Lab – Visualizing the Black Hats

Objectives

Research and analyze cyber security incidents

Background / Scenario

In 2016, it was estimated that businesses lost $400 million dollars annually to cyber criminals. Governments, businesses, and individual users are increasingly the targets of cyberattacks and cybersecurity incidents are becoming more common.

In this lab, you will create three hypothetical cyber attackers, each with an organization, an attack, and a method for an organization to prevent or mitigate the attack.

Note: You can use the web browser in virtual machine installed in a previous lab to research security issues. By using the virtual machine, you may prevent malware from being installed on your computer.

Required Resources

- PC or mobile device with Internet access

Scenario 1:

a. Who is the attacker?

Ans: Advanced Persistent Threat (APT) Group.

b. What organization/group is the attacker associated with?

Ans: They are a highly-skilled group of cyber criminals.

c. What is the motive of the attacker?

Ans: It will achieve access to sensitive information and intellectual property for financial gain or competitive advantage.

d. What method of attack was used?

Spear Phishing, Malware, and Social Engineering

e. What was the target and vulnerability used against the business?

Target: A technology company with valuable intellectual property.

Vulnerability: Exploited a weakness in the company's email system to launch a spear-phishing attack against employees.

f. How could this attack be prevented or mitigated?

Prevention: Implement multi-factor authentication.

Train employees on how to identify and avoid phishing emails.

Keep all software up to date with the latest security patches.

Mitigation: Deploy anti-virus and anti-malware software to detect and prevent malware infections.

Scenario 2:

a. Who is the attacker?

Ans: The Hacktivist Group

b. What organization/group is the attacker associated with?

Ans: A loosely affiliated group of politically or socially motivated hackers.

c. What is the motive of the attacker?

Ans: To advertise a social or political agenda and cause disruption or embarrassment to the targeted organization.

d. What method of attack was used?

DDoS attacks, website defacement, and social engineering

e. What was the target and vulnerability used against the business?

Target: A government agency responsible for controversial policies.

Vulnerability: Exploited a vulnerability in the agency's website to launch a DDoS attack, overwhelming the site with traffic and rendering it inaccessible.

f. How could this attack be prevented or mitigated?

Prevention: Use a content delivery network (CDN) or other DDoS protection services to help absorb traffic during a DDoS attack.

Train employees on how to identify and avoid social engineering attacks.

Mitigation: Deploy anti-DDoS and web application firewalls to detect and block malicious traffic.

Scenario 3:

a. Who is the attacker?

The Insider Threat

b. What organization/group is the attacker associated with?

The person who is working inside the organization and has all the access to an organization's systems and data abuses that access for personal gain or to cause harm to the organization.

c. What is the motive of the attacker?

Ans: To steal sensitive information or intellectual property, harm the organization or its employees, or gain personal benefit.

d. What method of attack was used?

Data theft, unauthorized access, and sabotage.

e. What was the target and vulnerability used against the business?

Target: A financial institution with sensitive customer data.

Vulnerability: An employee with privileged access stole confidential information by accessing the company's network from a remote location using a stolen password.

f. How could this attack be prevented or mitigated?

Prevention: Implement strict access controls and regularly audit employee access to sensitive data.

Mitigation: Use data loss prevention (DLP) tools to identify and block attempts to steal data.