**1. Introduction**

This project delivers a complete **Active Directory (AD) home lab** using Oracle VirtualBox, mirroring enterprise network environments to support cybersecurity research, monitoring, and defense workflows[[2]](#wu8q1eg8xtrf). AD labs are essential for Security Operations Center (SOC) staff and cybersecurity practitioners because almost all organizations rely on AD for user management, authentication, and authorization, making it a frequent target during security incidents[[1]](#4zd9stoh04zy)[[3]](#x886nts88iiz). Simulating attacks and blue team responses in such a lab helps analysts understand attacker tactics, enhance detection, and strengthen real-world defensive postures[[2]](#wu8q1eg8xtrf).

**2. Lab Architecture & Design**

**Network Topology**

The lab uses a segmented internal network as illustrated in the diagram[[4]](#fz8asj9gsxfg):

* **Domain Controller (AD)**: Controls authentication, user/group management, and Group Policy Objects (GPOs); core security component.
* **Windows 10 Client**: Represents a typical user workstation, with **Sysmon** for deep logging and **Atomic Red Team** for attack simulation.
* **Splunk Server**: Centralizes all logs and serves as the SIEM platform for alerting, dashboarding, and forensics[[5]](#nzrslvq3xfto).
* **Kali Linux**: Acts as the attacker, enabling penetration testing and adversary emulation.

**IP Addressing Scheme**

|  |  |  |
| --- | --- | --- |
| Component | Role | IP Address |
| Domain Controller | AD + Sysmon + Forwarder | 192.168.10.7 |
| Splunk Server | SIEM | 192.168.10.10 |
| Windows 10 Client | Workstation/Sim Attacker | DHCP (dynamic) |
| Kali Linux | Attacker | 192.168.10.250 |

The network subnet is **192.168.10.0/24** with routing and DHCP managed by the DC[[2]](#wu8q1eg8xtrf)[[6]](#v8tj3k46emdj).

**3. Tools & Technologies Used**

* **Splunk Universal Forwarder**: Transfers endpoint logs to the Splunk SIEM[[5]](#nzrslvq3xfto)[[7]](#h1x040cmkohp).
* **Sysmon**: Captures detailed endpoint activity - process creations, file changes, and network connections[[5]](#nzrslvq3xfto).
* **Atomic Red Team**: Executes MITRE ATT&CK technique simulations, helping analysts practice threat detection[[8]](#hdv3xhcf549c).
* **Kali Linux**: Comprehensive adversary toolkit; used for attack scenarios such as brute force, privilege escalation, and lateral movement[[9]](#yhltob6dz88c).

**4. Implementation Steps**

**Domain Controller Setup**

* Installed Windows Server, configured static IP, and set up **DEV.local** domain.
* Created OUs: Employees, Computers, Servers, Groups.
* Automated user creation with PowerShell scripts for scale and realism[[10]](#6a17mig0hcm2)[[11]](#vo1bihbjqyyh).

**Windows 10 Domain Join**

* Configured DHCP and DNS to use DC’s IP.
* Joined the workstation to the DEV.local domain using domain admin credentials[[12]](#slanfcp4k38k).

**Sysmon & Splunk Forwarder**

* Deployed Sysmon with a tuned config[[5]](#nzrslvq3xfto).
* Installed Splunk Universal Forwarder, pointed to Splunk server IP.

**Splunk Server**

* Configured data ingestion ports, set up dashboards for endpoint security monitoring[[13]](#m4lkkdd4xaar)[[5]](#nzrslvq3xfto).

**Kali Linux Setup**

* Assigned static IP, ensured network reachability.
* Installed standard attacker toolset: nmap, Metasploit, Hydra, etc[[14]](#w4wp6zuqhhis).

**5. Attack Simulation**

**MITRE ATT&CK Mapped Scenarios**

* **Brute force / Password spraying**: Used Hydra and CrackMapExec for credential attacks (T1110)[[8]](#hdv3xhcf549c).
* **Privilege escalation attempts**: Used mimikatz, MSF local exploits (T1068).
* **Lateral movement**: Pass-the-Hash with psexec, SMB exploitation (T1075/T1021).
* **Persistence**: Created scheduled tasks and modified registry keys for backdoors (T1053/T1112).

