ZCAS University

BACHELOR OF SCIENCE IN CYBERSECURITY

BACHELOR OF SCIENCE IN CYBERSECURITY & CRIME SCIENCE

CIT3342 - HACKING THEORY AND PRACTICE

MID-SEMESTER EXAMINATION

23RD OCTOBER 2023

08:30 HRS-11:30HRS

TIME ALLOWED: WRITING – THREE HOURS

READING – 5 MINUTES

INSTRUCTIONS:

1. Section A: this question is **compulsory** and must be attempted.
2. Sections B: Answer **THREE (3)** questions from this section.
3. This examination paper carries a total of **100 marks**.
4. Candidates must **not turn this page** until the invigilator tells them to do so.

SECTION A: Question 1 is compulsory and must be attempted.

Question 1

(a) You are working as a cybersecurity consultant for a company, and you have been provided with a scan of the core server. Consider the exhibit of the network security scan in Figure 1 and answer the questions that follow.

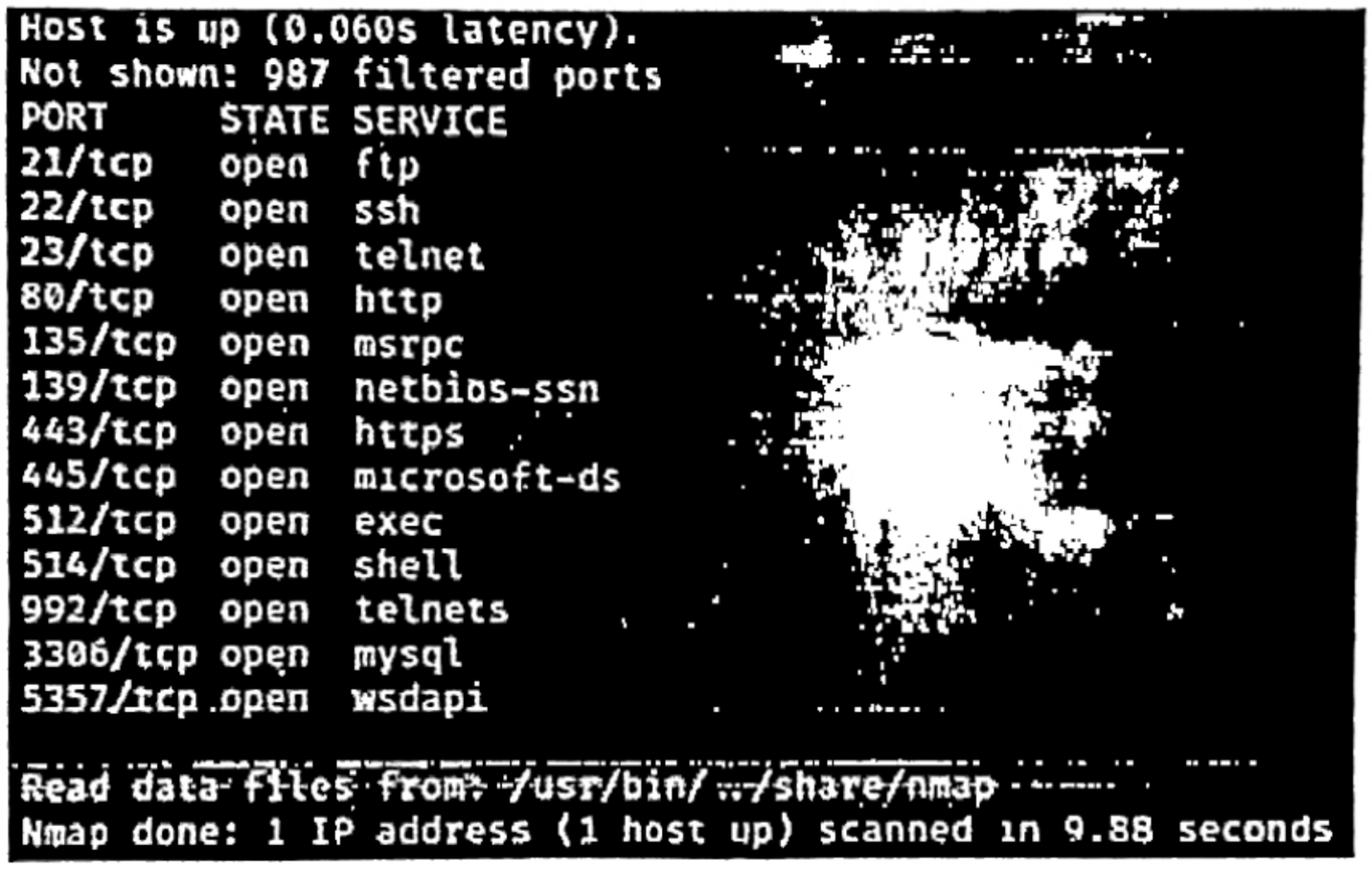

Fig. 1 Network Security Scan of the Server

i. Identify from the figure above, which protocols are used for unsecured and secured remote access services, and those used for unsecured and secured web services, and their corresponding port numbers. **[5 Marks]**

ii. Given that the company wants to be sharing their files securely from a central server, identify which protocol you would disable and which one you would replace it with to provide secure file services. **[5 Marks]**

iii. You are not sure whether the SSH version that the server is using has a vulnerability, explain how you would go about to ascertain whether the SSH software being used has a vulnerability. **[5 Marks]**

iv. Identify the software tool used to generate the details in Fig.1 and explain the process of how this is achieved. **[5 Marks]**

(b) An attacker has just learned that a certain system has a vulnerable unpatched server that is susceptible to a backdoor attack. The only thing that she knows about the target system is the IP address range.

i. Clearly explain how the attacker would go about to find the exact vulnerable server in the network. **[5 Marks]**
ii. Given that the vulnerable server is using ***vsftpd v2.3.4***, explain how the attacker can use RCE to have full control of the victim machine. **[8 Marks]**
iii. Given that the server is also using the vulnerable Apache Log4j library to log messages from applications, explain how the attacker can use the log4shell exploit to have full control of the victim machine. **[7 Marks]**

(Total: 40 marks)

SECTION B: Attempt any THREE questions in this section.

Question 2

