Day - 1 of CEH

Hacking :

Hacking is the process of **identifying weaknesses** in a computer system, network, or application and **exploiting them** to gain access, control, or information.

Hacking can be done for:

- Malicious purposes (illegal)
- Security testing and learning (legal, with permission)

What is Ethical Hacking?

Ethical hacking is the **authorized and legal practice** of testing systems for security vulnerabilities.

An **ethical hacker**:

- Has **written permission**
- Follows laws and rules
- Helps organizations improve security

Ethical hacking is also known as:

- Penetration Testing
- White Hat Hacking

Types of Hackers

Hackers are classified based on **intent and authorization**.

- **Ethical Hackers** – Hack to secure systems
- **Malicious Hackers** – Hack to steal, damage, or misuse data
- **Hacktivists** – Hack for political or social causes
- **Script Kiddies** – Use ready-made tools without deep knowledge
- **State-Sponsored Hackers** – Work for governments
- **Black Hat Hacker** - Hacks without permission, Intent is illegal or harmful, Steals data, spreads malware
- **White Hat Hacker** - Hacks with permission, Works legally, Focuses on security improvement
- **Grey Hat Hacker** - May hack without permission, Does not usually have malicious intent, Can report vulnerabilities after finding them

What are Vulnerability, Exploit, and Payload?

Vulnerability

A **weakness** in a system, software, or network.

Examples:

- Weak passwords
- Unpatched software
- Misconfigured servers

Exploit

A **technique or code** used to take advantage of a vulnerability.

Example:

- Using SQL Injection to access a database

Payload

The **actual malicious or intended action** delivered after exploitation.

Examples:

- Reverse shell
- Malware
- Data extraction

Types of GPTs

Freedom GPT

- GPTs with fewer restrictions
- May generate unrestricted responses
- High risk if misused

Pentest GPT

- Used for **penetration testing assistance**

- Helps with vulnerability analysis, reporting, and methodology
- Used by ethical hackers for learning and documentation

Worm GPT

- AI model associated with **malware development**
- Used to automate malicious code creation
- Considered dangerous and unethical

These GPT types are used or learn for **awareness and defense**, not for misuse.

Steps Performed in Hacking (CEH)

1. Reconnaissance (Information Gathering)

This is the **first step** of hacking.

The attacker collects information about the target such as:

- IP address
- Domain details
- Network structure
- Employee information (public sources)

Types of reconnaissance:

- **Passive**: No direct interaction with the target
- **Active**: Direct interaction with the target system

---

2. Scanning

In this phase, the attacker identifies **live systems and weaknesses**.

Activities include:

- Identifying open ports
- Discovering services
- Detecting operating systems
- Finding vulnerabilities

Scanning helps attackers decide **how to attack**.

---

3. Gaining Access

This phase involves **exploiting vulnerabilities** to enter the system.

The attacker may:

- Bypass authentication
- Access restricted data
- Take control of a system

This is where actual **intrusion** occurs.

---

4. Maintaining Access

After gaining access, the attacker tries to **stay connected** to the system.

Purpose:

- Maintain long-term access
- Perform repeated actions
- Avoid detection

Ethical hackers study this to learn how attackers persist.

---

5. Clearing Tracks

In this phase, the attacker attempts to **remove evidence**.

This may include:

- Deleting logs
- Hiding activities
- Avoiding detection

CEH teaches this phase to help defenders **detect and prevent attacks**.

Intrusion Kill Chain / Intrusion Detection Cycle :

The intrusion cycle describes **how an attack progresses** from start to finish.

1. Reconnaissance

The attacker gathers information about the target before launching an attack.

---

2. Weaponization

The attacker prepares tools or methods to exploit a vulnerability.

---

3. Delivery

The attack is delivered to the target.

Examples:

- Email
- Website
- Network-based methods

---

4. Exploitation

The vulnerability is exploited to gain access to the system.

---

5. Installation

Malicious components are installed to maintain access.

---

6. Command and Control (C2)

The attacker establishes communication with the compromised system.

---

7. Actions on Objectives

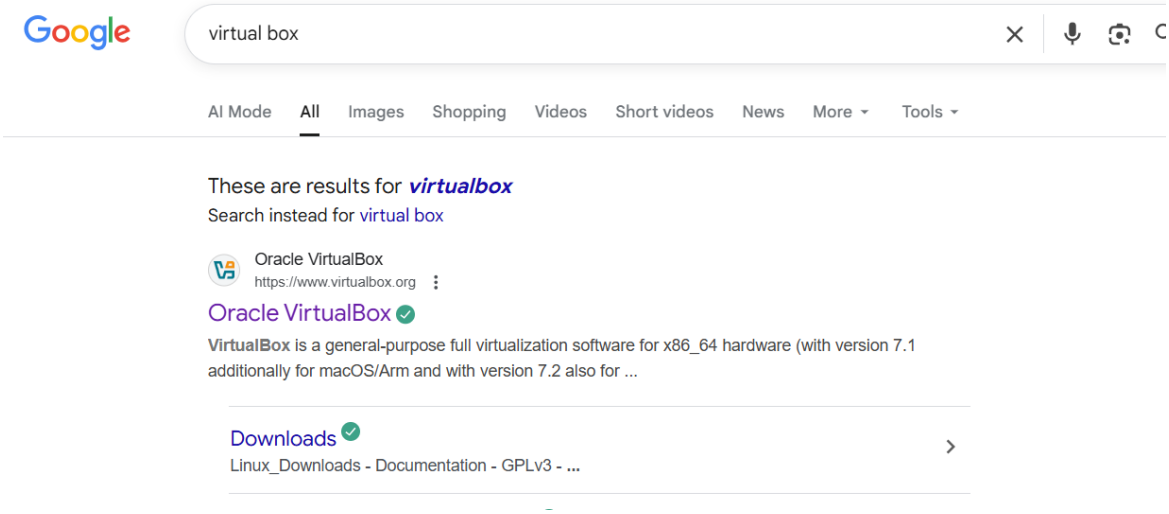
The attacker performs intended actions such as:

- Data theft
- System manipulation
- Service disruption

Steps to Install VirtualBox

VirtualBox is a **virtualization software** used to run virtual machines on a computer.
In CEH, it is commonly used to create **practice labs**.

