EC-Council

Building A Culture Of Security

C|HFI

Computer Hacking Forensic INVESTIGATOR

Computer Hacking Forensic Investigator v11

CLASSROOM LAB SETUP GUIDE

EC-Council Official Curricula

Table of Contents

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Classroom Setup Instructions: CHFIv11

This document contains setup instructions for the EC-Council Computer Hacking Forensic Investigator (CHFI) course. The course requires a standard modular classroom seating configuration, a computer for each student, a computer for the instructor, a dedicated hub or switch (hub preferred), a dedicated firewall, and an Internet connection. This class teaches digital forensics methodology, which includes searching and seizing, chain-of-custody, acquisition, preservation, analysis, and reporting of digital evidence. It is imperative that the network used for this class be separated both logically and physically from any other networks in the training facility to prevent students from "accidentally" conducting exploits on other computers within accessible networks.

Before beginning the class, install and configure all computers using the information and instructions that follow.

The information contained in this document is subject to change without notice. Unless otherwise noted, the names of companies, products, people, and data used in this document are fictional. Their use is not intended in any way to represent any real company, person, product, or event. Users of this document are responsible for compliance with all applicable copyright laws. No part of this document may be reproduced or transmitted by any means, electronic or mechanical, for any purpose, without the express written consent of the International Council of Electronic-Commerce Consultants, hereinafter referred to as the EC-Council. If, however, your only means of access is electronic, permission is hereby granted to print one copy.

The EC-Council may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering the material in this document. Except as expressly provided in any written license agreement from the EC-Council, providing this document does not give you any license to those patents, trademarks, copyrights, or other intellectual property.

Computer Hacking Forensic Investigator and CHFI are either registered trademarks or trademarks of the EC-Council in the USA and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Classroom Requirements

This section describes the classroom equipment required for the EC-Council Computer Hacking Forensic Investigator (CHFI) course.

Classroom Equipment

The following equipment is required for the general classroom setup:

- Climate control system, adjustable within the classroom
- Lighting controls, adjustable within the classroom
- Whiteboard, 3 feet × 6 feet (1 m × 2 m) or larger
- Markers of assorted colors and a whiteboard
- Eraser and whiteboard cleaner liquid (3 oz minimum)
- Towels and paper
- Easel with a flipchart or butcher paper pad, 24 in × 36 in
- Felt-tip pens with chisel tips (not fine point); blue and black are required, while other colors are optional
- Projection screen measuring 6 feet diagonally (a non-reflective whiteboard surface may be used as a substitute)
- Instructor station:
  - Ergonomic desk and chair
  - Power outlet
  - Network jack
  - LCD projector with a minimum resolution of 740 × 1280 pixels and all connecting cables
- Student station (per student):
  - Ergonomic chair
  - Workstation with a minimum horizontal workspace of 9 square feet (3 feet × 3 feet)
  - One power outlet
  - One network jack

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hardware

The hardware requirements for the instructor and student computers are identical:

- Intel Core i5 or equivalent CPU with a minimum clock speed of 3.2 GHz
- Minimum of 16 GB or more RAM
- Hard disk, 1 TB or higher and 7200 RPM or faster
- DVD drive (DVD R/W drive preferred)
- One network adapter (minimum of a 10/100 NIC, but a 10/100/1000 is preferred), full duplex (disable any additional network adapters installed)
- Monitor (minimum requirement is a 17-inch LCD monitor)
- Mouse or compatible pointing device and a sound card with amplified speakers
- Internet access
- Two wireless network adapters (PCI or USB)*

The following additional hardware is required:

- A switch with sufficient ports to allow the connection of all instructor and student workstations, in addition to at least five unused ports for connecting additional equipment or for use as "spares"

---

*If wireless network adapters are not available for all classroom machines, at least the instructor machine must be so equipped.

Software

All computers in the class require the following software:

- Any Windows/Linux/macOS operating system capable of running VMware Workstation Pro
- CHFI Tools downloadable from the Aspen portal
- VMware Workstation Pro v15.5.1 or later version
- Microsoft .NET Framework 6.0.415
- Adobe Acrobat Reader DC or later version
- WinRAR v6.24 or later version
- Web browsers: Internet Explorer, Firefox, and Chrome
- WinPcap driver
- Word, Excel, and PowerPoint viewers, preferably Microsoft Office 2016 or Open Office
- Java Runtime Environment v8u391 or later version

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Notepad++ v8.5.8 or later version
- PuTTY v0.79
- VMware Workstation Pro (built-in role in any Windows/Linux/macOS operating system capable of running VMware Workstation Pro)
    - Microsoft Windows 11 Enterprise or Professional (64-bit) with full patches applied
    - Microsoft Windows Server 2022 Standard Edition (64-bit) with full patches applied
    - Ubuntu 22.04.3 (64-bit) with full patches applied

Note: All the above-mentioned tools, except the Windows operating systems (Windows 11, Windows Server 2022) and Ubuntu, are available in the CHFI Tools downloads from the Aspen portal.

Classroom Connectivity

As this class teaches network attack and forensics methodologies, the network for the class must be logically and physically separated from any other networks present in the training facility and must have its own Internet connection.

Configuration

This section describes the procedures for setting up the instructor and student computers, as well as general directions for the configuration of the firewall appliance.

This guide assumes that you will use disk-imaging software to create images of the classroom computers for future use. To that end, configuration tasks (CTs) common to all computers are presented first. Perform these tasks on the computer that will become the instructor computer. Create a disk image after setting up a single student computer. You may then deploy this image to the remaining classroom machines while completing configuration of the instructor computer.

Because the Instructor computer is configured as a dynamic host configuration protocol (DHCP) server that provides IP addresses to the student machines, the installation and configuration of the Instructor computer must be completed before the final configuration of the student machines can begin.

Setup Document Overview

This document provides background information for the technical staff responsible for setting up a training room facility for the CHFI course. This guide describes the requirements for the network equipment and computer stations that are installed and configured by the facility's personnel for the training courses.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Training Room Environment

The training room environment consists primarily of the following equipment:

- Instructor computer
- Student workstations

Equipment	Number (Class of 12 Students)	Operating System	Minimum System Requirements
Instructor Computer	1	Any Windows/Linux/macOS operating system	Intel Core i5 or equivalent PC with 1 TB free disk space, a minimum of 16 GB RAM, one NIC, 17-inch monitor, two wireless network adapters (PCI or USB), and one compatible mouse
Student Workstations	12	Any Windows/Linux/macOS operating system	Intel Core i5 or equivalent PC with 1 TB free disk space, a minimum of 16 GB RAM, one NIC, 17-inch monitor, one wireless network adapter (PCI or USB), and one compatible mouse

Instructor Computer

Perform the following tasks on the instructor computer:

- Install **any Windows/Linux/macOS operating system** capable of running VMware Workstation Pro, updated with the latest service packs and patches.
- Download the ISO file from Aspen (see CT#4 in the Configuration Tasks section).
- Download all CHFI Tools from Aspen to the **E:\CHFI-Tools** folder on your hard drive for easy access (see CT#16 in the Configuration Tasks section).
- Install VMware Workstation Pro on the host machine (see CT#5 in the Configuration Tasks section).
- Configure a virtual network in the VMware Virtual Network Editor (see CT#6 in the Configuration Tasks Section).
- Install guest operating systems (Windows Server 2022 and Windows 11) on VMware Workstation (see CT#7 in the Configuration Tasks section).
- Configure the **Internet Explorer Enhanced Security Configuration** (see CT#8 in the Configuration Tasks section).
- Run the IP protocol.
- Install guest operating systems (Ubuntu Suspect and Ubuntu Forensics) on VMware Workstation (see CT#10 in the Configuration Tasks section).
- Turn off the firewall on all Windows virtual machines (see CT#11 in the Configuration Tasks section).

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install Windows components in all the Windows virtual machines (see CT#12 in the Configuration Tasks section).
- Install WinRAR and MS Office on the Windows 11 virtual machine (see CT#13 and CT#14 in the Configuration Tasks section).
- Create a partition in the Windows Server 2022 virtual machine (see CT#15 in the Configuration Tasks section).
- Have CHFI Tools shared as the **Z:** drive on the Windows and Ubuntu machines (mapping the **Z:** drive) (see CT#17 and CT#18 in the Configuration Tasks section).
- Create a Forensic Disk (F:) and Volume (G:) in Windows 11 and Delete Volume (G) for forensic investigation purposes (see CT#19)
- Install Adobe Acrobat Reader DC on all Windows virtual machines (see CT#20 in the Configuration Tasks section).
- Install WinRAR on the Windows Server 2022 (see CT#21 in the Configuration Tasks section).
- Install Notepad++, Web Browsers, and WinPCap in all Windows machines (all software can be found in the **CHFIv11 Lab Prerequisites** directory in the **Z:\CHFI-Tools** folder) (see CT#22, CT#23, and CT#24 in the Configuration Tasks section).
- Have Windows Explorer set to show all files, file types, and extensions (see CT#25 in the Configuration Tasks section).
- Install Java Runtime Environment on all the Windows virtual machines (see CT#26 in the Configuration Tasks section).
- Turn off screen savers on the Windows virtual machines (see CT#27 in the Configuration Tasks section).
- Conduct a ping test between all the machines in your network (see CT#28 in the Configuration Tasks section).
- Disable DEP in Windows Server 2022 Virtual Machine (see CT#29)
- Install PuTTY in Windows Server 2022 Virtual Machine (see CT#30)
- Take snapshots of the virtual machines (see CT#31 in the Configuration Tasks section).
- Connect an LCD projector.

Student Workstations

Perform the following tasks on the student workstations:

- Install **any Windows/Linux/macOS operating system** capable of running VMware Workstation Pro, updated with the latest service packs and patches.
- Download the ISO file from Aspen (see CT#4 in the Configuration Tasks section).
- Download all CHFI Tools from Aspen to the **E:\CHFI-Tools** folder on your hard drive for easy access (see CT#16 in the Configuration Tasks section).

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install VMware Workstation Pro on the host machine (see CT#5 in the Configuration Tasks section).
- Configure a virtual network in the VMware Virtual Network Editor (see CT#6 in the Configuration Tasks Section).
- Install guest operating systems (Windows Server 2022 and Windows 11) on VMware Workstation (see CT#7 in the Configuration Tasks section).
- Configure the **Internet Explorer Enhanced Security Configuration** (see CT#8 in the Configuration Tasks section).
- Run the IP protocol.
- Install guest operating systems (Ubuntu Suspect and Ubuntu Forensics) on VMware Workstation (see CT#10 in the Configuration Tasks section).
- Turn off the firewall on all Windows virtual machines (see CT#11 in the Configuration Tasks section).
- Install Windows components in all Windows virtual machines (see CT#12 in the Configuration Tasks section).
- Install WinRAR and MS Office on the Windows 11 virtual machine (see CT#13 and CT#14 in the Configuration Tasks section).
- Create a partition in the Windows 11 virtual machine (see CT#15 in the Configuration Tasks section).
- Have CHFI Tools shared as the **Z:** drive on the Windows and Ubuntu machines (mapping the **Z:** drive) (see CT#17 and CT#18 in the Configuration Tasks section).
- Create a Forensic Disk (F:) and Volume (G:) in Windows 11 and Deleting Volume (G) (see CT#19)
- Install Adobe Acrobat Reader DC on all Windows virtual machines (see CT#20 in the Configuration Tasks section).
- Install WinRAR on the Windows Server 2022 (see CT#21 in the Configuration Tasks section).
- Install Notepad++, Web Browsers, and WinPCap in all Windows machines (all software can be found in the **CHFIv11 Lab Prerequisites** directory in the **Z:\CHFI-Tools** folder) (see CT#22, CT#23, and CT#24 in the Configuration Tasks section).
- Have Windows Explorer set to show all files, file types, and extensions (see CT#25 in the Configuration Tasks section).
- Install Java Runtime Environment on all the Windows virtual machines (see CT#26 in the Configuration Tasks section).
- Turn off screen savers on the Windows virtual machines (see CT#27 in the Configuration Tasks section).
- Conduct a ping test between all the machines in your network (see CT#28 in the Configuration Tasks section).

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

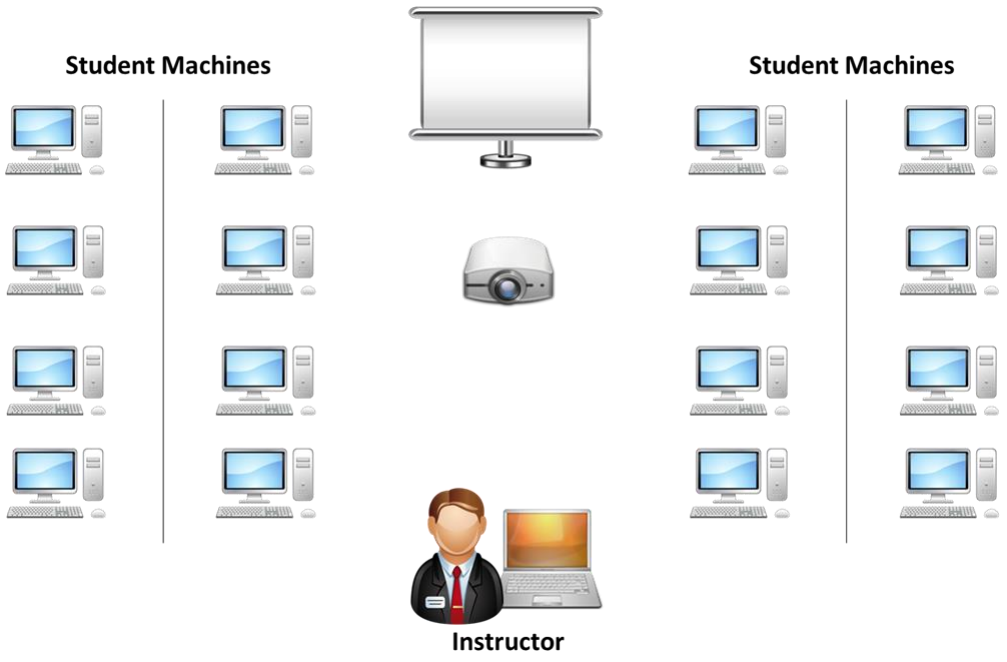
- Disable DEP in Windows Server 2022 Virtual Machine (see CT#29)
- Install PuTTY in Windows Server 2022 Virtual Machine (see CT#30)
- Take snapshots of the virtual machines (see CT#31 in the Configuration Tasks section).

Room Environment

- The room must contain a whiteboard measuring a minimum of 1 yard by 2–3 yards (1 m by 2–3 m).
- The room should contain an easel and a large tablet (optional).
- The room must be equipped with legible black and blue felt-tip pens with chisel point tips (not fine tip).

Classroom Configuration

The configuration of this classroom is modular. Computers can be added or removed either by row or column, depending on the needs of the class. The following is a sample room setup that provides optimal support. This setup allows for ease of access to "***troublespots***" by the instructor and allows students to break into functional teams of varying sizes.



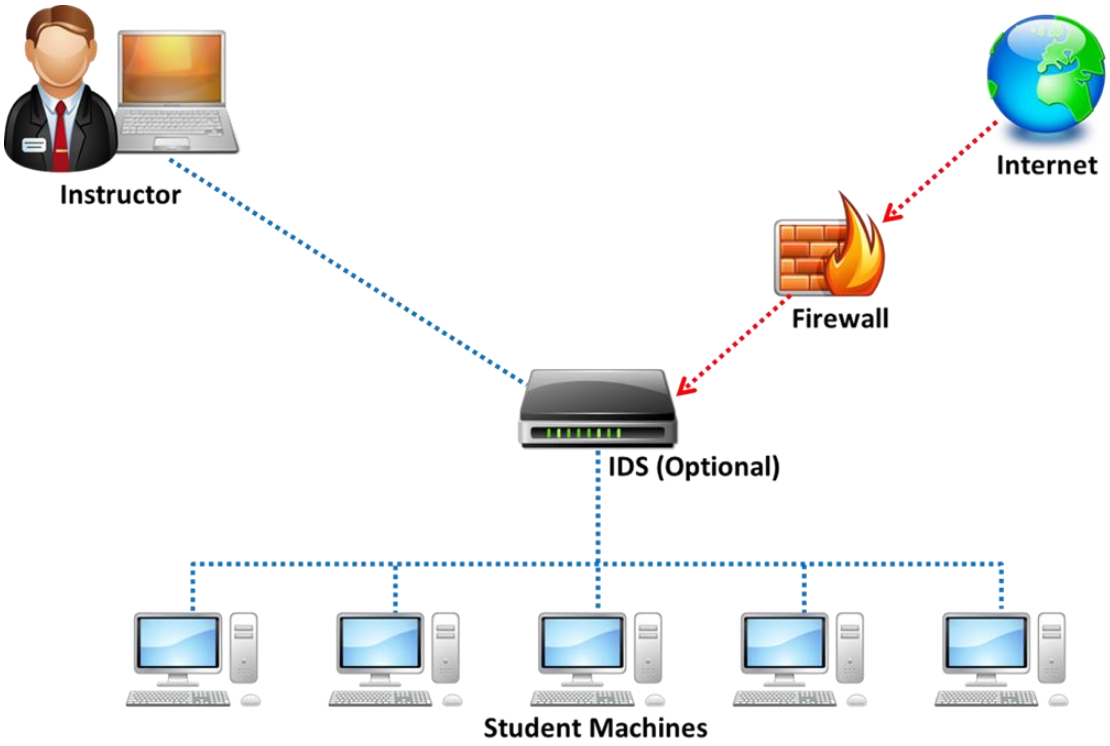
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Computer Names

Assign computer names to student machines, such as CHFISTUDENT1, CHFISTUDENT2, CHFISTUDENT3. The instructor machine should be named INSTRUCTOR.

Network Topology

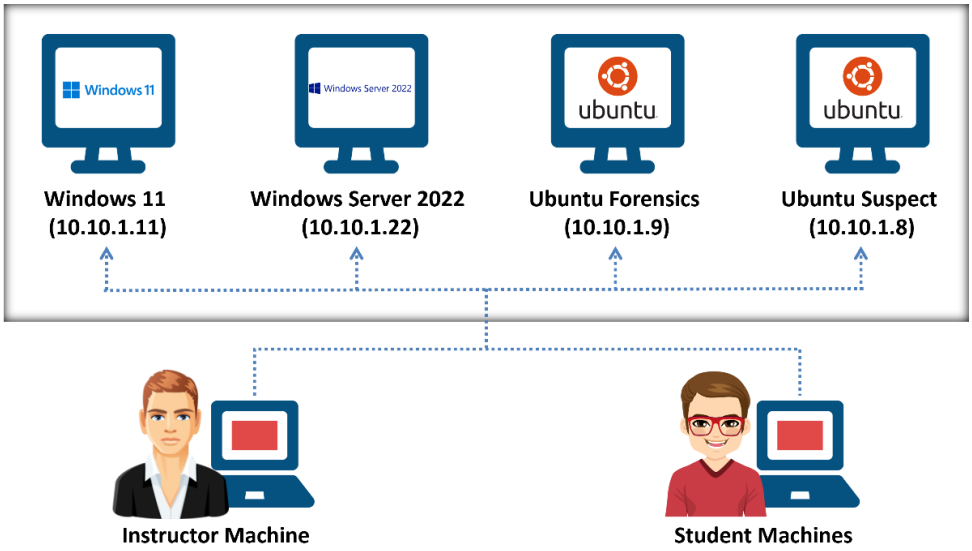
The training room must be physically isolated from any production network. Students must be able to access the Internet from their PCs. All computers are connected as one isolated network and domain. The common protocol is IP. All computers should have dynamic IP addresses using a DHCP server. Configure the DHCP server scope to 10.0.0.0/24 IP addresses. This reduces potential problems when booting the virtual machines. NICs can be of 10 Mbit or 100 Mbit (100 Mbit is recommended). Cables must be bundled and tied out of pathways and work areas and must be of sufficient length to avoid stress.



Set up the machines based on the classroom setup diagram. The lab exercises for the students are instructor-led and based on the digital forensics tools discussed in the trainer slides. The instructors are encouraged to demonstrate and guide the students on the use of digital forensics tools. Please feel free to include your own exercises.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CHFI VM Setup on Instructor and Student Machines



Instructor and Student Machine Operating System: Any Operating System Capable of Running VMware (Fully Patched)

Instructor Acceptance

Before the scheduled start of the training class, the instructor should visit the training facility to inspect and approve the setup. The technical contact (system administrator) for the facility must be available to answer questions and correct any setup issues. Both the instructor and technical contact must ensure the completion of the following checklists before the training setup is deemed acceptable.

Firewall Settings

Do not block any ports while accessing the Internet through the firewall. You should be able to ping servers on the Internet.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Blackboard

Write the following in the top-left corner of the blackboard:

- Instructor name: <Name of the instructor>
- Username/Password to login to the student machine

Setup Checklist

The arrangement of items in the setup checklists is designed to validate the setup in the most efficient manner possible. Before beginning the setup checklist, log off any connected users.

Tick Here	List
❑	Verify that VMware Workstation Pro is installed.
❑	Verify that all CHFI tools are on the computer in the **CHFI-Tools** folder in **E:**.
❑	Verify that Internet access is available.
❑	Visit **https://www.eccouncil.org** and view the page to check the Internet access.
❑	Open Command Prompt and enter **nslookup certifiedhacker.com** to look for a connection to the server.
❑	Verify that Acrobat Reader, WinRAR, WinPCap, and Command Prompt extensions are installed.
❑	Verify that the web browsers (Google Chrome and Mozilla Firefox) are installed.
❑	Verify that the instructor computer can display through the overhead projector.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

❑	Verify that each computer has 1 TB or more of free disk space.
❑	Verify whether you can successfully boot the Windows 11, Windows Server 2022, Ubuntu Suspect, and Ubuntu Forensics virtual machines using VMware Workstation.
❑	Verify that the CHFI-Tools folder is shared and mapped to the Windows virtual machines.
❑	Confirm that the cable wiring is organized and labeled.
❑	Confirm that the student workstation and chair are placed satisfactorily.
❑	Confirm that the placement of the LCD (overhead) projector is appropriate.
❑	Confirm that a whiteboard, dry erase markers, and erasers are available.
❑	Confirm that the instructor's station is properly organized and oriented.
❑	Confirm that computers are labeled with a client number.
❑	Ensure that the EC-Council courseware (Official EC-Council CHFIv11 Box) is available to students.
❑	Write down the phone number of the facility's technical contact person. Contact them in case of a network problem.
❑	Confirm that the internal network adapter is configured for the virtual machines and host.

Instructor Acceptance

The facility's technical contact (system administrator) must be available to answer questions and correct any setup issues.

The instructor should inspect both the classroom and the items covered in the setup checklist(s) to ensure that the classroom and setup meet EC-Council standards. Any deficiencies discovered by the instructor must be corrected before the scheduled start time of the class.

Assistance

If you have problems or require assistance in setting up the lab for your CHFI class, please e-mail partnersupport@eccouncil.org.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Detailed Setup Instructions — Configuration Tasks (CT)

CT#1: Install the Host Operating System

1. Install any Windows/Linux/macOS operating system capable of running VMware Workstation Pro using a DVD or USB drive.
2. Configure the hard disk to have one active primary partition (C:\ of 300 GB) and two extended logical partitions (D:\ of 700 GB).
3. Check for updates and, if found, update the host operating system.
4. Install the wireless network adapters according to the manufacturer's instructions.

[Back to Configuration Task Outline]

CT#2: Copy the Host Operating System Files

1. Browse the installation DVD.
2. Copy all the source files from the DVD to the **SOURCES** folder in the drive's active primary partition (e.g., Active Drive Partition Name:\SOURCES).
3. When completed, close all windows to return to the **Desktop**.

[Back to Configuration Task Outline]

CT#3: Install WinRAR on the Host Operating System

1. Download the latest version of **WinRAR** from the official WinRAR website (**https://www.win-rar.com/download.html**).

   Note: Download the latest version of **WinRAR** compatible with your host operating system from the official website (Here, we consider Windows to be the host OS).
2. Double-click on the **.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
3. The **WinRAR** setup window appears. Click **Install**.
4. Complete the installation by choosing the default settings.
5. After completing the installation, the installation location of the WinRAR files is automatically opened in an Explorer window; close the window.

[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#4: Download the ISO File

1. Log in to your **Aspen** account (you will see your course listed under **My Courses**) → click the **TRAINING** button under the course to access the e-Courseware, Lab Manuals, and Tools in the **Training** area → click the **Download Tools** tab from the left-hand pane.
2. Click the **CHFIv11 ISO.zip** file from the right-hand pane to download the ISO files.
3. Navigate to the location where you downloaded the **CHFIv11 ISO.zip** file, right-click the .zip files, and select the **Extract Here** option.

[Back to Configuration Task Outline]

CT#5: Install VMware Workstation Pro on the Host Machine

1. In your host system, navigate to the location where you have extracted the **CHFIv11 ISO.zip** file and then to **CHFIv11 ISO\VMware Workstation Pro**.
2. Double-click the file **VMware-workstation-full-15.5.1-15018445.exe**.

   Note: You can download the latest version of VMware Workstation Pro from https://www.vmware.com/in/products/workstation-pro/workstation-pro-evaluation.html.

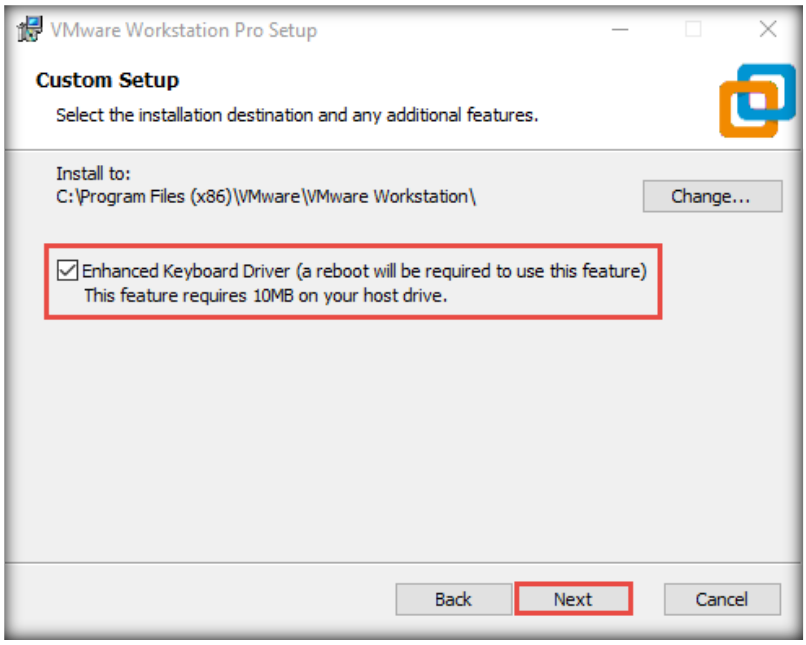
   Note: If you decide to download the latest version, the screenshots in your lab environment might differ from those shown in this guide.
3. A **User Account Control** pop-up window appears. Click **Yes**.

   Note: If a **VMware Product Installation** notification appears, click **Yes** to restart the system.

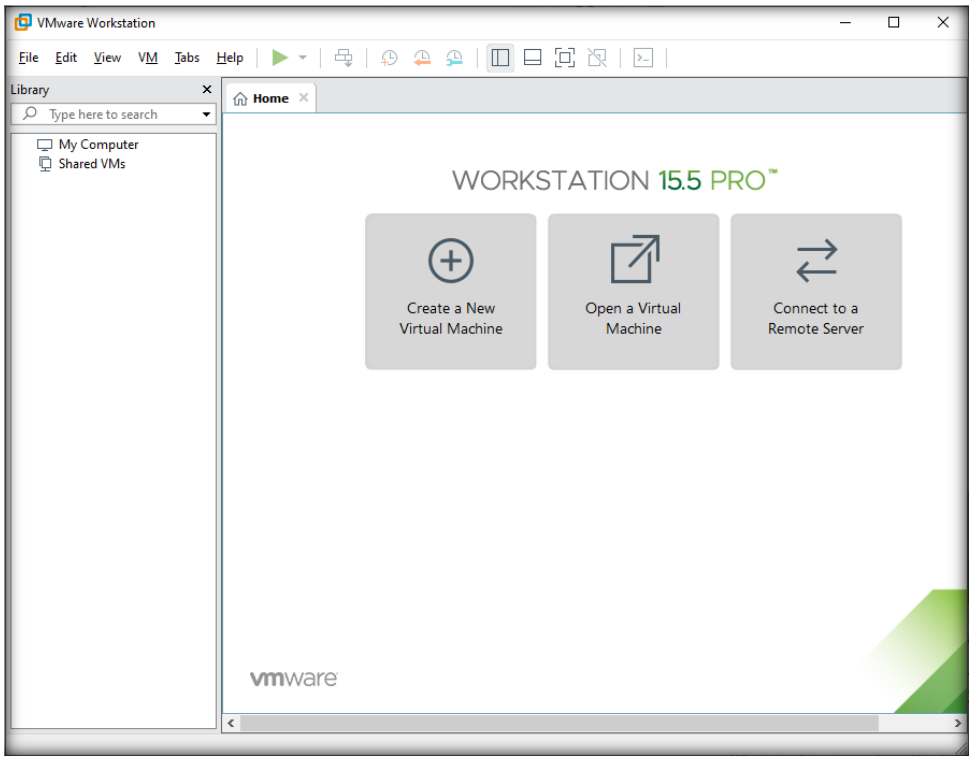
   Note: After the system reboots, double-click the file **VMware-workstation-full-15.5.1-15018445.exe**.
4. VMware Workstation Pro initializes; in the installation wizard, click **Next**.
5. Accept the user agreement and click **Next**.
6. In the **Custom Setup** wizard, check the **Enhanced Keyboard Driver** option and click **Next**.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Follow the wizard-driven installation steps to install VMware Workstation Pro using the default settings.



8. On completion of the installation, the machine will restart.
9. Once the machine has rebooted, launch VMware Workstation Pro.



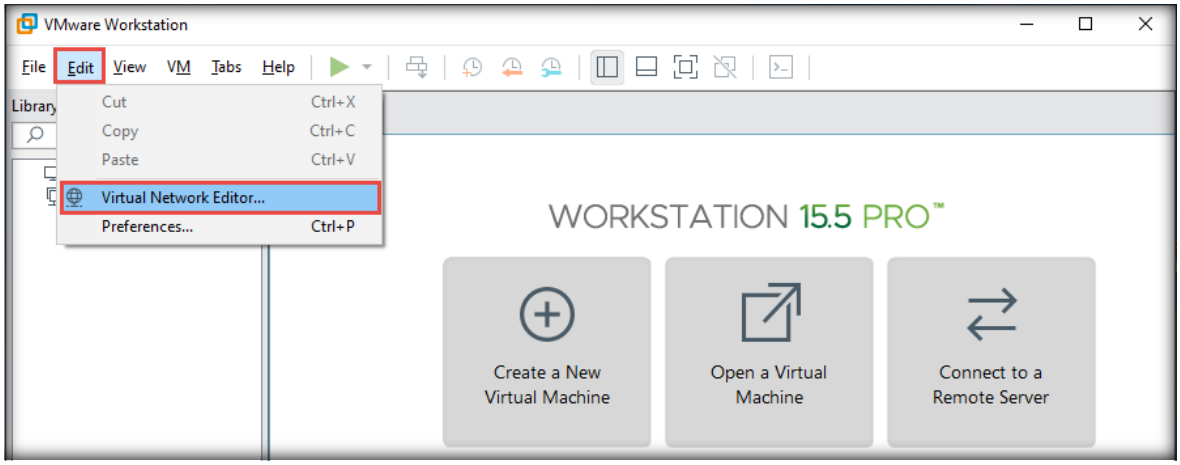
Note: If VMware Workstation Pro prompts for an activation key; provide it, if you have purchased one, or continue with the trial version.

