Roll No											

PRESIDENCY UNIVERSITY
BENGALURU

SCHOOL OF COMPUTER SCIENCE & ENGINEERING AND INFORMATION SCIENCE

END TERM EXAMINATION - JUNE 2024

Semester: Semester VI - B.Tech CSE - 2021	**Date:** June 14, 2024
Course Code: CSE2039	**Time:** 1.00 PM – 4.00 PM
Course Name: Ethical Hacking	**Max Marks:** 100
Program: B.Tech. Computer Science and Engineering	**Weightage:** 50%

Instructions:

(i) Read all questions carefully and answer accordingly.
(ii) Scientific and non-programmable calculator is permitted.

ANSWER ANY FIVE FULL QUESTIONS **(5X20=100M)**

1.

A). What do you mean by Cyber threat? What are the major differences between threat and attack?
(CO1) (4 Marks) [Knowledge]

B). Differentiate between vulnerability assessment and penetration testing. Explain with a real-time networking scenario. (CO1) (6 Marks) [Comprehension]

C). Assume you are performing penetration testing on a Wi-Fi Router. What are the major types involved in it? Explain different scenarios involved in this process
(CO1) (10 Marks) [Application]

OR

2.

A). Define Encryption and Decryption (CO1) (4 Marks) [Knowledge]

B). Name the Windows commands used to perform the following task
(1) Find the round trip time, (2). List all devices connected to your network (3). DNS details
(CO1) (6 Marks) [Comprehension]

C). The open systems interconnection (OSI) model is a conceptual model created by the International Organization for Standardization that enables diverse communication systems to communicate using standard protocols. Explain the roles and responsibilities of each layer in detail
(CO1) (10 Marks) [Application]

3.

A). Abbreviate NIST and OSSTMM. (CO2) (4 Marks) [Knowledge]

B). Which Linux commands are used to perform the following task
(1). Remote login (2). See the help file in Linux (3). Change the file mode
(CO2) (6 Marks) [Comprehension]

C). The entire penetration test can be classified into 3 major types depending on what the organization wants to test and how it wants the security paradigm to be tested. By taking a suitable example, explain these three types.

(CO2) (10 Marks) [Application]

OR

4.

A). Mention any four Linux operating system with its major usage in Ethical Hacking.

(CO2) (4 Marks) [Knowledge]

B). Write a short note on Port and Socket. How does it used in establishing a connection to any host in a network?

(CO2) (6 Marks) [Comprehension]

C). Backtrack is most widely used penetration testing tool in Linux platform. Briefly summarize the usage of Backtrack to test any vulnerabilities. Mention few advantages of using backtrack. Also justify why it is called as backtracking.

(CO2) (10 Marks) [Application]

5.

A). With respect to DES algorithm, what is the input block size, key size, various operations involved and number of rounds used for encryption and decryption.

(CO3) (4 Marks) [Knowledge]

B). Define encryption and decryption. Differentiate between symmetric and asymmetric key cryptography.

(CO3) (6 Marks) [Comprehension]

C). Data Encryption Standard is well known symmetric key cryptographic algorithm developed by IBM. It uses block cipher mechanism for encryption and decryption. Explain the process of 32 bits to 48 bits expansion which happens in each round of DES operation.

(CO3) (10 Marks) [Application]

OR

6.

A). Write a short note on information gathering techniques used in ethical hacking

(CO3) (4 Marks) [Knowledge]

B). Explain different sources of information gathering with the type of information you can fetch that can be used for ethical hacking. Illustrate with an example each.

(CO3) (6 Marks) [Comprehension]

C). Nowadays, Linux is the fastest-growing OS. It is used from phones to supercomputers by almost all major hardware devices. Explain the structure of Linux operating system and also brief about the Linux directory structure with appropriate diagram.

(CO3) (10 Marks) [Application]

7.

A). Write a short note on DHCP (CO4) (4 Marks) [Knowledge]

B). Compare and contrast active and passive information gathering used in ethical hacking by taking a suitable example.

(CO4) (6 Marks) [Comprehension]

C). Cyclic Redundancy Check is a popular error detection algorithm that works on binary division and XOR. Assume that the sender has sent a message binary pattern 101011 to the destination. Demonstrate how the CRC algorithm can be used to test whether the message has reached the destination without any error using proper calculations. Consider the divisor as 1100.

(CO4) (10 Marks) [Application]

OR

8.

A). What is the role of SNMP? Explain in brief. (CO4) (4 Marks) [Knowledge]

B). Flag fields are used in the IP header for the smooth flow of packets from source to destination. How many flag fields are there in IP header? Explain in brief.

(CO4) (6 Marks) [Comprehension]

C). The information-gathering process is the most important phase of Ethical Hacking. What are the methods used for gathering information? Explain with an example each. Classify these examples as active or passive information gathering.