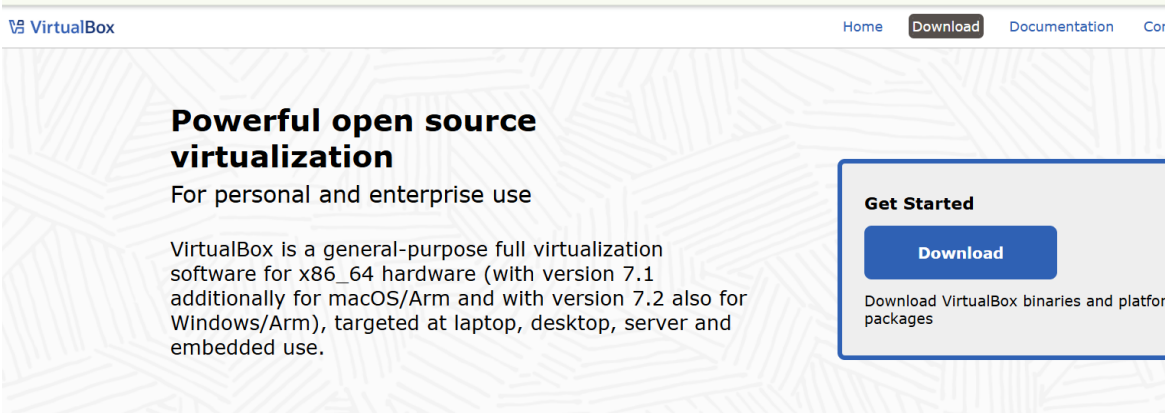
Step 1: Check System Requirements

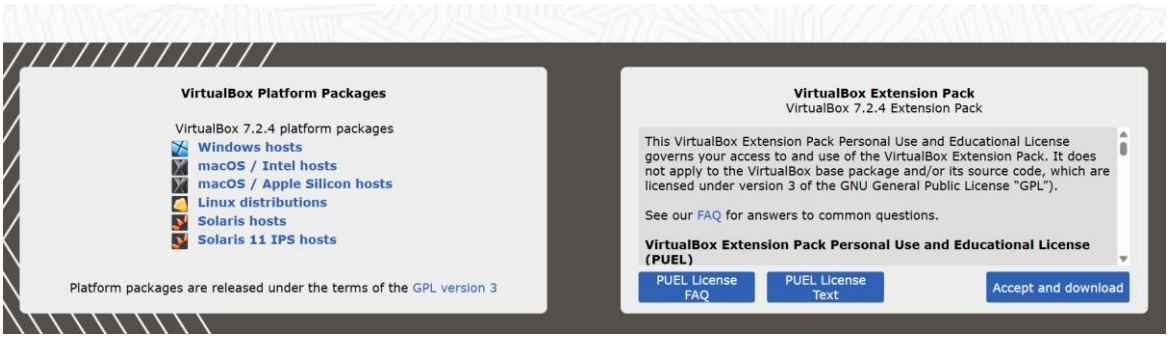


Before installing VirtualBox, ensure that:

- Your system supports virtualization
- Virtualization (VT-x / AMD-V) is enabled in BIOS
- You have administrator privileges