Understanding the attack process is a vital component of cyber security because this enables the security personnel to put up effective measures against cyber-attacks. Reconnaissance is not inherently malicious, as organizations and security professionals also perform reconnaissance to identify and mitigate potential weaknesses in their own systems. However, when it is part of a cyber-attack process, it serves as a crucial step in the attacker's attempt to gain unauthorized access or compromise the target system's security.

a) Explain the importance of reconnaissance as the first stage of an attack process. **[5 Marks]**
b) Describe what an attack vector is giving three clear examples. **[5 Marks]**
c) Explain what defence-in-depth strategy is and give a clear example. **[5Marks]**
d) Explain the term APT and give two clear examples explaining how reconnaissance is leveraged by APTs. **[5 Marks]**

(20 Marks)

Question 3

Cybersecurity has a lot of terminologies which are usually misplaced in the mainstream media. Briefly differentiate the following cybersecurity terms:

a) Darknet and Deep web. **[4 Marks]**
b) Whitehat vs Greyhat vs Blackhat hacker **[6 Marks]**
c) Ethical hacking vs penetration testing. **[4 Marks]**
d) Vulnerability, Threat, and Risk. **[6 Marks]**

(20 Marks)

Question 4

Generally, information security is based on certain principles. Attacks breach these principles of security.

(a) Describe the 3 major principles of security **[6 Marks]**
(b) Discuss any 4 DOS attacks found in information systems. **[4 Marks]**
(c) Discuss the basic four categories of threats and give one example. **[5 Marks]**
(d) Describe a CVE and how attackers use them in cyber-attackss. **[5 Marks]**

(20 Marks)

Question 5

The Social-Engineer Toolkit (SET) is a powerful open-source tool available in Kali Linux used for penetration testing and ethical hacking, particularly in the context of social engineering attacks.

(a) Explain how you can use the SET toolkit to harvest login credentials from a target. Describe the different methods available in SET for collecting usernames and passwords, and outline the risks associated with credential harvesting attacks. **[10 Marks]**

(b) In a social engineering context, describe the significance of understanding human psychology and behaviour. How can knowledge of social engineering techniques help individuals and organizations defend against such attacks? Additionally, what are the ethical responsibilities of security professionals when using tools like SET for testing and awareness purposes? **[10 Marks]**

(20 Marks)

(Total: 60 marks)

----------**END OF EXAMINATION**----------

HAVE A Wonderful DAY