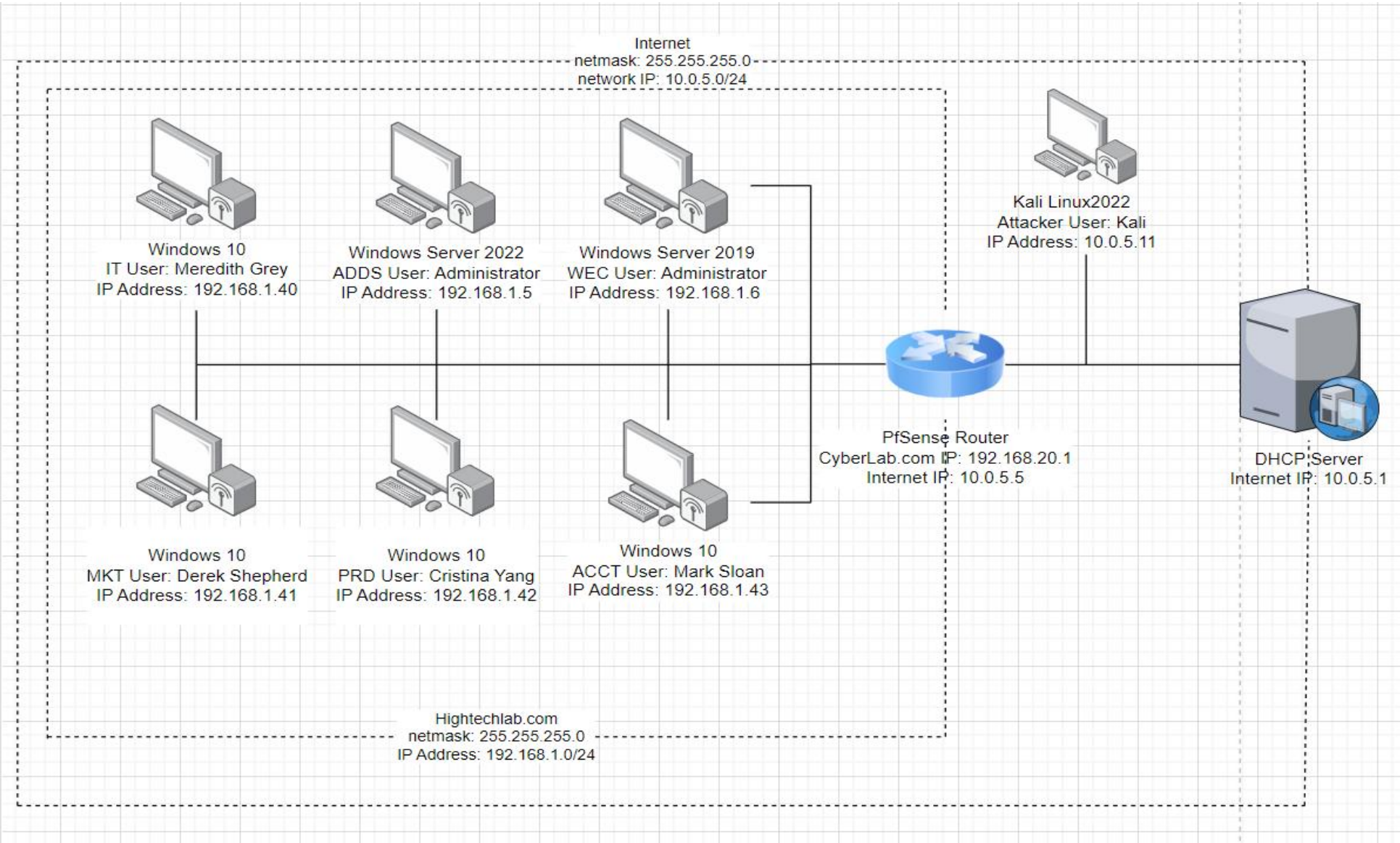
Open Threat Research for a Small Business Network

Pooja Bandla

Introduction – Network Diagram



Goal

- **Introduction to Network Security Importance**:
  - Network security is vital in today's digital landscape due to the increasing reliance on interconnected systems for various business operations.
  - Businesses depend on networks for data storage, communication, and transactions, making them prime targets for cyber attacks.
  - Cyber threats continuously evolve, posing risks such as data breaches, financial losses, and operational disruptions.

