Reg. No. : E N G G T R E E . C O M

Question Paper Code : 20407

B.E./B.Tech. DEGREE EXAMINATIONS, NOVEMBER/DECEMBER 2023

Fifth Semester

Computer Science and Engineering

CCS 344 – ETHICAL HACKING

(Common to Computer Science and Engineering (Artificial Intelligence and Machines Learning)/Computer Science and Engineering (Cyber Security) / Computer and Communication Engineering / Artificial Intelligence and Data Science and Information Technology)

(Regulations 2021)

Time : Three hours

Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. Compare IPV4 and IPV6 addressing.

2. Who are Script Kiddies?

3. What is port scanning?

4. What is dumpster diving?

5. Define Enumeration.

6. What are Null Sessions?

7. List four wireless devices used by people in their day to day life.

8. What are ActiveX Data Objects?

9. List the main hardware components in a Router.

10. List the criteria used by Extended IP access lists to restrict incoming / outgoing IP traffic at router's interface.

PART B — (5 × 13 = 65 marks)

11. (a) Explain the following terms with respect to Ethical Hacking.

(i) Hack value (3)

(ii) Exploit (3)

(iii) Vulnerability (3)

(iv) Target Evaluation (2)

(v) Zero day attack (2)

Or

(b) Compare Black, Gray and White Box Penetration Testing methods with example.

12. (a) Identify three unique attributes of a user's browser that a fingerprinting script could use to persistently identify the user even if they erase their cookies and other site data. Depict the complete procedure in detail.

Or

(b) Compare and contrast the network scanning procedure of IPV4, IPV6 on using the tools Nmap and Hping 3. Elaborate the complete scanning procedure in detail.

13. (a) Depict the complete SNMP procedure in finding suspicious network activities with neat architecture. Write how SMTP functionalities vary from SNMP.

Or

(b) What vulnerabilities are found in embedded systems, and how do they differ from traditional IT vulnerabilities? Why are embedded vulnerabilities are harder to remediate, and what can you do about them? Elaborate the complete vulnerability assessment procedure in detail.

14. (a) Enumerate the OWASP Top Ten Web Application Vulnerabilities and describe which among them plays crucial role in disrupting regular business activities.

Or

(b) Explain about the tools adopted by web hackers for system hacking and write the measures carried out by security testers to identify the same.

15. (a) A company has several offices around the world. Data is transmitted between offices over the internet. In order to keep the data safe the company uses the Secure Socket layer (SSL) and Firewall at each office. Explain how the SSL protocol and a firewall will keep the companies data safe.

Or

(b) Illustrate with a neat diagram the procedure of setting up a Demilitarized Zone with two firewalls. Also depict the role of Incident Response teams in case of violations in firewalls / Honey pots.

PART C — (1 × 15 = 15 marks)

16. (a) A social media company has grown and now has a couple of thousand users. The company uses Cisco Routers. There are multiple servers and routers in the datacenter now. One day it could be observed that some clients cannot connect to the servers. In a panic, you start dumping traffic on the ingress gateway router of the problematic servers and see the following packets (partial headers) :

Ver	Length	TOS	TTL	Protocol	Source Address	Destination Address
4	38	0	250	17	139.133.217.110	69.62.28.126
4	40	0	214	06	121.69.24.120	69.62.28.126
4	84	0	249	01	18.69.204.150	69.62.28.126
4	55	0	250	06	192.0.0.15	192.0.0
4	84	0	243	01	18.69.204.150	69.62.28.126
4	84	0	249	01	128..109.24.10	69.62.28.127
4	84	0	237	01	18.69.204.150	69.62.28.126
4	40	0	208	06	121.69.24.120	69.62.28.126

From the Table information, identify the issue. Explain, How can the attack be handled, and service be provided as before?

Or

(b) Consider the following scenario. In a class, we have students Alice, Bob, Eve, and an instructor Mallory. Suppose Alice, Bob, and Mallory each own a textbook, but Eve does not. Also suppose the instructor can ask students questions and students can answer; at the same time, students can also ask instructor, to which both instructor and other students can answer; however, a student cannot ask other students questions in class. Draw an access control list to model the above rules. List your assumptions.