Lab setup

**Updated Complete Lab Summary (No Windows 7, Added Windows 10 Details)**

**1. Virtual Machines Setup (VMware Workstation 2019)**

* Created multiple VMs:
  + **Windows Server 2019** (Domain Controller)
  + **Windows 10** (Client machine)
  + Various Linux distros planned later (Kali, BlackArch, etc.)
* Network adapters configured as **NAT or Bridged** depending on connectivity needs.
* Disk storage dynamically allocated.

**2. Windows Server 2019 Setup**

* Installed Windows Server 2019 on VM.
* Set static IP for server:
  + **IP Address:** 192.168.138.2
  + **Subnet Mask:** 255.255.255.0
  + **Default Gateway:** [Your router IP or host machine IP in NAT mode]
  + **Preferred DNS Server:** 192.168.138.2 (itself, as DNS server)
* Installed and configured Active Directory Domain Services (AD DS).
* Created domain: lab.local.
* Installed and configured DNS Server to handle domain name resolution.

**3. Windows 10 Client VM Setup**

* Configured Windows 10 VM with static IP to be on the same subnet as Windows Server:
  + **IP Address:** 192.168.138.10
  + **Subnet Mask:** 255.255.255.0
  + **Default Gateway:** Same as server’s gateway (router IP or host machine IP)
  + **Preferred DNS Server:** 192.168.138.2 (pointing to domain controller DNS)
* Joined Windows 10 VM to the domain lab.local successfully after correcting DNS settings.
* Verified network connectivity:
  + Able to ping Windows Server (192.168.138.2).
  + Network communication confirmed between server and Windows 10 client.

**4. Network Configuration**

* Ensured all VMs (Windows Server, Windows 10 client) are on the **same subnet (192.168.138.x)**.
* DNS settings on clients pointed to the server IP for domain join and resolution.
* Network adapter type chosen (NAT or Bridged) to allow communication.
* Initial DNS misconfiguration fixed to allow domain join.

**5. Domain Controller & DNS Details**

* Windows Server runs as domain controller for lab.local.
* DNS service on Windows Server resolves internal domain names.
* Clients use server as primary DNS for domain services.

**6. Troubleshooting**

* DNS misconfiguration was the main issue preventing domain joins.
* After fixing DNS, domain join for Windows 10 succeeded.
* Ping tests between server and client VMs confirmed network health.

**7. Pending / Next Steps**

* No Windows 7 VM joined or configured — currently focusing on Windows 10 client.
* Plan to install and configure Wazuh server on Linux VM and deploy agents on Windows clients.
* Setup honeypot VM (T-Pot) on Linux.
* Expand lab for offensive and defensive practice.

**Summary Table of IPs and Key Network Settings:**

| **Device** | **IP Address** | **Subnet Mask** | **Default Gateway** | **DNS Server** | **Role** |
| --- | --- | --- | --- | --- | --- |
| Windows Server 2019 | 192.168.138.2 | 255.255.255.0 | Router IP (e.g., 192.168.138.1) | 192.168.138.2 | Domain Controller, DNS |
| Windows 10 Client | 192.168.138.10 | 255.255.255.0 | Router IP | 192.168.138.2 | Domain Joined Client |
| (hide ip ) |  |  |  |  |  |

**✅ Step-by-Step Guides Based on Your Current Lab Setup**

**🔹 1. Configure Windows Server 2019 as Domain Controller with DNS**

**Pre-Requirements:**

* Static IP set (already done): 192.168.138.2

**Steps:**

1. Open **Server Manager** → Click **Manage** → **Add Roles and Features**.
2. Select **Role-based or feature-based installation** → Click **Next**.
3. Select your server → Click **Next**.
4. Choose **Active Directory Domain Services (AD DS)** → Click **Add Features** → **Next**.
5. Also select **DNS Server** role if not already added.
6. Click **Next** through features → Install.
7. After installation, go to **Server Manager** → Click yellow exclamation ⚠ → **Promote this server to a domain controller**.
8. Select: **Add a new forest** → Root domain: lab.local.
9. Set **Directory Services Restore Mode (DSRM)** password.
10. Continue setup and restart when prompted.

**🔹 2. Join Windows 10 Client to Domain**

**Pre-Requirements:**

* Static IP: 192.168.138.10
* DNS: 192.168.138.2 (Server)

**Steps:**

1. Go to **Control Panel** → **System** → **Change Settings** (under Computer Name).
2. Click **Change** → Set domain as: lab.local.
3. Enter domain admin credentials when prompted.
4. Upon success: **"Welcome to the lab.local domain"** → Restart the system.

✅ Now your Windows 10 client is part of the domain!

**🔹 3. Test Connectivity (Ping/DNS)**

On Windows 10:

bash

CopyEdit

ping 192.168.138.2

nslookup lab.local

On Windows Server:

bash

CopyEdit

ping 192.168.138.10

Expected: Ping replies and name resolution success.

**🔹 4. Plan Next Setup Tasks**

Here’s a roadmap you can follow next:

| **Task** | **OS/Tool** | **Description** |
| --- | --- | --- |
| ✅ Domain Setup | Win Server + Win 10 | Done |
| 🔄 Install Kali Linux | Kali ISO | For attacking tools (offense) |
| 🔄 Install T-Pot Honeypot | T-Pot ISO | Run on Linux VM (deception) |
| 🔄 Setup pfSense | pfSense ISO | Network segmentation + firewall |
| 🔄 Wazuh Server | Ubuntu/CentOS | For EDR server |
| 🔄 Wazuh Agent | Win Server + Win 10 | EDR endpoint monitoring |

Inside the **Lab** menu:

* **Overview**
* **Network Diagram**
* **Machine List**
* **Honeypot Setup**
* **EDR Monitoring**
* **Scenarios (Attacks + Defense)**
* **Logs and Analysis**
* Screenshots + CLI output

This is the option inside lab

I will upload my work and write up screen shot later

And if possible give a separate html,css etc etc