**Day 1 – Ethical Hacking**

**🛠️ Tools Installed**

* **VirtualBox**: Oracle VM VirtualBox for virtualization
* **Kali Linux**: Security testing OS based on Debian

**🔽 Installation Summary**

**VirtualBox:**

* Downloaded from: https://www.virtualbox.org/
* Installed version: 7.x (latest)
* Host OS: Windows 10 (64-bit)

**Kali Linux:**

* Downloaded from: https://www.kali.org/get-kali/
* Version: kali-linux-2024.2 XFCE (amd64)
* Size: ~3.5 GB ISO

**Virtual Machine Configuration:**

| **Setting** | **Value** |
| --- | --- |
| RAM | 2.5 GB |
| CPU Cores | 2 |
| Disk Size | 20 GB |
| Video Memory | 128 MB |
| Graphics | 3D Enabled |
| Network | NAT |

**💡 Key Definitions**

| **Term** | **Definition** |
| --- | --- |
| **Ethical Hacking** | Testing systems legally to find vulnerabilities |
| **White Hat** | Legal/ethical hacker |
| **Black Hat** | Illegal, malicious hacker |
| **Gray Hat** | Hacks without permission, but not for harm |
| **Penetration Testing** | Simulating cyberattacks to test defense |
| **Kali Linux** | A Linux distro with built-in security tools |

**✅ Setup Results**

* Kali Linux installed successfully in VirtualBox
* Smooth performance with assigned resources
* Tools like Nmap, Metasploit, and Wireshark available
* VirtualBox snapshots created as backup

**🔚 Conclusion**

Day 1 focused on setting up the ethical hacking environment. I installed Kali Linux inside VirtualBox with optimized settings and learned key cybersecurity terms. Ready to explore Kali’s toolset in the next session.