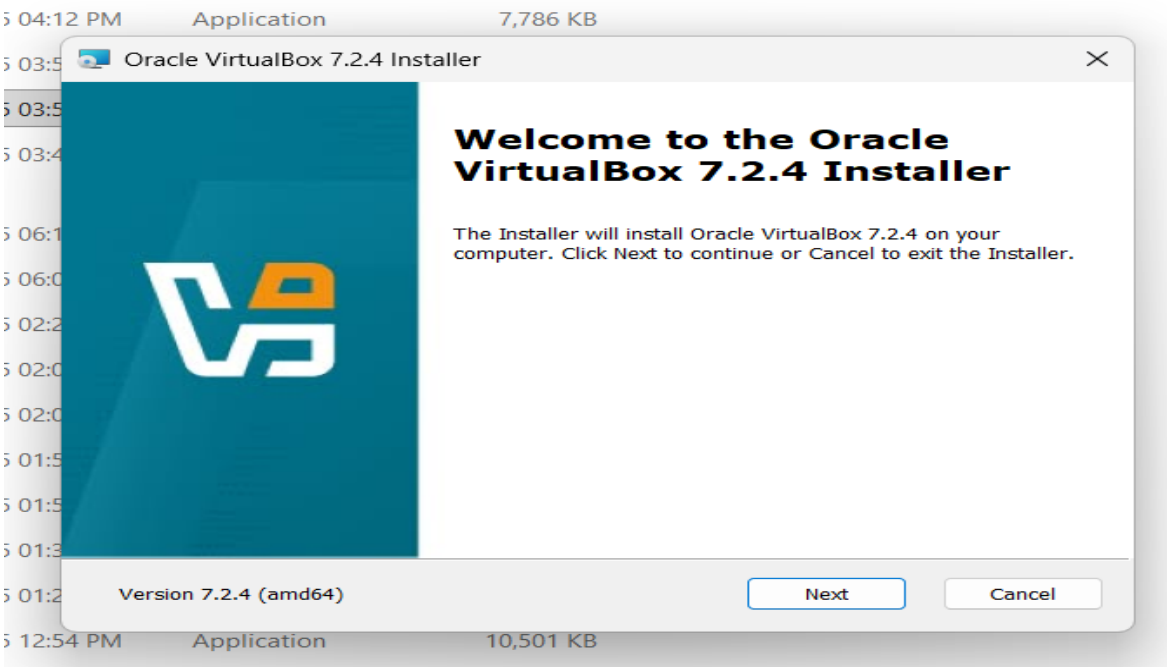
Step 2: Download VirtualBox





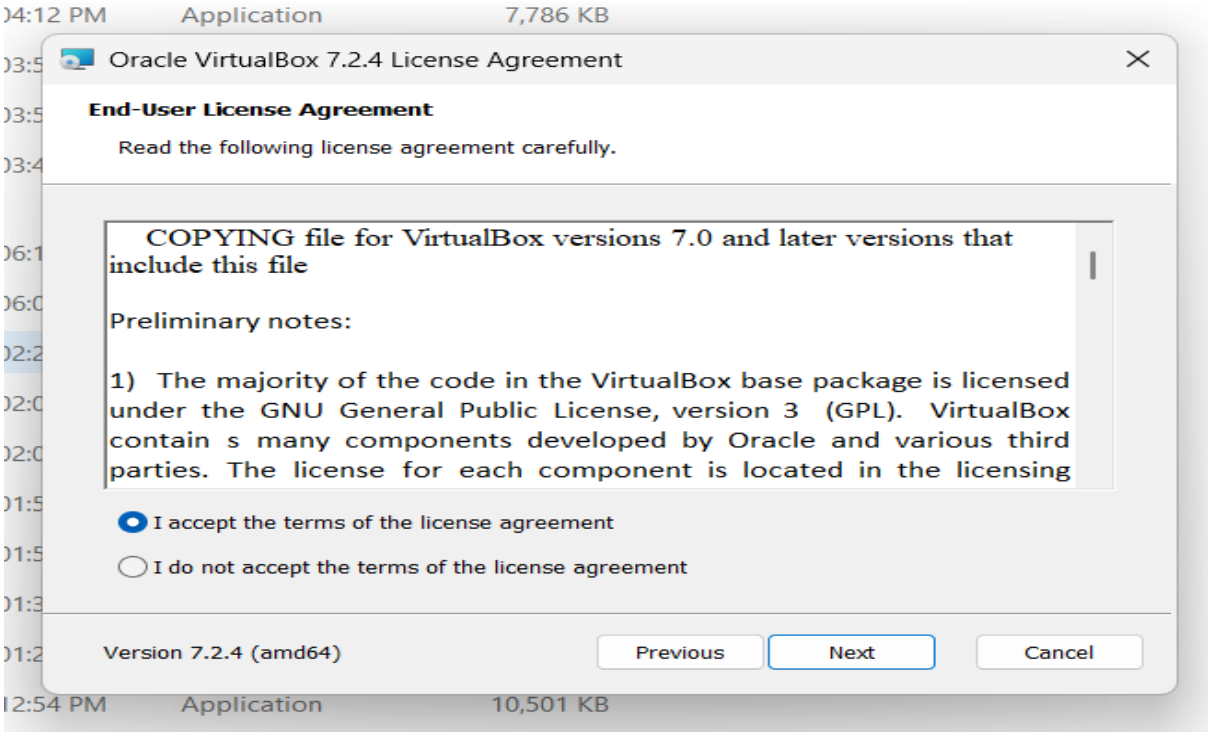
1. Open a web browser
2. Go to the official VirtualBox website
3. Download VirtualBox for your operating system:
    - Windows
    - macOS
    - Linux

