Cybersecurity Lab Setup Guide

Active Directory + Splunk server + kali linux

Part 1 - Objective

Set up a virtualized cybersecurity lab using VMware Workstation with multiple VMs for hands-on security testing, monitoring, and attack simulation. The lab includes configuring Windows 10, Windows Server 2022, Kali Linux, and Ubuntu Server machines, network setup, installing Splunk for log analysis, setting up Active Directory, and performing brute force attacks using Hydra.

Part 2 - IP Address Scheme

Machine	IP Address	Notes
Splunk Server (Ubuntu)	192.168.20.20	Log collection and analysis
Windows Server 2022	192.168.20.21	Active Directory Domain Controller
Windows 10 (Target)	192.168.20.100	Target machine for attacks
Kali Linux (Attacker)	192.168.20.50	Attack machine using Hydra

---

Part 3 - VM Installation on VMware Workstation

1. **Install VMware Workstation Player or Pro.**
   https://www.vmware.com/products/workstation-player.html

2. **Create the following VMs:**

   - **Windows 10**: 4 GB RAM, 50 GB disk
   - **Kali Linux**: VMware image from kali.org
   - **Windows Server 2022**: With GUI, 4 GB RAM, 50 GB disk

- **Ubuntu Server 22.04**: 8 GB RAM, 2 CPUs, 100 GB disk

Part 4 - Network Configuration in VMware

1. **Create a custom VMnet (e.g., VMnet2):**
   - Use the **Virtual Network Editor**
   - Set as **Host-Only** or **Custom**, with subnet `192.168.20.0/24`
2. **Attach all VMs to this network:**
   - VM > Settings > Network Adapter > Custom: VMnet2
3. **Assign Static IPs to VMs**
   - Windows 10: `192.168.20.100`
   - Windows Server: `192.168.20.21`
   - Ubuntu Server: `192.168.20.20`
   - Kali Linux: `192.168.20.50`
   - Subnet Mask: `255.255.255.0`
   - Gateway: `192.168.20.1`
   - DNS: `8.8.8.8`

Part 5 - Install Splunk on Ubuntu Server

1. Download the `.deb` package from splunk.com.
2. Transfer the file to the VM using shared folders or SCP.
3. Install Splunk, accept the license, and set up an admin account.

4. Start Splunk and enable boot-start.
5. Access via: `http://192.168.20.20:8000`

Part 6 - Configure Windows Machines

1. **Install Splunk Universal Forwarder** on Windows 10 and Windows Server.
    - Configure it to forward logs to `192.168.20.20:9997`
2. **Install Sysmon** using Olaf Hartong's config
3. **Configure `inputs.conf`** to monitor Application, Security, System, and Sysmon logs
4. Restart Splunk Forwarder service

Part 7 - Setup Active Directory on Windows Server 2022

1. Install **Active Directory Domain Services** via Server Manager
2. Promote to Domain Controller for forest: `demodomain.local`
3. Open **Active Directory Users and Computers**
4. Create **Organizational Units (OUs):**
    - **Security**
    - **Engineering**
5. Create these users:

First Name	Last Name	Username	OU
Ethan	Robot	erobot	Security
Jon	Snow	jsnow	Engineering

6. Assign secure passwords and uncheck “User must change password at next logon”

Part 8 - Join Windows 10 to Domain

1. Set Preferred DNS to `192.168.20.21`
2. Go to **System > Rename this PC > Change settings**
3. Join the domain: `demodomain.local`
4. Restart and log in with domain users: `erobot` or `jsnow`

Part 9 - Enable Remote Desktop on Windows 10

1. Go to **This PC > Properties > Remote Settings**
2. Enable **Allow Remote Connections**
3. Add **domain users** `erobot` and `jsnow` to **Remote Desktop Users**
4. Ensure firewall allows RDP connections

Part 10 - Brute Force Attack with Hydra (Kali Linux)

1. Assign Kali static IP: `192.168.20.50`

Install Hydra:

bash
CopyEdit

```
sudo apt update && sudo apt install hydra
```

2.

Prepare a password list:

bash
CopyEdit
```
head -n 20 /usr/share/wordlists/rockyou.txt >
~/Desktop/passwords.txt
```

3.

Run Hydra brute-force RDP attack:

bash
CopyEdit
```
hydra -l jsnow -P ~/Desktop/passwords.txt rdp://192.168.20.100
```

4.
    - If one of the passwords matches, Hydra will report success.

Part 11 - Analyze Activity in Splunk

1. Login to Splunk Web on `http://192.168.20.20:8000`
2. Check for multiple failed login attempts (Event ID 4625)
3. Look for success logins (Event ID 4624) immediately after
4. Use time correlation and username filters (e.g., `jsnow`, `erobot`) to trace brute-force events

---

Part 12 - Summary

You now have a working lab with:

- **VMware Workstation** networking via VMnet

- **Active Directory domain**: `demodomain.local`
- **User accounts**: `erobot` (Security) and `jsnow` (Engineering)
- **Log monitoring** with Splunk
- **Brute-force testing** using Hydra

This setup simulates a real-world corporate network for practicing blue team and red team skills in a safe environment.