Module: Cybersecurity

Assignment No.: 1

Weightage: 30%

Total Marks: 120

Deadline: 30th March 2024

Instructions:

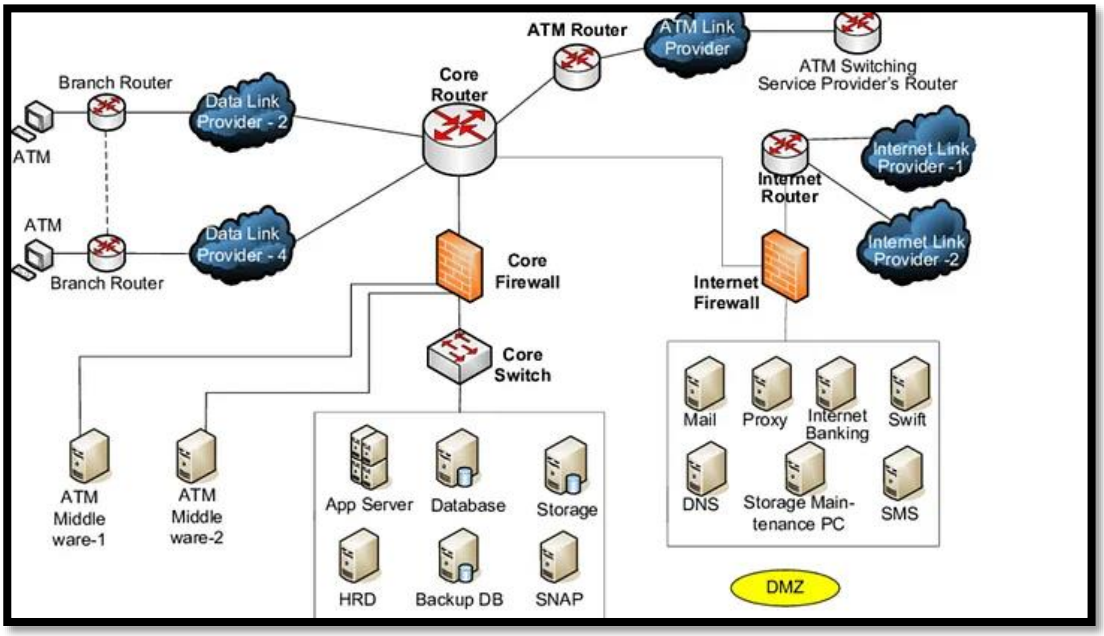
- Submit your assignment in PDF format.
- The word limit is 4000 words.
- Submit your assignment on Blackboard. A Turnitin link will be provided to upload your assignments to check the plagiarism.
- Do not share your assignment answers with anyone and do not copy the assignment from others. Both will get zero marks.
- The names of the files should include the course short name, student name, student number, and assignment number. (Name-L123456-Cyber-Assignment1)

PART 1: Security report

Assignment Specification

You have started working in a bank (or a FinTech company) (choose any company - FTSE - ISEQ). This bank has received a directive from its CEO to increase security awareness. The security awareness should include possible threats documentation and their mitigation strategies. You have been asked to compile a report for the company.

Imagine the diagram below for the network diagram.



Task 1: (10 marks)

Describe the business of your selected bank or company. Identify the assets that will need the most protection (their "Crown Jewels") such as client lists, current products, future acquisitions, safety, intellectual property, etc.

The company is concerned about its cybersecurity awareness. You must:

- Identify at least four websites where you can get details of the most current malware threats related to your company business.

  (2 mark)

- Compile a list of eight of the most recent threats (excluding Ransomware) which may be of specific interest to the company, including the following information:
  - Description of each threat and the mitigation strategy.
  - Risk analysis of each threat.
  - The CEO is particularly concerned about ransomware so you must detail ransomware in online attacks. Its execution steps and mitigation strategies.

  (8 marks)

Task 2: (10 marks)

Assume you are an ethical hacker (white hat hacker), and you are being assigned the task of protecting the company's network. As a first step, you need to know, how an unethical hacker can penetrate your network. Initially, they will require some information about your business, network (LAN), servers, applications, services, software and their versions, and operating system. *Identify the ways through which an unethical hacker can gather the information about the above related to your company. Also, mention which type of information is expected from each method or way identified above.*

There is a concern about how the company's internet presence makes it vulnerable. You will write a report on the footprint of the company.

- The first part of this section should consist of a discussion on footprinting.
  (must)
- What are the different ways/methods through which information can be gathered about the company?
  (2 marks)
- What type of data that is publicly available can be exploited from the identified method?
  (2 marks)
- Which part of the company's network could be potentially vulnerable due to information exposure? (weakness identification)
  (2 marks)
- Write up the details of any weaknesses that could be exploited in the targeted company based on your research of the company activities and footprint.
  (2 marks)
- Give solutions to resolving these weaknesses.
  (2 marks)

** Imagine the network diagram above for the network.
** You can discuss social engineering here, wherever necessary.
** Do not use any penetration tool for this task 2.

Task 3: (10 marks)

The company has several concerns about physical and digital access to private assets of the company. An external security expert has informed management that social engineering could be used to bypass the authentication systems.

.