Goal

- **Significance of Enhancing Security and Resilience:**
  - Enhancing network security is crucial for protecting valuable assets, including customer data, intellectual property, and financial information.
  - Improving resilience ensures that businesses can withstand and recover from cyber attacks, minimizing the impact on operations and reputation.
- **Challenges in Network Security:**
  - Cybercriminals employ sophisticated tactics to exploit vulnerabilities in network infrastructures.
  - Attacks range from malware and phishing to sophisticated hacking techniques, threatening the confidentiality, integrity, and availability of sensitive data and resources.

Project Goal:

- **Enhancing Security and Resilience**:
  - The primary objective of this project is to enhance the security and resilience of business networks.
  - Through the implementation of innovative techniques and best practices, I aim to fortify network defenses and mitigate potential risks.
  - Ultimately, my goal is to contribute to the creation of a safer and more secure digital environment for organizations and users.

Objectives

Network Configuration

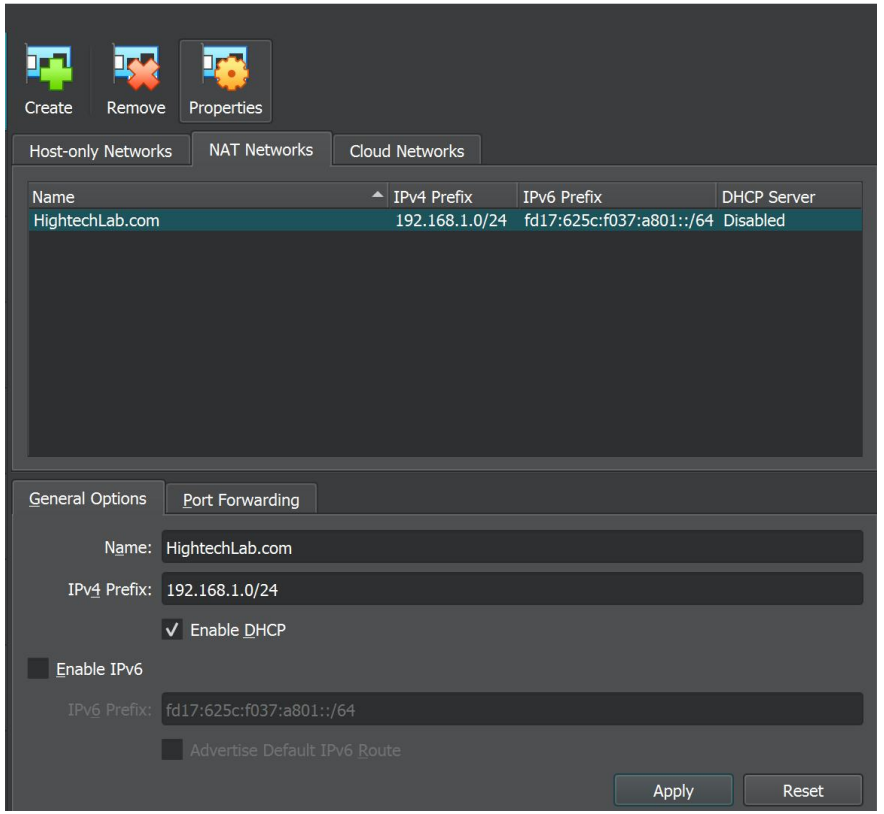
System Deployment and Configuration

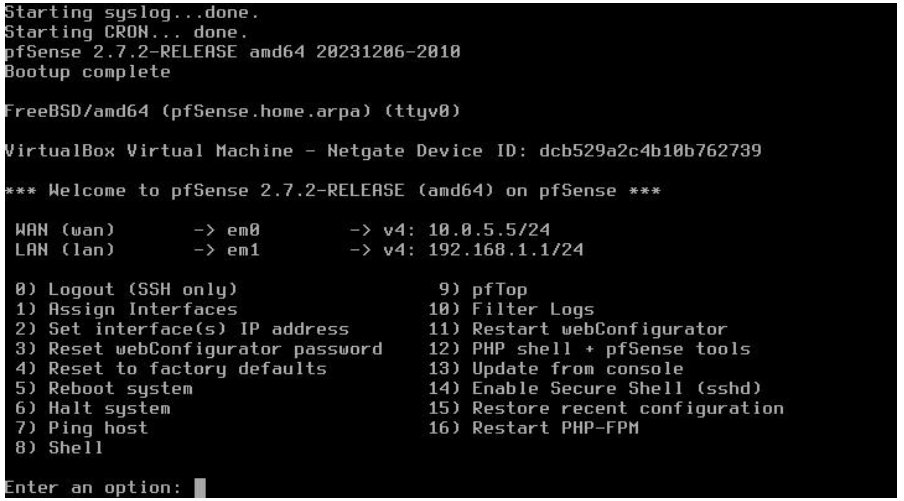
. Security Enhancement

Threat Simulation and Mitigation

Approach - Network Configuration

- **Virtual Networking Setup:**
  - Utilized VirtualBox 7.10.14.
  - Configured "**Intel PRO/1000 MT Desktop" adapters**.
  - Choose NAT Network for the "**HightechLab.com**" network (**192.168.1.0/24**).
  - Enabled **DHCP**.
- **PfSense Router:**
  - Configured PfSense with WAN (**10.0.5.5**) and LAN (**192.168.1.1**) IPs..
- **Kali Linux Setup**
  - Installed Kali Linux as an **adversary node**.
  - Configured for "internet" network.
  - Verified connectivity with PfSense using ping.





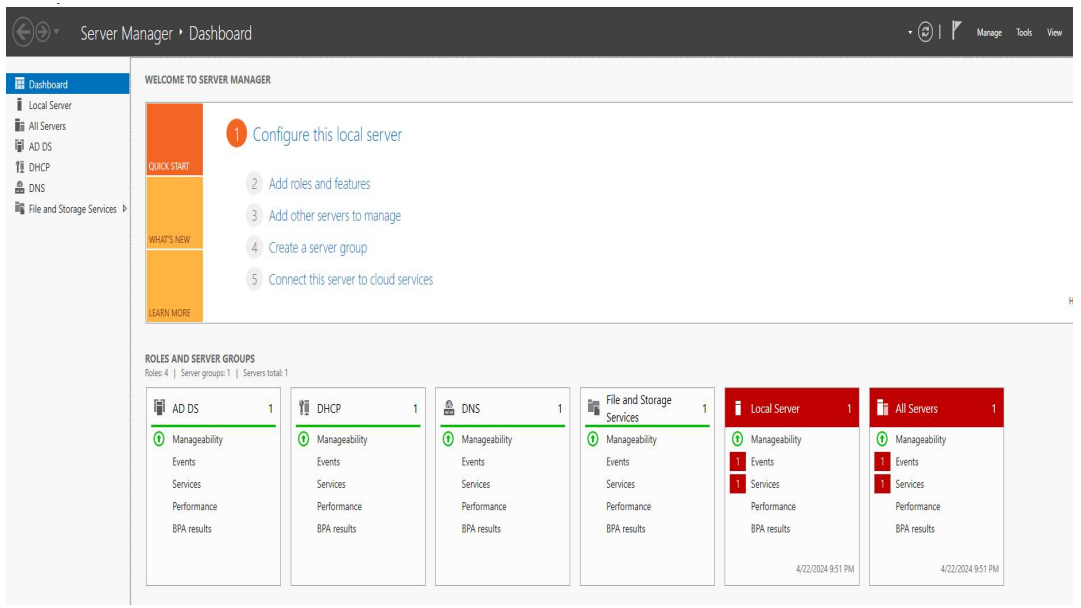
Approach - System Deployment and Configuration

- **Windows Server 2022 Setup:**
  - Configured general settings and network adapter to **NAT network "Hightechlab.com"**.
  - Installed **Windows Server 2022**, designated as Domain Controller for "Hightechlab.com".
  - Installed **VirtualBox Guest Additions** for enhanced features.