(CO4) (10 Marks) [Application]

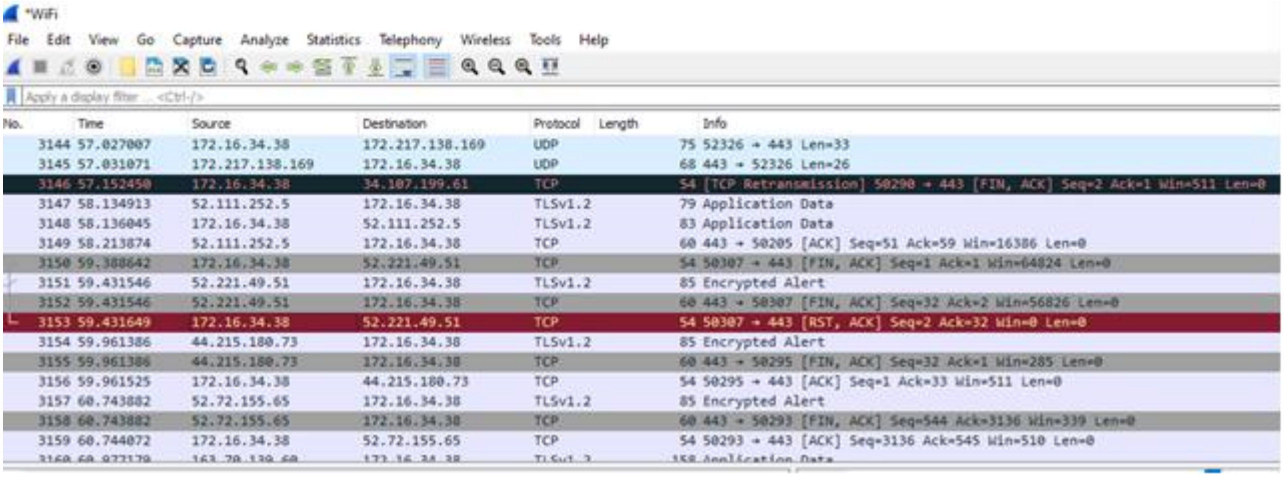
9.

A). Briefly explain the Denial of Service attack. Which Ethical Hacking software can be used to perform this attack? (CO3) (4 Marks) [Knowledge]

B). What do you mean by Connection-oriented and connectionless protocol? Give an example for each. Mention any two differences between these two.

(CO3) (6 Marks) [Comprehension]

C). Analyze the following output. In Sl. No 3153, it is the error packet. mention any two reasons for error packets. How do you test all the outgoing packets from the same source? Mention the proper filter. For the same destination how do you test all incoming packets? Also write the appropriate filter for source and destination port.


