Cyber Security Final Assessment Part 1

This assessment is comprised of 2 case studies, a network setup, and a Cyber security policy.

Question 1 – Case Study (20)
Question 2 – Case Study (20)
Question 3 – Network Setup (70)
Question 4 - Cyber Security Policy (30)

Introduction

With the widespread availability of internet connectivity for computing devices, the need to safeguard against cyber-attacks and prevent the unauthorized disclosure of private and confidential information has become increasingly critical. Moreover, the motivations behind these attacks have diversified, encompassing financial gains, retaliatory actions, political influence, and infrastructure disruption. No one is immune to the threat of cyber-attacks.

Question 1

Please read the case study carefully and answer the questions that follow.

Case Study 1: LionRoar
On May 12, 2017, a malware outbreak swiftly propagated, affecting numerous computers worldwide. This resulted in the inaccessibility of data files on the infected computers. What transpired?

In a span of 24 hours, LionRoar had infiltrated more than 200,000 computers across 150 nations. The impact was widespread, affecting diverse sectors such as universities, government departments, hospitals, manufacturers, telecommunications companies, and various organizations. Notable entities, including Mabili, HackMe, Umbrella, the National Health Service of South Africa, Haval Motoring Manufacturing EU, O2 Africa, BigBoy AUS, and Eskom, were among those affected by the attack.

Fortuitously, the proliferation of the malware encountered a significant impediment when a security researcher stumbled upon and inadvertently triggered the 'kill switch' the following day, on May 13, 2017. During an examination of the malware's code, the researcher observed an unusually lengthy internet domain name embedded in it. Upon discovering that the domain name was unregistered, the researcher took the initiative to register it. Unbeknownst to them at that moment, this action effectively deactivated the malware, preventing its continued spread.

Subsequent analysis by security experts affirmed that the malware utilized the registered domain as a kill switch, allowing its owner to halt its propagation in situations where events went awry or became unmanageable. However, these experts cautioned that variants of the malware lacking a kill switch could exist or be developed by malicious actors in the future.

While this extensive attack appeared to pass swiftly, it served as a stark reminder of society's susceptibility to cyber-attacks and its lack of readiness to confront them. The abrupt conclusion of the incident was purely fortuitous.

Answer the following questions thoroughly:

1.1 What was the nature of the attack and explain how the attack works. (5)
1.2 How was the attack carried out on LionRoar? (5)
1.3 Who could have been responsible for the attack? And state your reason. (5)
1.4 What could have been done to prevent the attack? (5)

Introduction

In the realm of cybersecurity, there exists a menacing technique where a multitude of compromised computers, unknowingly conscripted into a collective force, inundate a target system with an overwhelming volume of requests. This orchestrated deluge of traffic overwhelms the target's capacity to respond effectively, causing disruptions, slowdowns, or even complete unavailability of services. This surreptitious method, employed by malicious actors, leverages the sheer volume of hijacked devices, creating a formidable and decentralized network that can be mobilized to unleash a concerted assault on digital infrastructure. The aim is not to breach security perimeters but rather to cripple operations through sheer force, posing a significant threat to the stability and functionality of online systems.

Question 2:

Please read the case study carefully and answer the questions that follow.

Case Study 2: Iron

On October 21, 2019, a significant network disruption unfolded, causing extended inaccessibility to several prominent websites like Twitch, Evetech, BOB, DataZa, FrameWorkz, and MarvelDC. The disruption stemmed from an assault on a vital internet infrastructure protocol known as the Domain Name System (DNS). This protocol plays a crucial role in translating user-friendly alphabetic domain names into numeric IP addresses essential for computer communication. The attack on DNS hindered this translation process, preventing web browsers from establishing connections to the desired websites. The responsibility for hosting this pivotal 'web directory' falls on a select few companies globally, with Iron being one of them. Iron extends DNS services to approximately 30 international corporations, including those mentioned earlier.

On that particular day, Iron encountered a sequence of highly intricate and prolonged cyber assaults. The initial incident commenced around 01:00 a.m. CAT, and the company successfully resolved the issue within two hours. However, a subsequent attack occurred at 5 a.m., demanding an additional three hours for the company to fully restore its primary services.

Despite suggestions from security experts that this could be a state-sponsored attack, it wasn't the first occurrence of such a cyber threat. Similar incidents unfolded in September 2016, involving exceptionally high-traffic attacks on the blog of security journalist Luke BTW (620 Gbit/s) and the African cloud company WTF (1 Tbit/s). Typically, a traffic volume of 20–40 Gbit/s suffices to bring down an ordinary website, making the traffic in these two attacks significantly surpass the required levels.