- The first part of this section should detail what social engineering is and how it might affect the company's security and authentication system and provide examples.
  (5 marks)

- The second part of this section should detail good practices that should be employed in the company for both physical and digital authentication, this should consider the nature of the business.
  (5 marks)

Reporting:

For this first part of the report. First start by introducing the company you have chosen. Then describe its business and its network and data flow with diagrams. This should include the list of the main components being used in the company's network (server, firewalls, DMZ, LAN, HW, SW, OS, etc). Then pinpoint in the diagram where exactly each threat can affect. After this, you can start describing each task. For example, in the first task of this part 1, when you describe the threats, also relate them to the diagram provided. A table might be good here showing, the threat, affected network area/parts, significance, mitigation, etc.

PART 2: Penetration testing

Task 1: (15 marks)

Use Metasploit to run payloads and gather information about a Windows machine or Metasploitable machine. (You might need to turn off the Windows firewall and antivirus)

- Gather system information (using at least one method, two would be good)
- Gather open ports information.
- Provide information about the application related to each open port.

**Show the steps using the screenshots.

You also might need to run services (SQL etc or any) on your Windows VM or Metasploitable machine to see the open ports.

Task 2: (15 marks)

Choose 2 ports from Task 2.

Provide the steps and information to secure these ports on the target machine. Identify why they are open. Can you provide a way for those open ports to remain undetected by any vulnerability scanner?

Part 3: Traffic analysis

Task: (30 marks)

a. A traffic capture is provided with this assignment. This capture contains a LAN segment trace in which a host was targeted. The network information is as follows.

LAN segment range: 10.0.19.0/24 (10.0.19.0 through 10.0.19.255)
Domain: you need to find
Domain controller: 10.0.19.9 – name you need to find
LAN segment gateway: 10.0.19.1
LAN segment broadcast address: 10.0.19.255

You need to write an incident report based on the PCAP provided. The report should contain three sections as,

Executive Summary:

State in simple, direct terms what happened (when, who, what).

- When the incident occurred.
- Who was the Victim?
- What infected him? (optional)(would be good to see)

Details:

- Details of the victim.
- Find the victim's hostname.
- Find the victim's IP Address and MAC address.
- Find the victim's Windows user account name.
- Locate the domain controller name and IP address

Indicators of Compromise (IOCs):

- Find the IP address, domain name, and URLs which are associated with the infection. (who is sending traffic and to whom response is going)
- Generate the hash (SHA256) of any malware binary which can be extracted from a pcap file. (This part is optional, and won’t affect your marks)

Additional questions as a hint:

- How many protocols you can see?
- How many conversations you can see? (between different source and destination addresses)
- Locate the transmission between the PCs belonging to the same domain.

*****you need to provide screenshots as evidence in the report for each part*****
*****Without the evidence the information won't be accepted to mark*****

*****Use the PCAP file to analyze, in your Virtual Machine only*******

(25 marks)

b. Name the attacks that can be identified by using Wireshark and how they can be identified. Attacks in general, are not related to the pcap file provided. Generate a throughput graph in Wireshark of any victim conversation.

(5 marks)

Part 4: Malware analysis

Task 1: (30 marks)

In this part, you will need to analyse the malware sample. Apply the tools and techniques you have learned and practiced in lectures and labs to analyse it. You need to apply static and dynamic analysis techniques to find the malware characteristics.

It would be good if you could download malware from the website 'Malware Bazaar'. It contains different and recent sources of malware. However, you need to be extra cautious in downloading malware. Soon after downloading malware from the website (any malware RAT, Mirai, keylogger, elf) turn off your network immediately, and no matter what do not turn it on. This is to contain the malware and use a safe environment for your analysis.
Alternatively, you can use the same sources from the link that was provided to you during the lab (chapter 2 and 3 folders, pick an exe and related dll file to analyze)

Once you have downloaded the malware in your Virtual Machine and contained it (turned off your Network connection). Make sure you have downloaded all the required tools before downloading the malware. Then answer the following questions.

1. Describe, how you would perform the static analysis and why.
2. Describe, how you would perform the dynamic analysis and why.
3. Which DLL files (system or custom-based) are involved with the malware and what is their purpose?
4. Extract the strings and based on the string values, analyze the type of malware and its functions.
5. Mention and describe the import functions, export functions, and libraries involved with the malware.
6. Type of malware with evidence. (RAT, keylogger, network trojan, Bot, etc)
7. Flow and working of malware, I mean, you need to show the way the malware will work after executing it.
8. Mention the processes involved with their process IDs when you execute the program. How can you find the process under which malware is running?
9. You need to mention the indicators of compromise. Such as the host indicators, file indicators, or network indicators. Whichever indicator you can find, mention it.
10. Is there any code obfuscation used in the malware? Or memory modification happening?
11. Any registry changes you have observed.
12. Any remote connection or remote file transfer you have observed.

NOTE: **Any content copied and pasted will be discarded**; all work must be your own.
The report should be in 12pt Times New Roman font, single line spacing. Your report should include a title page, table of contents, page numbers, and references.
Provide screenshots where necessary to show the steps.

Marking:

Part 1:

- Task 1: 10 marks
- Task 2: 10 marks
- Task 3: 10 marks

Part 2

- Task 1: 15 marks
- Task 2: 15 marks

Part 3:

- Task 1: 25 marks
- Task 1: 5 marks

Part 4:

- Task 1: 30 marks

Marks will be given based on the accuracy and details of the information and steps provided.