[Back to Configuration Task Outline]

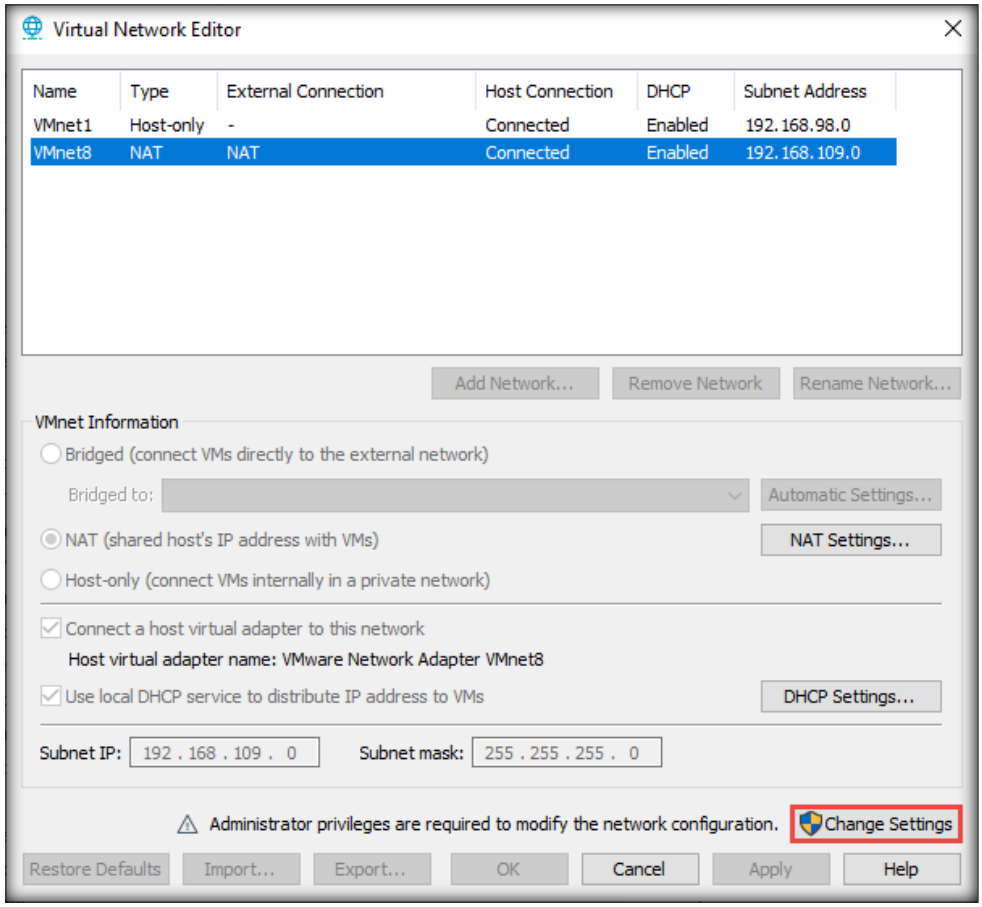
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#6: Configure a Virtual Network in VMware Virtual Network Editor

1. Launch **VMware Workstation Pro**.
2. Navigate to **Edit** and click **Virtual Network Editor...** as shown in the screenshot below.

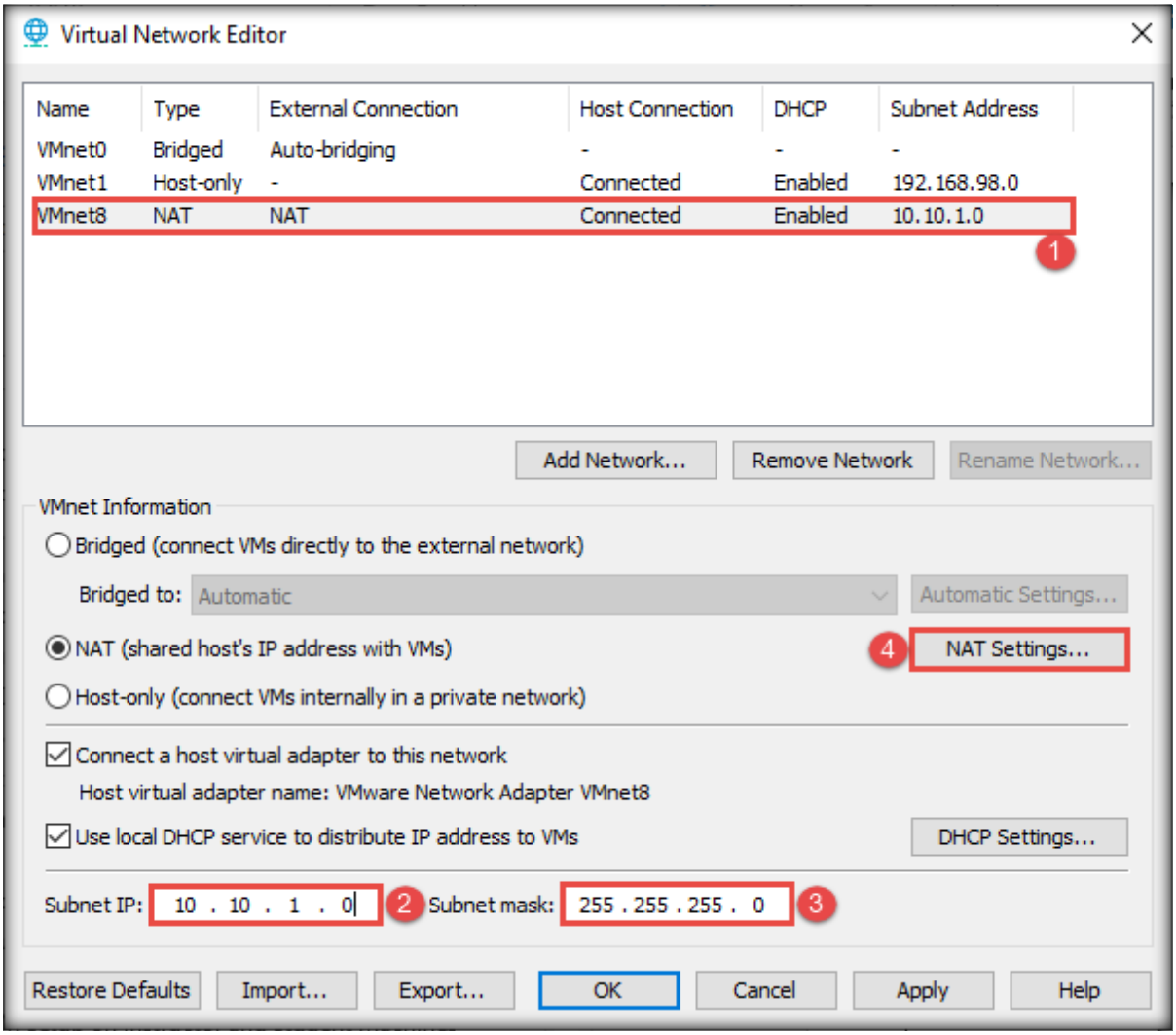


3. The **Virtual Network Editor** window appears; choose the **VMnet8 NAT** network and click **Change Settings** from the lower-right section of the window.



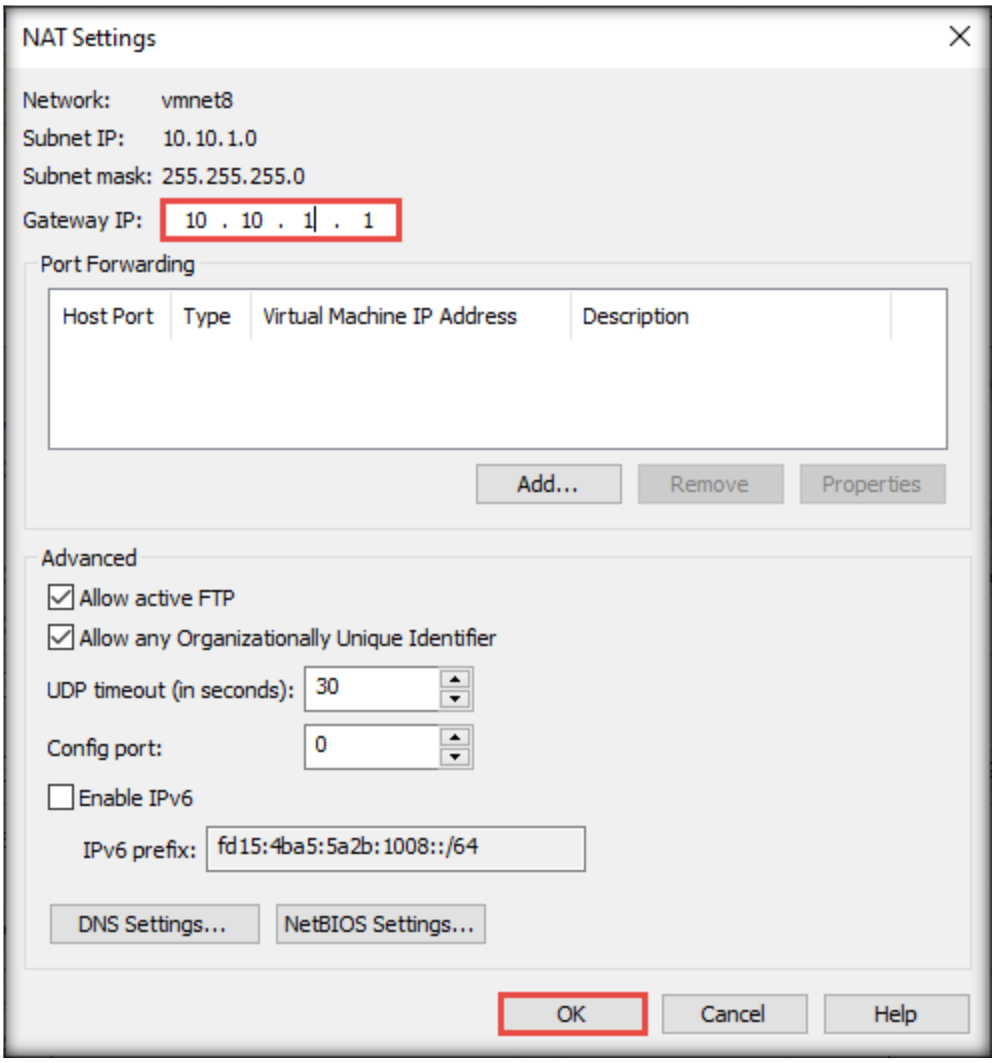
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. If a **User Account Control** pop-up appears, click **Yes**.
5. In the **Virtual Network Editor** window, select **VMnet8** again in the lower section of the window, define **Subnet IP** as **10.10.1.0** and **Subnet mask** as **255.255.255.0**, and click **NAT Settings...**.



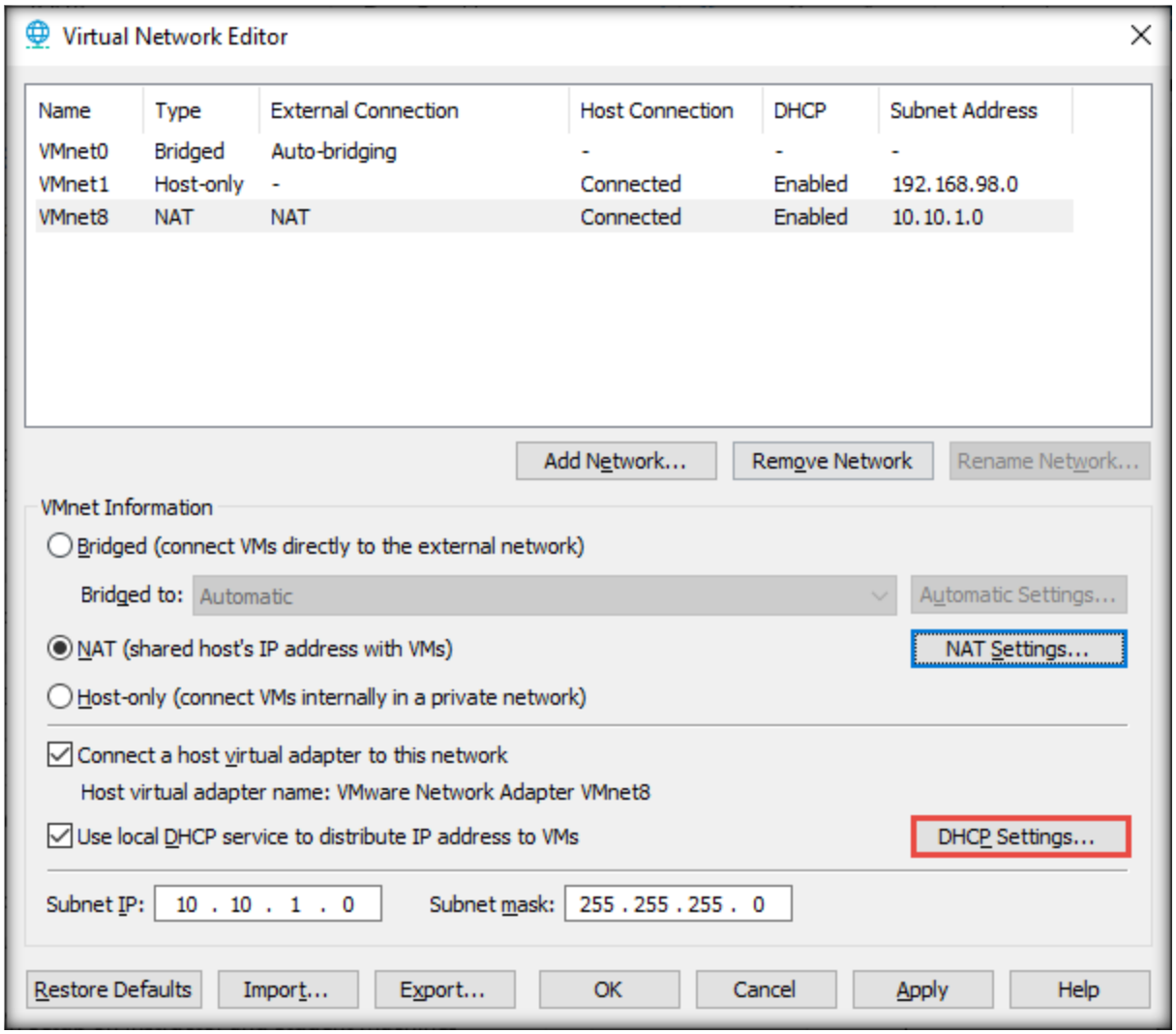
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **NAT Settings** window appears; enter **10.10.1.1** as the **Gateway IP** and click **OK**.



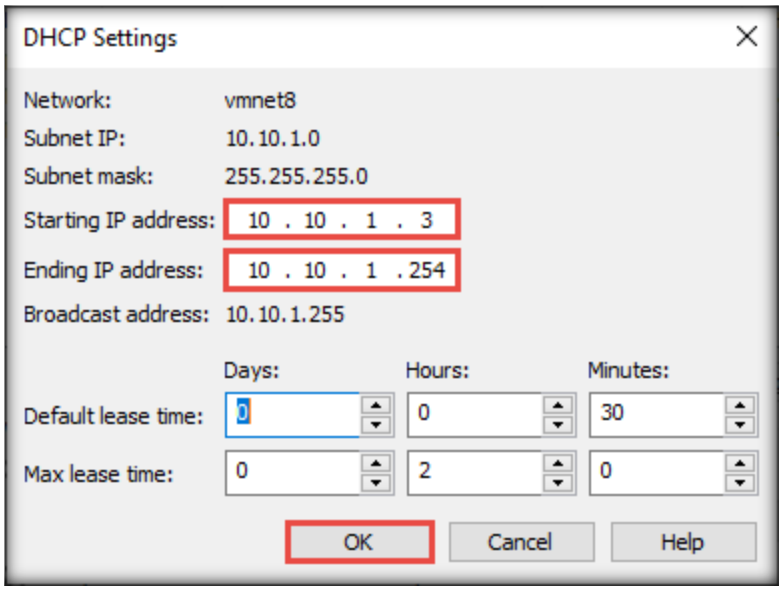
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Now, keep **VMnet8** selected and click **DHCP Settings...**.

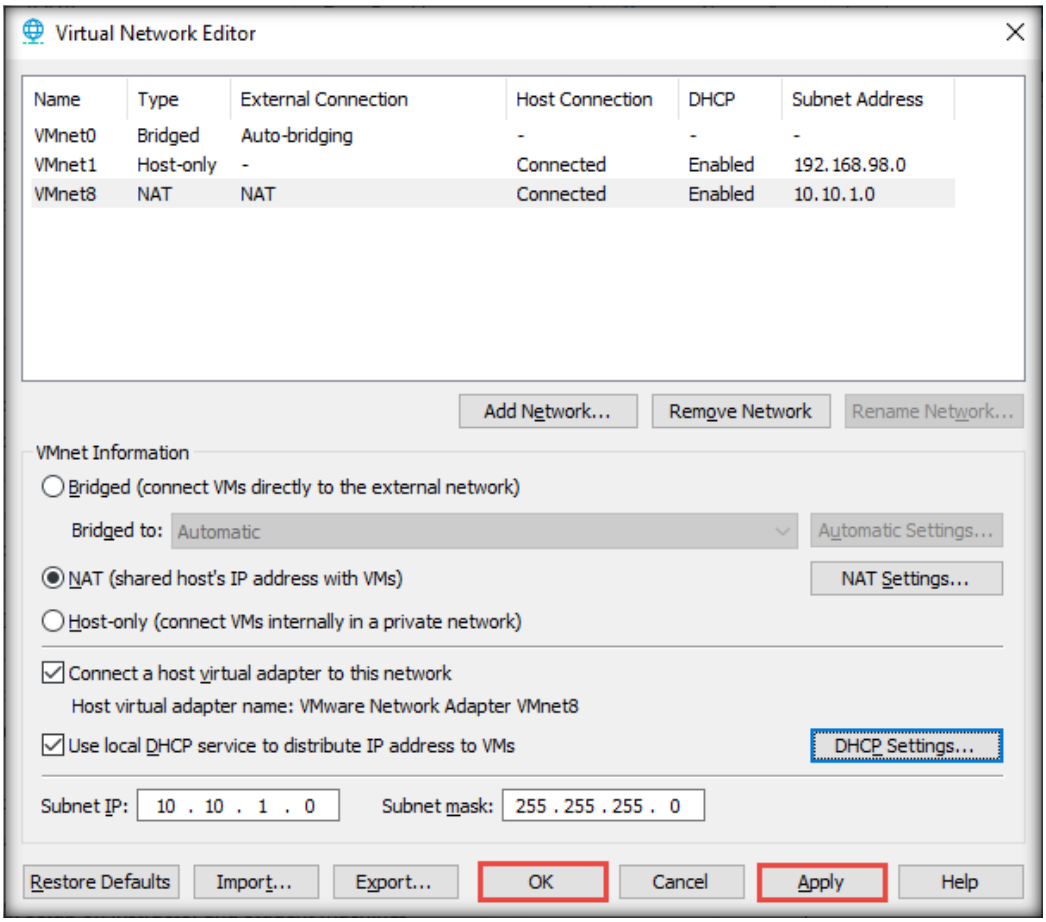


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In the **DHCP Settings** window, define the **Starting IP address** as **10.10.1.3** and the **Ending IP address** as **10.10.1.254**. Click **OK**.



9. Click **Apply** and **OK** in the **Virtual Network Editor** window to complete the configuration.



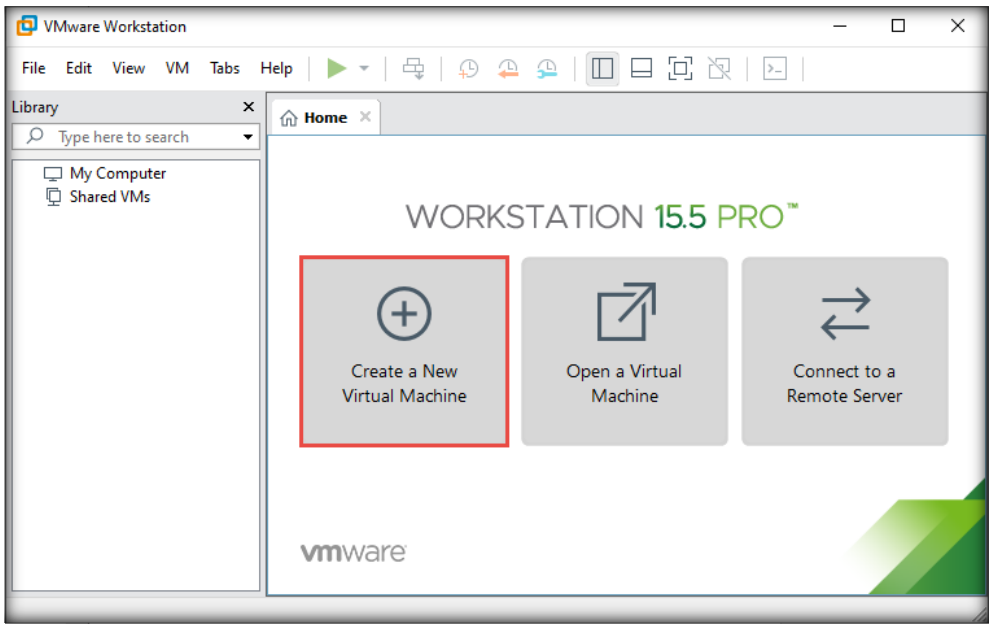
[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

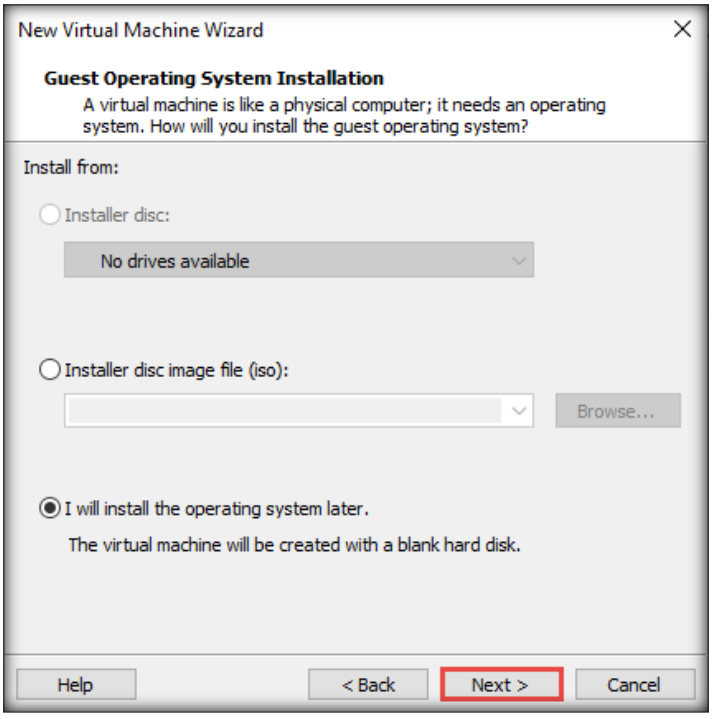
CT#7: Install Windows Virtual Machines in VMware

Install the Windows Server 2022 Virtual Machine

1. In the **VMware Workstation** window, click **Create a New Virtual Machine**.



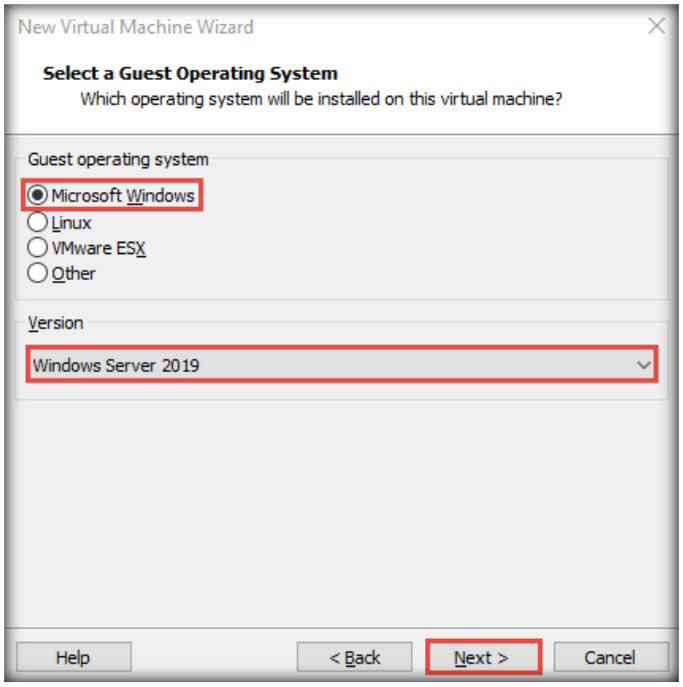
2. In the **New Virtual Machine Wizard** window, leave the settings to default (**Typical**) and click **Next**.
3. In the **Guest Operating System Installation** wizard, choose the **I will install the operating system later** radio button (if you have an ISO of **Windows Server 2022**) and click **Next**.



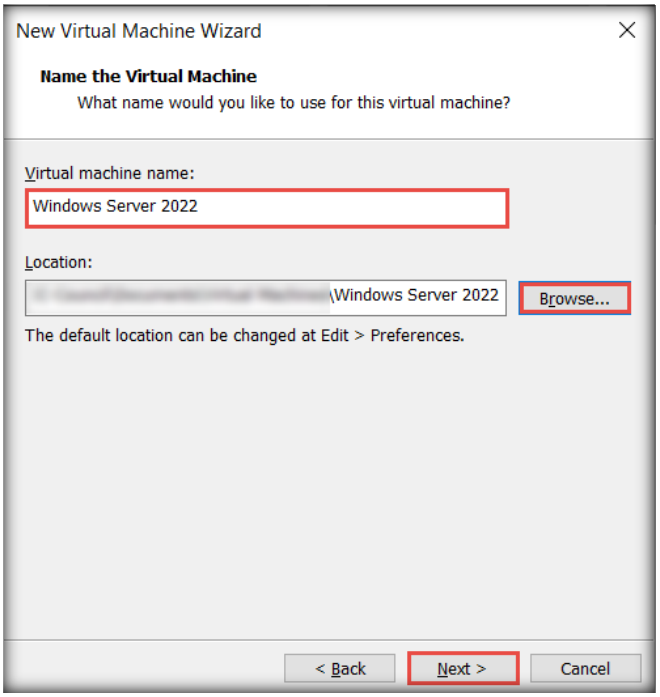
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. In the **Select a Guest Operating System** wizard, ensure that the **Microsoft Windows** radio button is selected in the **Guest operating system** section and that **Windows Server 2019** is selected under **Version**. Click **Next**.

   Note: If the **Windows Server 2019** option is not available in the **Version** drop-down list, then select **Windows Server 2016**.

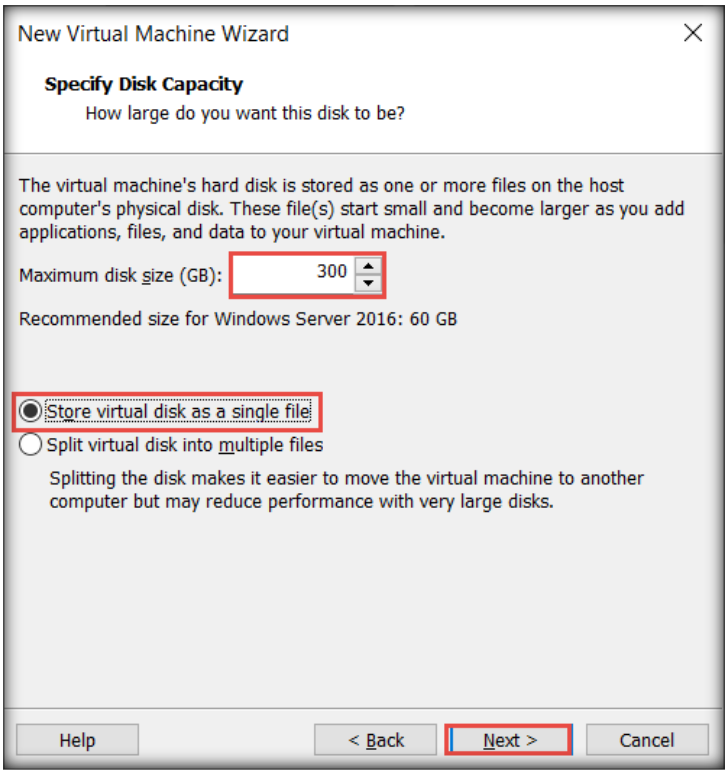


5. The **Name the Virtual Machine** wizard appears; type **Windows Server 2022** in the **Virtual machine name** field and click the **Browse** button to store the virtual hard disk. Choose your desired location to store the hard disk and then click **Next**.

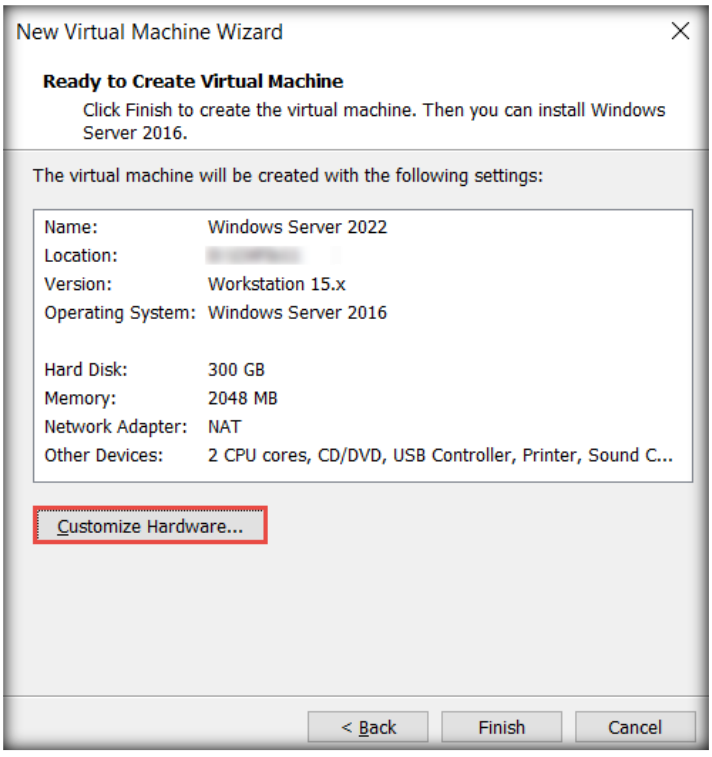


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **Specify Disk Capacity** wizard appears. In the **Maximum disk size (GB)**, set it to **300 GB**, select the **Store virtual disk as a single file** radio button, and click **Next**.

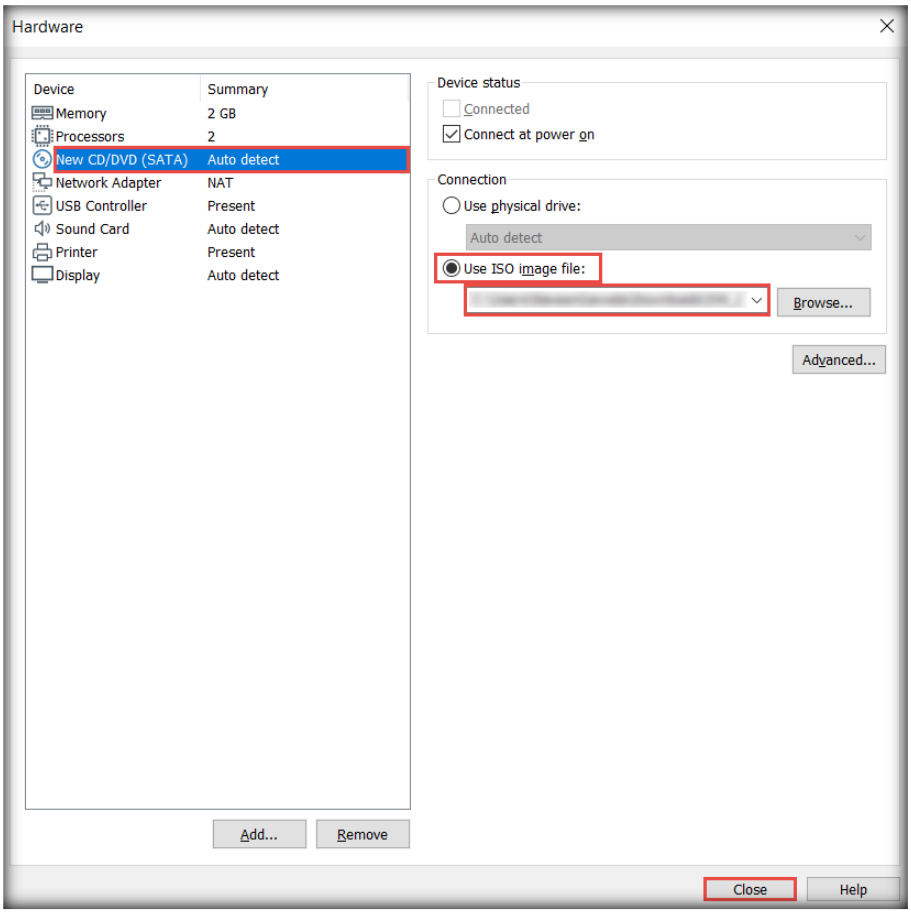


7. The **Ready to Create Virtual Machine** wizard appears; confirm the settings and click the **Customize Hardware...** button.