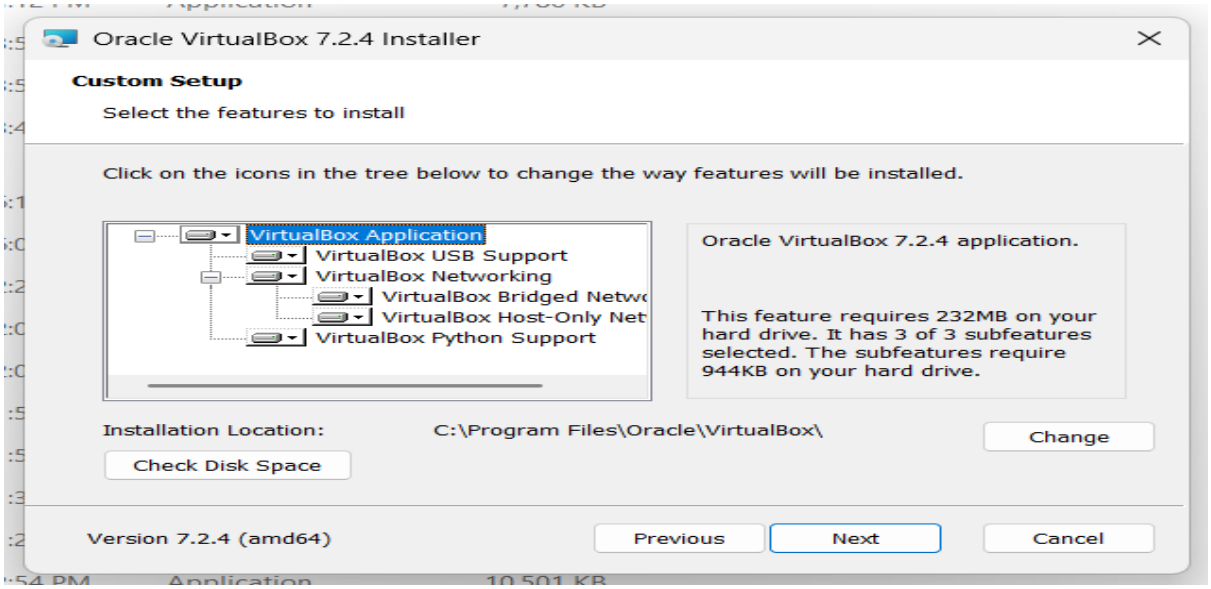
Step 3: Run the Installer



1. Open the downloaded installer file
2. Click **Next**
3. Choose the installation location (default is recommended)

Step 4: Select Components



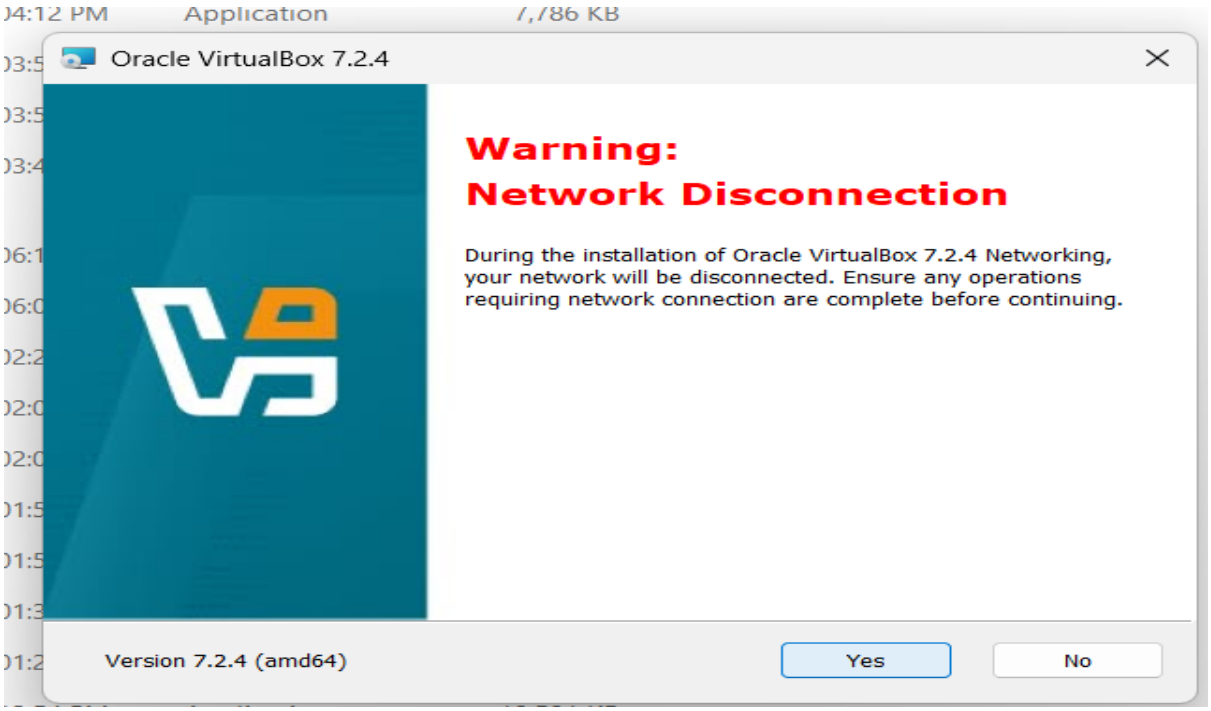


During installation:

- Keep default components selected
- Network and USB options can remain unchanged

Click **Next** to continue.