- **Installing ADDS, DHCP, and DNS Roles:**
  - Configured IP addressing for business network design.
  - Installed roles using **Server Manager**, encountered and resolved static IP error.
  - Deployed **DHCP scope** and created organization units and user accounts.

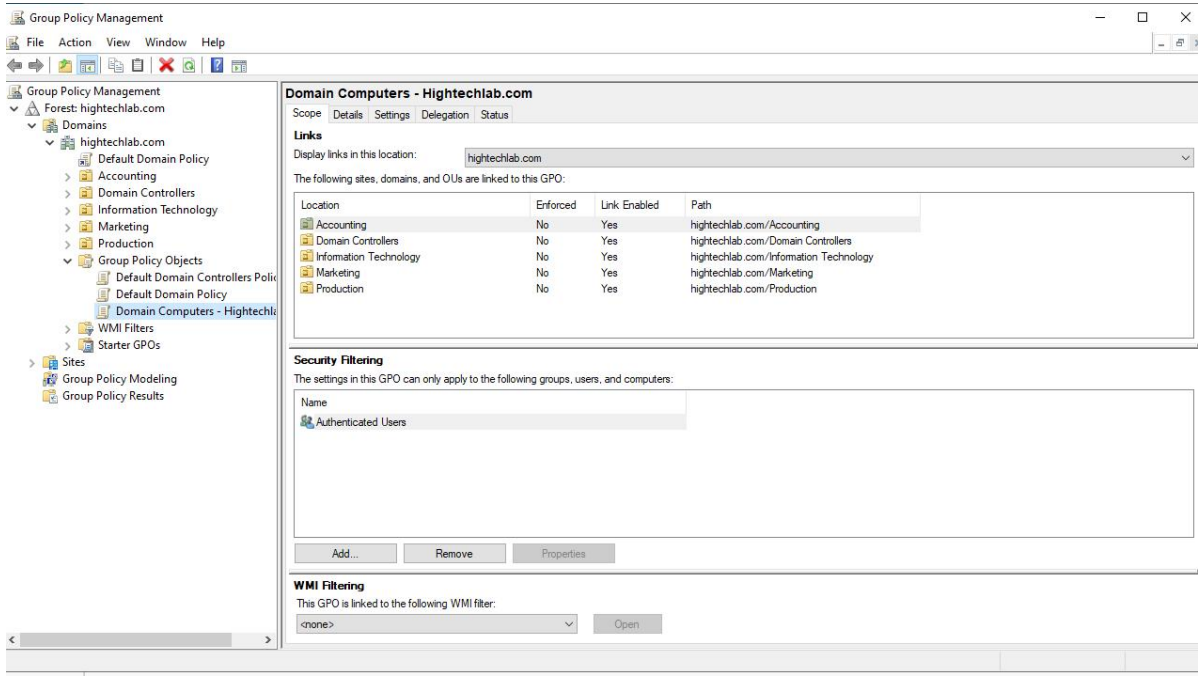
Approach - System Deployment and Configuration

- **Creating DHCP Scope**:
  - Defined IPv4 scope under "**dc01.hightechlab.com**" with a specific range.
  - Configured DHCP settings and **disabled NAT network DHCP server.**
- **Creating Organization Units and User Accounts:**
  - Established **organizational units and user accounts** within the "Hightechlab.com" domain.
  - Created user accounts for **IT, Marketing, Production, and Accounting departments**



Approach - Security Enhancement

- **Creating Group Policy Object (GPO) for Window Domain:**
  - Defined **GPOs** to enforce security policies centrally.
  - Configured **Windows update services, security settings, and event logging.**
- **Windows Updates Services:**
  - ConfiguAred automatic update settings and download options.
- **Security Settings:**
  - Enabled **real-time protection, behavior monitoring, and Windows Defender Smart Screen settings**.