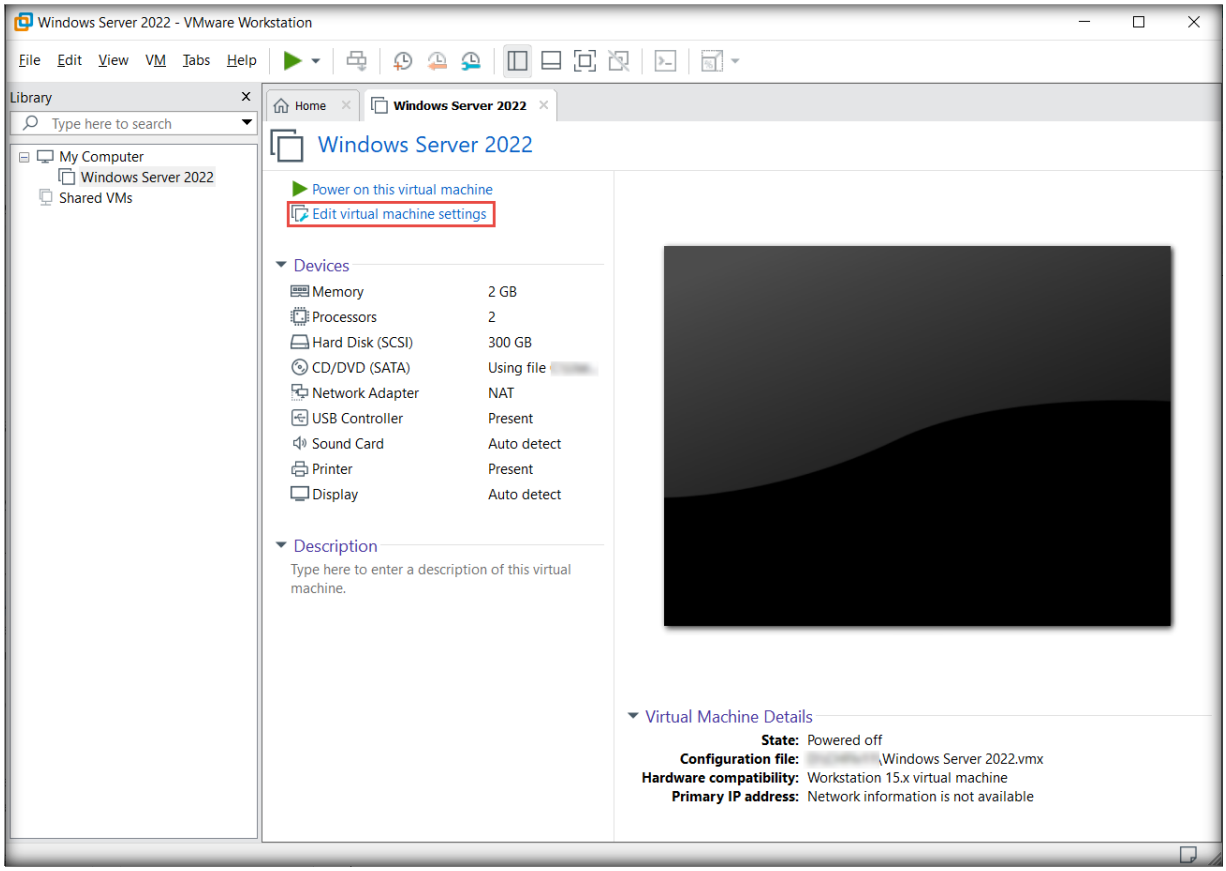
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **Hardware** window appears; click the **New CD/DVD (SATA)** option from the left-hand pane. In the right-hand pane, select the **Use ISO image file** radio button and then click the **Browse...** button to provide the ISO path of **Windows Server 2022** ISO file. Click **Close**.



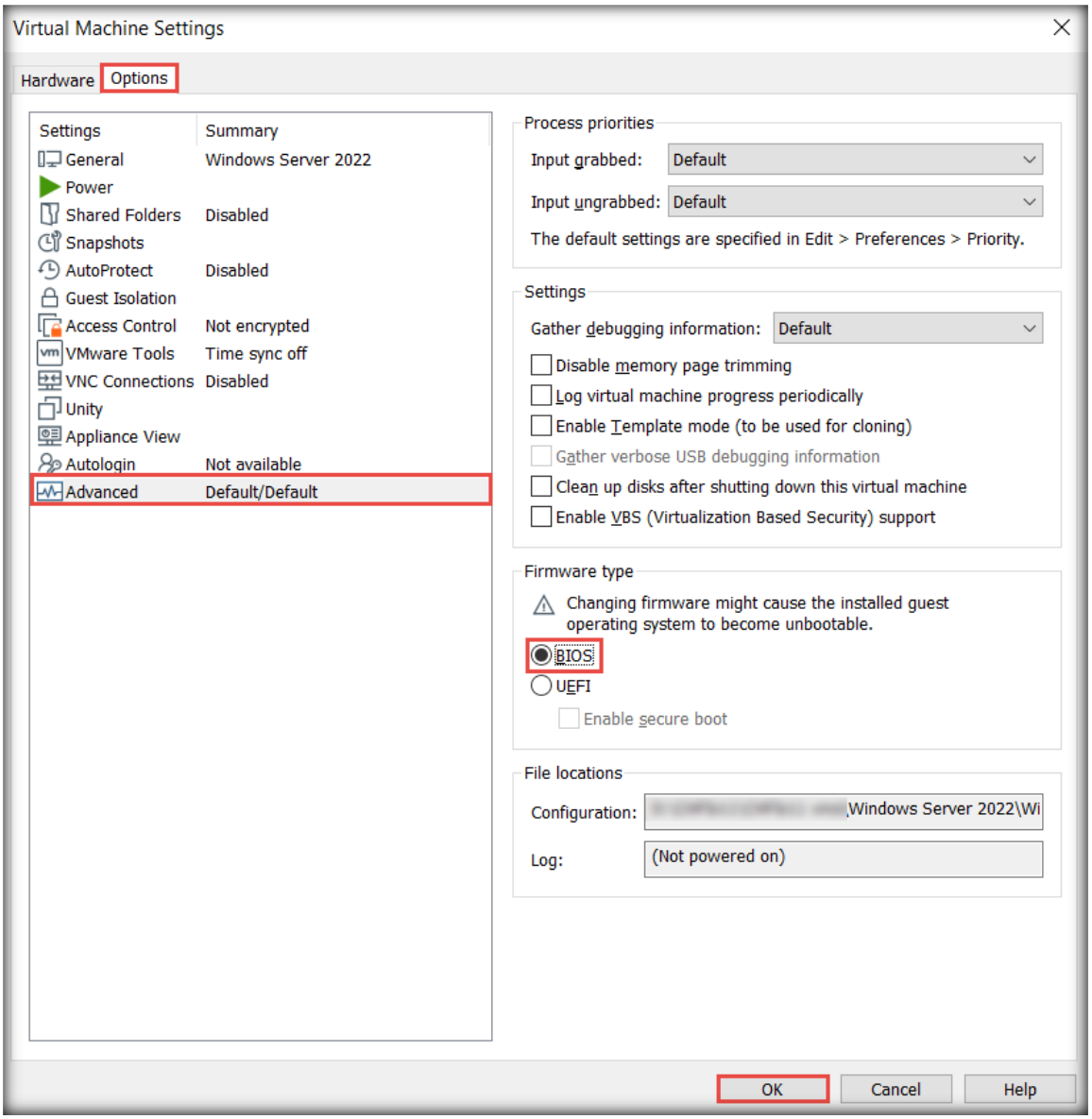
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. In the **Ready to Create Virtual Machine** wizard, click **Finish**.
10. The **Windows Server 2022** virtual machine appears; click the **Edit virtual machine settings** option.



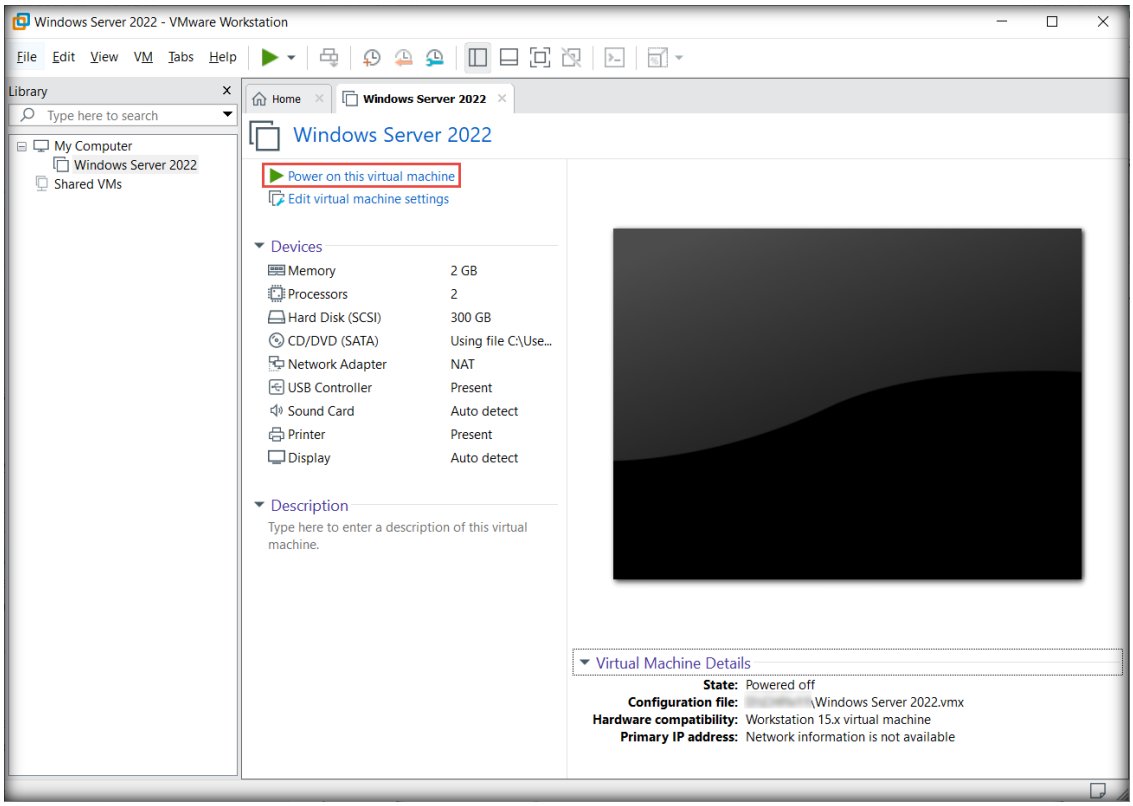
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The **Virtual Machine Settings** window appears; click the **Options** tab.
12. In the **Options** tab, click the **Advanced** option from the left-hand pane.
13. Select the **BIOS** radio button under the **Firmware type** section in the **Advanced** options and click **OK**.



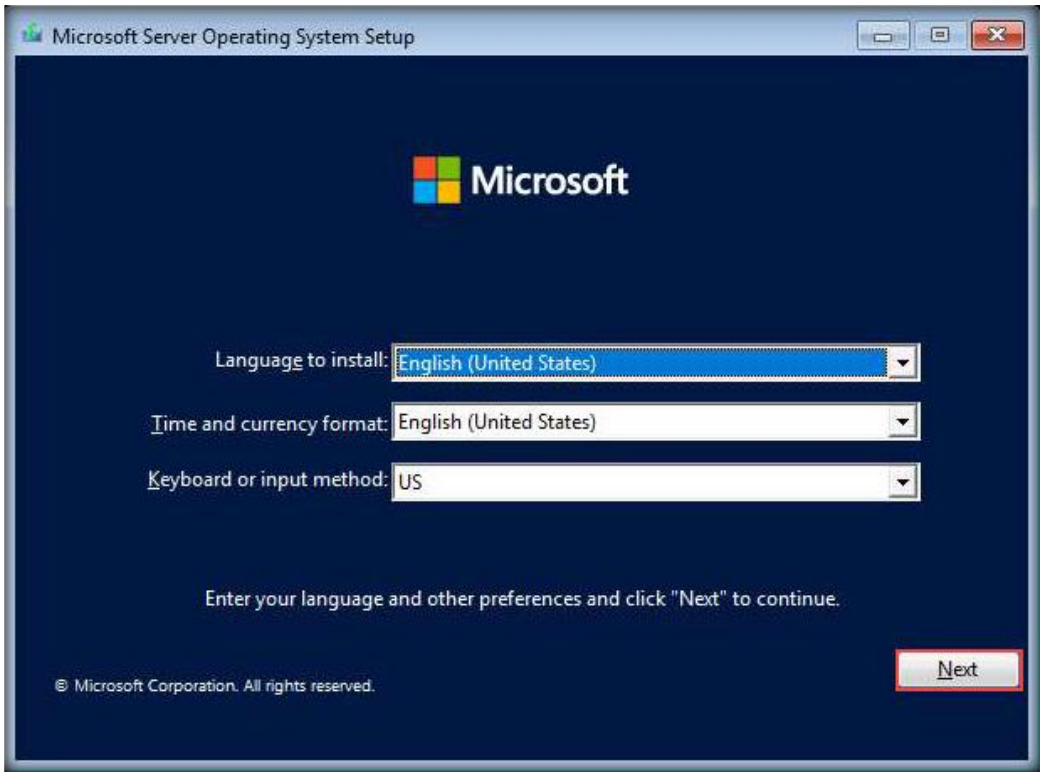
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Click the **Power on this virtual machine** option to launch the **Windows Server 2022** virtual machine.

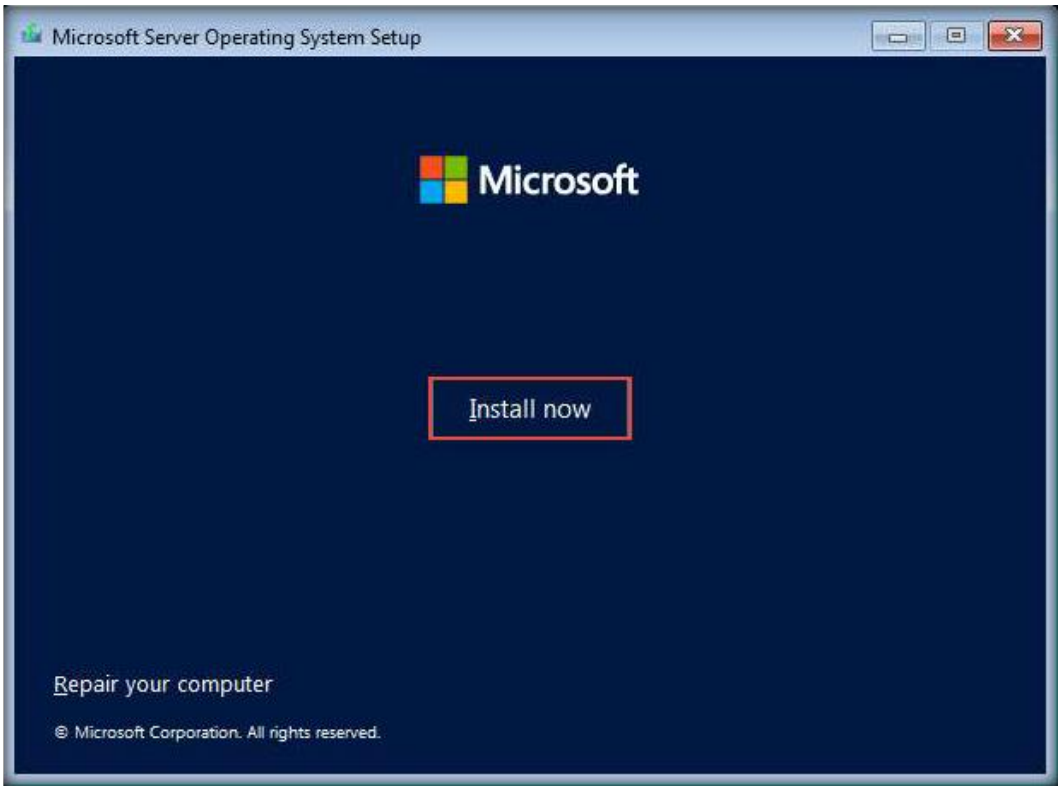


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. The virtual machine initializes, and the **Windows Setup** window appears. In the first window of the setup, leave the default settings and click **Next**.

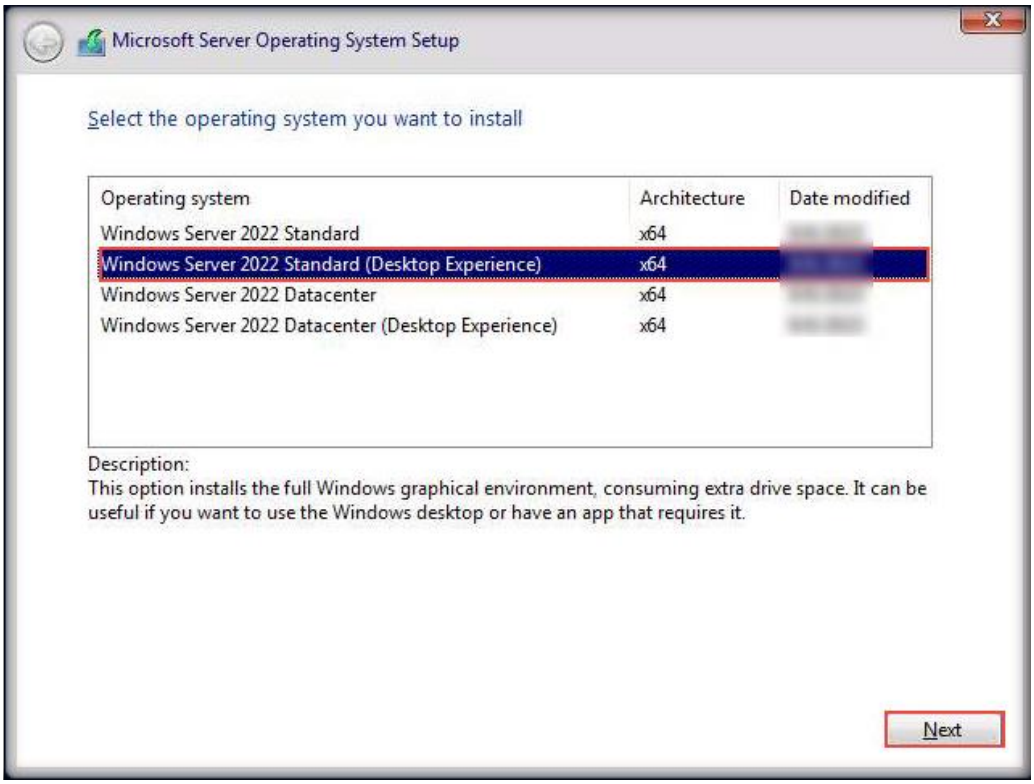


16. In the next window, click the **Install now** button to begin the installation.

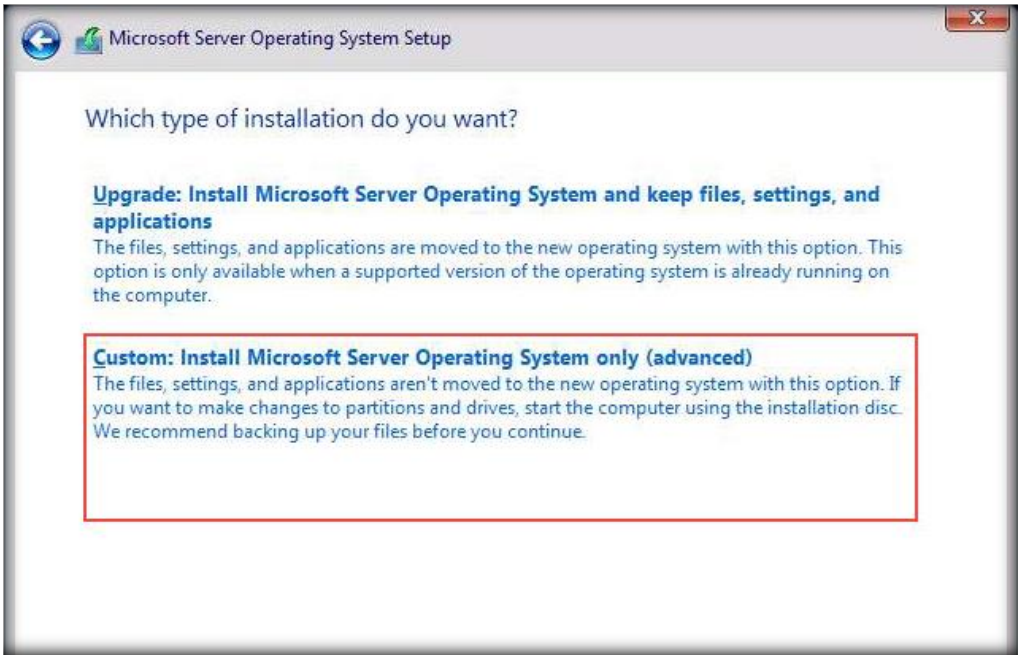


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. In the **Select the operating system you want to install** wizard, select **Windows Server 2022 Standard (Desktop Experience)**, and click **Next**.

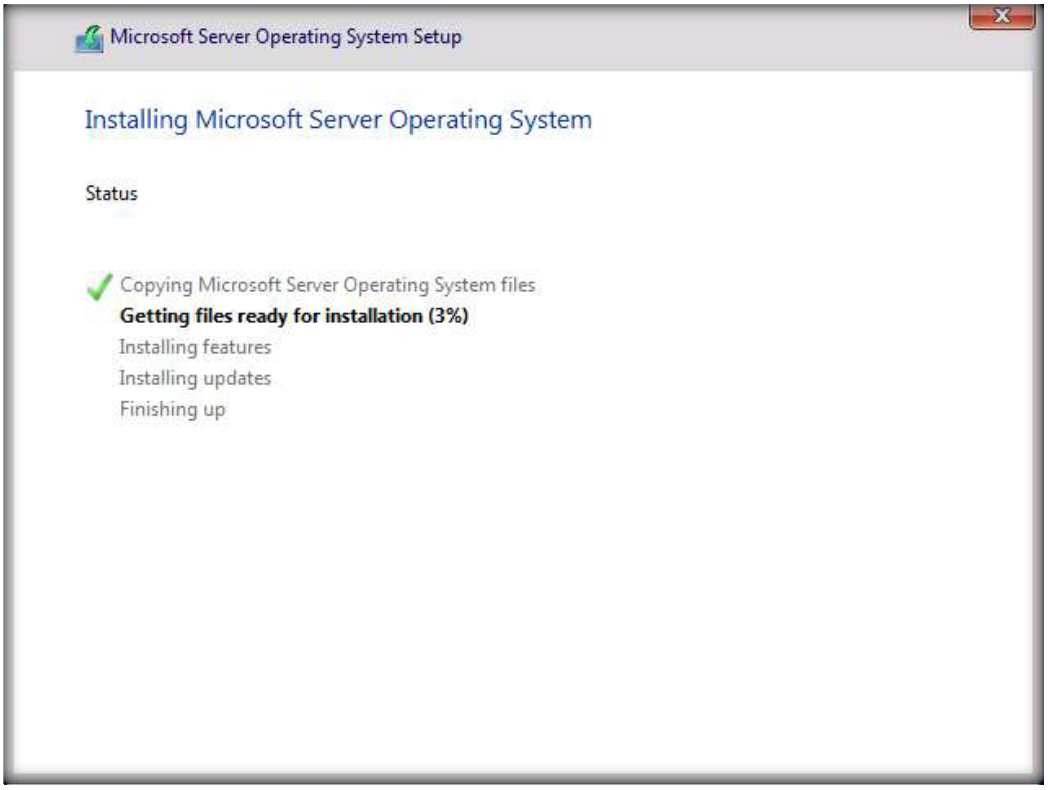


18. In the **Applicable notices and license terms** wizard, check the **I accept the license terms** checkbox and click **Next** to proceed.
19. In the **Which type of installation do you want?** wizard, click the **Custom: Install Microsoft Server Operating System only (advanced)** option.

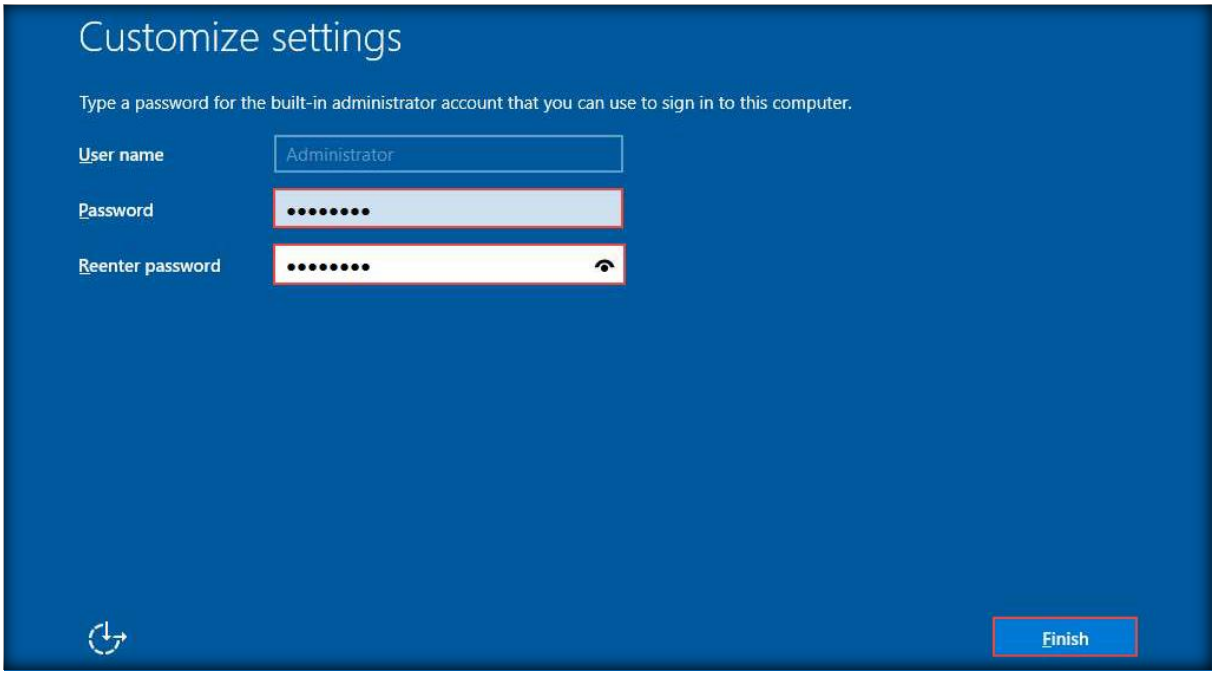


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. In the **Where do you want to install Windows?** wizard, click **Next**.
21. The installation of the **Windows Server 2022** operating system begins. The machine restarts once the installation has been completed.

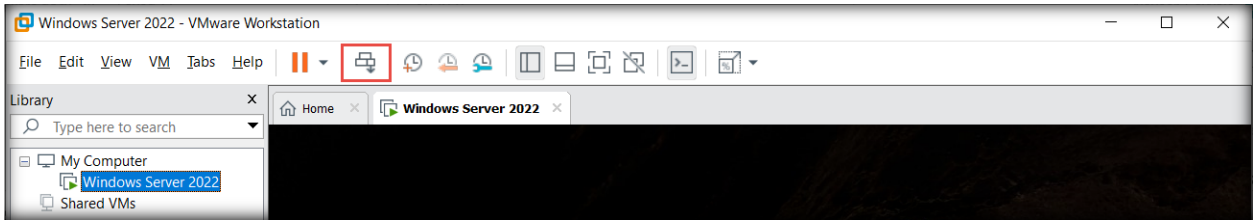


22. After the system reboots, the **Customize settings** wizard appears; leave the default **User name**, which is **Administrator**. Type **Pa$$w0rd** in the **Password** and **Reenter password** fields. Click **Finish**.



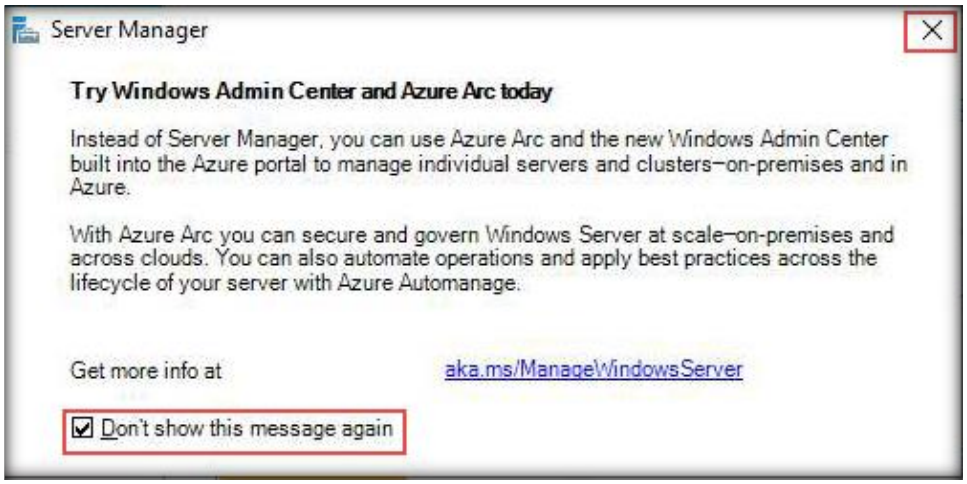
Computer Hacking Forensic Investigator Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. The machine starts and the lock screen appears; click the **Send Ctrl+Alt+Del to this virtual machine** icon ( ) from the menu bar.