Step 5: Install VirtualBox

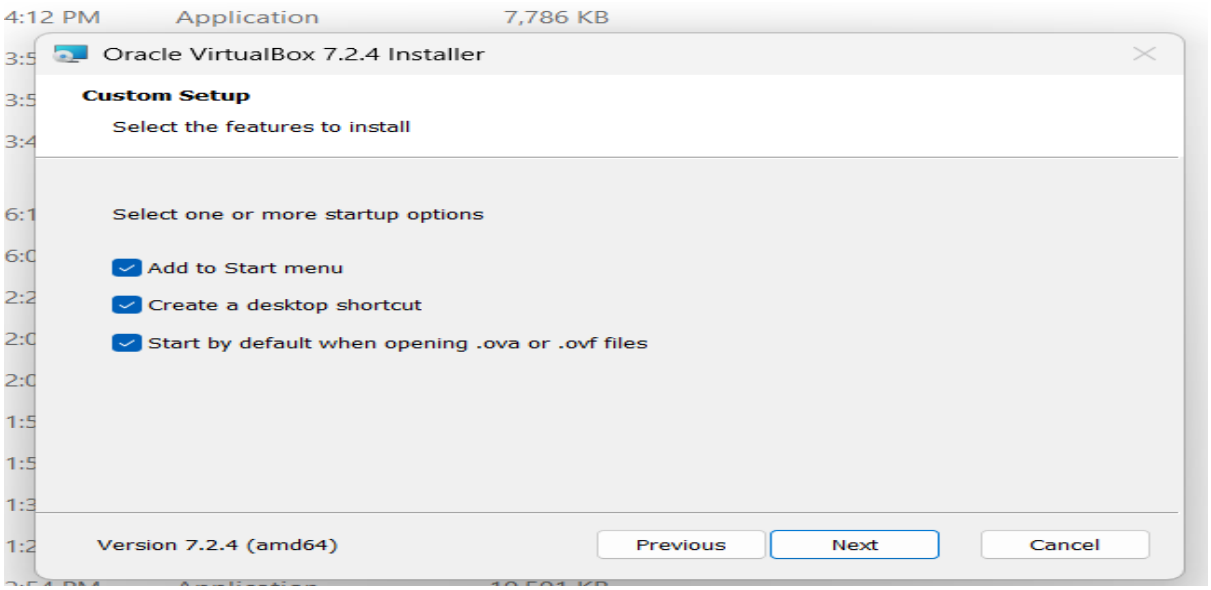


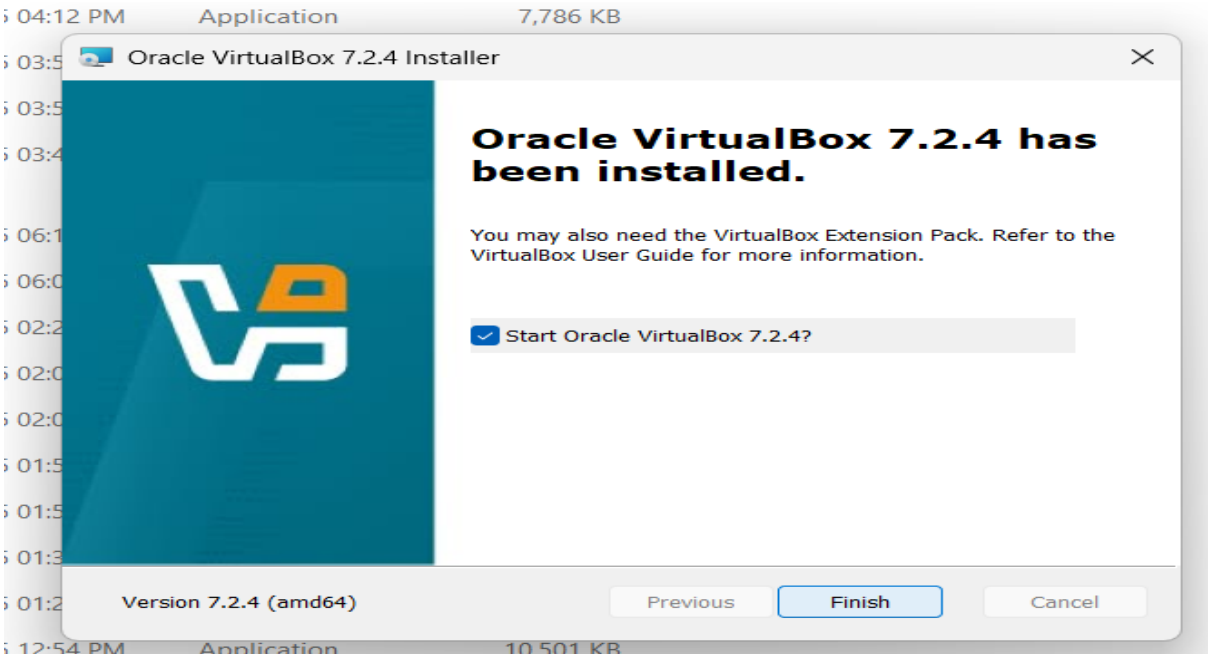
1. Click Install

2. Allow permissions if prompted

3. Wait for the installation to complete

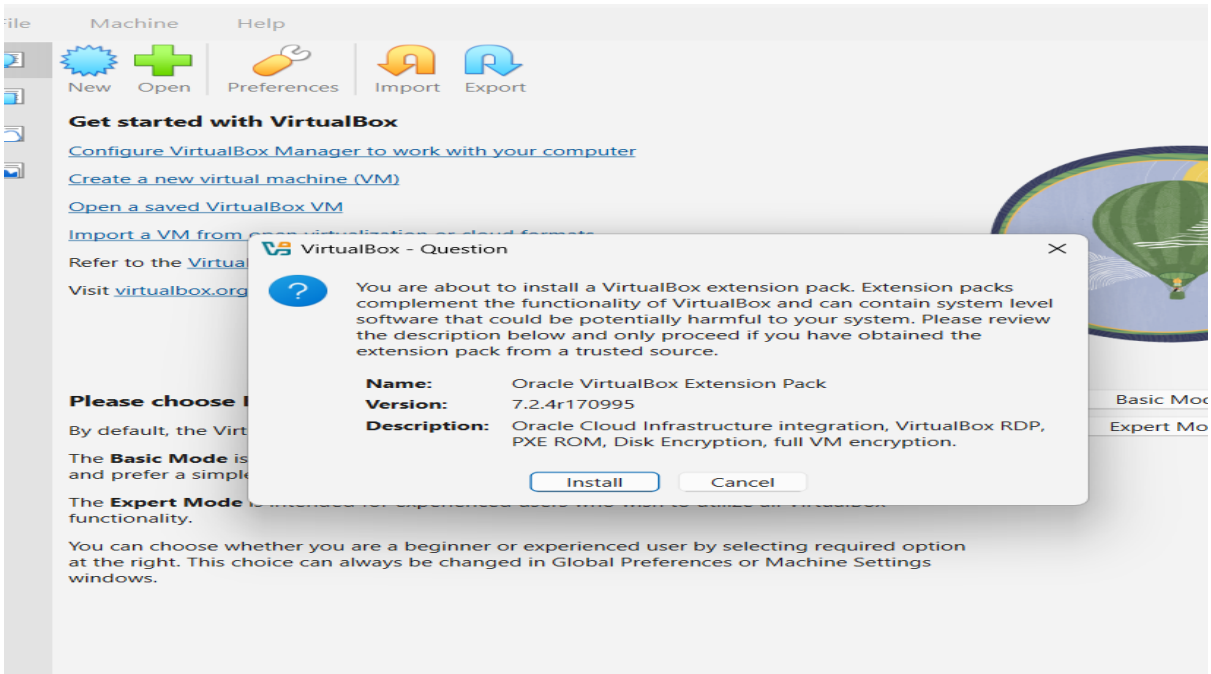
Step 6: Finish Installation





1. Click **Finish**
2. VirtualBox will launch automatically

Step 7: Verify Installation



- Open VirtualBox
- Ensure the main dashboard loads without errors

VirtualBox is now successfully installed and ready for use.