**Example Tools/Commands**

* Hydra: hydra -l admin -P passwords.txt 192.168.10.7 smb
* CrackMapExec: cme smb 192.168.10.7 -u users.txt -p passwords.txt
* Metasploit: exploit/windows/local/ms16\_032

**6. Detection & Monitoring**

**Log Capture in Splunk**

* Universal Forwarder sent Sysmon logs to Splunk[[5]](#nzrslvq3xfto)[[7]](#h1x040cmkohp).
* Dashboards visualized:
  + Login failures by account/IP
  + Execution of uncommon binaries/processes
  + Registry or scheduled task anomalies

**Key Indicators of Compromise (IoCs)**

* Multiple failed logins from Kali’s IP
* Process creation with suspicious parent/child relationships (e.g., powershell.exe invoking mimikatz)
* Registry writes to autostart locations
* Creation of unfamiliar scheduled tasks

Screenshots included for Splunk dashboard highlights.

**7. Blue Team Response**

**Detection Queries**

* Detect brute force:  
  index=sysmon EventCode=4625 | stats count by AccountName, src\_ip
* Identify lateral movement:  
  index=sysmon CommandLine="\*psexec\*" OR CommandLine="\*wmic\*"
* Persistence:  
  index=sysmon EventCode=13 RegistryPath="\*Run\*" OR EventCode=1 CommandLine="schtasks\*"

**SOC Automation**

* Alerts configured for suspicious process tree or abnormal login patterns.
* Potential for Splunk to trigger automated responses (disable account, block IP).

**Mitigations**

* Password policies enforced via GPO.
* Block brute force at the network layer.
* Scheduled task and registry monitoring to detect persistence.

**8. Challenges Faced & Solutions**

**Network Issues**

* NAT and internal VirtualBox adapters required careful setup for correct routing[[15]](#3caclf83tfct).
* Resolved by ensuring correct adapter bindings in each VM.

**Time Sync & Log Ingestion**

* AD Kerberos logins sensitive to time drift; fixed by enabling NTP sync on all systems.

**Sysmon Config Tuning**

* Reduced noise by filtering benign processes and focusing on suspicious behavior patterns[[5]](#nzrslvq3xfto).

**9. Key Learnings & Takeaways**

* AD labs grant hands-on insight into real-world attacker TTPs.
* MITRE ATT&CK mapping makes detection practical and actionable.
* Centralized logging in Splunk enables effective monitoring, triage, and fast response, foundational for SOC operations[[3]](#x886nts88iiz).

**10. Future Enhancements**

* Integrate SOAR tools (TheHive + Cortex) for auto-response workflows.
* Add more endpoints (e.g., Linux servers, additional Windows clients).
* Expand attack surface—ransomware detonation, phishing simulation, Kerberoasting scenarios for added realism.

**11. Conclusion & Demo**

This project demonstrates the full SOC lifecycle: attack simulation, detection, alerting, and blue team response, mirroring what happens in real enterprises. A demo sequence might show the attacker trigger an incident, logs flow to Splunk, an IoC is detected, and an automated mitigation action proves blue team efficiency.

This end-to-end approach is vital for building practical SOC expertise and is highly valued in hackathon/judging settings because it shows a complete understanding from incident generation to security response[[2]](#wu8q1eg8xtrf)[[3]](#x886nts88iiz)[[1]](#4zd9stoh04zy).

⁂

1. <https://blog.davidvarghese.dev/posts/building-home-lab-part-6>

1. <https://activedirectorypro.com/create-active-directory-test-environment/>

1. <https://dev.to/adamkatora/building-an-active-directory-pentesting-home-lab-in-virtualbox-53dc>

1. <https://hurricanelabs.com/splunk-tutorials/deploying-the-splunk-universal-forwarder-on-windows/>

1. <https://www.kindsonthegenius.com/how-to-setup-active-directory-domain-with-virtualbox-and-join-computers-part-2/>

1. <https://help.splunk.com/en/splunk-enterprise/forward-and-process-data/universal-forwarder-manual/9.4/install-the-universal-forwarder/install-a-windows-universal-forwarder>

1. <https://github.com/redcanaryco/invoke-atomicredteam/wiki/Installing-Invoke-AtomicRedTeam>

1. <https://viehgroup.com/how-to-enable-the-network-in-kali-linux-virtual-box/>

1. <https://www.archy.net/automated-random-user-creation-script-for-active-directory/>

1. <https://activedirectorypro.com/create-bulk-users-active-directory/>

1. <https://stackoverflow.com/questions/35745516/joining-windows-10-virtualbox-image-to-an-active-directory-domain>

1. <https://help.splunk.com/splunk-enterprise/get-started/install-and-upgrade/9.2/install-splunk-enterprise-on-windows/install-on-windows-using-the-command-line>

1. <https://www.youtube.com/watch?v=6WKuY43Zel8>

1. <https://msftwebcast.com/2020/02/configure-windows-server-2019-as-a-nat-router.html>