24. Log in to the **Administrator** account by typing **Pa$$w0rd** as the password and pressing **Enter**.

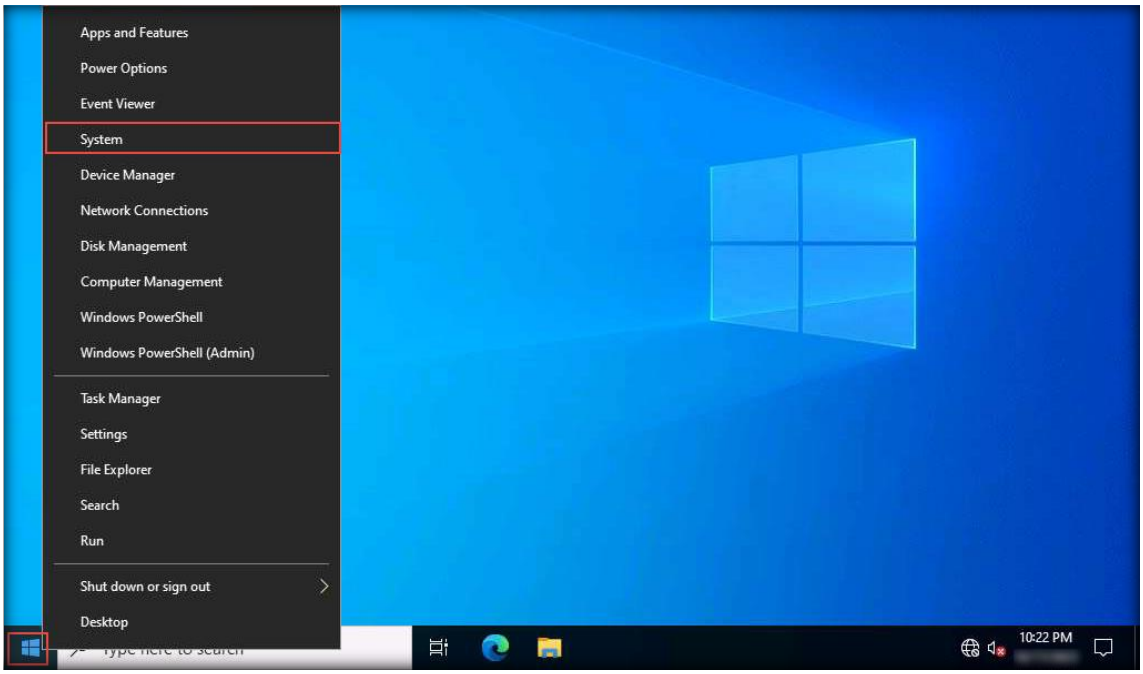
25. The **Networks** notification appears in the right-hand pane; click **Yes**.
26. The **Server Manager** window also appears, along with the **Server Manager** pop-up window. Select the **Don't show this message again** checkbox and close both the **Server Manager** pop-up and **Server Manager** windows.



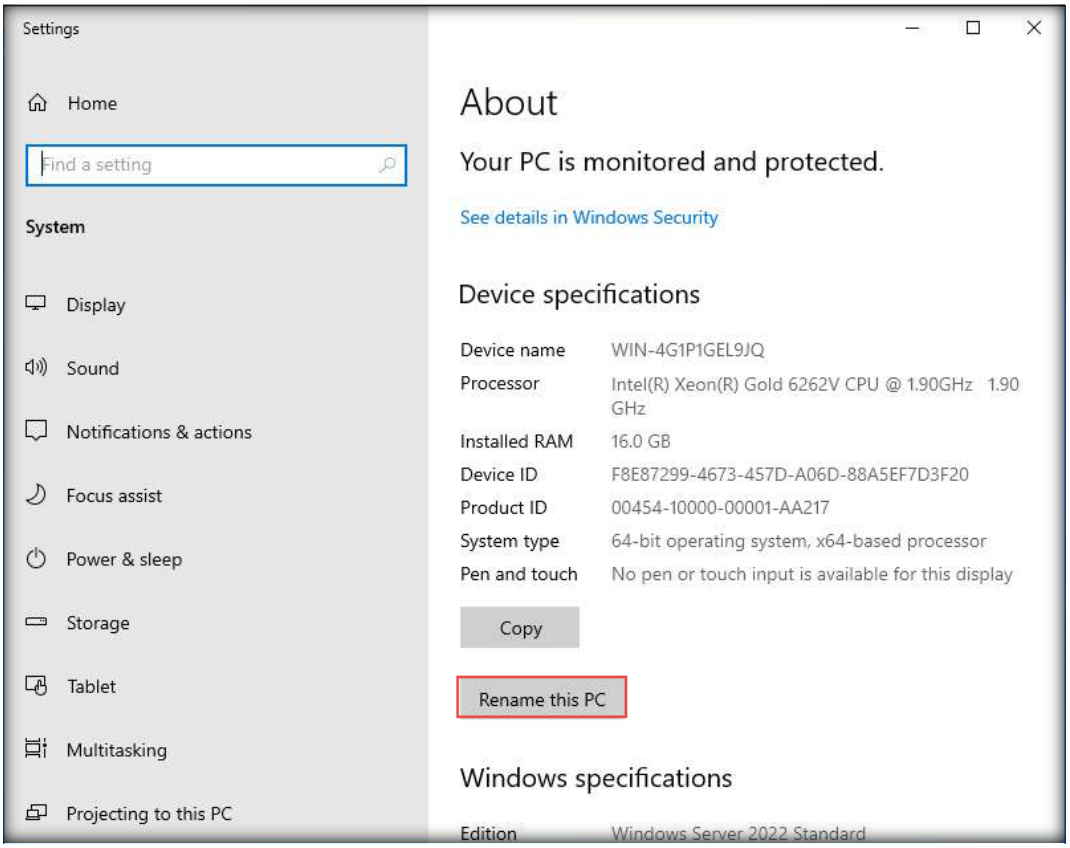
Note: If the **VMware Tools Setup** wizard appears, wait for the installation to complete. After the installation has been completed, if a prompt to restart the machine appears, click **Yes**. Log in to the **Administrator** account by typing **Pa$$w0rd** as the password and pressing **Enter**.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Right-click the **Start** button in the bottom-left corner of the **Desktop** and click **System** from the context menu.

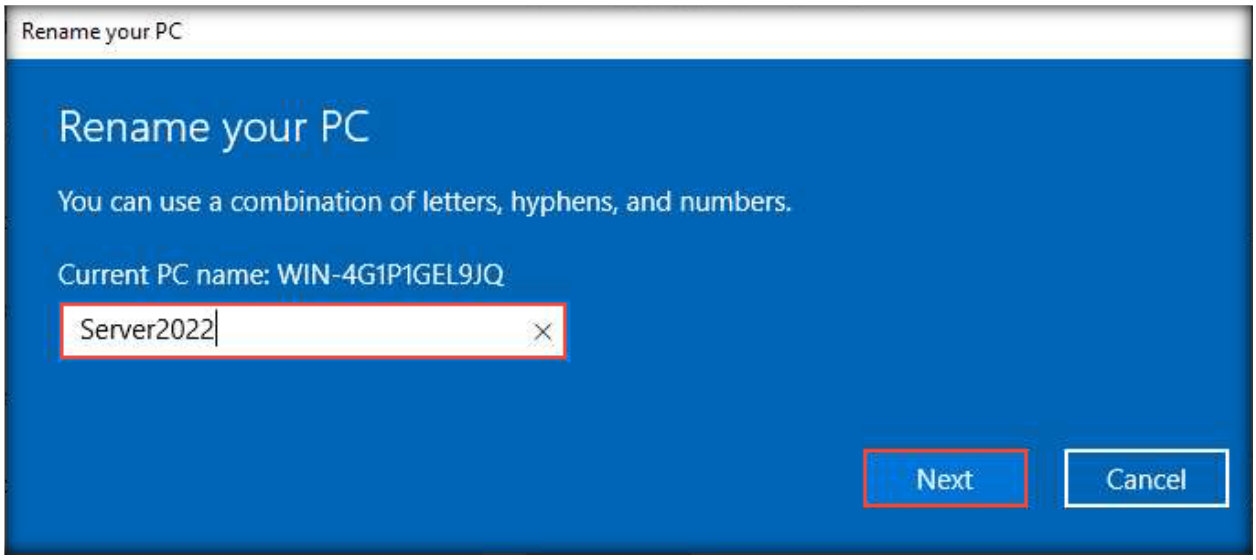


28. The **Settings** window appears; click **Rename this PC**.

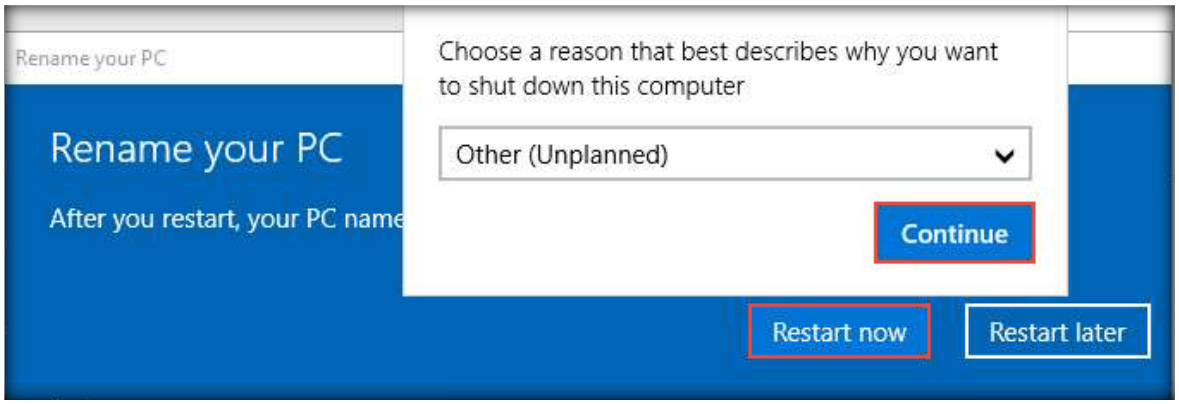


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. The **Rename your PC** pop-up window appears; type **Server2022** in the box and click **Next**.



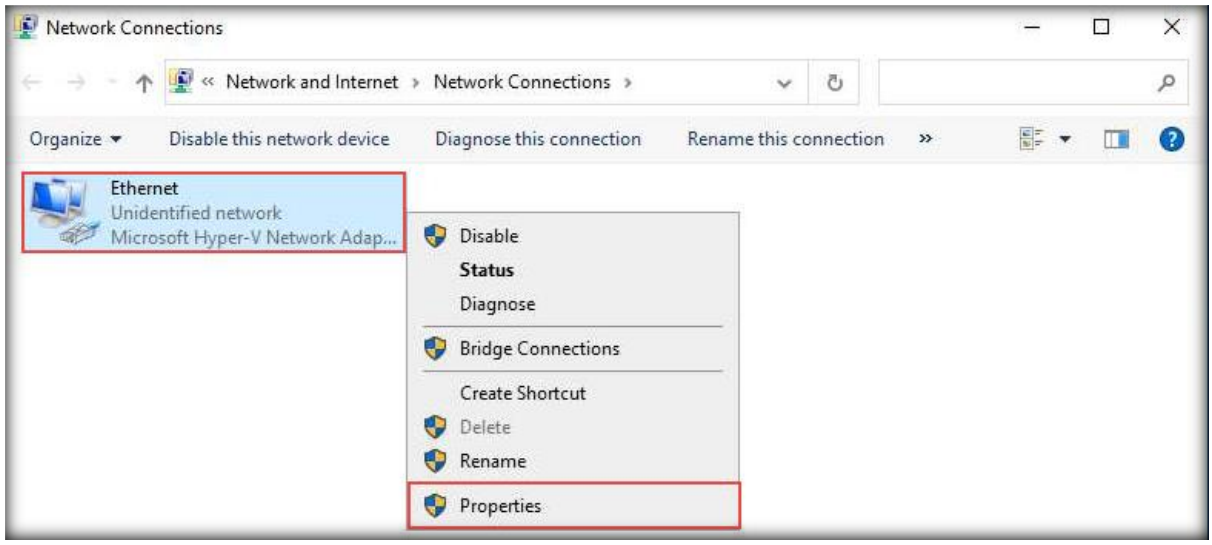
30. After the renaming process, click the **Restart now** and then **Continue** buttons to apply the changes.



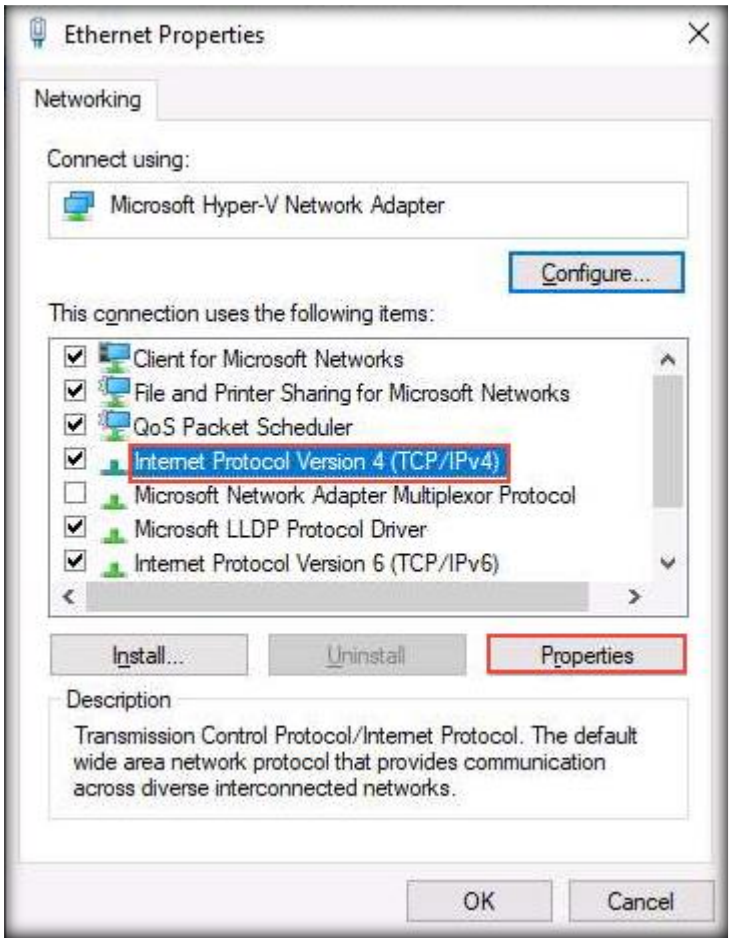
31. After the virtual machine restarts, log in to the virtual machine with the credentials **Administrator** and **Pa$$w0rd** and close the **Server Manager** window. Open the **Network and Sharing Center** and click the **Change adapter settings** link from the left pane.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. The **Network Connections** window appears. Right-click the network interface (here, **Ethernet**) and click **Properties**.

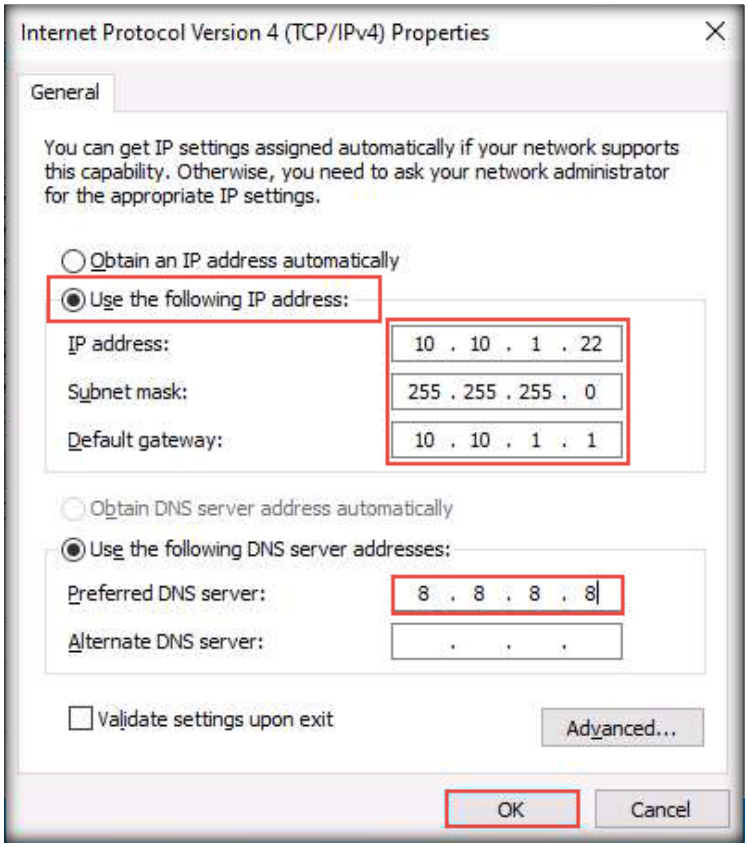


33. The **Ethernet Properties** window appears; scroll down the list, select **Internet Protocol Version 4 (TCP/IPv4)**, and click on **Properties**.

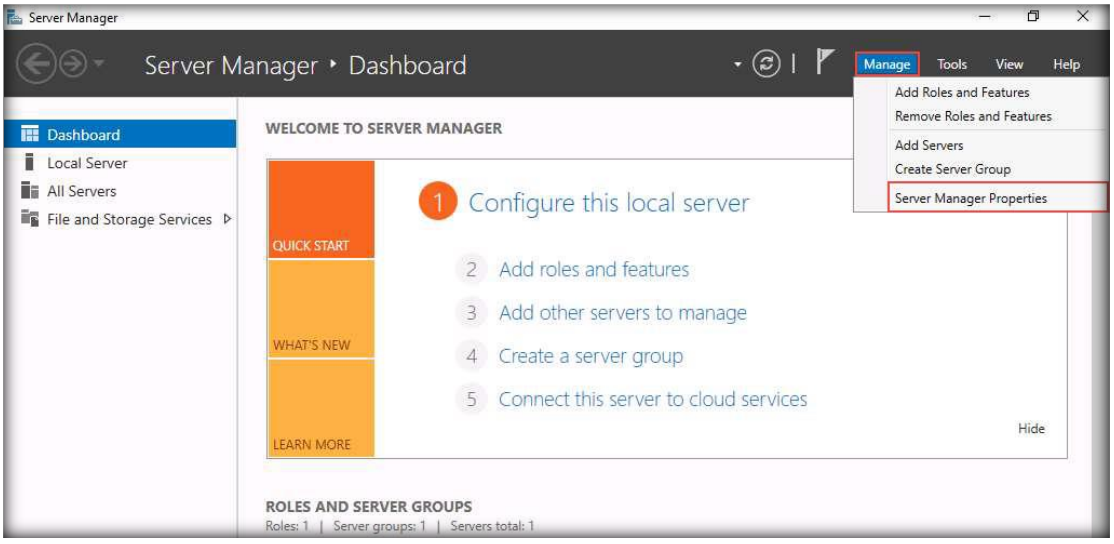


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

34. Select the **Use the following IP address** radio button. Assign **10.10.1.22** as the **IP address**, **255.255.255.0** as the **Subnet mask**, and **10.10.1.1** as the **Default gateway**.
35. Assign **8.8.8.8** as the **Preferred DNS server** address and click **OK**.

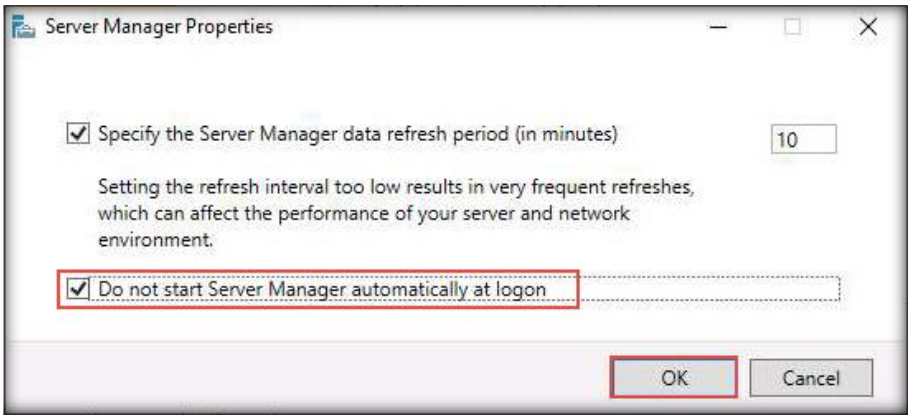


36. Close the **Ethernet Properties** window, then close all open windows.
37. Click on the **Start** icon in the bottom-left corner of the **Desktop**. Click **Server Manager** from the available applications.
38. In the **Server Manager** window, navigate to **Manage** → **Server Manager Properties**.

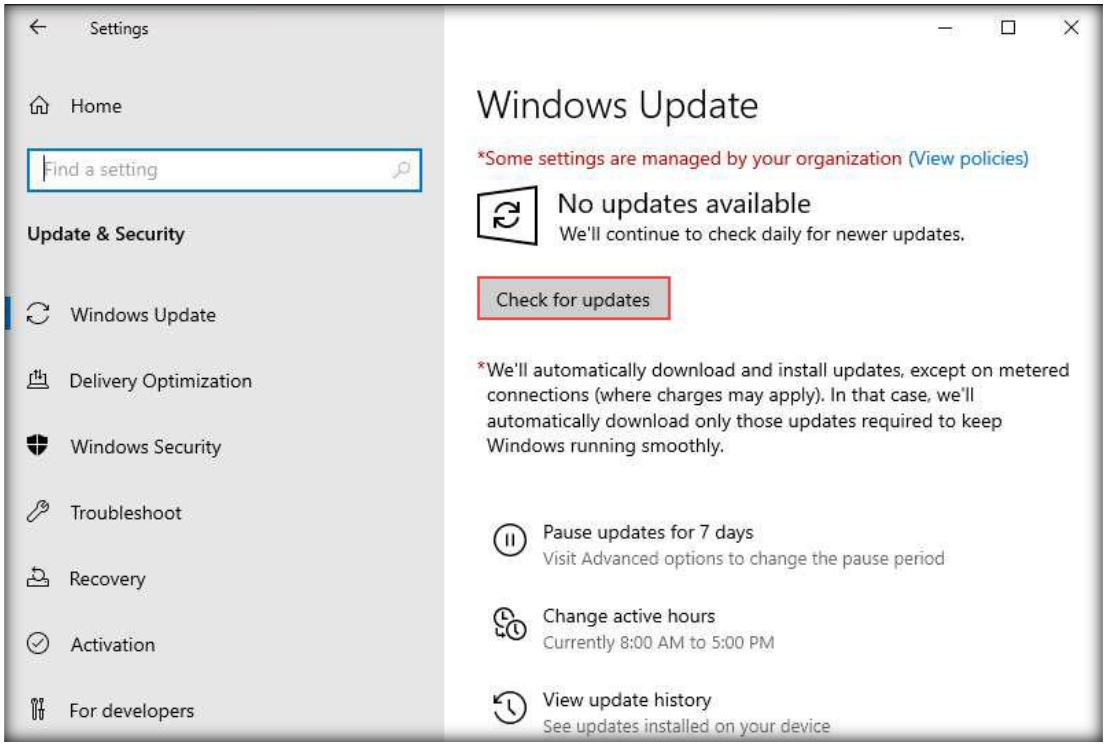


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. The **Server Manager Properties** window appears. Check the **Do not start Server Manager automatically at logon** option and click **OK**.



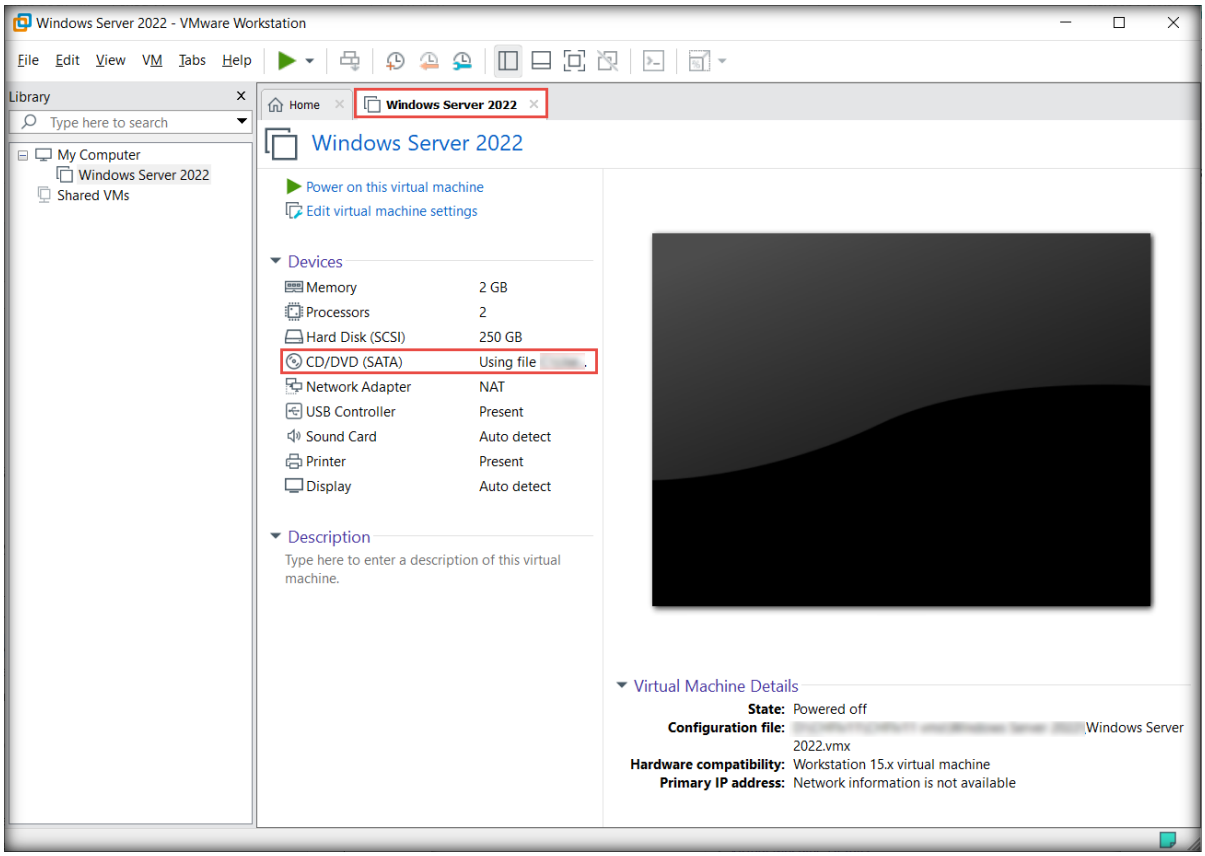
40. Close the **Server Manager** window.
41. Right-click the **Windows** button in the lower-left corner of the screen and click **Settings**.
42. In the **Settings** window, click **Update & Security**.
43. Click **Check for updates** from the right-hand pane.



44. Check for and install the latest updates.
45. After installing all the updates, restart the machine.

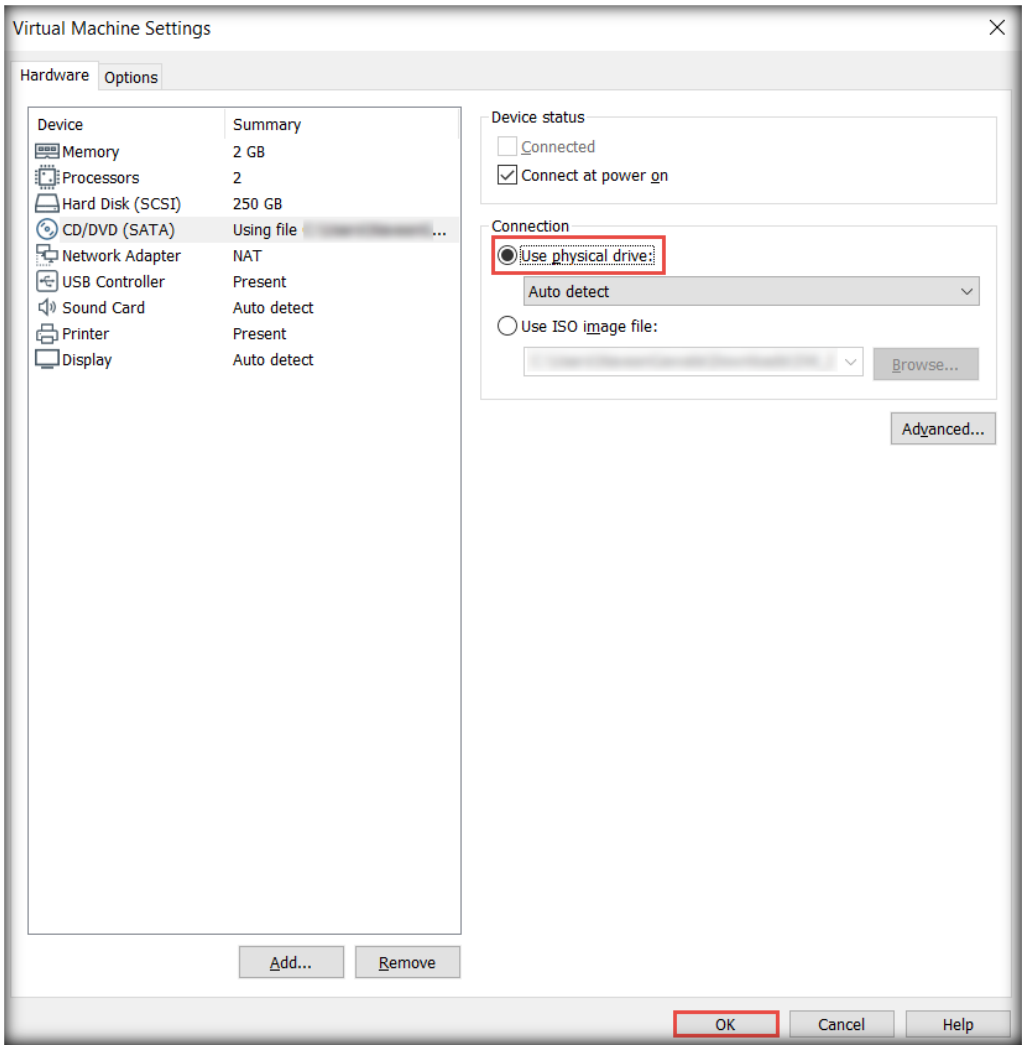
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

46. Turn off the virtual machine. In the **Devices** section of the **Windows Server 2022** tab, click **CD\DVD (SATA)**.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

47. The **Virtual Machine Settings** window appears; choose the **Use physical drive:** radio button in the **Connection** section and click **OK**.



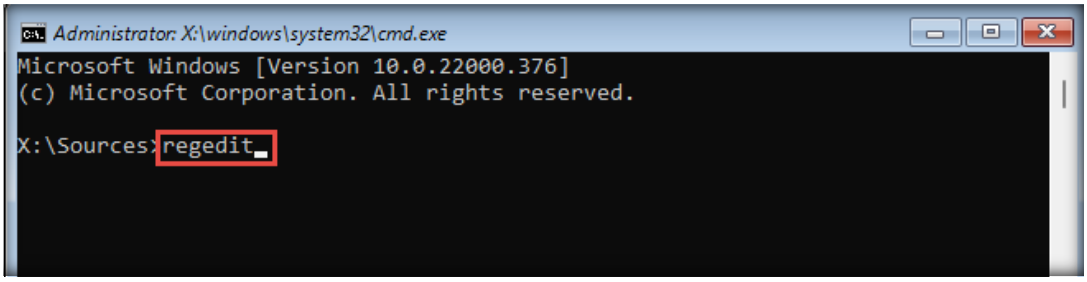
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Install the Windows 11 Virtual Machine

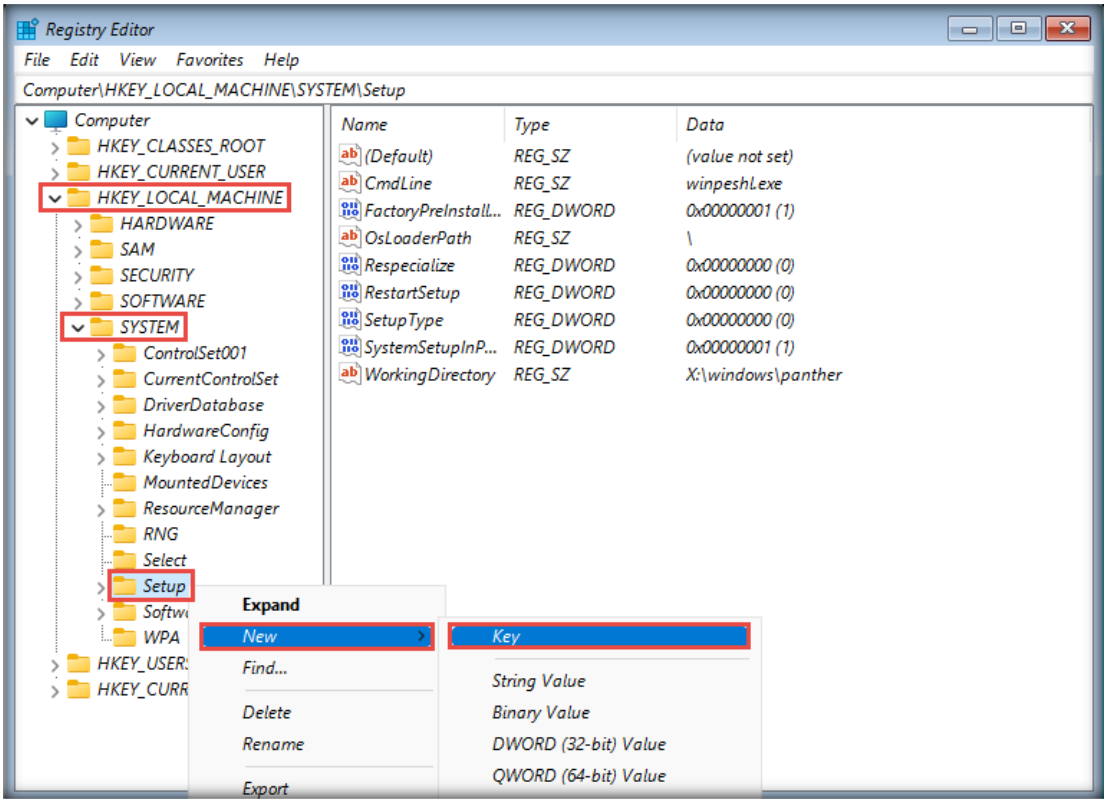
48. Similarly, create and install a **Windows 11 Enterprise** virtual machine with a hard disk space of **80 GB** and **2048 MB** of RAM. Include the following changes:
    - In the **Select a Guest Operating System** wizard, select **Windows 10 x64** as the **Version**.
    - Virtual machine name: **Windows 11.**
    - In the **Select the operating system you want to install** wizard, select **Windows 11 Pro** and click **Next**.

