**Network Security Monitoring Lab – Detecting Attacks in a controlled Environment**

***Introduction:***

I have created a simulation lab, where we have an attacker box and a victim machine. This lab demonstrates basic attacks performed on the victim machine. Basic attacks like network scanning, web vulnerability scanner, and downloading a malicious payload file to get the access to the machine. So while performing these attacks in the lab, we can monitor these logs via zeek and push the logs to an elastic agent to get an overview of what’s happening in the machine and the network.

Tool Used:

* Nmap, Nikto (for scanning)
* Zeek (for network monitoring)
* SIEM ( for monitoring logs)
* Sysmon( for detailed windows logs)
* Python(as a server)
* Parrot OS – attacker machine, Windows – victim machine, Ubuntu (for running Zeek)

***Lab Overview:***

This simulation lab is designed to demonstrate fundamental **offensive and defensive cybersecurity techniques** in a controlled environment. The lab setup includes:

* **Attacker Machine (Parrot OS)**, **Windows-based Victim Machine**, **Monitoring Infrastructure** powered by **Zeek** and the **Elastic Stack (ELK) (on Ubuntu)**

**Offensive Activities**

The attacker machine simulates common adversary behavior, including:

* **Network Scanning** using **Nmap**
* **Web Vulnerability Scanning** with **Nikto**
* **Payload Generation & Delivery**:
  + PowerShell-based Meterpreter payloads created via **msfvenom**
  + Remote code execution techniques mimicking real-world exploitation scenarios

These activities represent key phases of a typical cyber attack: **reconnaissance**, **exploitation**, and **post-exploitation**.

**Defensive Monitoring**

The network employs **Zeek** to monitor and log all network traffic, capturing:

* Connection attempts, HTTP requests, DNS queries, File downloads

These logs are forwarded in real time using the **Elastic Agent** to the **ELK Stack**:

* **Elasticsearch** stores and indexes the data, **Logstash** processes and enriches it, **Kibana** provides a visualization layer for real-time security analysis

**Outcome:**

* Understand attacker tactics and techniques
* Learn how to detect and analyze suspicious activity using modern security tools
* Gain hands-on experience in both offensive and defensive cybersecurity operations

***Abstract:***

This simulation lab demonstrates fundamental offensive and defensive cybersecurity practices in a controlled environment. It consists of an attacker machine, a Windows-based victim machine, and a monitoring infrastructure using Zeek and the Elastic Stack. The attacker machine performs various basic attacks such as network scanning with Nmap, web vulnerability scanning with Nikto, and the delivery of PowerShell-based Meterpreter payloads generated via msfvenom. These activities simulate real-world attacker behaviors including reconnaissance, exploitation, and remote code execution.

Zeek is deployed within the network to monitor and log traffic, providing visibility into the attack surface. All logs generated by Zeek—including connection attempts, HTTP requests, DNS lookups, and file downloads—are forwarded via the Elastic Agent to the ELK stack (Elasticsearch, Logstash, and Kibana). This enables real-time monitoring and visualization of both host and network activity within the lab environment.

***Conclusion:***

This simulation lab effectively bridges the gap between offensive and defensive cybersecurity by providing a hands-on environment where realistic attack techniques are executed and monitored in real time. By simulating common threats such as network scanning, web exploitation, and remote payload delivery, participants gain valuable insights into attacker behavior. Simultaneously, the integration of Zeek and the Elastic Stack demonstrates how modern security monitoring tools can be leveraged to detect, log, and analyze malicious activity across the network. This comprehensive setup not only reinforces key cybersecurity concepts but also builds critical skills necessary for identifying and responding to real-world threats.