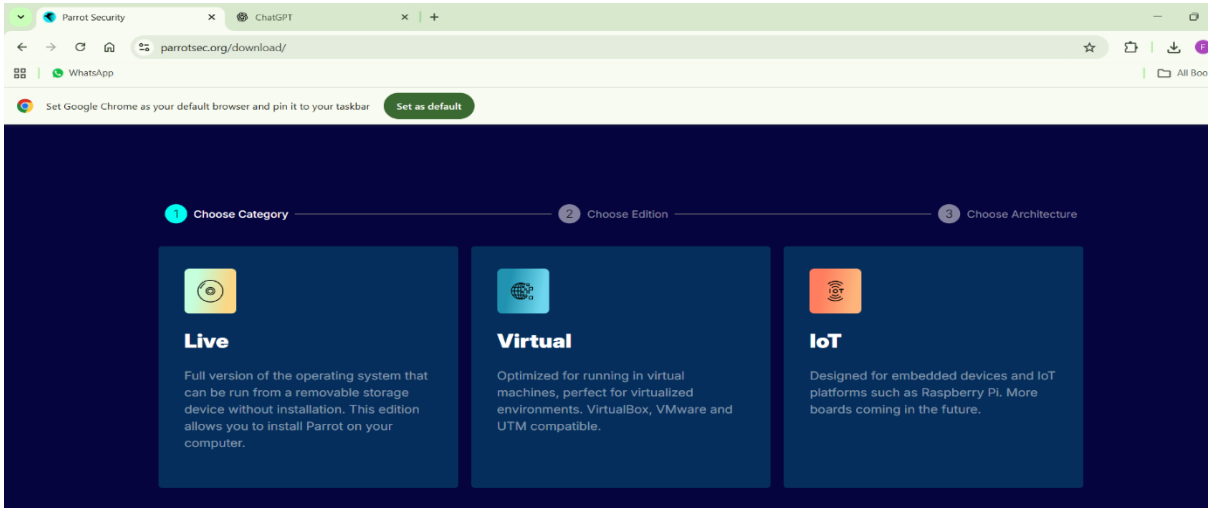
Steps to Install Parrot OS Using OVA File (VirtualBox)

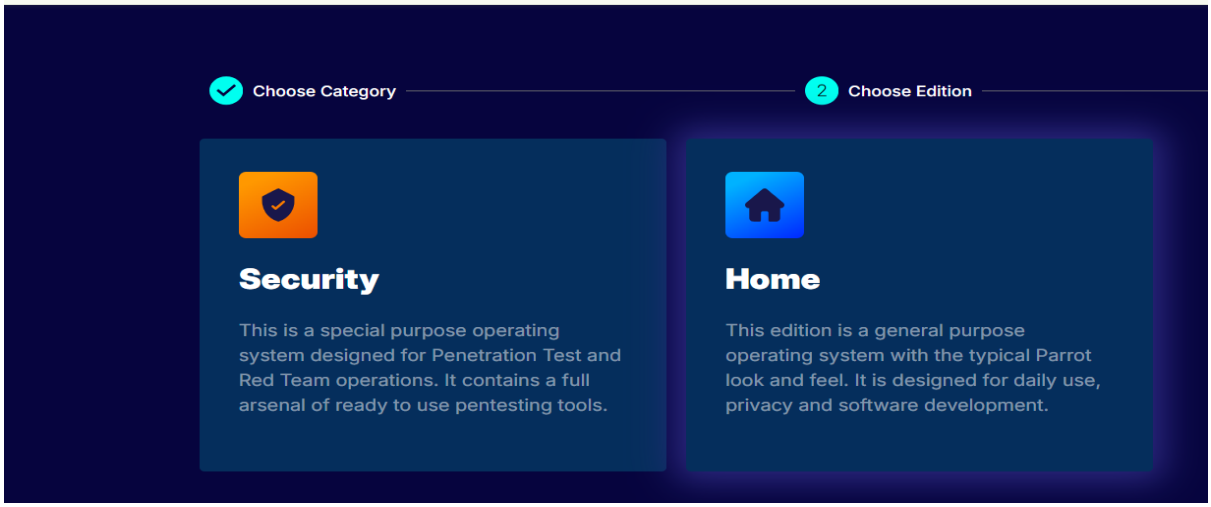
An **OVA (Open Virtual Appliance)** file contains a **pre-configured virtual machine**, making installation faster and easier.
This method is commonly used in **CEH labs**.