Approach - Security Enhancement

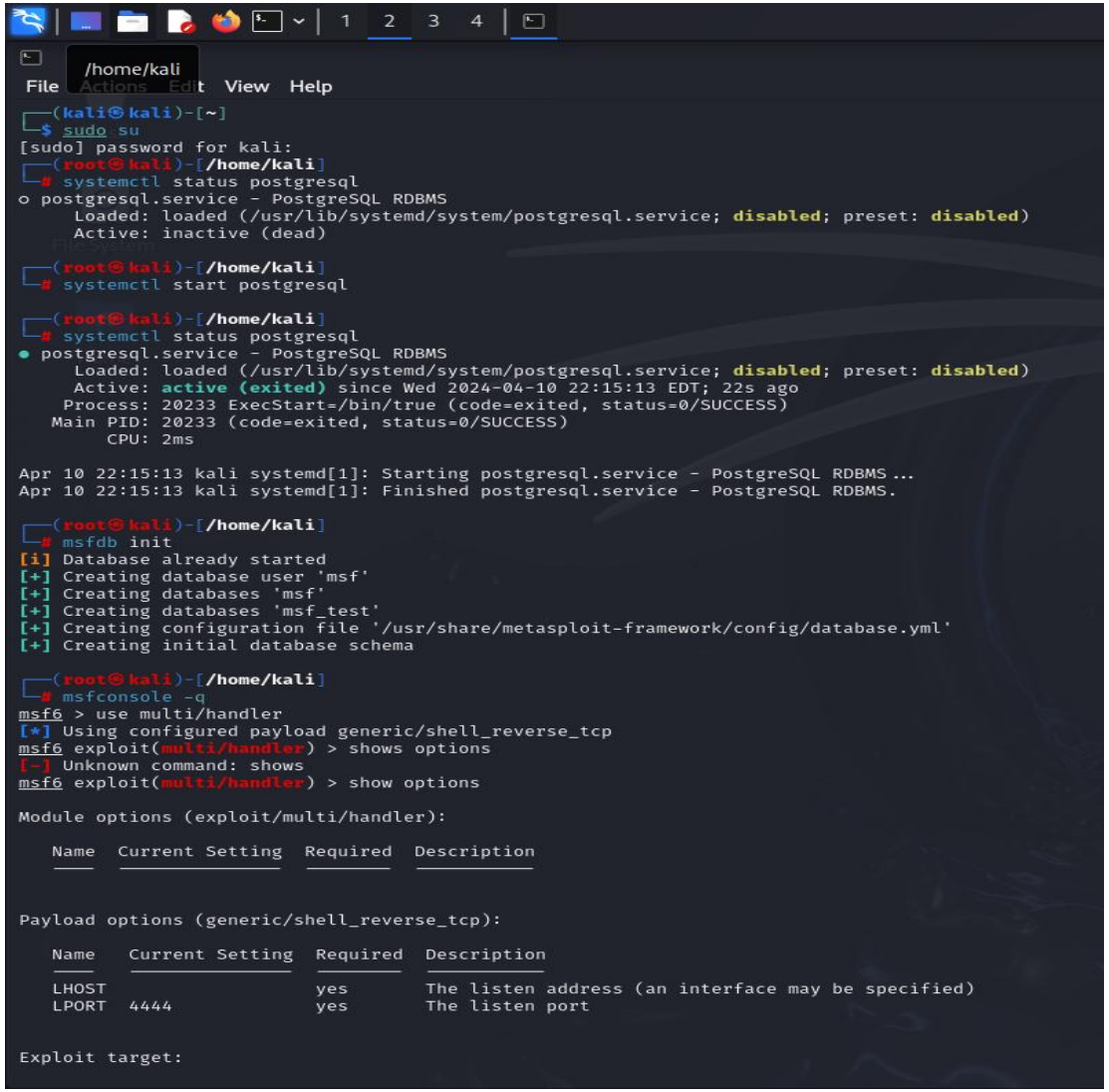
- **Security Logging:**
  - Set event log file sizes and enabled detailed tracking for security purposes.
  - Configured PowerShell script block logging and other **advanced audit policies.**
- **Installing Sysmon in Windows System:**
  - Installed **Sysmon** to monitor and log system activity.
  - Set Sysmon log size to the maximum for comprehensive event logging
- **Execution of OS Credential Dumping: LSASS Memory Technique:**
  - Simulated **OS credential dumping** technique using Kali Linux and Windows 10 devices.
  - Demonstrated steps for payload creation, execution, and mitigation strategies.
  - Discussed relevant tactics and techniques associated with credential access and privilege escalation.

