Lab - Visualizing the Black Hats
Objectives
Research and analyze cyber security incidents.

In this lab, we will create three hypothetical cyber attackers, each with an organization, an attack, a motive. In addition, suggest a method by which an organization could prevent or mitigate the attack

Scenario 1:

Who is the attacker?

Attacker is from a hacking group specialzing in DDOS attacks.

What organization or group is the attacker associated with, if any?

The attacker is associated from a hacking group where all the group are trained or skilled specially for performing DDOS attacks.

What is the motive of the attacker?

Their motive is to extort money from businesses by threatening to continue the attack unless a ransom is paid.

What method of attack was used?

They have developed a network of compromised computers and use them to flood target websites or online services with overwhelming traffic, rendering them inaccessible to legitimate users

What was the target and vulnerability used against the business?

They exploited the vulnerabilities in their Intrusion Detection System (IDEs) and firewalls which will filter or monitors the incoming requests.

How could this attack be prevented or mitigated?

This attack can be prevented or mitigated by applying new set of rules on the incoming traffic and monitoring the threats and requests and processing accordingly.

Scenario 2:
Who is the attacker?

Attacker is from a state sponsored hacking group.

What organization/group is the attacker associated with?

The attacker is from a organization which is a state-sponsored hacking group focused on corporate espionage.

What is the motive of the attacker?

Their motive is to gain a competitive advantage by providing the stolen information to rival companies or state entities, thereby undermining their targets and potentially disrupting industries.

What method of attack was used?

Method of attack used was Advanced Persistent Threat (APT)

What was the target and vulnerability used against the business?

They employ sophisticated techniques, including zero-day exploits and social engineering, to gain unauthorized access to target organizations' networks

How could this attack be prevented or mitigated?

To prevent or mitigate this attack company or bussinesses could have applied more principles/rules and maintaining security principles and strong authentication needed.

Scenario 3:

Who is the attacker?
Attacker is from a group of Hacktivism.

What organization/group is the attacker associated with?

Attacker is from a organization which is a loosely affiliated group of hackers with a strong focus on hacktivism

What is the motive of the attacker?

Their motive is to expose wrongdoing, raise awareness about social justice issues, and exert pressure on their targets to change their practices.

What method of attack was used?
Hacktivist groups may use botnets or other techniques to launch coordinated DDoS attacks, disrupting the target's operations and causing inconvenience or financial loss

What was the target and vulnerability used against the business?

They target organizations or individuals whom they perceive as engaging in unethical activities or contributing to societal harm.

How could this attack be prevented or mitigated?

Strong authentication and access controls, Website security and DDOS mitigation