      Note: If **This PC can't run Windows 11** error appears, follow the below steps:

      - Press **Shift+F10**, and a **Command Prompt** window appears.
      - In the **Command Prompt** window, type **regedit** and press **Enter**.

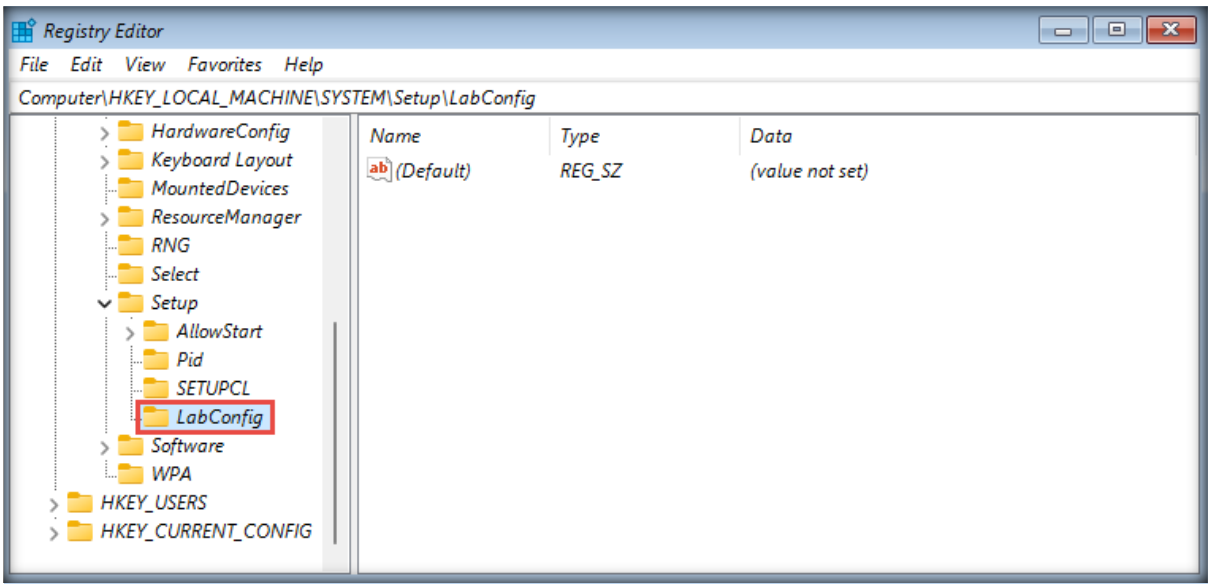


      - **Registry Editor** window appears, from the left-pane navigate to **HKEY_LOCAL_MACHINE → SYSTEM**. Right-click the **Setup** node and navigate to **New → Key**.

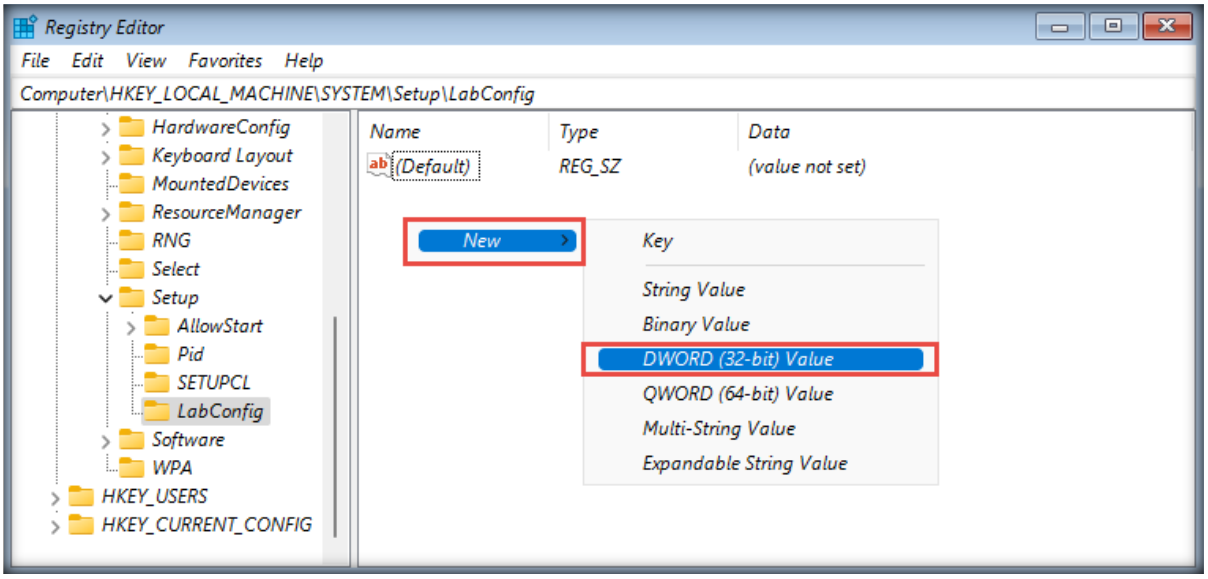


Computer Hacking Forensic Investigator Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- A new key has been created. Rename it as **LabConfig** and press **Enter**.

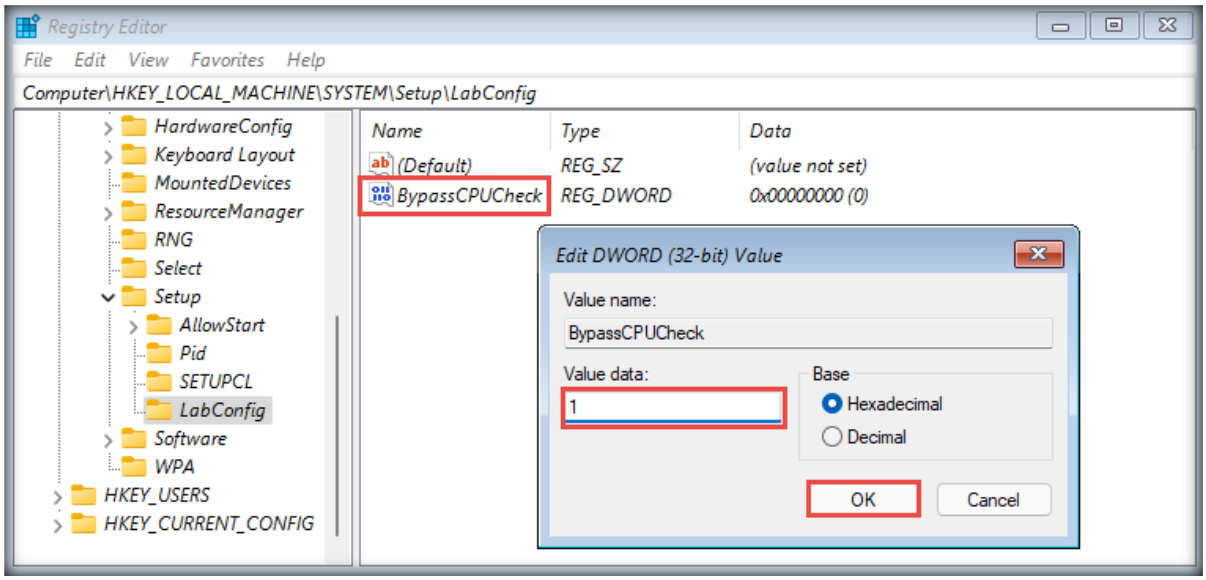


- Right-click anywhere in the right-pane and navigate to **New → DWORD (32-bit) Value**.

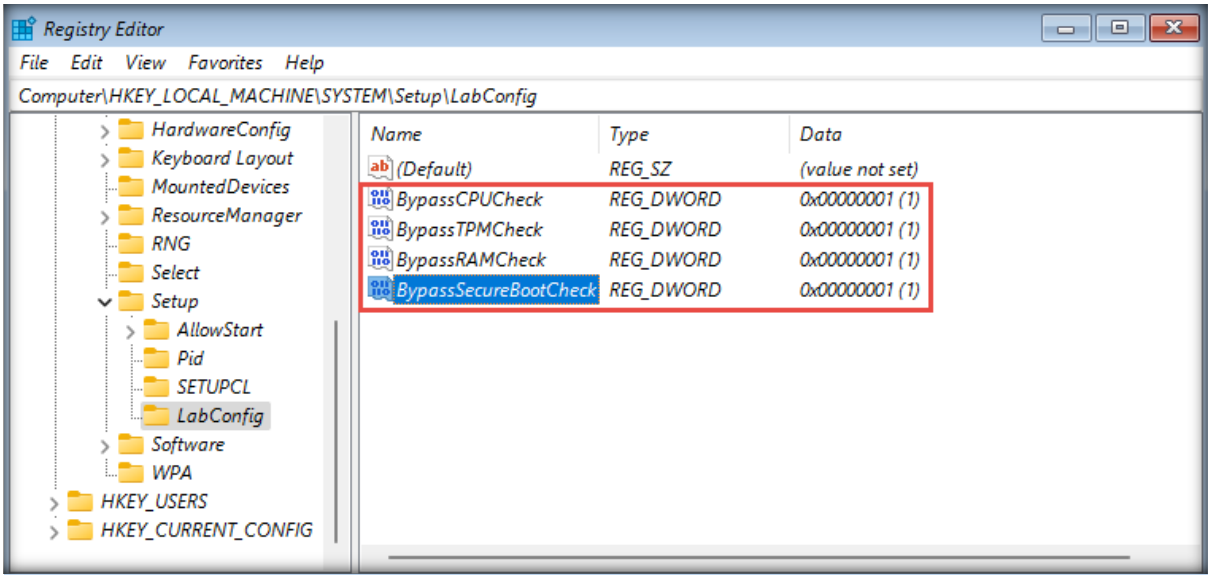


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Rename the value as **BypassCPUCheck** and press **Enter**.
- Now, right-click **BypassCPUCheck** value and select **Modify...** option.
- **Edit DWORD (32-bit Value)** pop-up appears, change the **Value data** to **1** and click **OK**.



- Similarly, create **BypassTPMCheck**, **BypassRAMCheck** and **BypassSecureBootCheck** values (For each of the values, set the **Value data**=**1**).



- Now, close all the windows (Registry Editor, Command Prompt and Error window).
- In the **Windows Setup** window, click **Yes**.
- Click the **Install Now** button and proceed with the default installation steps.

o After completing the installation, **Is this the right country or region?** wizard appears. Select your country and click **Yes**.

o Similarly, select the preferred keyboard layout (here, **US**) in the next wizard and click **Yes**.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Skip the second keyboard option.
- In **Let's name your device**, enter **Windows11** and click **Next**.
- In the **How would you like to set up this device?** wizard, select the **Set up for personal use** option and click **Next**.
- In the **Let's add your Microsoft account** wizard, click the **Sign-in options** link and select the **Offline account** option. In the next wizard, click **Skip for now**.
- In the **Who's going to use this device?** wizard, enter **Admin**, and click **Next**. In the next wizard, set **Pa$$w0rd** as the password and click **Next**. Similarly, in the **Confirm password** wizard, enter the same password and click **Next**.
- Add security questions in the next wizards.
- In the **Privacy settings** wizard, disable all the options and click **Accept**.
- After Windows initializes, if an app window appears, close it.
- Network settings:
  - IP address: **10.10.1.11**
  - Subnet mask: **255.255.255.0**
  - Default gateway: **10.10.1.1**
  - Preferred DNS server: **8.8.8.8**
- Check for and install the latest updates.

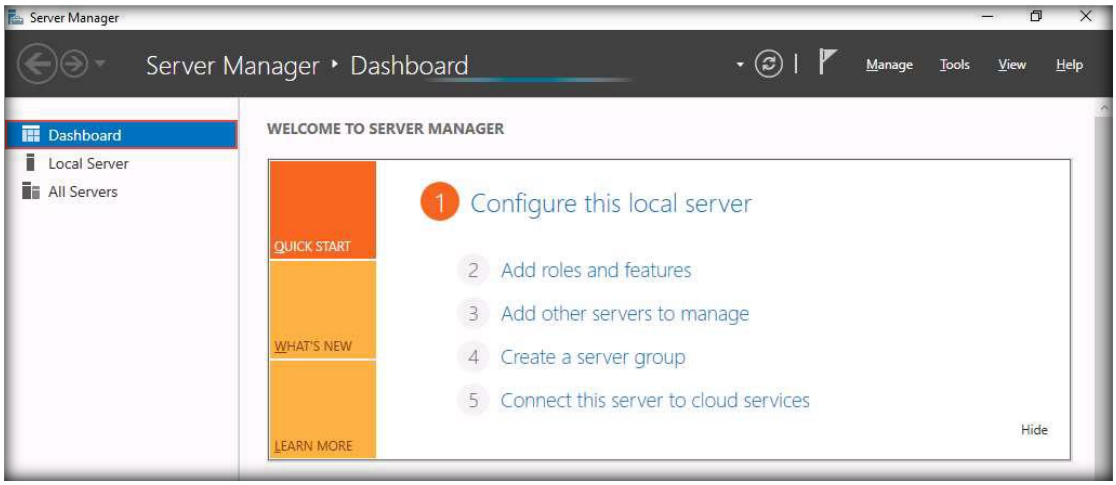
[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

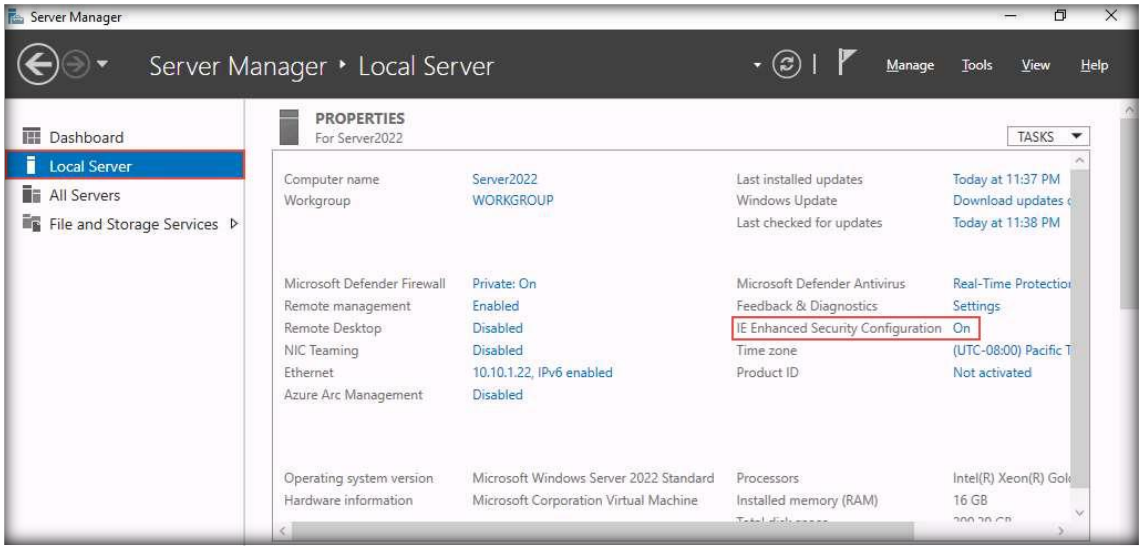
CT#8: Configure the Internet Explorer (IE) Enhanced Security Configuration in Windows Server 2022 Virtual Machine

Configure IE Enhanced Security in the Windows Server 2022 Virtual Machine

1. Log in to the **Windows Server 2022** virtual machine using the credentials **Administrator** and **Pa$$w0rd**.
2. If a **Shutdown Event Tracker** pop-up appears, click **Cancel**.
3. To configure the **Internet Explorer Enhanced Security Configuration**, go to the **Start** menu → **Server Manager** application.
4. The main window of **Server Manager** appears. By default, the **Dashboard** will be selected.

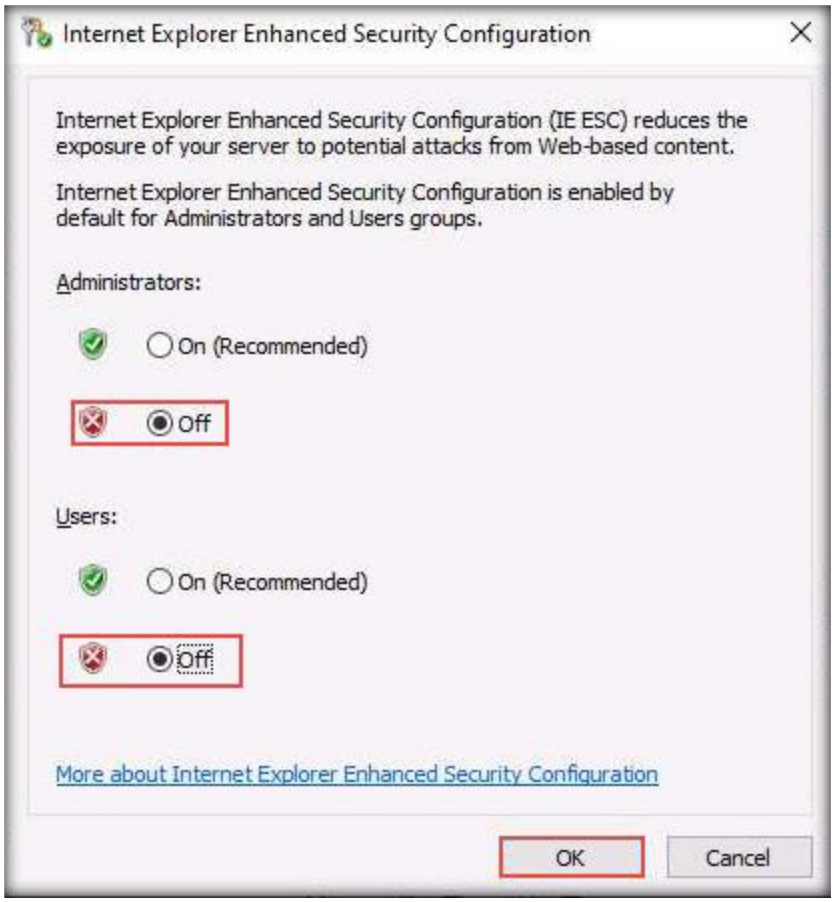


5. Select **Local Server** in the left pane of the window. In the right pane, click **On** for **IE Enhanced Security Configuration**.



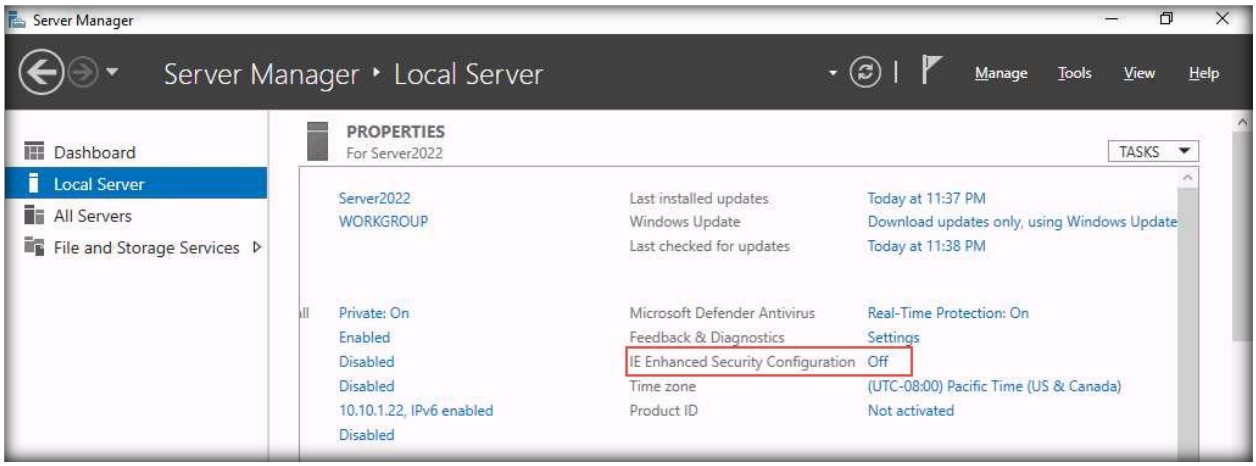
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **Internet Explorer Enhanced Security Configuration** window appears; select the **Off** radio button for both **Administrators** and **Users** and click **OK**.



7. The **IE Enhanced Security Configuration** will be **Off**.

   Note: It takes some time to turn off the **IE Enhanced Security Configuration**.

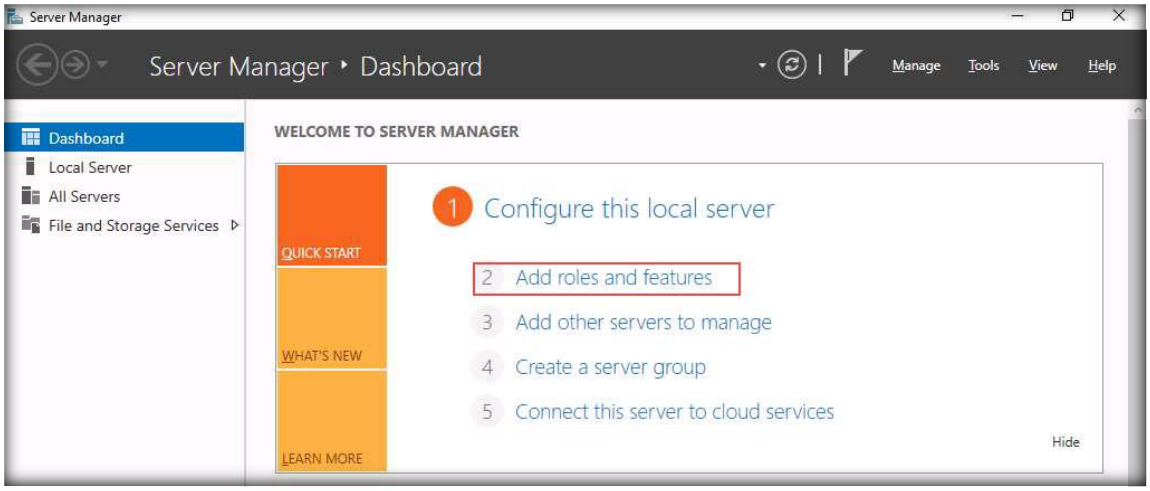


[Back to Configuration Task Outline]

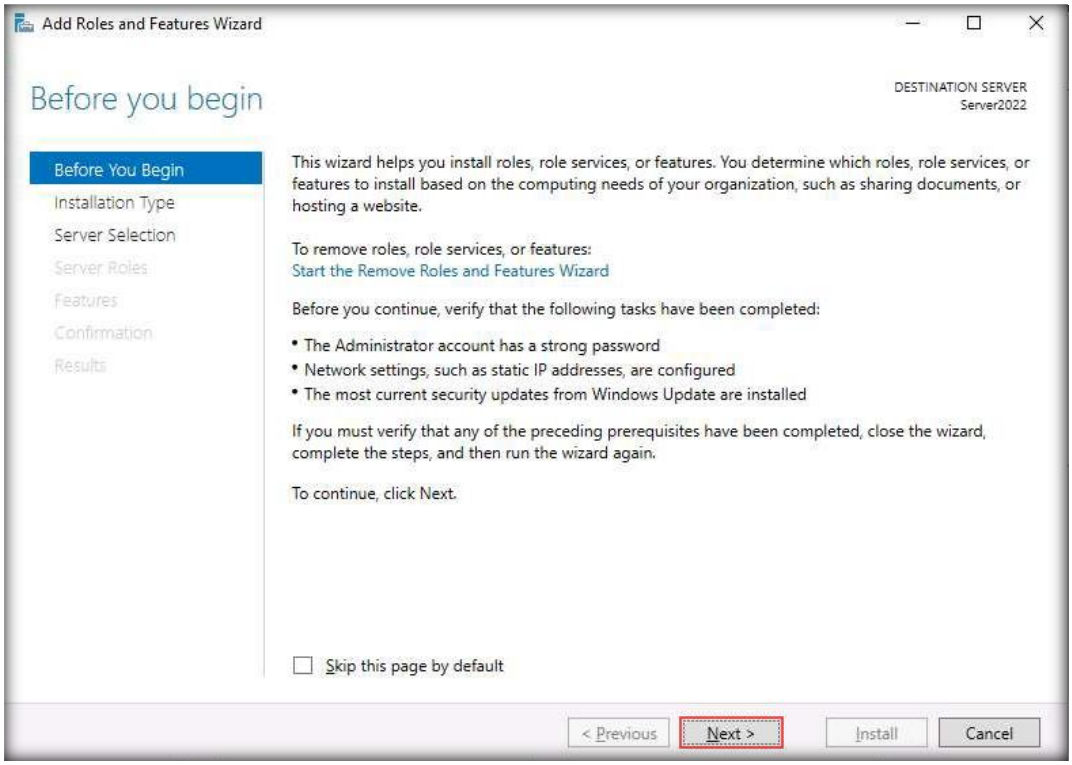
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#9: Install .NET Framework in Windows Server 2022 Virtual Machine

1. Log in to the **Windows Server 2022** virtual machine using the credentials **Administrator** and **Pa$$w0rd**.
2. Launch the **Server Manager**. Click **Add roles and features**.

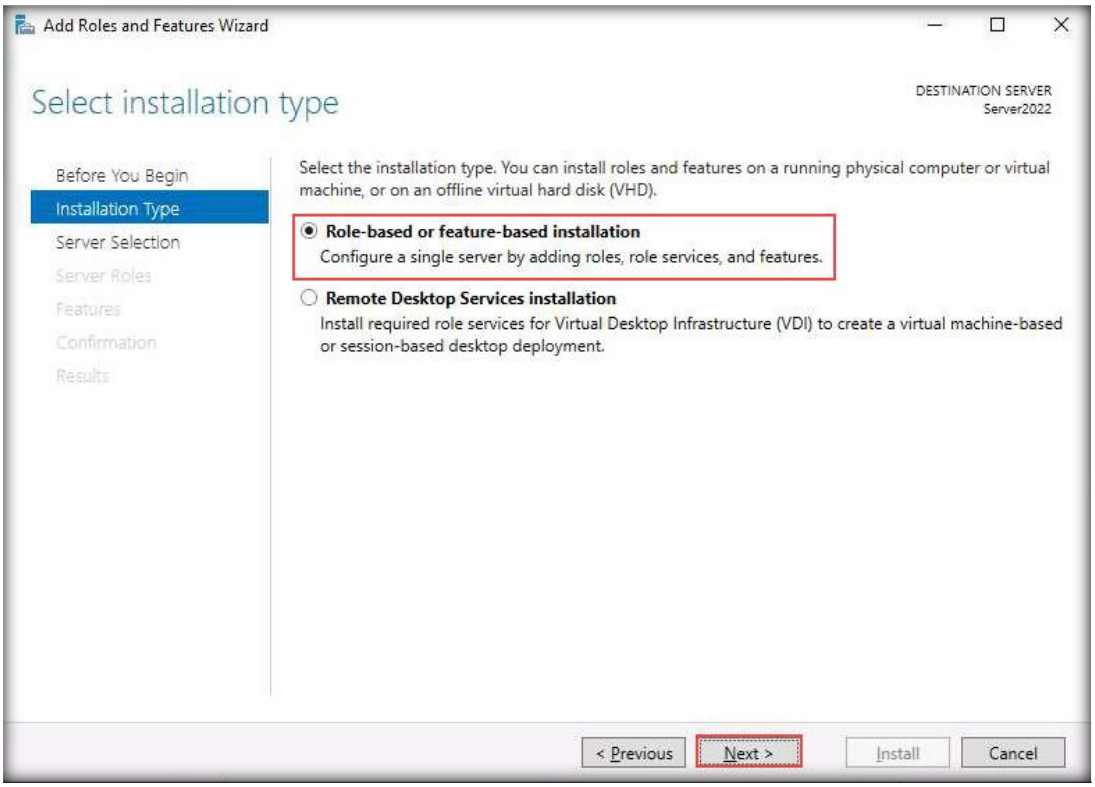


3. **Add Roles and Features Wizard** window will appear; click **Next**.

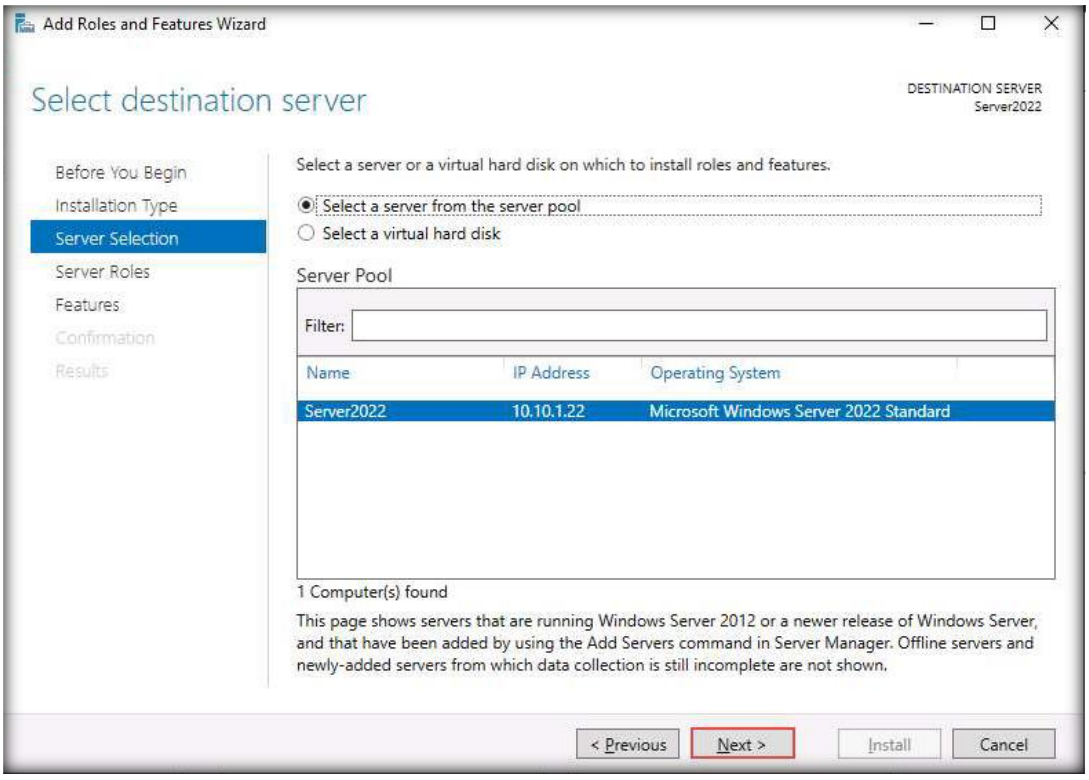


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. In the **Installation Type** section of the wizard, select the **Role-based or feature-based installation** radio button and click **Next**.

