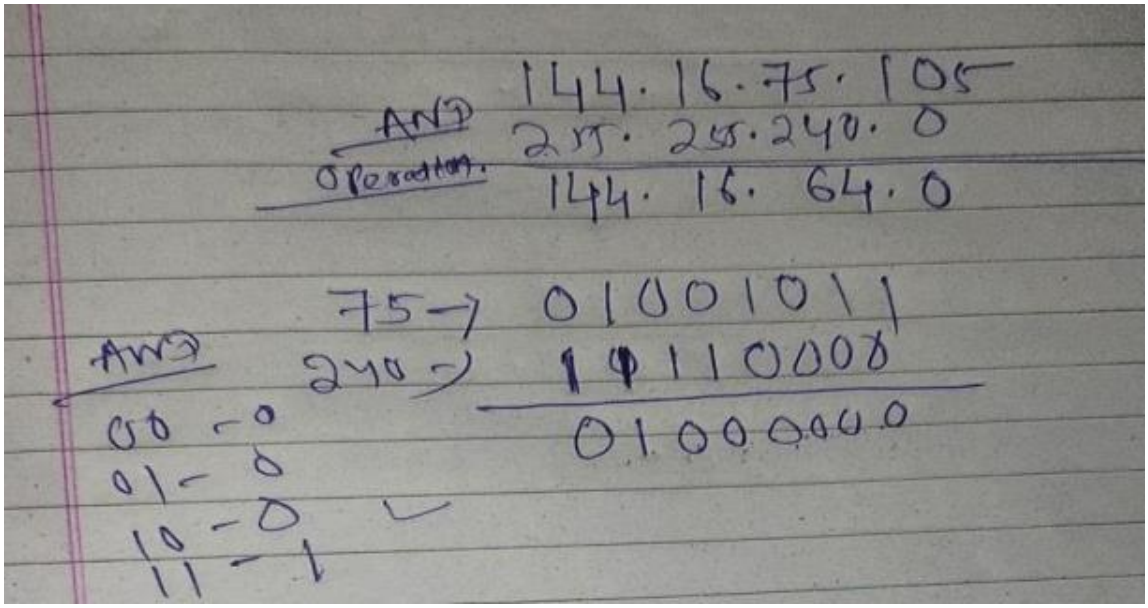
Solution- The TOTAL-LENGTH field in the IP header is 16 bits, which can contain values from 0 to $2^{16} – 1 = 65536-1$, the total size of an IP packet can be 65535 bytes.

Also, the minimum size of the IP header is 20 bytes, which makes the maximum size of data as

65535 – 20 = 65515 bytes.

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

Solution: Doing AND operation with destination IP address and the subnet mask. **(Ans: -144.16.64.0)**



5. The maximum number of hosts that are possible in a class B network is _____ .

Ans: - For a class B network, 16 bits are provided to specify the host.

Host bits: 16

Number of hosts = $2^{16} - 2 = 65,534$

Address	Network id	Host id
Class A	Network:7 bits = Number of networks = 2^7 – 1 = 127	Host: 24 bits = Number of hosts = 2^24 – 2 = 16,777,214
Class B	Network bits:14 bits = Number of networks = 2^14 – 1 = 16,383	Host bits: 16 = Number of hosts = 2^16 – 2 = 65,534
Class C	Network bits: 21 = Number of networks = 2^21 – 1 = 2,097,151	Host bits: 8 =Number of hosts = 2^8 – 2 = 254

6. Which of the following host address represents the default route in a routing table?

a. 0.0.0.0

b. 0.0.0.1

c. 127.0.0.1

d. 255.255.255.255

Ans: a

Solution- Default Route is used when no specific address for next hop is available. In Routing table default Route is specified an address 0.0.0.0

- **0.0. 0.1** is a private IP address, and is only used in internal network environments. Any abusive activity you see coming from an internal IP is either coming from within your network itself, or is the result of an error or misconfiguration.
- The IP address **127.0. 0.1** is a special-purpose IPv4 address and is called the localhost or loopback address. All computers use this address as their own.
- 255.255. 255.255 – Represents the broadcast address, or place to route messages to be sent to every device within a network.