Approach - Threat Simulation And Mitigation

- **Access the Credential Material using OS Credential Dumping: LSASS Memory Technique:**
  - Utilized a network environment with Pfsense Router, Kali Linux, and Windows 10 devices.
  - Executed **LSASS memory technique** as an admin to access credential material.
- **Implemented tactic and technique:**
  - **Resource Development** (**TA0042**): Developed tools and procedures for malicious activities.
  - **Execution** (**TA0002**): Ran malicious code on the victim system, targeting LSASS.
  - **Discovery** (**TA0007**): Gathered information about the target environment.
  - **Privilege Escalation** (**TA0004**): Escalated privileges to access credential material.
  - **Defense Evasion** (**TA0005**): Attempted to evade detection.
  - **Credential Access** (**TA0006**): Accessed credentials stored in LSASS memory.

Approach - Threat Simulation And Mitigation

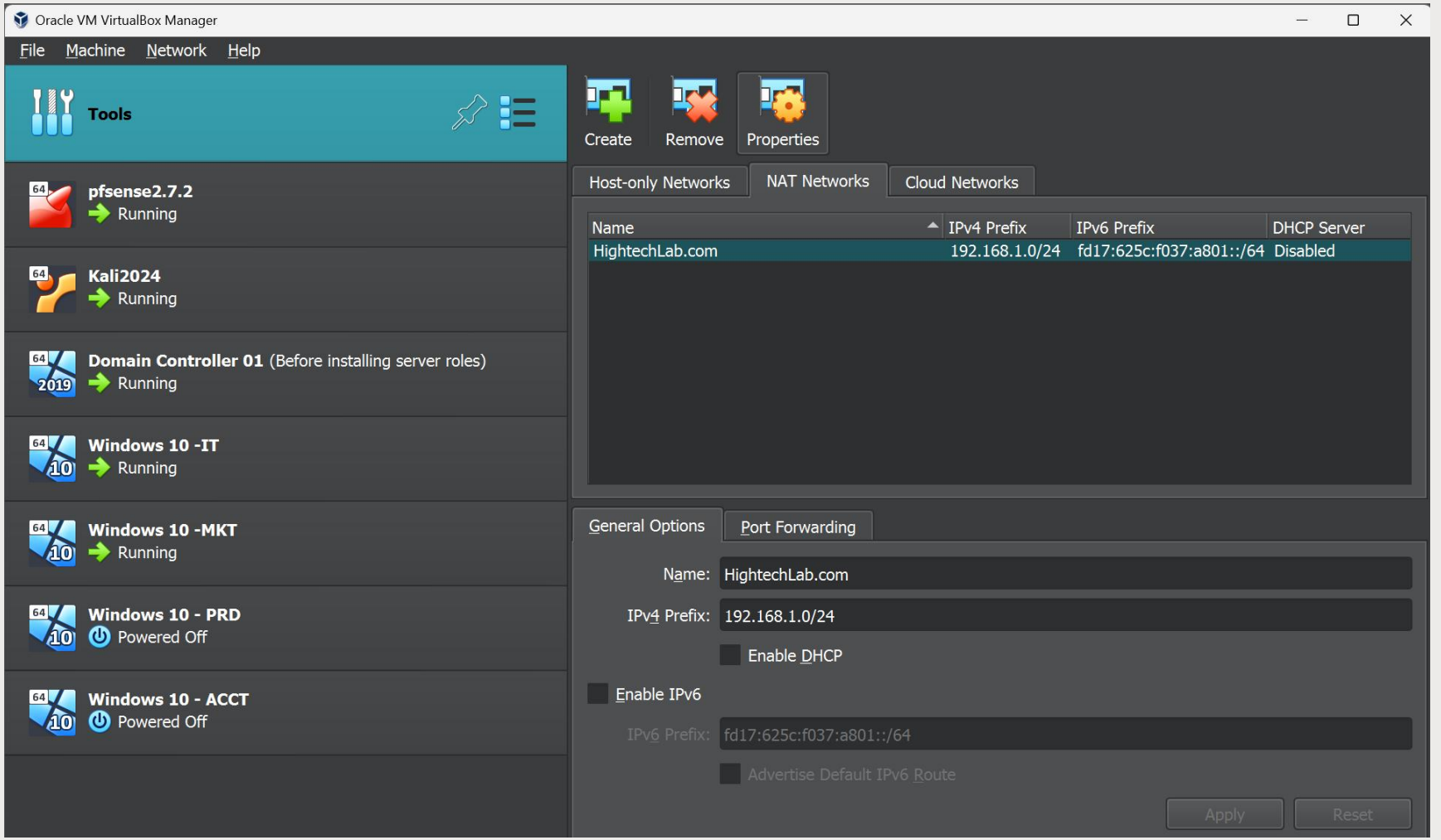
- **Execution of OS Credential Dumping: LSASS Memory Technique:**
  - Created payload in Kali Linux and made it available through a **fake website**.
  - Attempted to **download payload** on Windows 10 device but faced security settings error.
  - Resolved error and ran payload as administrator, **encountered blocking by Pfsense firewall**.
  - Demonstrated tactics and techniques for accessing credentials in a simulated environment.