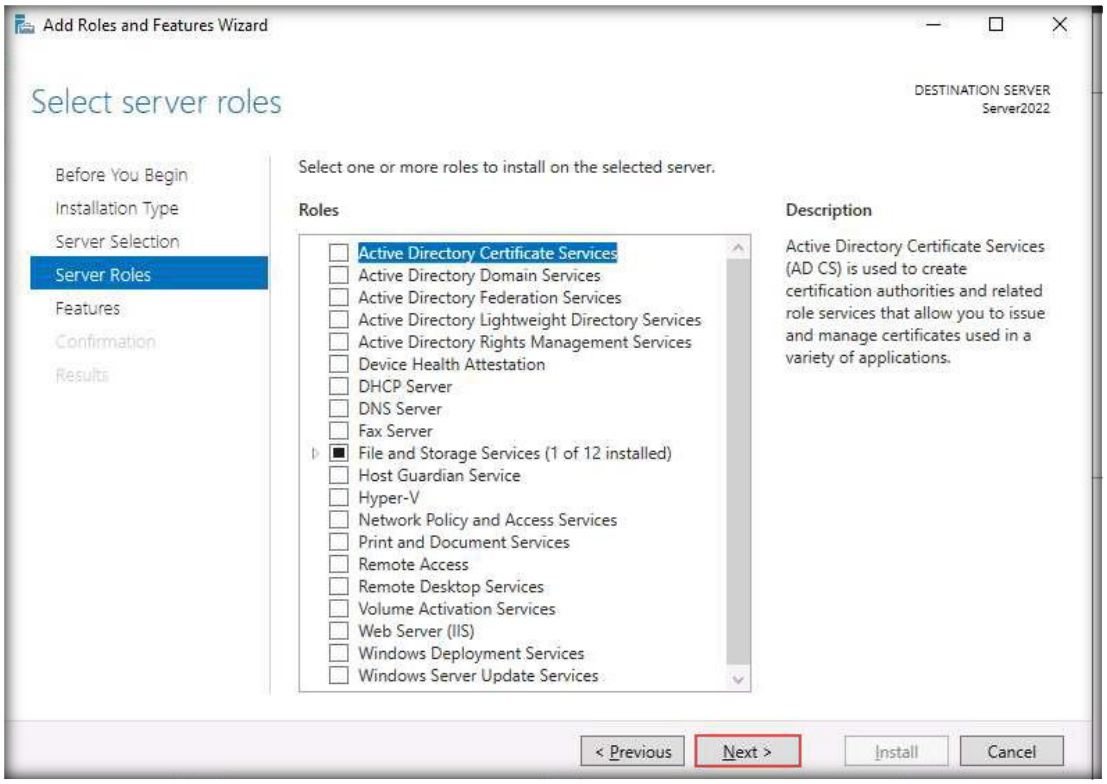


5. In the **Server Selection** section, leave the selections to default and click **Next**.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

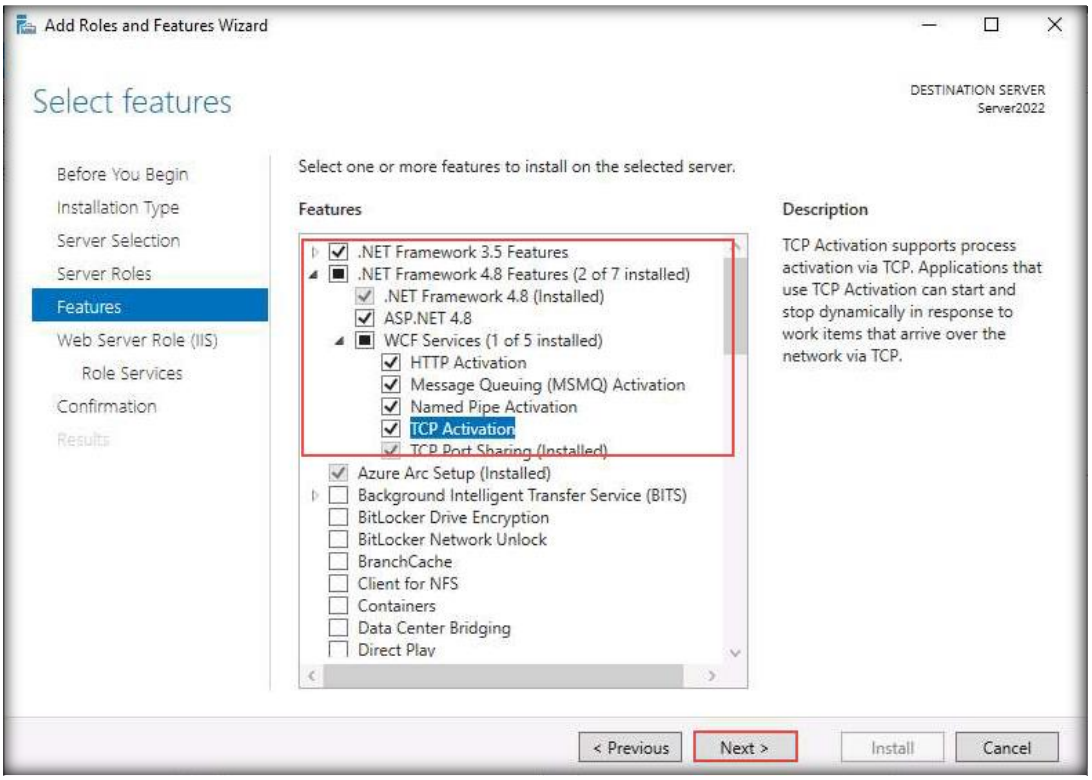
6. **Server Roles** section will appear; click **Next**.



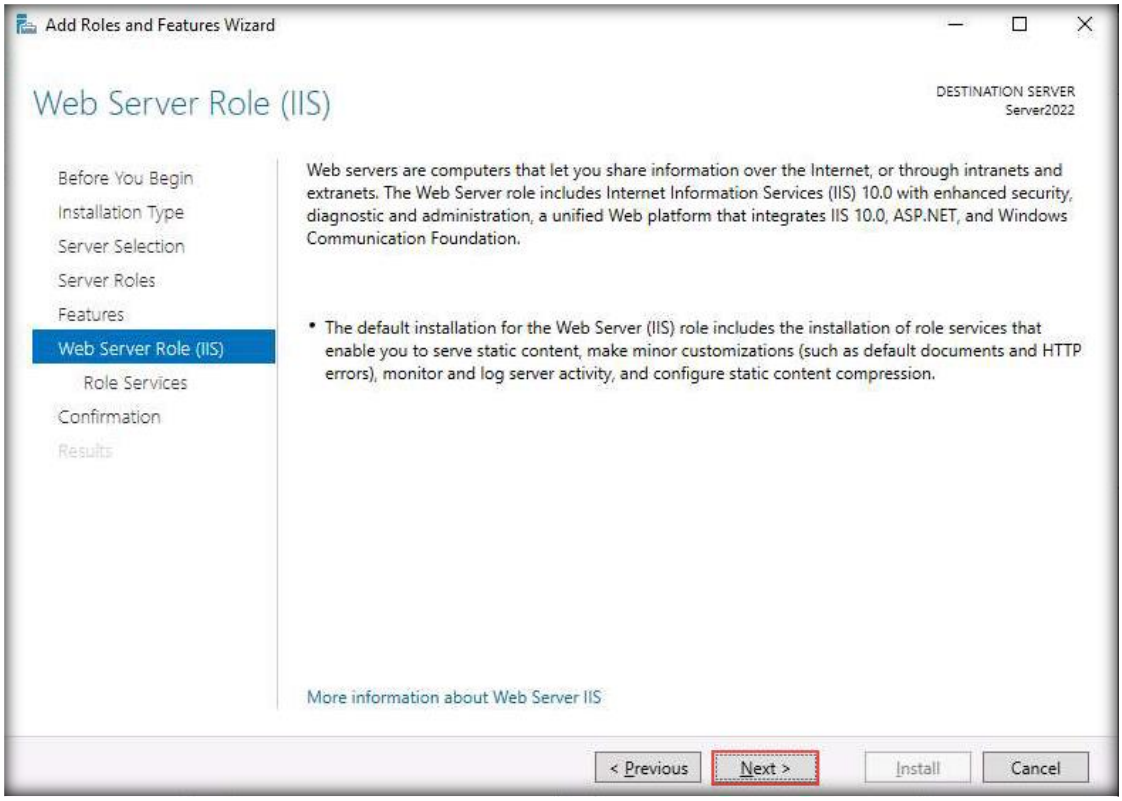
7. **Features** section will appear; select the checkbox for **.NET Framework 3.5 Feature** and select all the checkboxes under **.NET Framework 4.6 Features**.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. **Note**: If the **Add Roles and Features Wizard** pop-up appears, click **Add Features**.

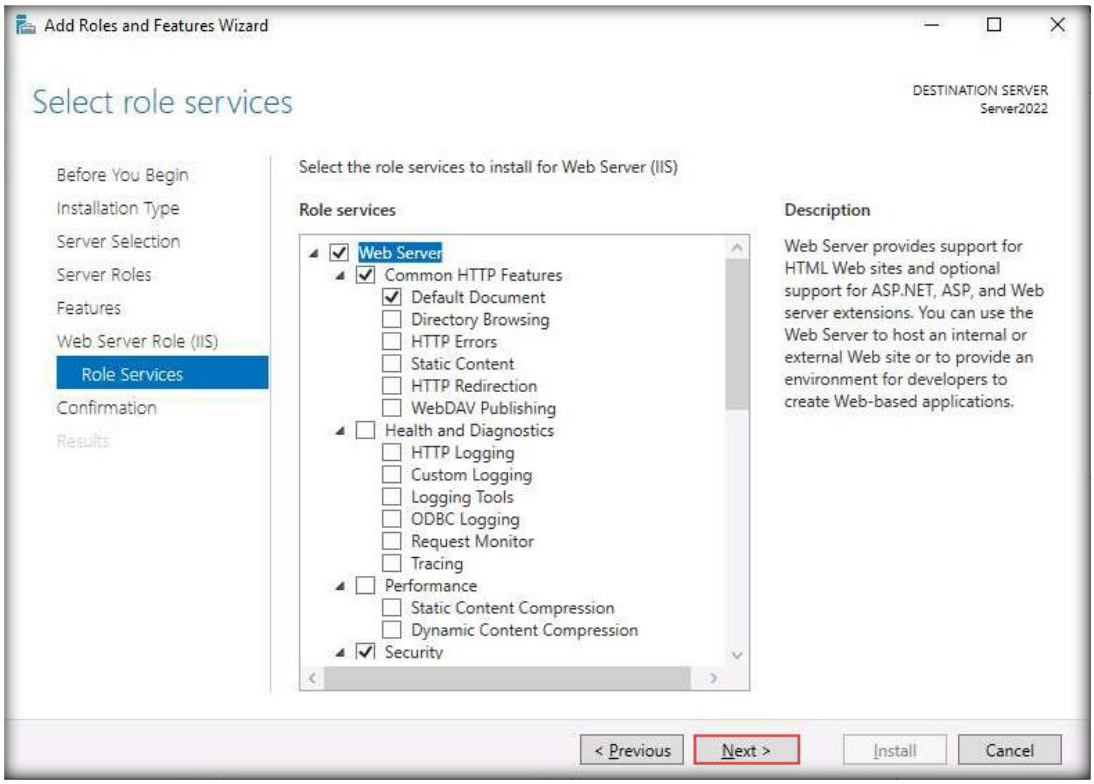


9. **Web Server Role (IIS)** section will appear; click **Next**.

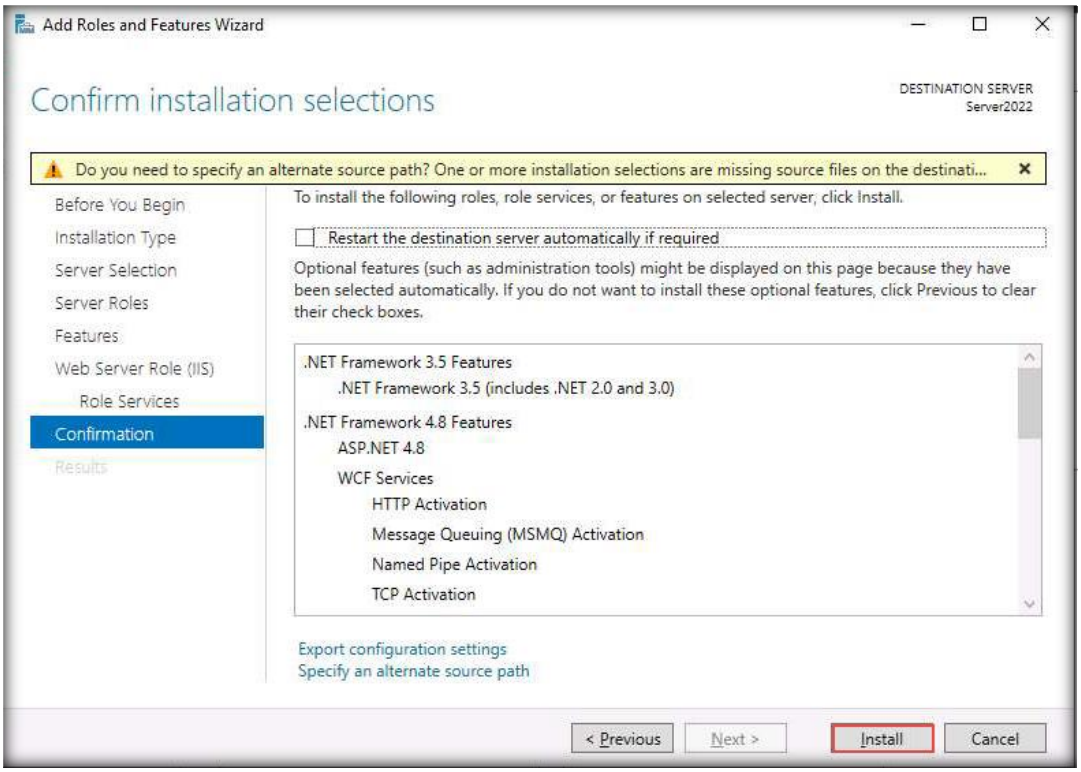


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. **Role Services** section will appear in the wizard; click **Next**.

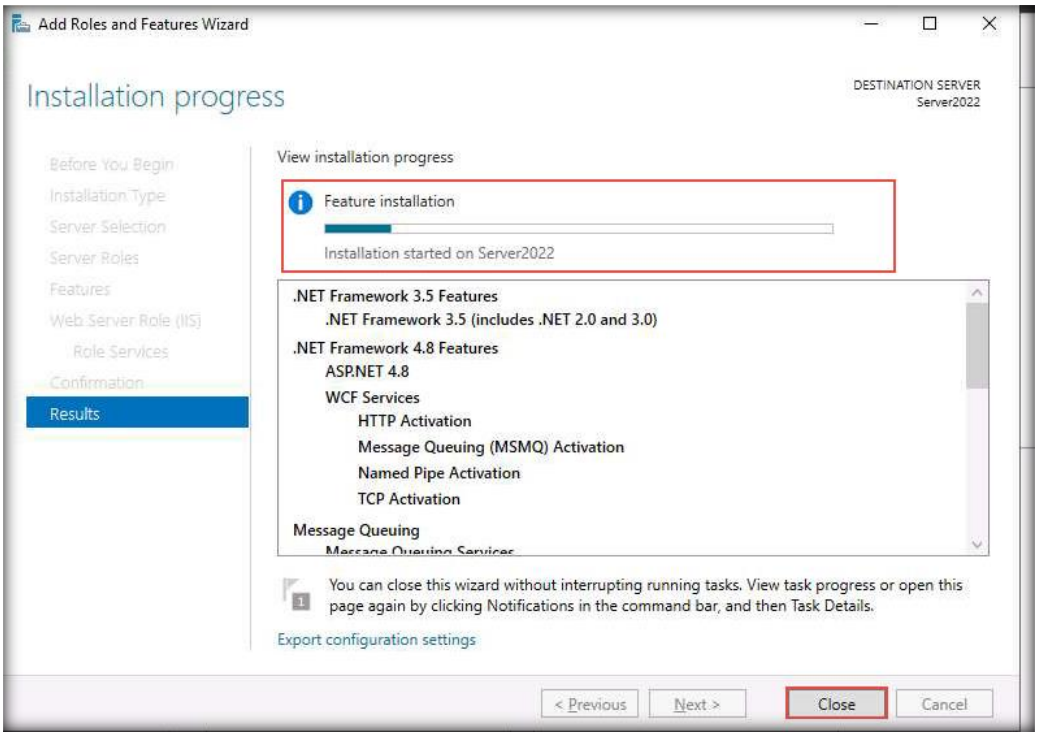


11. **Confirmation** section will appear in the wizard; click **Install**.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. **Add Roles and Features Wizard** will show the installation progress of the features. It will take a while to **complete** the installation of selected roles.



13. After the completion of installation, click **Close**.

[Back to Configuration Task Outline]

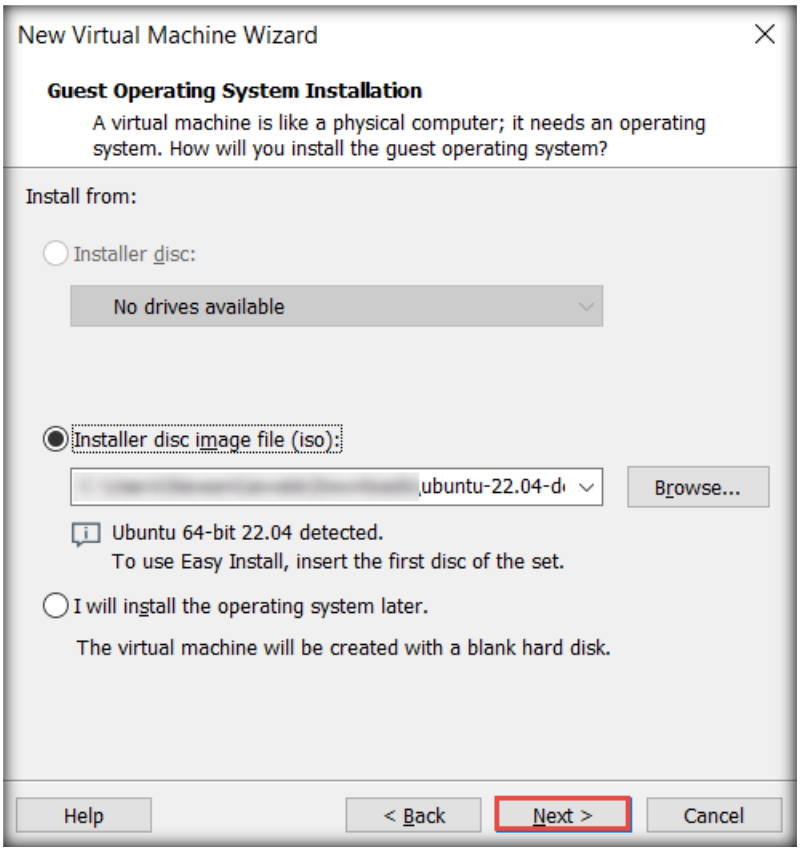
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#10: Install the Ubuntu Suspect and Ubuntu Forensics Virtual Machines in VMware

1. The next step is to set up the **Ubuntu Suspect** virtual machine in VMWare Workstation Pro.
2. In the **VMware Workstation** window, click **Create a New Virtual Machine**.
3. In the **New Virtual Machine Wizard** window that appears, retain the default settings (**Typical**) and click **Next**.
4. In the **Guest Operating System Installation** wizard, select the **Installer disc image file (iso)**: radio button. Click **Browse** to provide the ISO path of the Ubuntu ISO file. Then, select the Ubuntu ISO file and click **Open** to provide the ISO path. Finally, click **Next**.

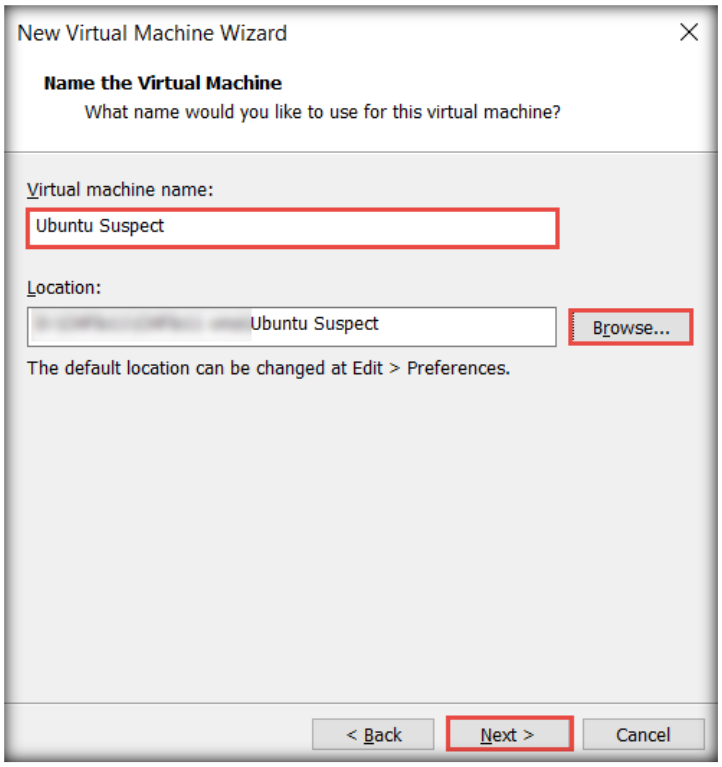
   Note: Here, we have used the **Ubuntu** .iso file **ubuntu-22.04-desktop-amd64.iso** for creating the **Ubuntu** virtual machine. However, you can download the latest ISO file from **https://ubuntu.com/download/desktop**.

   Note: If you decide to download the latest version, the screenshots presented here might differ from what you see in your lab environment.

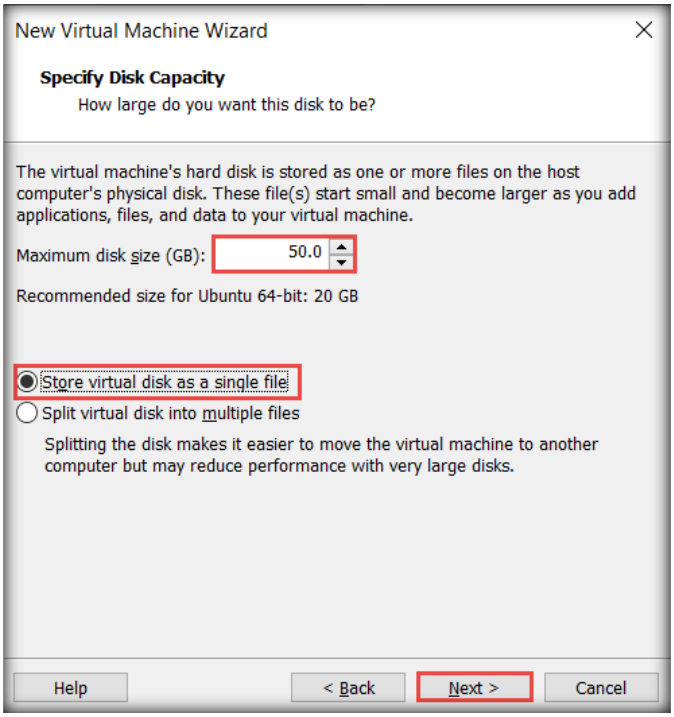


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The **Name the Virtual Machine** wizard appears; type **Ubuntu Suspect** in the **Virtual machine name** field and click the **Browse** button to store the virtual hard disk. Click **Next**.

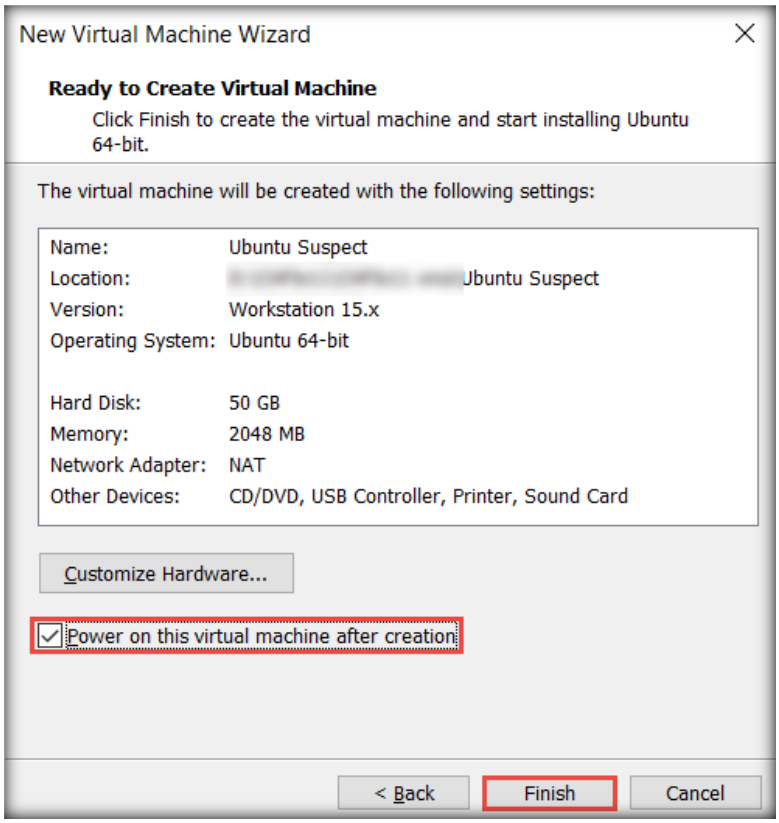


6. The **Specify Disk Capacity** wizard appears. In the **Maximum disk size (GB)** field, type **50 GB** and select **Store virtual disk as a single file**; click **Next**.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

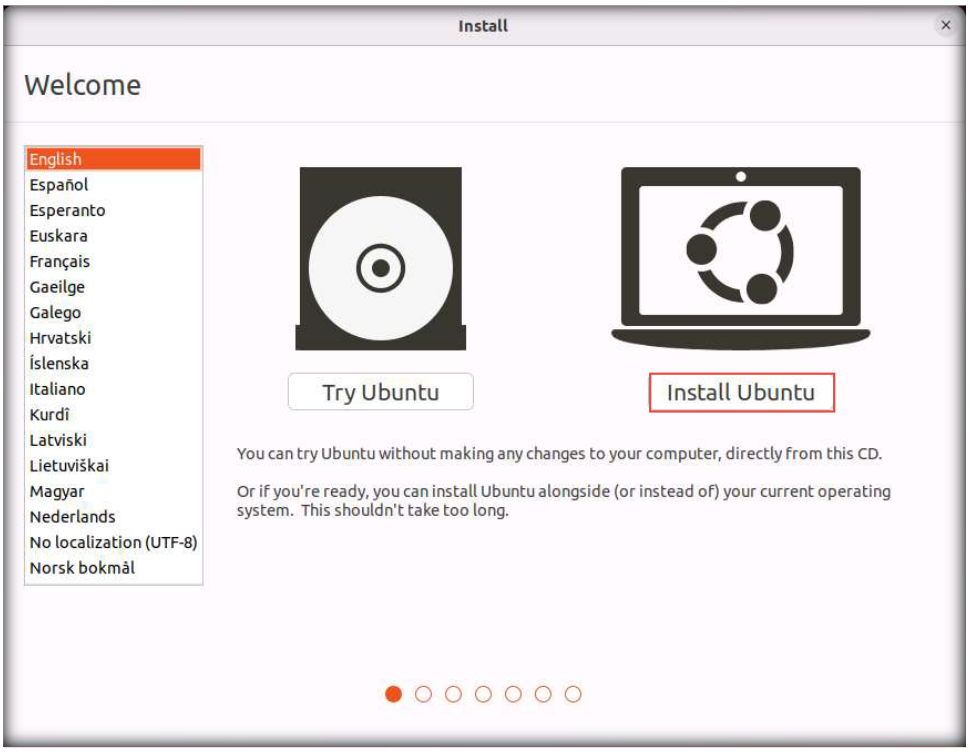
7. In the **Ready to Create Virtual Machine** wizard, ensure that **Power on this virtual machine after creation** checkbox is selected and click **Finish**.



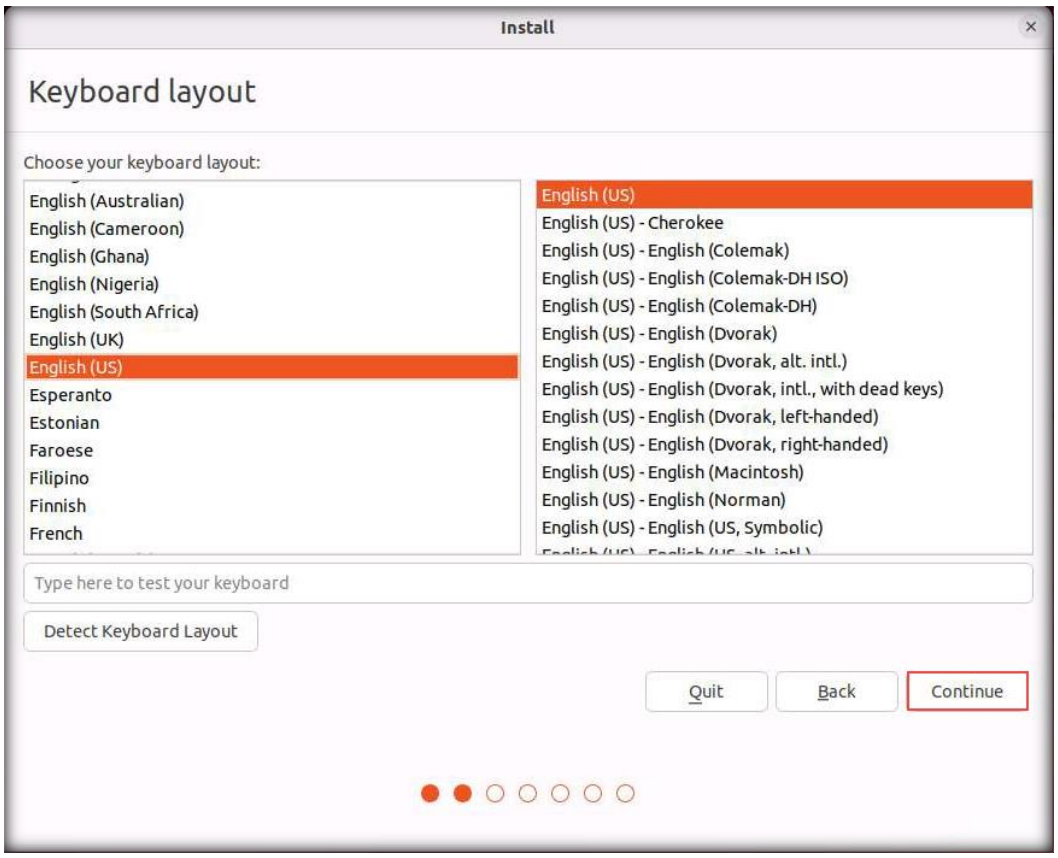
8. As soon as you click the **Finish** button, the **GNU GRUB** window appears. Press **Enter** to select **Try or Install Ubuntu** option.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. **Ubuntu** initializes and the **Welcome** wizard appears. Click the **Install Ubuntu** option.