7. In which routing protocol all the participating routers presents in the same autonomous systems?

a. Exterior routing protocol
b. Interior routing protocol
c. Default routing protocol
d. None of these
Ans- b
Solution- Routers in the same autonomous system exchange messages to update their routing tables.

8. 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

Solution:

PAGE NO.
Date : / /20

(10) 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

Soln

→ To find the interface, we need to do AND of incoming IP addresses and subnet mask.

→ compare the result of AND with the destination.

→ Note that if there is a match between multiple destinations, then we need to select the destination with longest length subnet mask of number of 1's is highest.

(i) IP address is

161.44.64.120

AND operation Truth table

AND 255.255.0.0

161.44.0.0 (matched with the destination)

0 - 0	
1 - 0	(ii)
0 - 0	
1 - 1	

No. of 1's is 16

AND 161.44.64.120 | 64 → 0100000

255.255.224.0 | 224 → 1110000

161.44.64.0 | 0100000

(matched with the destination)

No. of 1's is 19

(iii) 161.44.64.120
AND 255.255.255.0
161.44.64.0

64 → 01000000
255 → 11111111
01000000

(Destination is not matched)

(iv) 161.44.64.120
AND 255.255.255.224
161.44.64.

(Destination is not matched)

Q.9 Hydra What kind of attack may be executed with this tool?

a. Dictionary Attack (Crunch tool used)

b. Password Attack (Hydra tool)

c. XSS (Cross-Site Scripting) (Burp suite tools used)

d. Denial-of-Service (DoS) (Slow Loris tools)

Ans- b

Solution- Hydra is a pre-installed tool in Kali Linux used to brute-force usernames and passwords to different services such as FTP, ssh, telnet, MS SQL, etc. Brute force can be used to try different usernames and passwords against a target to identify the correct credentials.

Q.10 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.

Q.11. 25 parties want to exchange messages securely using a symmetric key algorithm. The number of distinct key values required will be _____?

Ans: -

Solution: - 25 parties want to exchange messages securely using a symmetric key (Private key) = So, the number of distinct key values required will be (M value) (let say m)

$$= \frac{n(n-1)}{2}$$

$$= \frac{25(25-1)}{2}$$

$$= \frac{25*24}{2}$$

$$= 300$$

Q.12 For encryption using public-key cryptography, we use the

a. Receiver's public key

b. Receivers' private key

c. Sender's public key

d. Sender's private key

Ans. A

Solution: - Anyone can encrypt a message by using your public key, but only you can read it. When you receive the message, you decrypt it by using your private key.

Q.13 Consider a colour image of size 1000 x 1000, where each pixel is stored in 24-bits (containing red, green and blue components as 8-bits each). How many bytes of information can be hidden in the image by using single-LSB steganography technique?

Ans: - Each pixel consists of 24 bits or 3 bytes, and hence 3 bits 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 3 bits = 1000 x 1000 x 3 / 8 = 375000 bytes.

Q.14 Which of the following protocols is/are vulnerable to sniffing attack?

a. HTTP

b. Telnet

c. SSH

d. SSL

Correct Answer: a,b

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.

Q.15 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

Ans: - b

Explanation: -

$$X^{25}$$

Step (i) = 1st convert it into binary form of 25 = 11001

Step (ii) = X^{11001}

$= X^{16} * X^{8} * X^{1}$

$= (X^{4})^{4} * (X^{2})^{4} * X$

$= (X^{4} * X^{2})^{4} * X$

$= \{\{(X^{2})^{2} * X^{2}\}^{2}\}^{2} * X$

$= \{(X^{2} * X)^{2})^{2}\}^{2} * X$

So, here we found that 4 squaring and 2 multiplications