All these orchestrated attacks made use of an exceptionally extensive network comprised of computing devices spanning the globe. In contrast to traditional networks of compromised devices, this network comprised everyday consumer devices like IP cameras, network-enabled media players, and home routers. Many of these devices exhibited inadequate security measures, with users often neglecting to modify default settings, including factory usernames and passwords. The device owner typically remains oblivious to the hijacking, as the device continues to function, albeit potentially at a slightly diminished pace.

Answer the following questions thoroughly:

2.1 What was the nature of the attack and explain how the attack works. (5)
2.2 How was the attack carried out on all corporations? (5)
2.3 Who could have been responsible for the attack? And state your reason. (5)
2.4 What could have been done to prevent the attack? (5)

MABILI

Question 3

In this question, you will be creating a small network containing a router/s, switches, and devices ie: computers/laptops. You will need to make use of **CISCO PACKET TRACER** to complete the assignment. This assignment will also test your skill in setting up a virtual environment and compiling the necessary documentation for creating the Cyber Security network.

Scenario:

As a compact organization, we require a modest network infrastructure to enable internet access for users. This infrastructure must support 5 subnets, as each department will have its own set of devices. However, seamless data transfer between departments is essential. The existing network is on the 196.188.15.0/27 subnet. Each department will operate with five devices, utilizing class C IPv4 addresses, enabling users to work and exchange data across departments (IT department, Accounts department, Delivery department, and Transfer department). Within the network, we will furnish the following:

- Router x1
- Switches x4
- Devices x20 (Laptops/Desktops)
- Hub x1
- DNS Server x1
- Floorplan of all departments and implemented devices

How marks would be allocated:

1. **Inside Packet Tracer:**

   - The layout of the network in packet tracer. (10)
   - Devices can communicate with other devices within the network. (10)
   - Labelling and naming conventions (10)
   - Departments can connect to the DNS server (20)

2. **Subnet plan:**

   - Present a subnet plan to include all subnet addresses that were used in the assessment. Show all subnet addresses, first host IP addresses, last host IP address according to the subnet, and the broadcast according to each subnet. Also, show the subnet mask the network would use and how you have allocated the subnet mask.
   Use Microsoft Word and covert it to .pdf (5)

3. **Creating the DNS server each department will need to have its own website which each department can reach**.

   - IT department (www.MITec.co.za)
   - Accounts department (www.MAccounts.co.za)

-

- Delivery department (www.MDelivery.co.za)

- Transfer department (www.MTransfer.co.za)

(Please give the website Title as the department name and the body of the website as “You have reached the (department name)”). (10)

4. **Floorplan of all departments and implemented devices** (5)

- Prepare the floorplan on a program of your choice
- Convert it to a .pdf or .Jpeg

Question 4

Use this framework to complete a Cyber Security policy document for a company of your choice. (30)

CYBER SECURITY POLICY AND PROCEDURES

Purpose

The purpose of this policy is to establish the guidelines for computer security and the protection of an organization's networks and its content or knowledge base and to minimize the risk of internal and external cyber threats.

Scope

This policy applies to all employees, contractors, consultants, and others specifically authorized to access information and associated assets owned, operated, controlled, or managed by the company.

Policy

The company is committed to building a strong cybersecurity program to support, maintain, and secure critical infrastructure and data systems. To achieve this, the company will identify, evaluate, and take steps to avoid or mitigate risk to the company's information assets and prevent unauthorized digital or physical access, damage, theft, compromise, or interference with the company's information systems and facilities.

1. **Responsibilities**

CTO – Chief Technology Officer
IT Manager
All users

2. **Standards**

3. **Asset Management**

Personally Identifiable Information (PII)
Identity Management, Authentication and Access Control

4. **Awareness and Training**

5. **Data Security**

Data Storage
Data Transmission
Data Destruction

6. **Information Protection Processes and Procedures**

Secure Software Development
Contingency Planning
Network Infrastructure
Network Servers
Network Segmentation

7. **Protective Technology**

Email Filtering
Internet Filtering
Network Vulnerability Assessments

8. **Anomalies and Events**

9. **Security Continuous Monitoring**

Anti-Malware Tools
Patch management.

10. **Response Planning**

Electronic Incidents
Physical Incidents
Notification

11. **Recovery & Restoration**

12. **Confidentiality and Non-Disclosure Agreement**