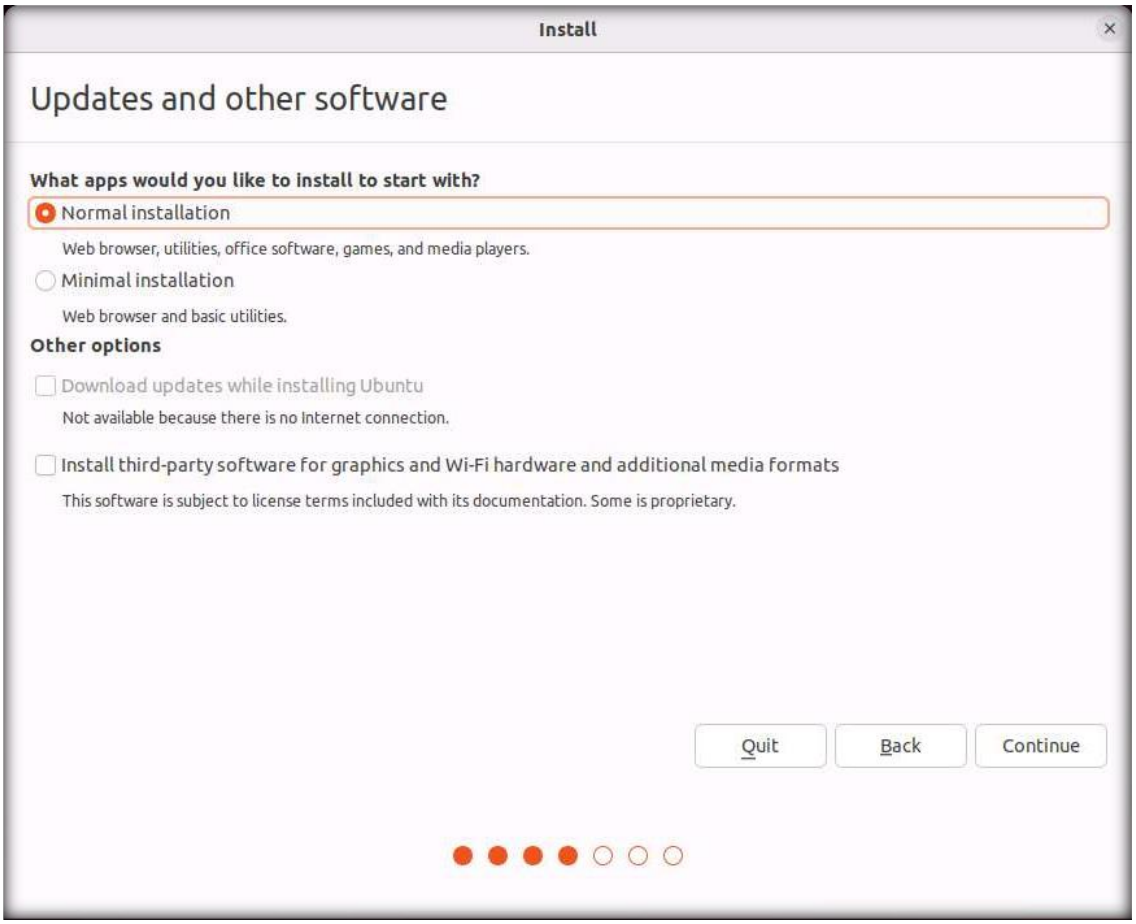


10. A **Keyboard Layout** wizard appears, leave default settings and click **Continue**.



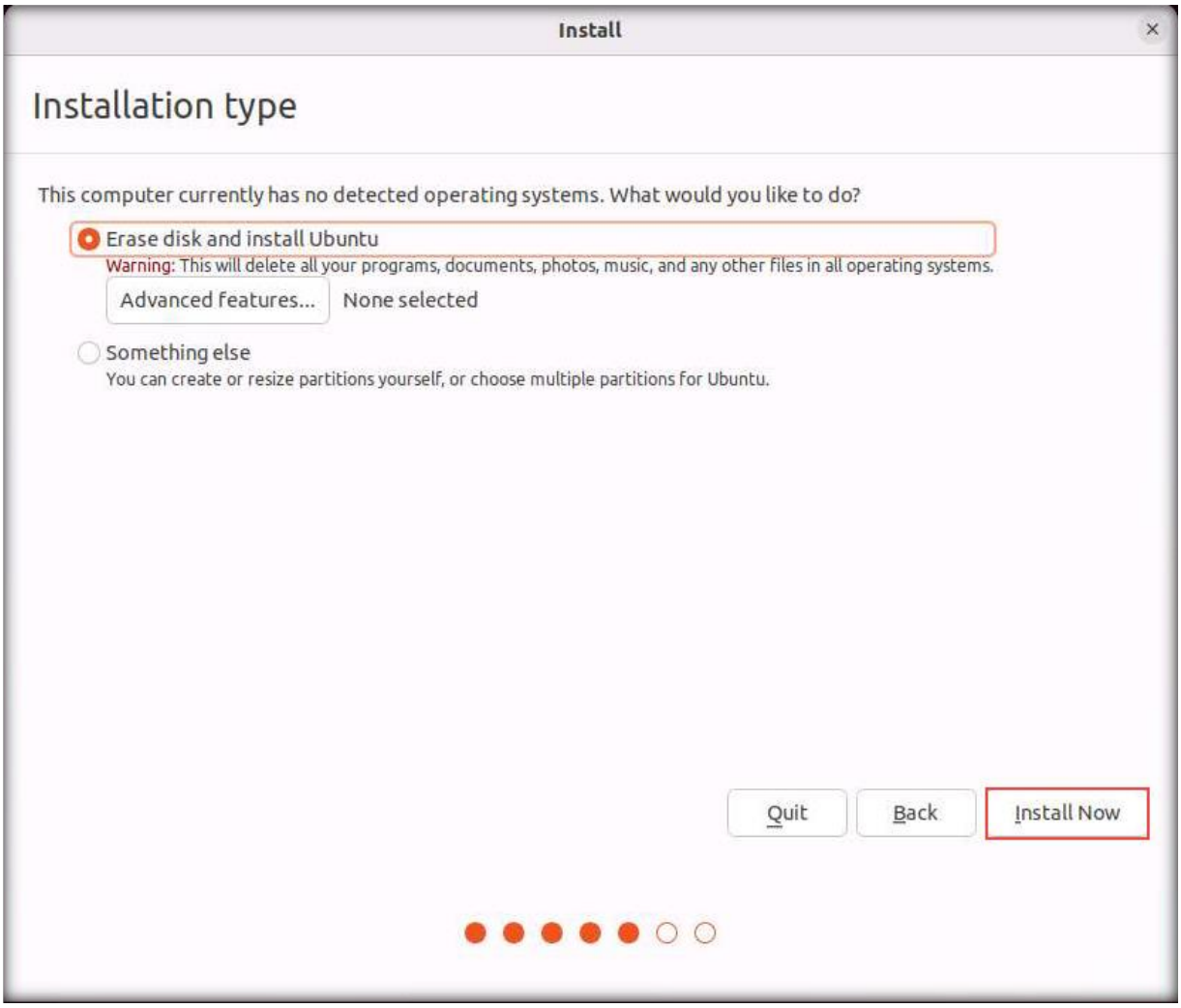
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

11. In the **Updates and other software** wizard, ensure that the **Normal installation** radio button is selected in the **What apps would you like to install to start with?** section. Click **Continue**.

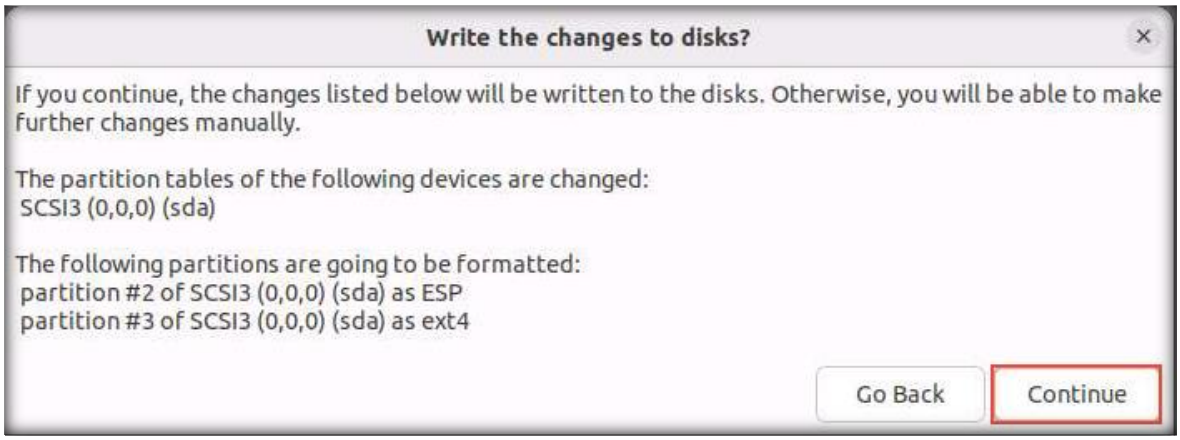


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **Installation type** wizard appears. Ensure that the **Erase disk and install Ubuntu** radio button is selected and click **Install Now**.



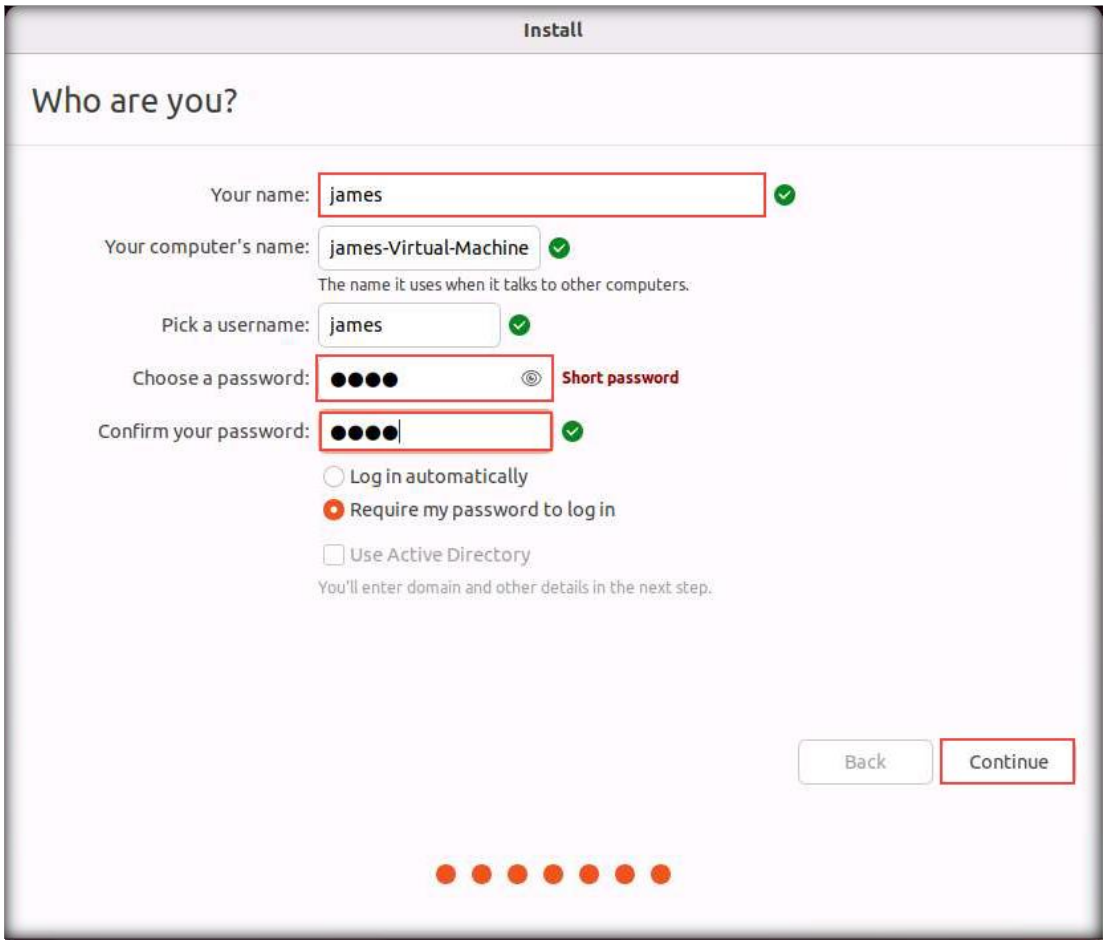
13. A **Write the changes to disk?** pop-up appears; click **Continue**.



14. In the **Where are you?** wizard, retain the region selected by default, and click **Continue**.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. A **Who are you?** wizard appears. Enter **james** in the **Your name** field. In the **Choose password** and **Confirm your password** fields, enter **toor** and click **Continue**.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

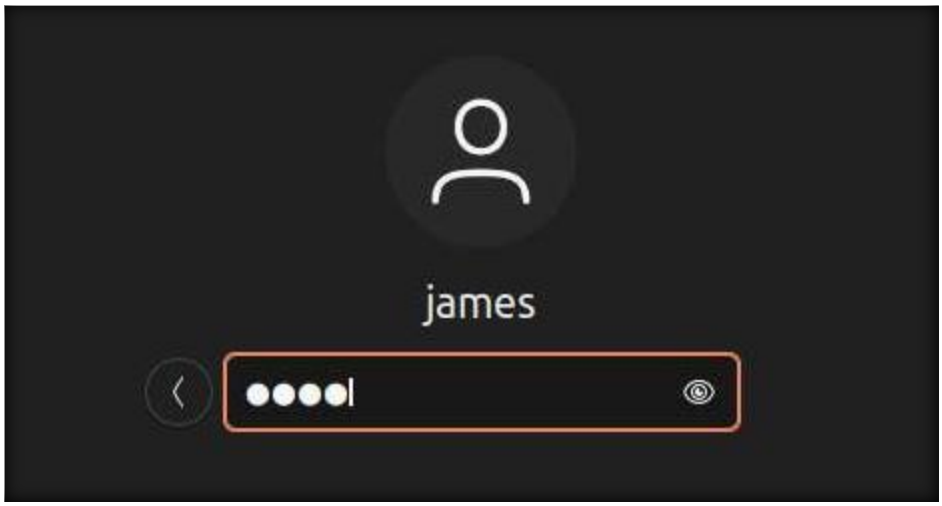
16. The **Welcome to Ubuntu** wizard appears, and installation begins. Wait for it to complete.

17. Once the installation has completed, an **Installation Complete** pop-up appears. Click **Restart Now**.

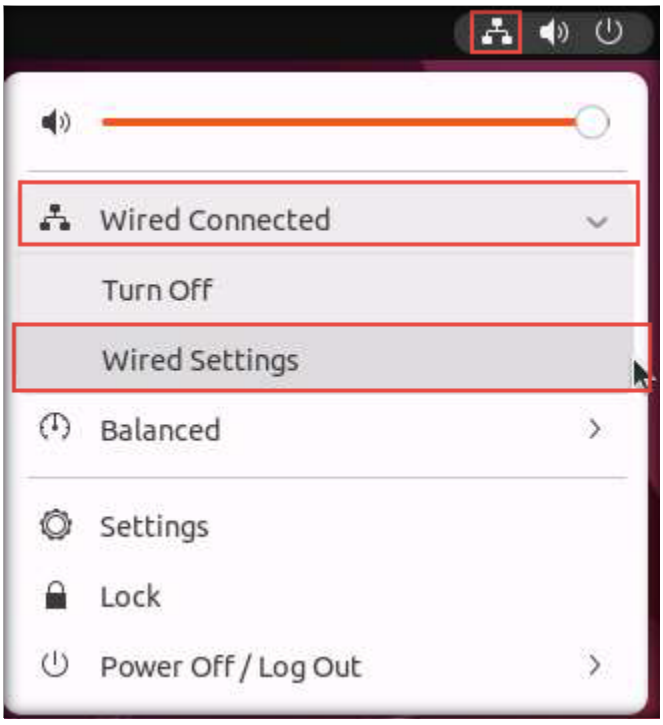
18. In the **Ubuntu** screen, press **Enter** to restart the machine.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The machine restarts and displays a login screen with the username **james**. Click **Ubuntu**, type **toor** in the **Password** field, and press **Enter** to sign in.

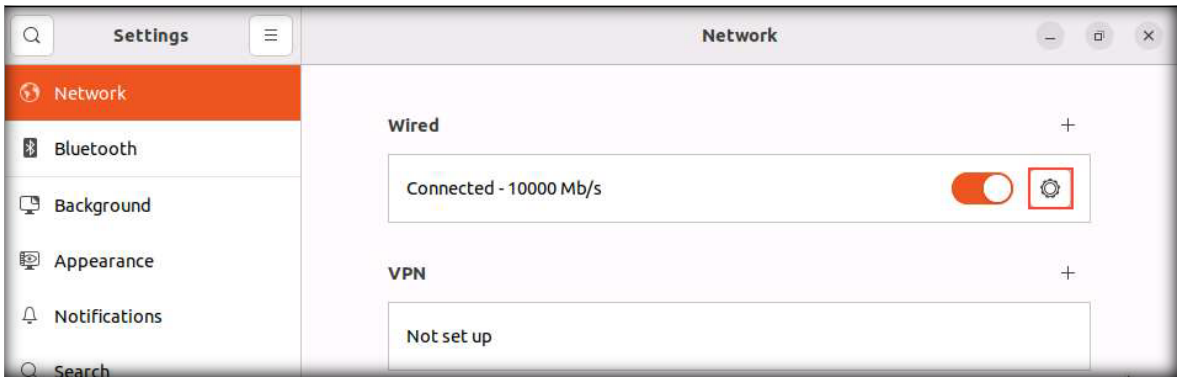


20. An **Online Accounts** pop-up window appears; click **Skip**. Follow the steps and click **Next** in each step. In the last step, click **Done**.
21. Now, we must configure the IP address as static.
22. Click the **Network** icon in the top-right corner of the **Desktop**. Then, click **Wired Connected** → **Wired Settings**, as the screenshot demonstrates.

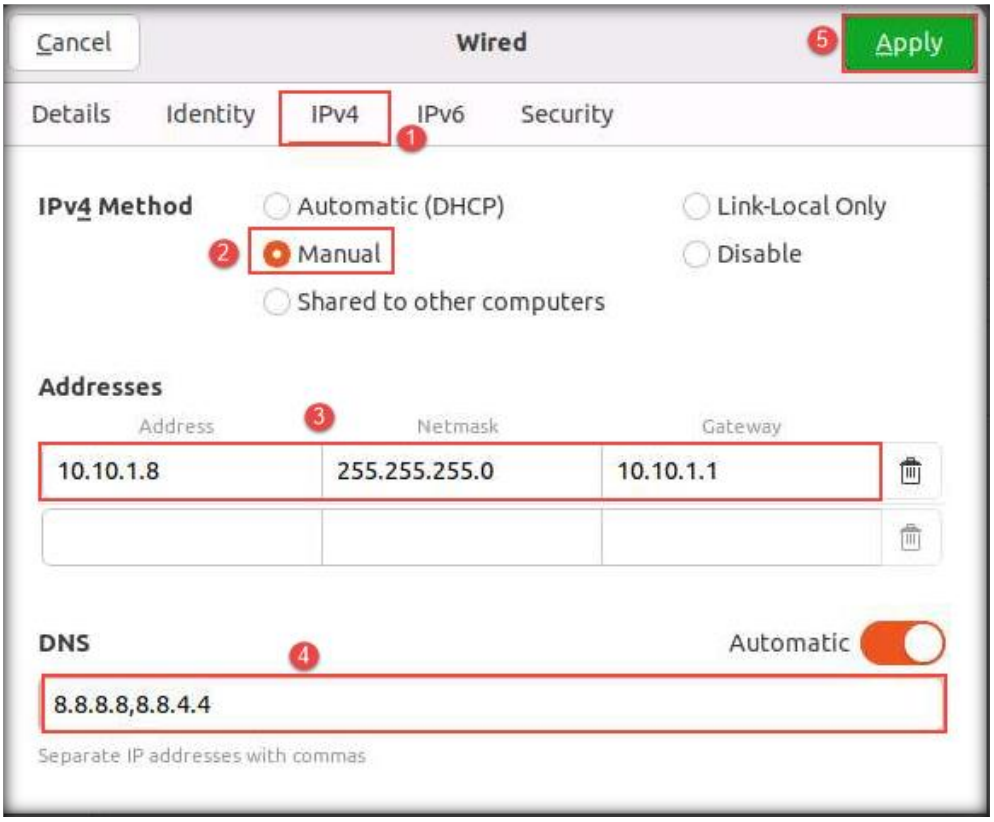


Computer Hacking Forensic Investigator Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Click the **Settings** icon in the **Wired** section.



24. Navigate to the **IPv4** tab and select the **Manual** radio button in the **IPv4 Method** section. In the **Addresses** section, type **10.10.1.8**, **255.255.255.0**, and **10.10.1.1** in the **Address**, **Netmask**, and **Gateway** cells, respectively. Then, type **8.8.8.8,8.8.4.4** in the **DNS** field and click **Apply**, as the screenshot demonstrates.

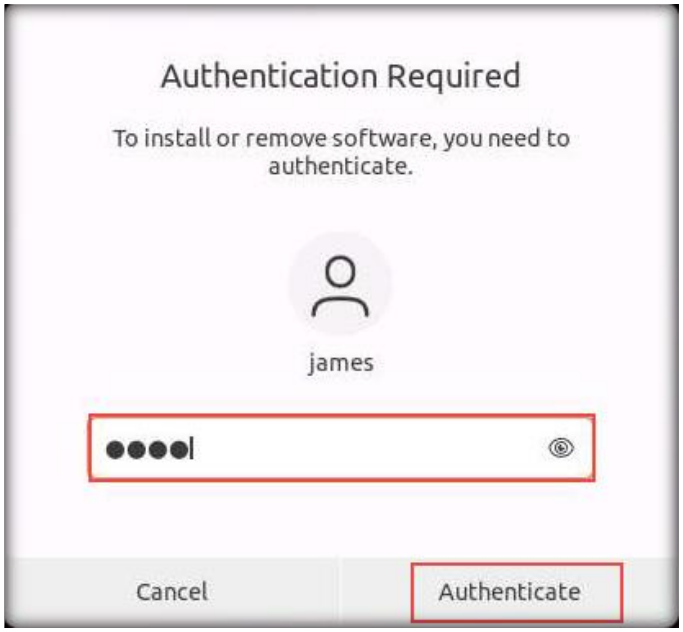


25. Close all windows and reboot the virtual machine. After the machine restarts, log in as the user **Ubuntu** with the password **toor**.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

26. If a **Software Updater** pop-up window appears, click **Install Now** to install the latest updates. This process may take some time.

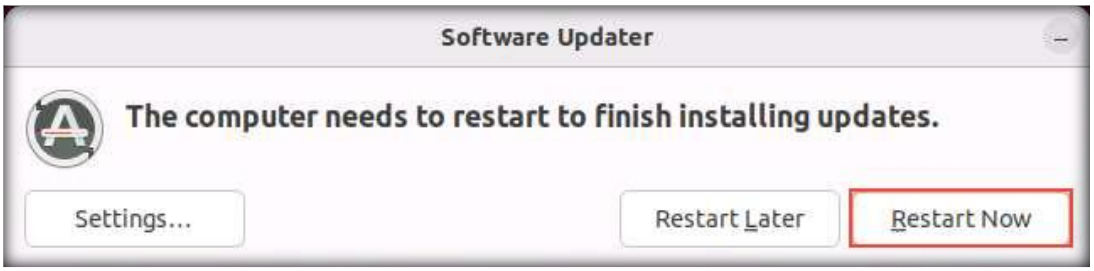
27. An **Authentication Required** pop-up appears. Enter **toor** in the **Password** field and click **Authenticate**.



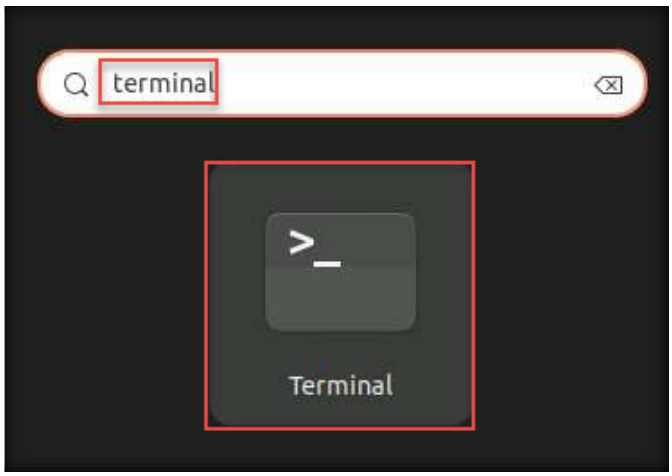
28. **Software Updater** begins to install updates. Wait for it to complete.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. After the updates have installed, click **Restart Now**.

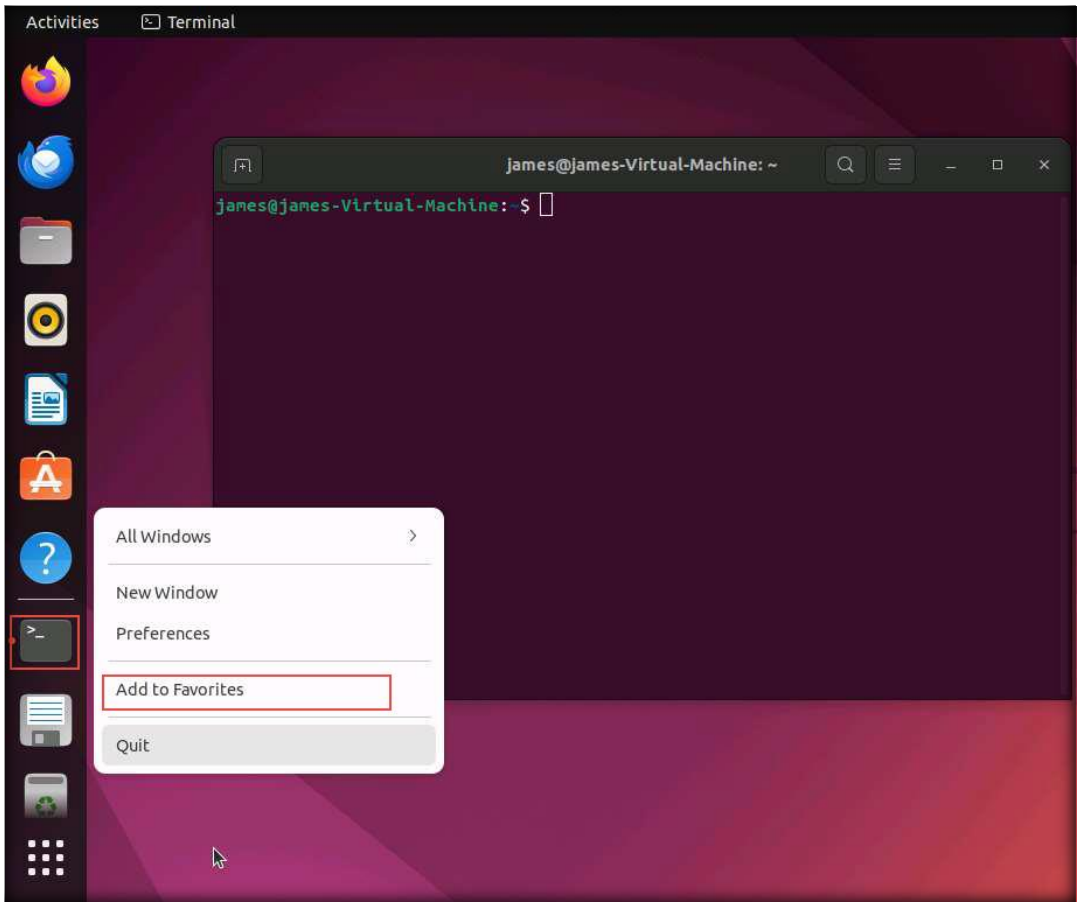


30. Click the **Show Applications** ( ) icon in the bottom-left corner of the **Desktop**. Then, type **terminal** in the search bar and, from the search results, click the **Terminal** icon to launch a terminal window.

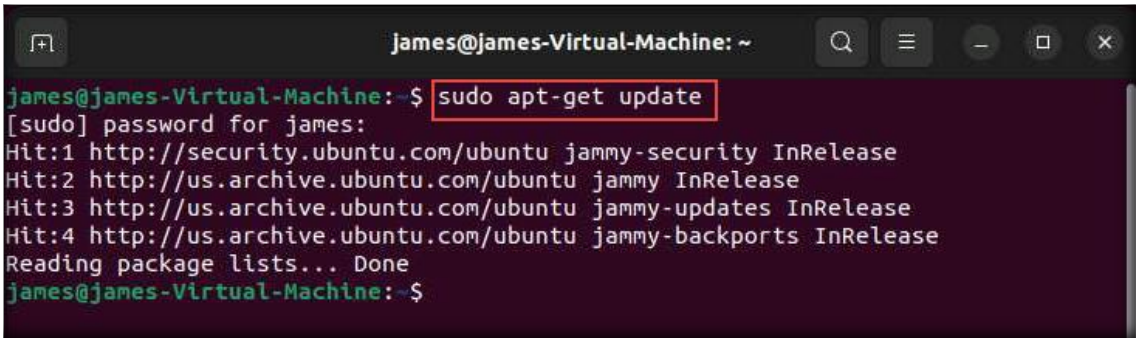


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

31. The **Terminal** window appears. Right-click on the **Terminal** icon in the **Favorites** bar on the left-hand side of the window and click **Add to Favorites**, as shown in the screenshot, to lock the terminal on the launcher.



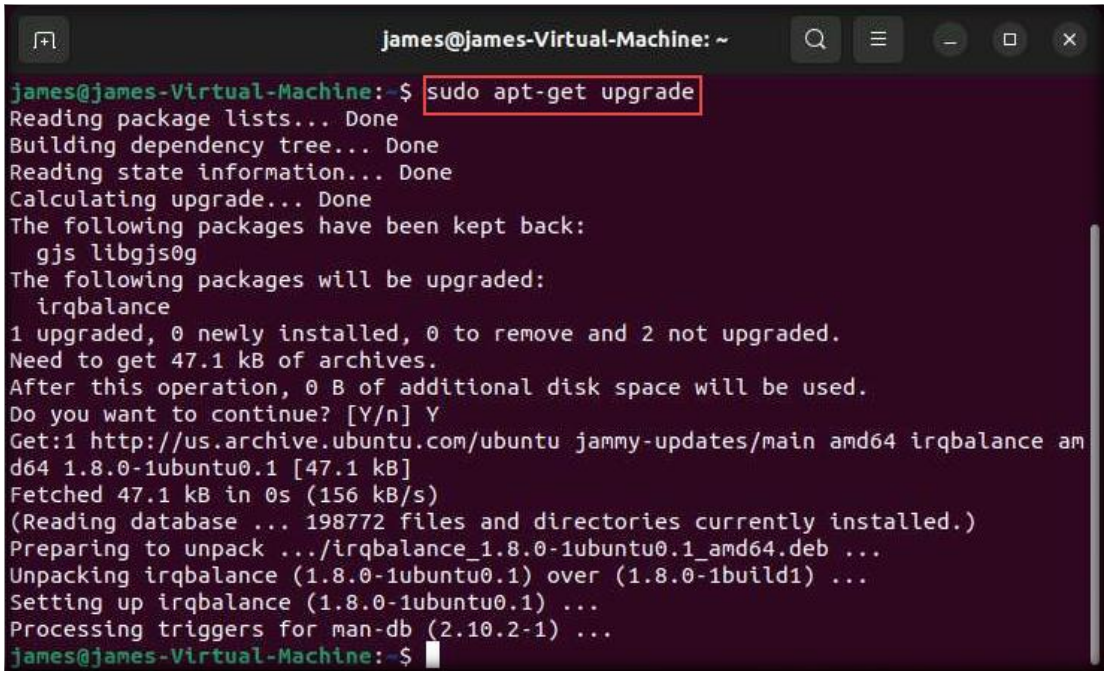
32. In the terminal window, type **sudo apt-get update** and press **Enter**. In the **password for james** field, type **toor**, and press **Enter**. The password that you type will not be visible.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

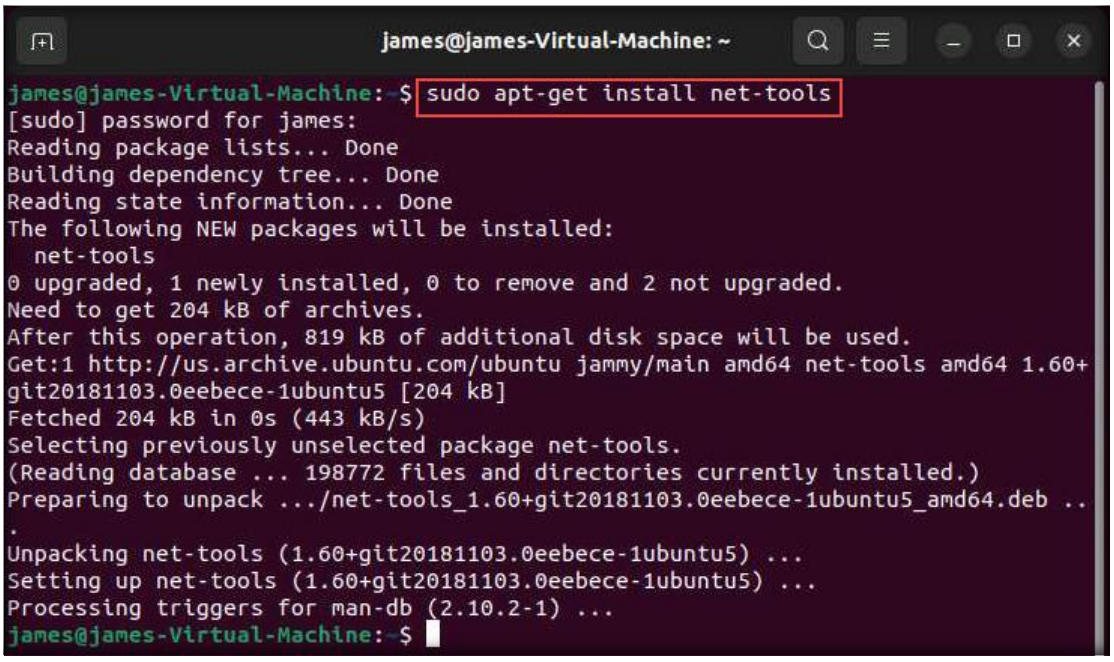
33. In the terminal window, type **sudo apt-get upgrade** and press **Enter**.

