**Torium Crescent Cybersecurity Lab - Project Overview**

**📌 Introduction**

The **Torium Crescent Cybersecurity Lab** is a **virtual enterprise network** designed to simulate a real-world corporate environment. This lab serves as a hands-on learning platform for cybersecurity professionals, system administrators, and ethical hackers. It provides an opportunity to explore **network security, system administration, penetration testing, and threat hunting** using industry-standard tools and best practices.

**🎯 Objectives**

This project aims to:

* Build and secure a **corporate-style IT infrastructure**.
* Deploy and configure **Windows Server** and **Ubuntu Server**.
* Implement a **next-generation firewall** using **OPNsense**.
* Explore **Active Directory, DNS, and File Sharing**.
* Implement **threat hunting** and **security monitoring** using **Elasticsearch**.
* Simulate **real-world cyber attacks** to test security defenses.

**🛠️ Technologies Used**

The project incorporates a wide range of technologies across different cybersecurity domains:

|  |  |
| --- | --- |
| **Category** | **Tools & Technologies** |
| **Networking & Firewall** | OPNsense, VLANs, Subnetting, pfSense |
| **Operating Systems** | Windows Server 2022, Ubuntu Server 22.04, Kali Linux |
| **Security Monitoring** | Elasticsearch, Kibana, Elastic Security, Zeek, Suricata |
| **Active Directory & Management** | Windows Server AD, DNS, File Shares, Group Policy |
| **Pentesting & Red Teaming** | Metasploit, Nmap, BloodHound, Mimikatz, Burp Suite |