Approach - Threat Simulation And Mitigation

- **Challenges Faced:**
  - Initial **download error** due to security settings on Windows 10 device.
  - Blocking of **reverse handling** process by Pfsense firewall, hindering communication.
- **Conclusion:**
  - Successful **execution of LSASS memory** technique demonstrates potential security vulnerabilities.
  - Identified challenges highlight the importance of robust security measures and mitigation strategies.

Result


Oracle VM VirtualBox Manager
File
Machine
Network
Help
Tools
pfsense2.7.2
Running
Kali2024
Running
Domain Controller 01 (Before installing server roles)
Running
Windows 10 -IT
Running
Windows 10 -MKT
Running
Windows 10 - PRD
Powered Off
Windows 10 - ACCT
Powered Off
Create
Remove
Properties
Host-only Networks
NAT Networks
Cloud Networks
Name
IPv4 Prefix
IPv6 Prefix
DHCP Server
HightechLab.com
192.168.1.0/24
fd17:625c:f037:a801::/64
Disabled
General Options
Port Forwarding
Name:
HightechLab.com
IPv4 Prefix:
192.168.1.0/24
Enable DHCP
Enable IPv6
IPv6 Prefix:
fd17:625c:f037:a801::/64
Advertise Default IPv6 Route
Apply
Reset

Conclusion:

- **Successful achievement of objectives:** Enhanced network configuration, security, and resilience.
- **Infrastructure fortification:** Establishment of NAT network, deployment of PfSense routers, and implementation of security measures (GPOs, Sysmon).
- **Insightful simulations:** OS credential dumping techniques provided valuable vulnerability insights.
- **Overcoming challenges:** Addressed DHCP server errors and firewall restrictions.
- **Evaluation focus:** Adherence to objectives, effectiveness in security enhancement, and resilience impact.
- **Ongoing refinement:** Continuous improvement for a safer digital ecosystem.
- **Contribution to network security practices:** Lay foundation for further research and development.
- **Significance encapsulation:** Advances in network security practices, encapsulating project's importance.

Thank you!

Any Questions?