Home Lab:

Objective:

- Build an isolated, multi-tier lab environment using Kali Linux, pfSense, a web-facing server (DMZ), Metasploitable, and a Windows Domain Controller
- Simulate a realistic external attack path: **web exploitation → firewall bypass via pivoting → internal compromise**
- Establish system, network, and application **baselines** prior to exploitation
- Perform controlled exploitation and lateral movement using **free offensive tools**
- Capture and preserve logs and artifacts **before and after exploitation**
- Detect attacker activity using **free defensive tooling** (Sysmon, Hayabusa, RITA, pfSense logs, Wireshark)
- Compare baseline versus post-exploitation data to identify anomalies and attacker behavior
- Develop and document detection logic and use cases based on observed telemetry
- Reuse the same environment for a future **SIEM and detection engineering lab**
- Present the lab with clear objectives, evidence, and defensive mitigations in a **GitHub portfolio**

Scope:

- Lab environment is hosted entirely on **VMware** using isolated virtual networks
- Systems in scope:
    - Kali Linux (attacker)
    - pfSense firewall
    - Web-facing Linux server (DMZ)
    - Mr. Robot vulnerable VM
    - Metasploitable (internal Linux host)
    - Windows Server Domain Controller
- Attacks are limited to intentional exploitation of vulnerable services and applications within the lab
- Pivoting and lateral movement are performed only through compromised hosts
- Active Directory activity is limited to enumeration and credential dumping for detection purposes
- Logging, monitoring, and analysis are performed using **free tools only**
- Baseline and post-exploitation data collection is limited to artifacts generated within the lab
- No external networks, real user data, or production systems are involved

Tools:

Offensive Security / Attack

- Kali Linux
- Metasploit Framework
- Nmap
- Burp Suite (Community)
- Netcat
- Chisel (pivoting / tunnelling)
- SSH (port forwarding)

- Vulnerable Web Applications (DVWA, Juice Shop)
- Metasploitable2
- Mr. Robot vulnerable VM
- PowerShell (offensive usage)
- Bash (offensive usage)
- Hashcat
- Mimikatz

Defensive Security / Detection

- pfSense (firewall & logging)
- Sysmon
- Hayabusa
- RITA
- Wireshark
- Zeek
- Elastic / OpenSearch (free SIEM)
- Winlogbeat / Filebeat
- RegShot
- Redline
- Volatility (memory forensics)
- PowerShell (defensive / hunting)
- Bash (analysis / automation)

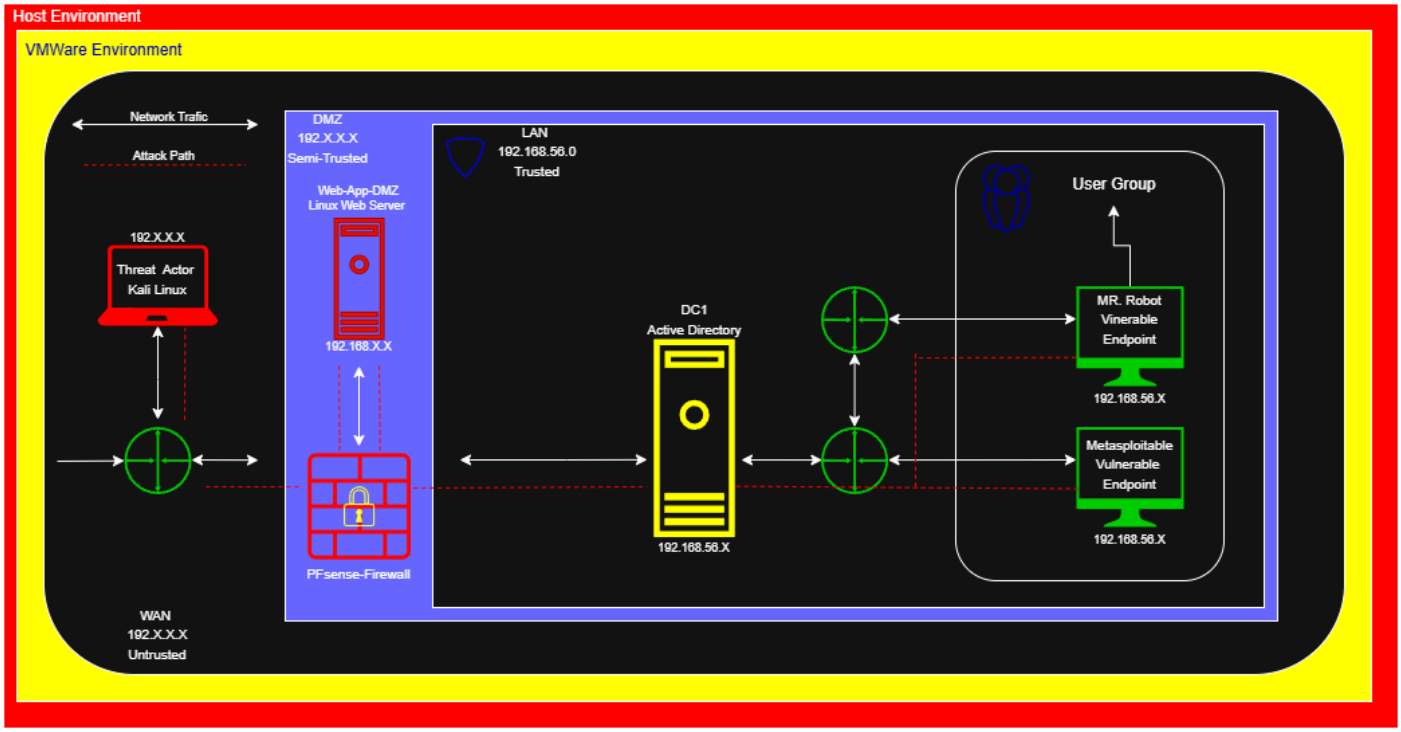
Special Considerations

- All virtual machines are hosted in **VMware** using isolated virtual networks
- Firewall rules and segmentation are intentionally designed to allow misconfiguration scenarios for pivoting and detection testing
- System, network, and application baselines are captured **before exploitation**
- Time synchronization (NTP) is consistent across all systems to support accurate event correlation
- Logging is enabled and preserved on all systems prior to attack execution
- Offensive activity is conducted in a controlled manner to generate realistic, reproducible telemetry
- Exploitation and post-exploitation actions are limited to techniques that produce observable artifacts
- Sensitive outputs (e.g., credential hashes) are sanitized before documentation or publication
- The environment is designed for reuse across both **attack simulation** and **SIEM/detection engineering** labs
- All tools and platforms used are **free and open source**

Success Criteria

- Baseline data is successfully captured across hosts, network, and applications
- Exploitation results in measurable changes from the baseline
- Pivoting from a web-facing system to internal assets is achieved
- Credential material is obtained from the Domain Controller in a controlled manner
- Defensive tools detect and surface attacker activity
- Before-and-after differences can be clearly explained and documented
- The environment can be reused for a standalone SIEM and detection lab

Conceptual Lab Design:



Protocols & Ports:

Category	Protocols
Web/DMZ	HTTP/HTTPS, DNS
Remote/Pivot	SSH, Reverse TCP, SOCKS
Internal/AD	SMB, NetBIOS, LDAP/LDAPS, Kerberos, RPC, WinRM, NTLM, DCSync
Recon	ICMP, ARP, TCP/UDP scans
Logging	Syslog, Beats
SIEM	HTTP/HTTPS (APIs)
Infra	NTP, DHCP
Optional	FTP, SQL, RDP