UNIRAZAK
UNIVERSITI TUN ABDUL RAZAK

FINAL EXAMINATION

MARCH 2024

COURSE TITLE	**ETHICAL HACKING**
COURSE CODE	**RCIT3833**
DATE/DAY	**30 JUNE 2024 / SUNDAY**
TIME/DURATION	**01:00 PM - 03:00 PM / 02 Hour(s) 00 Minute(s)**

INSTRUCTIONS TO CANDIDATES :

1. Please read the instruction under each section carefully.
2. Candidates are reminded not to bring into examination hall/room any form of written materials or electronic gadget except for stationery that is permitted by the Invigilator.
3. Students who are caught breaching the Examination Rules and Regulation will be charged with an academic dishonesty and if found guilty of the offence, the maximum penalty is expulsion from the University.

(This Question Paper consists of **8** Printed Pages including front page)

*****DO NOT OPEN THE QUESTION PAPER UNTIL YOU ARE TOLD TO DO SO*****

This question paper consists of TWO (2) sections. Answer ALL questions in the answer booklet provided. [100 MARKS]

SECTION A (40 Marks)

There are TWENTY (20) questions in this section. Answer ALL questions in the answer booklet provided.

1. What is the primary purpose of using Nmap in ethical hacking?

   A. To encrypt data packets
   B. To perform network scanning and enumeration
   C. To create digital certificates
   D. To manage network traffic

2. Which tool is used for detecting the web application firewalls in use on a target site?

   A. Metasploit
   B. Dig
   C. WafW00f
   D. WhatWeb

3. What does the dig command primarily retrieve information about?

   A. User's credentials
   B. DNS settings and records
   C. System vulnerabilities
   D. Network traffic patterns

4. Which of the following tools is a graphical tool for pre-attack planning and information gathering?

   A. Nmap
   B. Maltego
   C. WhatWeb
   D. Searchsploit

5. What is the primary use of theHarvester in ethical hacking?

   A. Breaking into wireless networks
   B. Gathering email accounts, subdomain names, hosts, and public information about a target
   C. Executing active attacks against networks
   D. Sniffing data packets

6. Which command in Kali Linux is used to search for exploits in the Metasploit framework?

   A. dirb
   B. searchsploit
   C. msfconsole
   D. airmon-ng

7. What is the Metasploit Framework primarily used for?

   A. Analyzing network traffic
   B. Executing penetration tests and managing security assessments
   C. Filtering network packets
   D. Monitoring system performance

8. In the context of TCP/IP, what is the purpose of the SYN flag in the TCP header?

   A. To acknowledge received packets
   B. To indicate the end of communication
   C. To initiate a TCP connection
   D. To prioritize packets

9. Which tool would you use to identify the technology stack of a website?

   A. Burp Suite
   B. Nmap
   C. WafW00f
   D. WhatWeb

10. How does Metasploit differ from Maltego in terms of usage?

A. Metasploit is used for exploitation, while Maltego is used for information gathering.
B. Metasploit is used for encryption, while Maltego is used for reconnaissance.
C. Metasploit and Maltego are both primarily used for vulnerability scanning.
D. There is no difference; both are used for the same purposes.

11. What is the role of reconnaissance in ethical hacking?

A. To collect as much information as possible about the target before launching an attack
B. To perform the attack on the target system
C. To secure the network from other hackers
D. To cover tracks after the hacking is completed

12. Which Linux command can display all network interfaces and their IP addresses on a system?

A. ipconfig
B. iwconfig
C. ifconfig
D. netstat

13. What is the significance of WafW00f in the reconnaissance phase of ethical hacking?

A. To identify and characterize the web application firewalls protecting a site
B. To exploit vulnerabilities in web applications
C. To map the internal network structure of an organization
D. To monitor real-time traffic to and from the network

14. In Kali Linux, which tool is designed for DNS footprinting?

A. Nessus
B. Netcat
C. Dig
D. Etherape

15. How is searchsploit used in ethical hacking?

A. To perform automated penetration tests
B. To search for known vulnerabilities in software
C. To sniff network packets
D. To map network devices

16. Which of the following is true about the TCP/IP model?

A. It is the foundational network model for the Internet.
B. It only includes three layers.
C. It is primarily used for data storage.
D. It is less comprehensive than the OSI model.