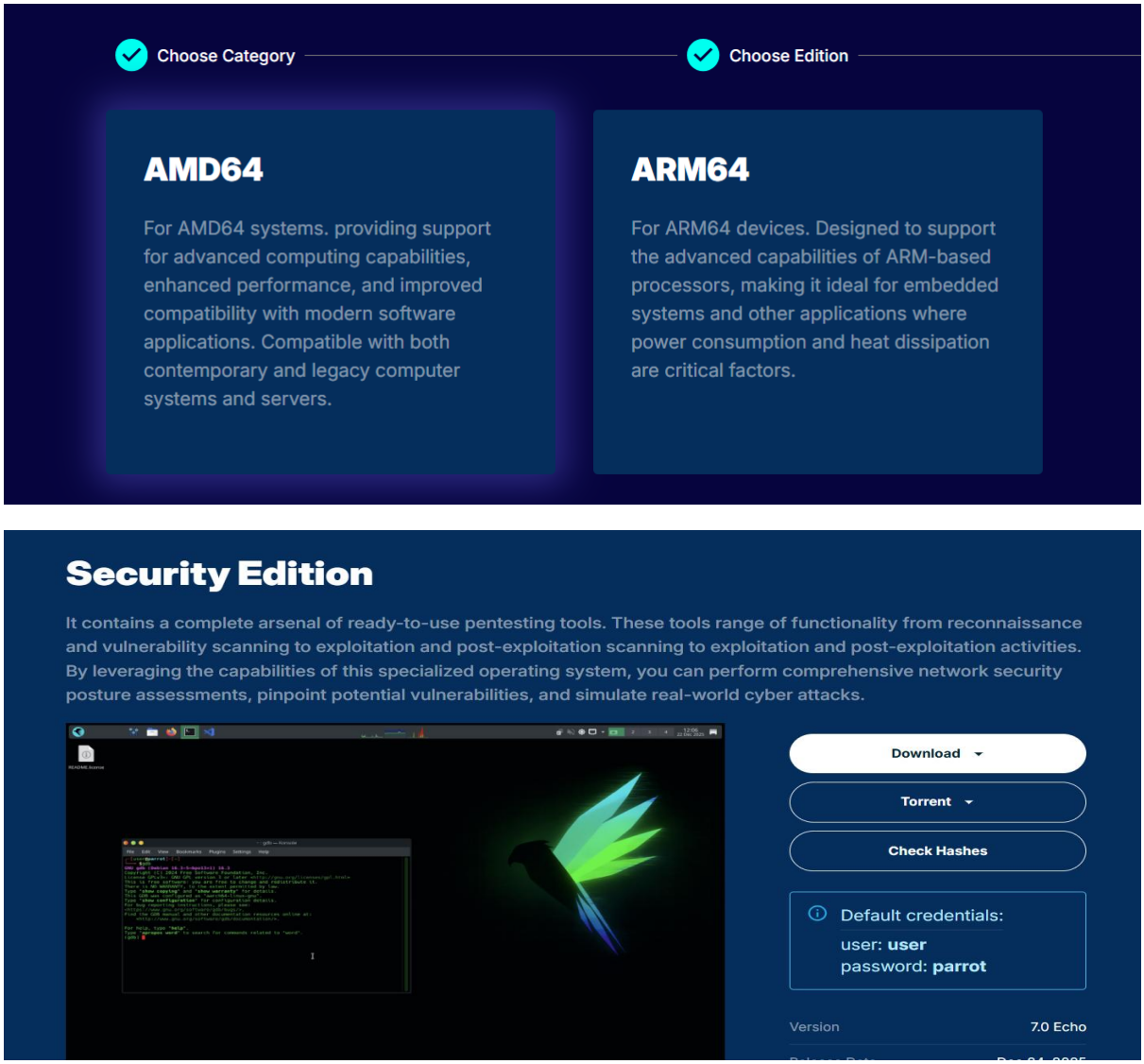
Step 1: Install VirtualBox

- Ensure Oracle VirtualBox is installed on your system
- VirtualBox is required to import the OVA file

Step 2: Download Parrot OS OVA File

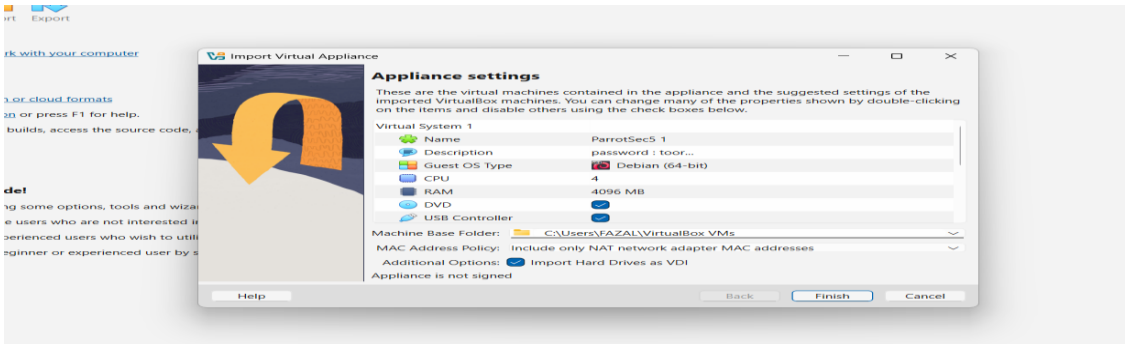






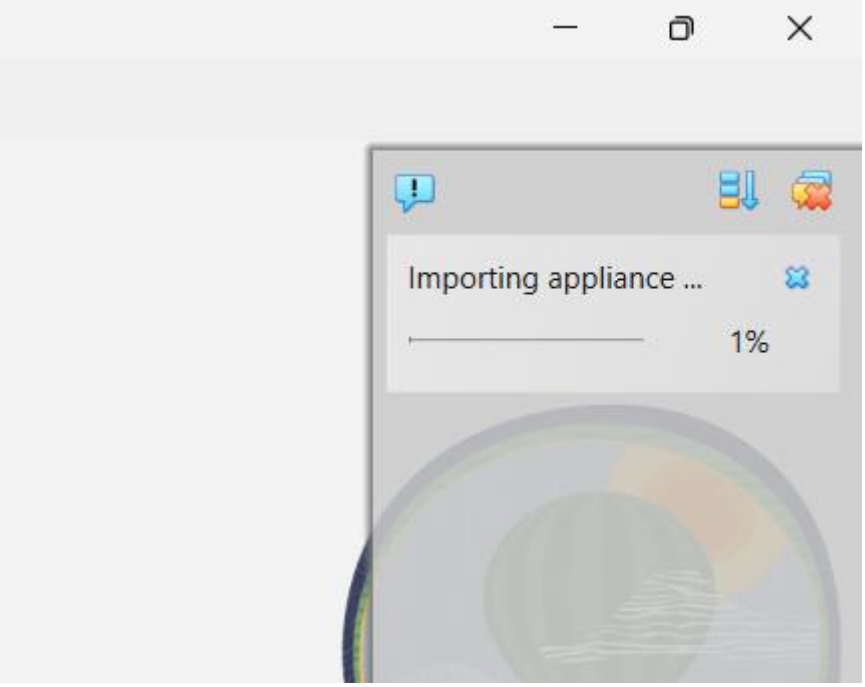
- Download the official **Parrot OS OVA file**
- Save it to an accessible location on your system

