**Detection of network attacks and their mitigations techniques**

# **Introduction**

# The continuous development and extensive usage of the internet are making the world move towards digitalization. With the digitalization of the modern world, networks have become one of the essential components for communication. Nowadays, most public, private, and government-based organizations are using networks to transmit and store data. Networks and data are always at the radar of cybercriminals who perform different cyber security attacks to target various organizational network infrastructure and steal data. These cyber-attacks are not restricted to individuals or PCs, and attackers are additionally focusing on enormous companies, government workplaces, and national banks to prevent cybercriminals from network attacks, as discussed in [1]. Information security has become one of the leading parts of network infrastructure. To secure a network from potential attacks and evolving threats, different types of mitigation techniques are used. This research will use various attack mitigation techniques to protect the network from potential attacks and find out advanced persistent threats to our organization.

# **Reason for selecting the research topic**

# Cyber security attacks have become one of the worst nightmares for different organizations dealing with data and online communication, so detecting various cyber security attacks has been mandatory for digitalized organizations to save their data from cybercriminals. After the detection of cyber security attacks, its mitigation is also essential because once the attack is detected, its mitigation is the only way to neutralize the attack or threat possessed by organizations. It is essential to provide a successful framework to identify and shield attacks and keep yourself updated with the advancement in the domain of network security [2].

# **Aims**

This research aims to provide an organization with complete knowledge and understandability of cyber security attacks and their mitigation techniques in a real-life scenario.

# **Objectives**

* The objective of this research is to perform real-time cyber security network attacks and mitigate them using desired mitigation techniques.
* To perform different types of network-based cyber security attacks.
* Deployment of different tools for detection of cyber security attacks.
* Using different frameworks for mitigation of cyber security attacks.
* Monitor Network for Advance Persistent Threats.

# **Methodology**

# We will use two different virtual machines to launch attacks and detect cyber security attacks based on networks. An attacker or controller machine will be used for targeting the victim machine. Wireshark will be used for monitoring the network [3], and the behaviour of the network will be monitored to detect advanced persistent threats using Mitre Attack Matrix.

# **TimeLine**

Table 1 shows the timeline for the completion of the thesis.

Table 1: TimeLine for the Project

|  |  |  |
| --- | --- | --- |
| S.NO | MODULE | NUMBER OF DAYS |
| 1 | Gathering of Data | 3 |
| 2 | Literature Review | 2 |
| 3 | Implementation | 3 |
| 4 | Testing | 3 |
| 5 | Writing | 5 |

# **References**

1. Chowdhury, A. *Recent cyber security attacks and their mitigation approaches–an overview*. in *International conference on applications and techniques in information security*. 2016. Springer.

2. Wu, Y., et al., *Network attacks detection methods based on deep learning techniques: a survey.* 2020.

3. Goyal, P. and A. Goyal. *Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark*. in *2017 9th International Conference on Computational Intelligence and Communication Networks (CICN)*. 2017. IEEE.