17. What is the main purpose of using tools like Maltego in ethical hacking?

A. To create fake phishing pages
B. To perform open-source intelligence gathering
C. To decrypt password hashes
D. To inject SQL queries

18. What function does theHarvester serve in the context of gathering intelligence?

A. It creates backdoors in systems.
B. It compiles useful data about people and organizations.
C. It checks the network for misconfigurations.
D. It encrypts data transfers.

19. Which stage of ethical hacking involves using tools like Metasploit and Searchsploit?

A. Exploitation
B. Reconnaissance
C. Reporting
D. Remediation

20. In TCP/IP, what is the role of the IP protocol?

A. To establish a secure connection
B. To provide hardware addressing
C. To encrypt data packets
D. To handle packet routing and delivery.

SECTION B **(60 Marks)**

There are THREE (3) questions in this section. Answer ALL questions in the answer booklet provided.

QUESTION 1 **(20 Marks)**

Discuss the **FIVE (5)** main stages of ethical hacking as defined in the ethical hacking process. For each stage, provide a brief explanation of the activities involved and explain how each contributes to a comprehensive security assessment. Include examples of tools that might be used in each stage and the type of vulnerabilities or security issues they can help identify.

QUESTION 2 **(20 Marks)**

Scenario:
You are a cybersecurity analyst at a cybersecurity firm, and you have been tasked with conducting a security assessment for ACME Corp. ACME Corp has given you permission to perform a penetration test on their web-facing services to identify potential vulnerabilities and assess the robustness of their security measures.

Provided Details:

Target IP Address Range: 192.168.100.10 to 192.168.100.15
Domain Name: acme-services.com
Host Names and IP Addresses:
webserver1.acme-services.com - 192.168.100.10
mailserver.acme-services.com - 192.168.100.15

You decide to use tools such as Nmap for network scanning, WhatWeb for identifying technologies, and WafW00f to check for the presence of web application firewalls. Based on initial findings, you plan to use Metasploit for further exploitation testing.

Provided Tool Outputs:

- Nmap Output for 192.168.100.10 (webserver1.acme-services.com):
  PORT STATE SERVICE
  80/tcp open http
  443/tcp open https
  3306/tcp open mysql

- Nmap Output for 192.168.100.15 (mailserver.acme-services.com):
  PORT STATE SERVICE
  25/tcp open smtp

110/tcp open pop3
143/tcp open imap
993/tcp open imaps
995/tcp open pop3s

- WafW00f Output for webserver1.acme-services.com:
  Checking for presence of WAF on webserver1.acme-services.com:
  The site is behind a Cloudflare Web Application Firewall.

Write a short report based on your findings from the reconnaissance phase. Your report should include:

Open Ports and Services: Results from using Nmap to scan the target IP addresses.
Technologies Identified: Information gathered from WhatWeb for each host (assume typical findings such as WordPress for webserver1, Microsoft Exchange for mailserver, and Pure-FTPd for ftp server).
Web Application Firewalls: Detection results from WafW00f for the webserver.
Proposed Next Steps for Exploitation: Recommendations for exploiting identified vulnerabilities, considering the technologies and defenses in place.
Guidelines for the Report:

Begin with an executive summary that encapsulates your overall findings.
Provide a detailed analysis of each host, categorizing findings by IP address/host name.
Conclude with strategic recommendations for the exploitation phase, highlighting any critical vulnerabilities that could be prioritized.
Ensure your language is clear, professional, and technical, suitable for an audience of security professionals.

QUESTION 3 **(20 Marks)**

Reconnaissance is a critical initial phase in the ethical hacking process, where information about a target system is gathered to identify potential vulnerabilities. Various tools are available to assist in this phase, each with specific features that suit different types of information gathering. Discuss the differences and similarities between at least **FOUR (4)** of the following reconnaissance tools: Nmap, TheHarvester, Maltego, WhatWeb, WafW00f, and DIG. For each tool, provide an explanation of its typical use cases, the unique features that distinguish it from the others, and the type of vulnerabilities or security issues it helps to identify.

***** END OF QUESTION PAPER *****