Step 3: Open VirtualBox



1. Launch **VirtualBox**
2. Click on **File → Import Appliance**

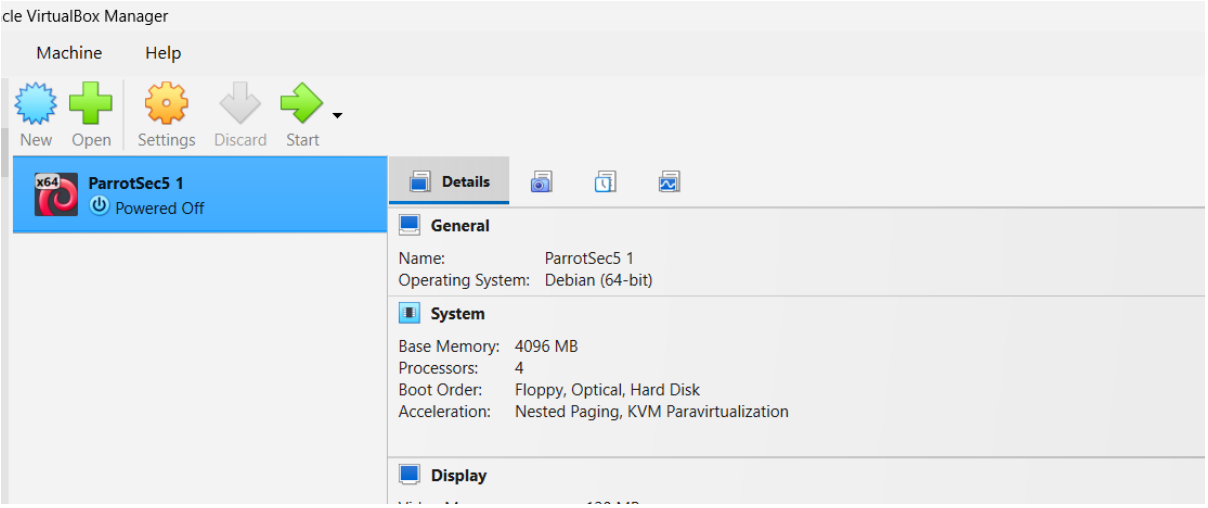
Step 4: Import the Appliance



1. Click **Import**
2. Wait for the import process to complete

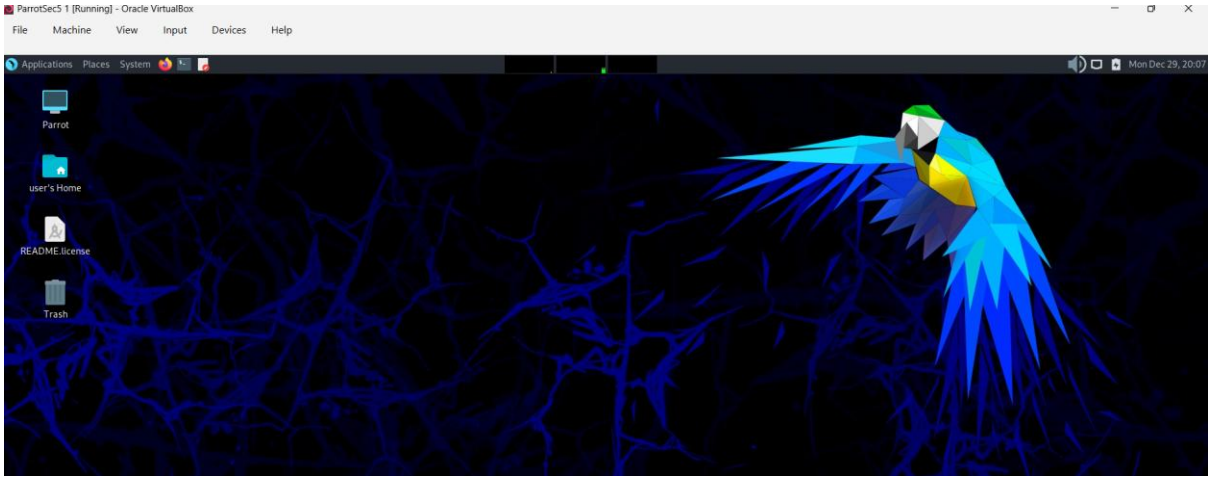
VirtualBox will automatically create the virtual machine.

Step 5: Start Parrot OS



1. Select **Parrot OS** from the VirtualBox list
2. Click **Start**
3. Parrot OS will boot automatically

Step 6: Login to Parrot OS



- Use the default credentials provided with the OVA file
- Change the password after first login (recommended)

Verification

- Parrot OS desktop loads successfully
- System tools are accessible

Advantages of OVA Installation

- No manual installation required
- Preconfigured environment
- Time-saving and beginner-friendly

Conclusion

- Ethical hacking is legal, authorized, and focused on improving security.

- A strong understanding of hacking steps and the intrusion kill chain is essential for both attackers and defenders.
- Setting up VirtualBox and Parrot OS prepares you for hands-on penetration testing and lab exercises.