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source           Destination      Protocol Length Info
 3144 57.027007  172.16.34.38     172.217.138.169  UDP      75 52326 → 443 Len=33
 3145 57.031071  172.217.138.169  172.16.34.38     UDP      68 443 → 52326 Len=26
 3146 57.152450  172.16.34.38     34.107.199.61    TCP      54 [TCP Retransmission] 50290 → 443 [FIN, ACK] Seq=2 Ack=1 Win=511 Len=0
 3147 58.134913  52.111.252.5     172.16.34.38     TLSv1.2  79 Application Data
 3148 58.136045  172.16.34.38     52.111.252.5     TLSv1.2  83 Application Data
 3149 58.213874  52.111.252.5     172.16.34.38     TCP      60 443 → 50205 [ACK] Seq=51 Ack=59 Win=16386 Len=0
 3150 59.388642  172.16.34.38     52.221.49.51     TCP      54 50307 → 443 [FIN, ACK] Seq=1 Ack=1 Win=64824 Len=0
 3151 59.431546  52.221.49.51     172.16.34.38     TLSv1.2  85 Encrypted Alert
 3152 59.431546  52.221.49.51     172.16.34.38     TCP      60 443 → 50307 [FIN, ACK] Seq=32 Ack=2 Win=56826 Len=0
 3153 59.431649  172.16.34.38     52.221.49.51     TCP      54 50307 → 443 [RST, ACK] Seq=2 Ack=32 Win=0 Len=0
 3154 59.961386  44.215.180.73    172.16.34.38     TLSv1.2  85 Encrypted Alert
 3155 59.961386  44.215.180.73    172.16.34.38     TCP      60 443 → 50295 [FIN, ACK] Seq=32 Ack=1 Win=285 Len=0
 3156 59.961525  172.16.34.38     44.215.180.73    TCP      54 50295 → 443 [ACK] Seq=1 Ack=33 Win=511 Len=0
 3157 60.743882  52.72.155.65     172.16.34.38     TLSv1.2  85 Encrypted Alert
 3158 60.743882  52.72.155.65     172.16.34.38     TCP      60 443 → 50293 [FIN, ACK] Seq=544 Ack=3136 Win=339 Len=0
 3159 60.744072  172.16.34.38     52.72.155.65     TCP      54 50293 → 443 [ACK] Seq=3136 Ack=545 Win=510 Len=0
 3160 60.977179  163.70.139.60    172.16.34.38     TLSv1.2  158 Application Data
```

(CO3) (10 Marks) [Application]

OR

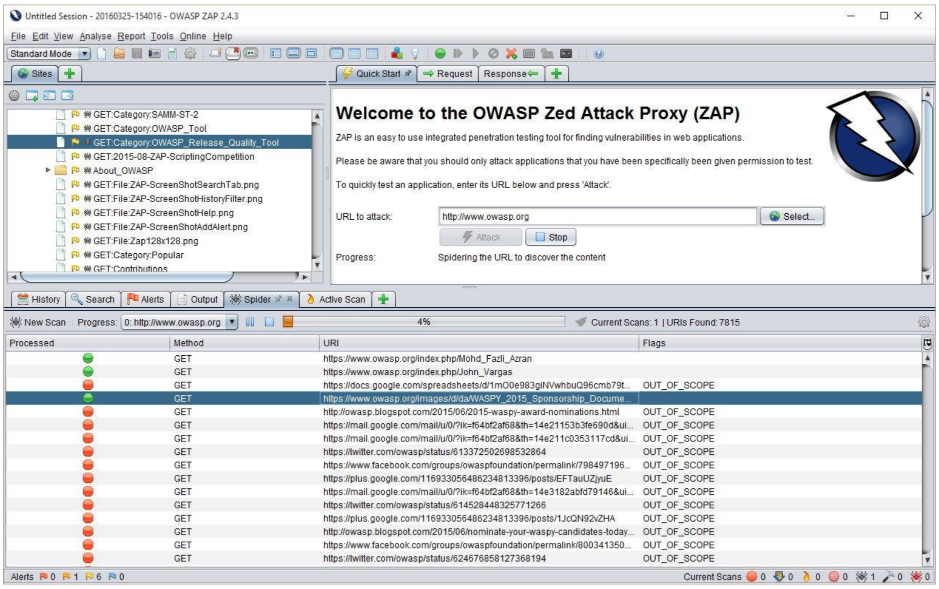
10.

A). What do you mean by DNS? Briefly explain the role of DNS. Which command will give you the DNS IP address in both windows and Linux operating system? (CO4) (4 Marks) [Knowledge]

B). Define an IP address. Mention the different classes of IP address with network ID and host ID. How many number of networks can be connected in each class? And how many hosts can be connected on each subnet?

(CO4) (6 Marks) [Comprehension]

C). URL scanners work by scanning the URL for various indicators of potential security issues, such as malicious code, phishing attempts, malware, or suspicious behavior. What type of error reports you will get in OWSAP scanning tool? Using the below diagram explain any 3 varieties of results for URL scanning.


Untitled Session - 20160325-154016 - OWASP ZAP 2.4.3
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
History
Search
Alerts
Output
Spider
Active Scan

GET:Category:SAMM-ST-2
GET:Category:OWASP_Tool
GET:Category:OWASP_Release_Quality_Tool
GET:2015-08-ZAP-ScriptingCompetition
About_OWASP
GET:File:ZAP-ScreenShotSearchTab.png
GET:File:ZAP-ScreenShotHistoryFilter.png
GET:File:ZAP-ScreenShotHelp.png
GET:File:ZAP-ScreenShotAddAlert.png
GET:File:Zap128x128.png
GET:Category:Popular
GET:Contributions

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://www.owasp.org Select...

Attack Stop

Progress: Spidering the URL to discover the content

New Scan Progress: 0: http://www.owasp.org 4% Current Scans: 1 | URIs Found: 7815

Processed	Method	URI	Flags
●	GET	https://www.owasp.org/index.php/Mohd_Fazli_Azran	
●	GET	https://www.owasp.org/index.php/John_Vargas	
●	GET	https://docs.google.com/spreadsheets/d/1mO0e983giNVwhbuQ96cmb79t...	OUT_OF_SCOPE
●	GET	https://www.owasp.org/images/d/da/WASPY_2015_Sponsorship_Docume...	
●	GET	http://owasp.blogspot.com/2015/06/2015-waspy-award-nominations.html	OUT_OF_SCOPE
●	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e21153b3fe690d&ui...	OUT_OF_SCOPE
●	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e211c0353117cd&ui...	OUT_OF_SCOPE
●	GET	https://twitter.com/owasp/status/613372502698532864	OUT_OF_SCOPE
●	GET	https://www.facebook.com/groups/owaspfoundation/permalink/798497196...	OUT_OF_SCOPE
●	GET	https://plus.google.com/116933056486234813396/posts/EFTauUZjyuE	OUT_OF_SCOPE
●	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e3182abfd79146&ui...	OUT_OF_SCOPE
●	GET	https://twitter.com/owasp/status/614528448325771266	OUT_OF_SCOPE
●	GET	https://plus.google.com/116933056486234813396/posts/1JcQN92vZHA	OUT_OF_SCOPE
●	GET	http://owasp.blogspot.com/2015/06/nominate-your-waspy-candidates-today...	OUT_OF_SCOPE
●	GET	https://www.facebook.com/groups/owaspfoundation/permalink/800341350...	OUT_OF_SCOPE
●	GET	https://twitter.com/owasp/status/624676858127368194	OUT_OF_SCOPE

Alerts 0 1 6 0 Current Scans 0 0 0 0 1 0 0

(CO4) (10 Marks) [Application]