    Note: If a prompt appears asking **Do you want to continue?**, type **Y** and press **Enter**.



34. Restart the machine and log in again with **james** and **toor** as the username and password, respectively.

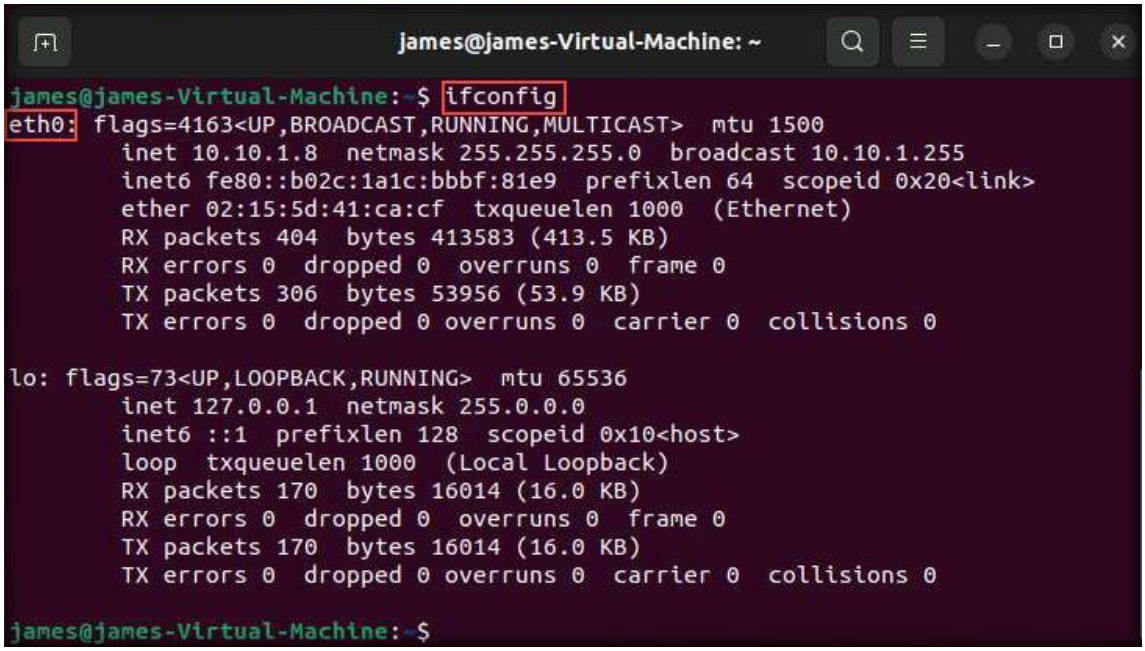
35. In the terminal window, type **sudo apt-get install net-tools** and press **Enter**. In the **password for james** field, type **toor** and press **Enter**. The password that you type will not be visible.



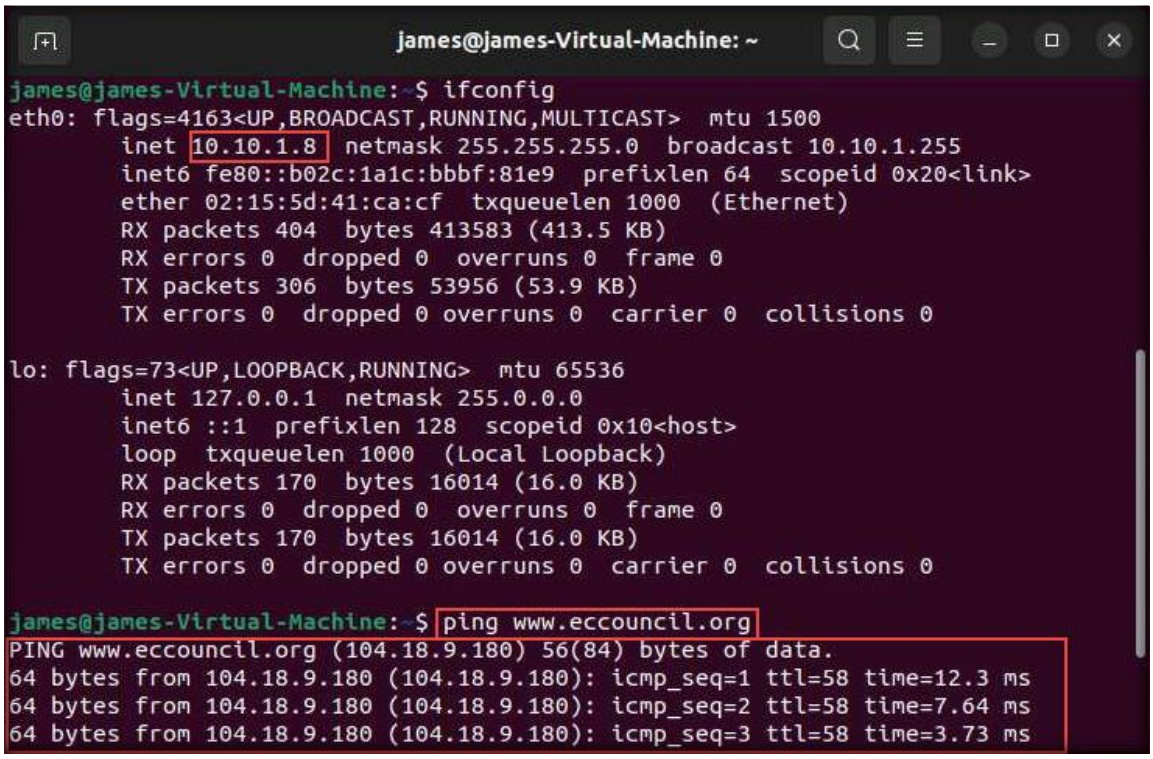
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

36. After the installation, type **ifconfig** and press **Enter** to check the enabled network adapter. Here, the network adapter is **eth0**, as shown in the screenshot.

    Note: The network adapter may vary in your lab environment.

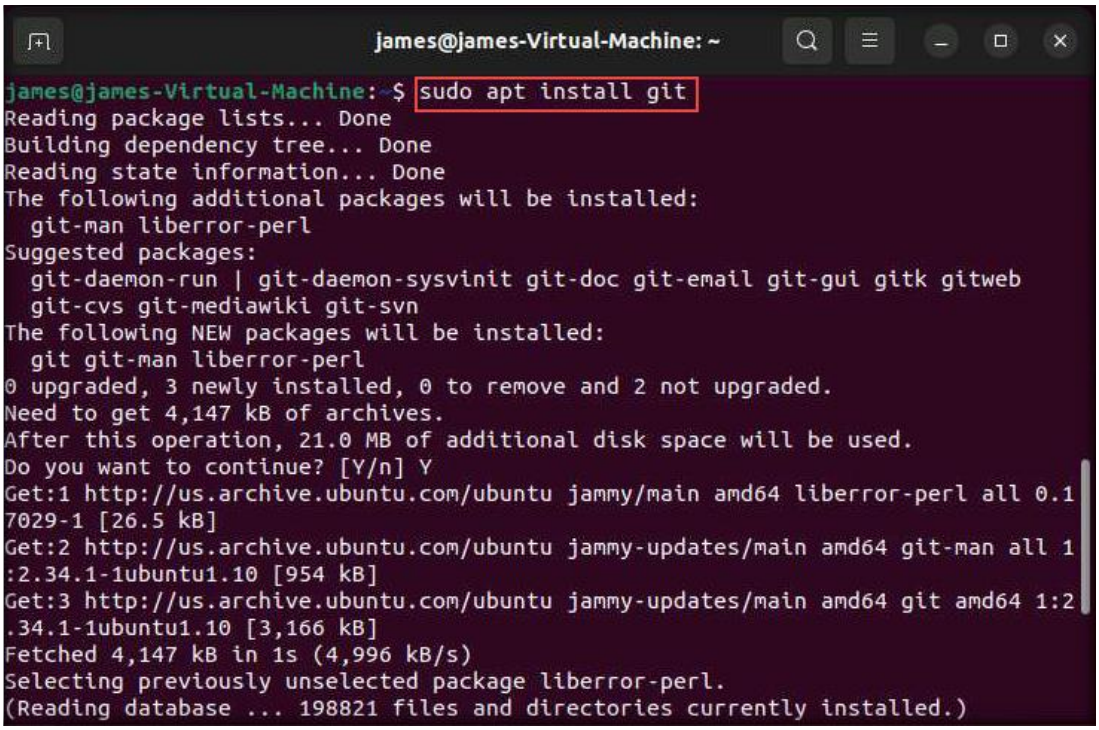


37. Verify the configured IP address. Then, enter **ping www.eccouncil.org** to verify the Internet connectivity. Press **CTRL+C** to stop the ping command.

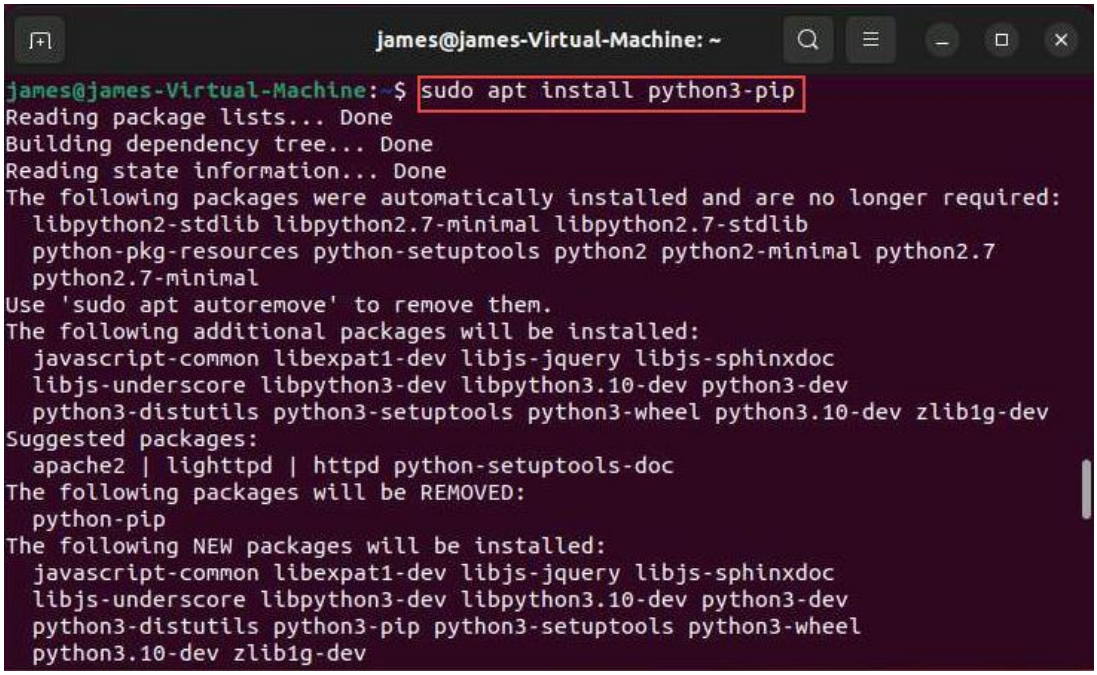


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

38. Install git on the Linux system. To install git, type **sudo apt install git** and press **Enter**. A notification about the disk space that will be used for this operation will be shown. Type **Y** and press **Enter** to proceed with the installation.

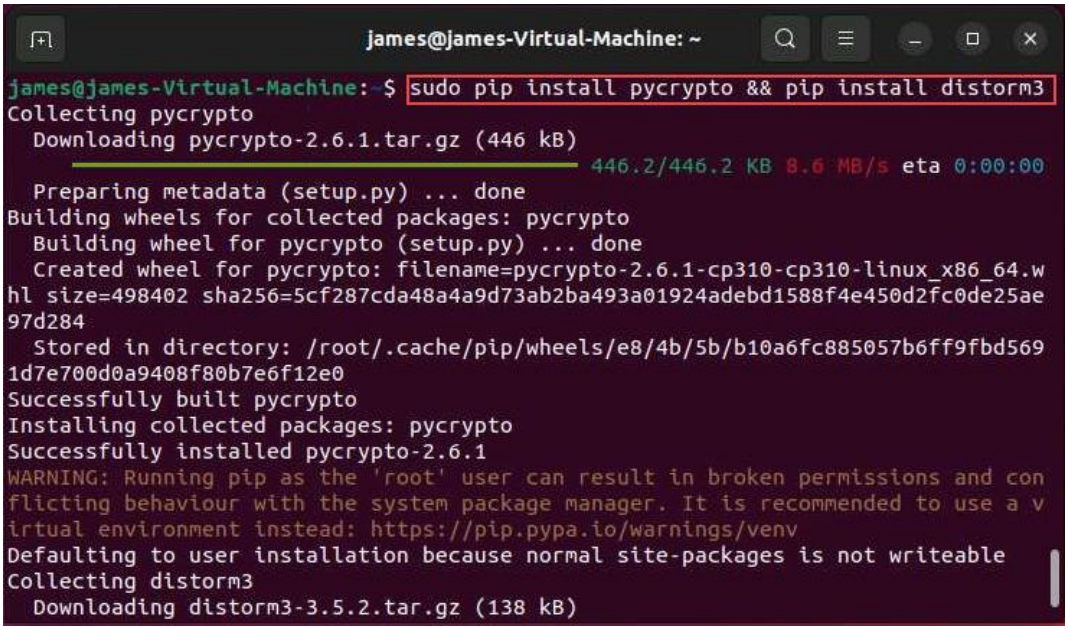


39. Now, install pip on the computer, which will be used while running the labs. To install pip, type **sudo apt install python3-pip** and press **Enter**. A notification about the disk space that will be used for this operation will be shown. Type **Y** and press **Enter** to proceed with the installation.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

40. Install pycrypto and distorm3 on the Linux system. So, type the command **sudo pip install pycrypto && pip install distorm3**, and press **Enter** as shown in the screenshot below:



41. Close the terminal
42. This concludes setting up the **Ubuntu Suspect** virtual machine. Now follow the same steps demonstrated above to install and configure the Ubuntu Forensics virtual machine with the following parameters:
    a. User credentials: **jason:toor**
    b. **eth0** on Manual,
    c. IP address of eth0 interface as **10.10.1.9**

[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

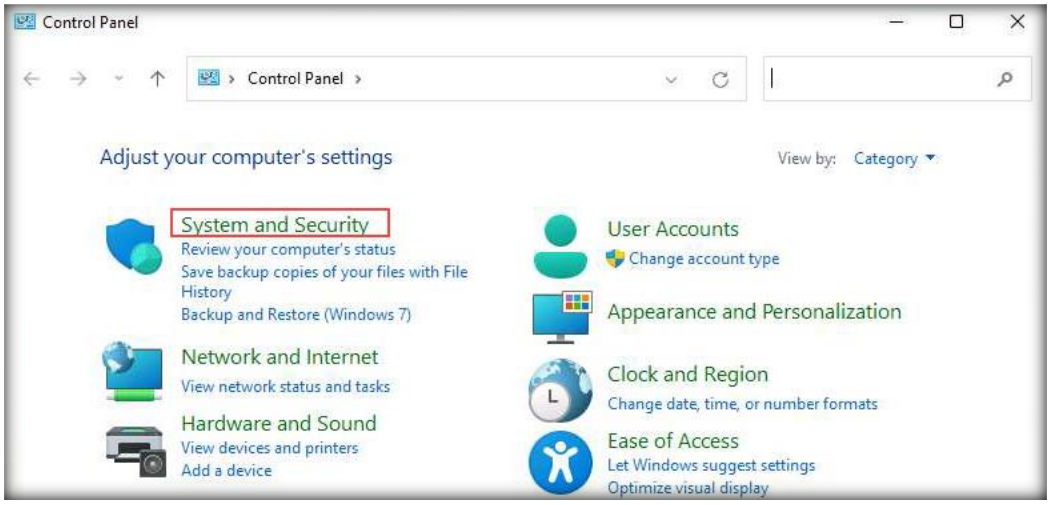
CT#11: Turn the Windows Defender Firewall Off on all Windows Virtual Machines

1. Turn on the **Windows 11** virtual machine, press any key, and log in with the credentials **Admin** and **Pa$$w0rd**.

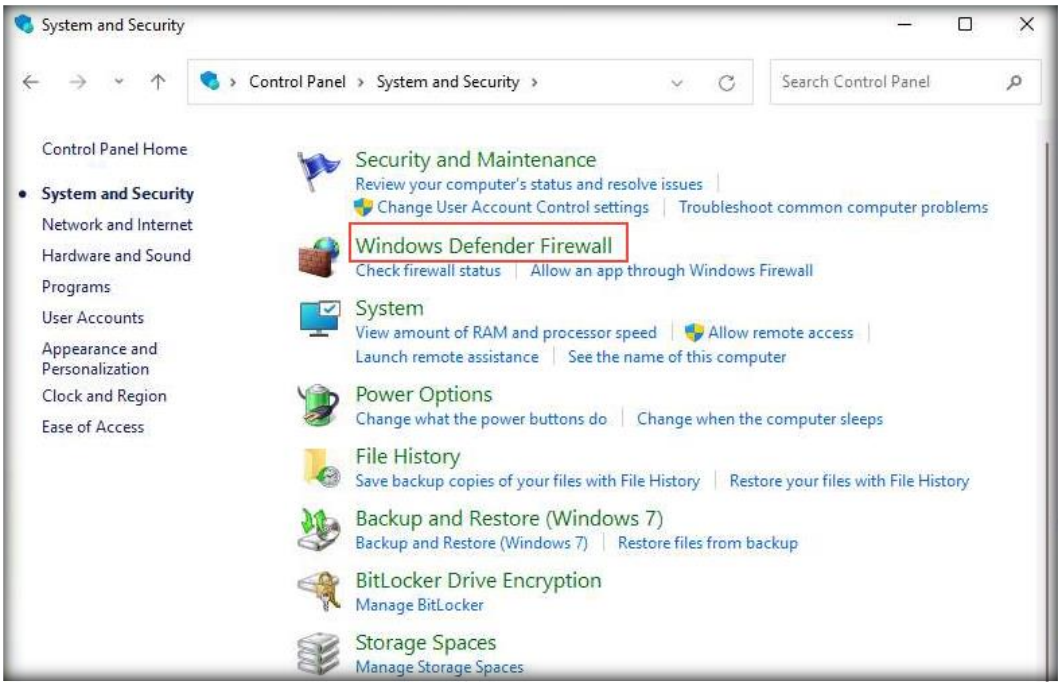
   Note: If a **Windows 11 – VMware Workstation** pop-up appears, click **Yes**.

2. Click the **Type here to search** icon, type **control panel**, and select **Control Panel** from the search results.

3. The **Control Panel** window appears; click the **System and Security** category.

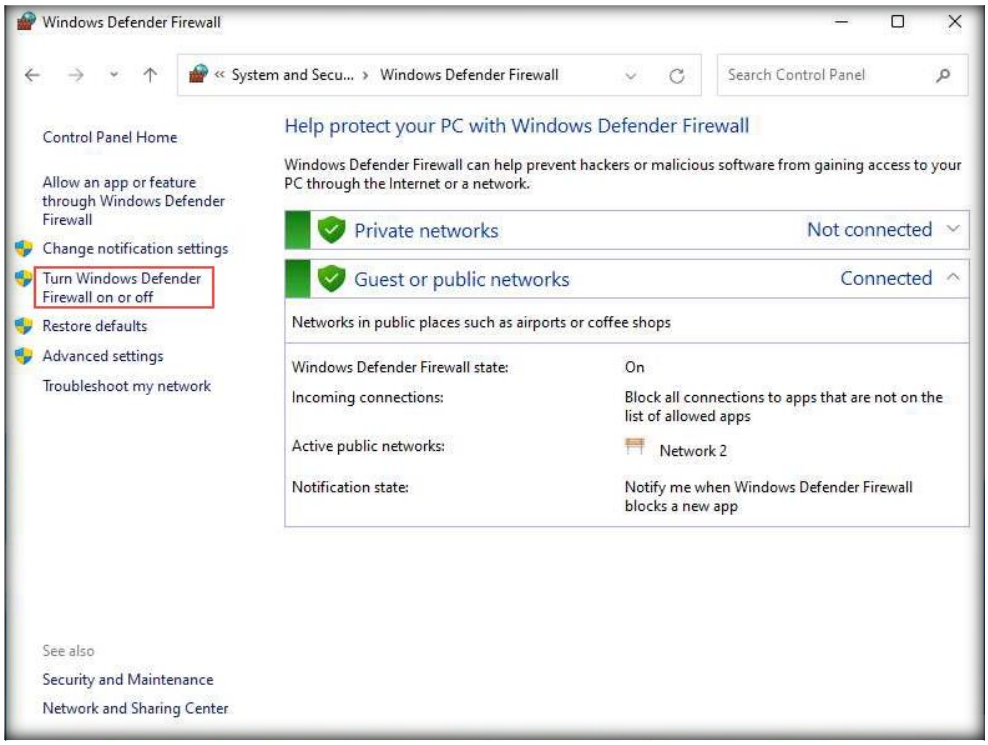


4. Click **Windows Defender Firewall** in the **System and Security** window.

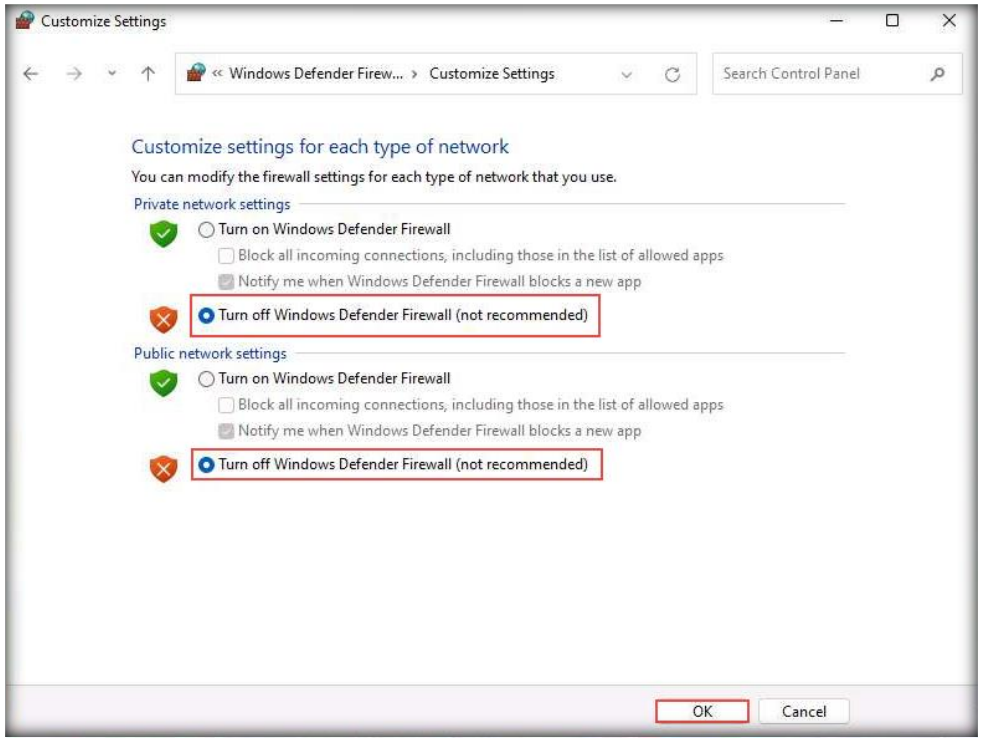


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. In the **Windows Defender Firewall** window, click the **Turn Windows Defender Firewall on or off** link in the left-hand pane.

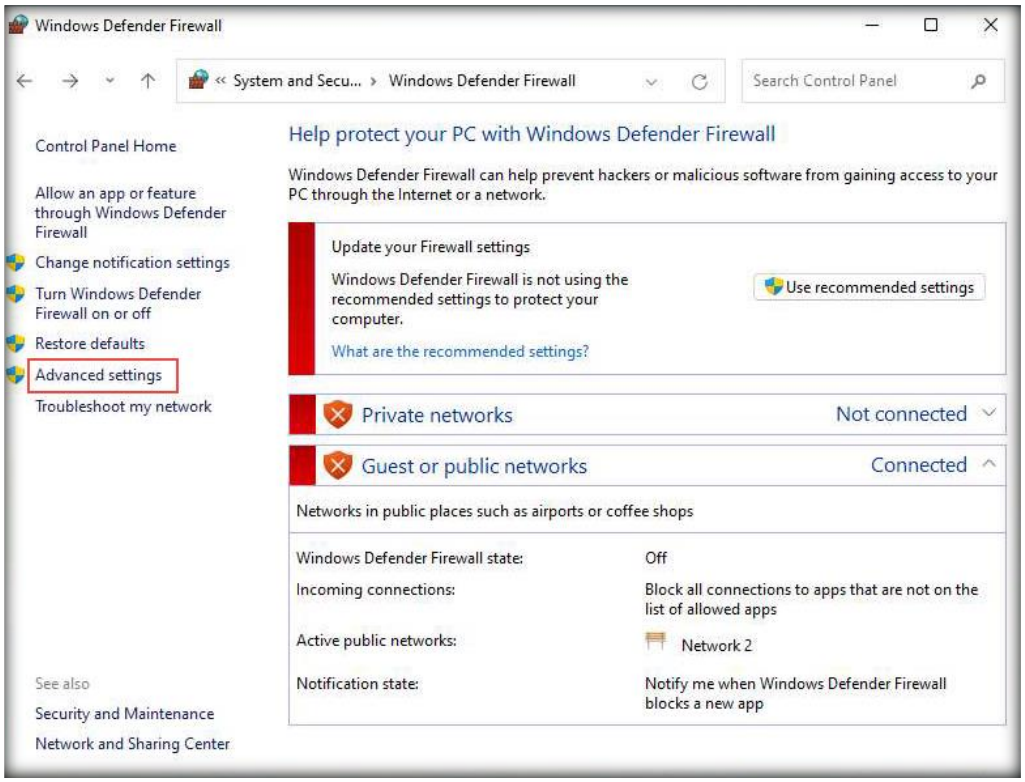


6. In the **Customize Settings** window, select the **Turn off Windows Defender Firewall (not recommended)** radio button for all Domain, Private, and Public network settings and click **OK**.

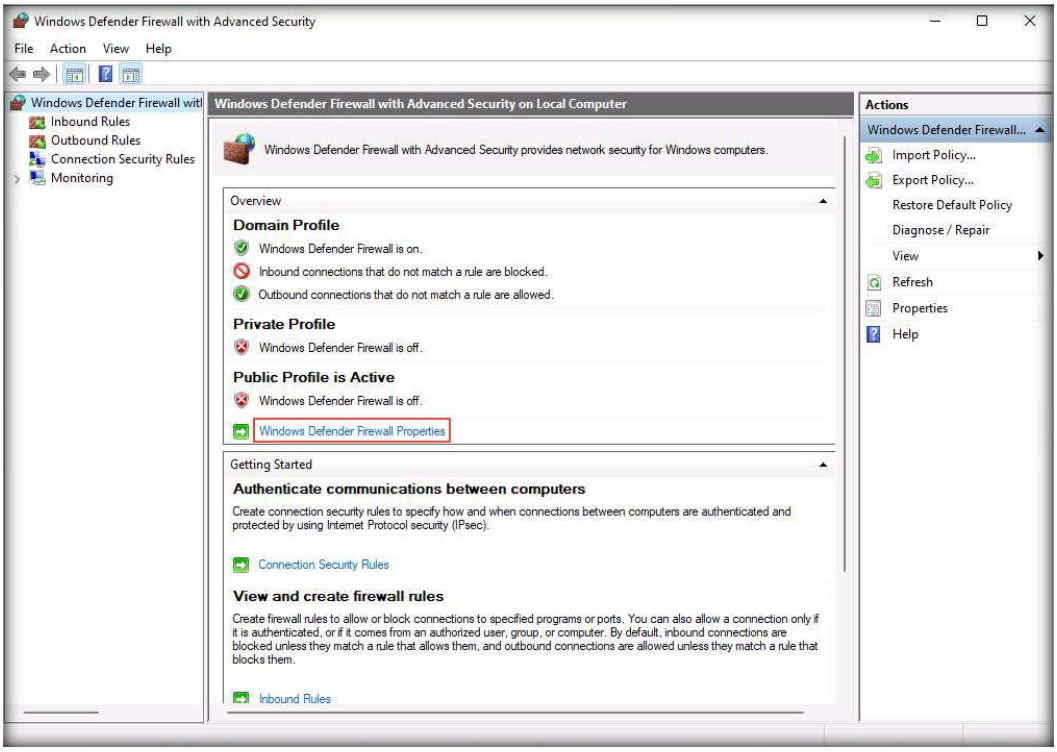


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Again, in the **Windows Defender Firewall** window, click the **Advanced settings** link in the left-hand pane.

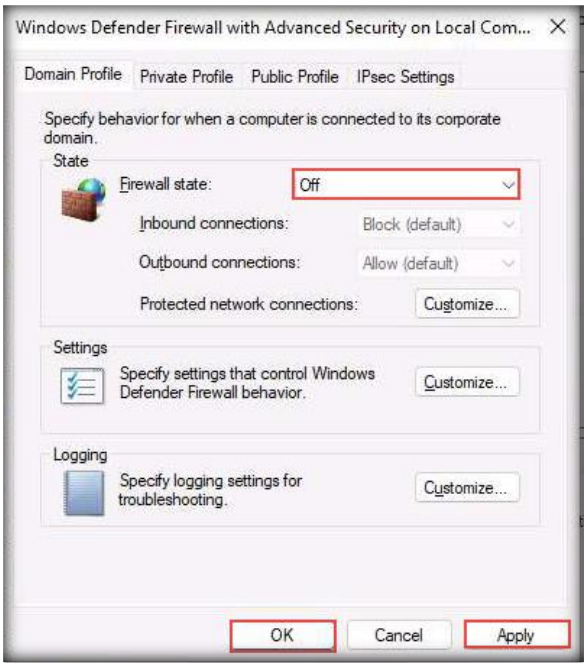


8. Once the **Windows Defender Firewall with Advanced Security** window appears on the screen, click the **Windows Defender Firewall Properties** link in the **Overview** section.

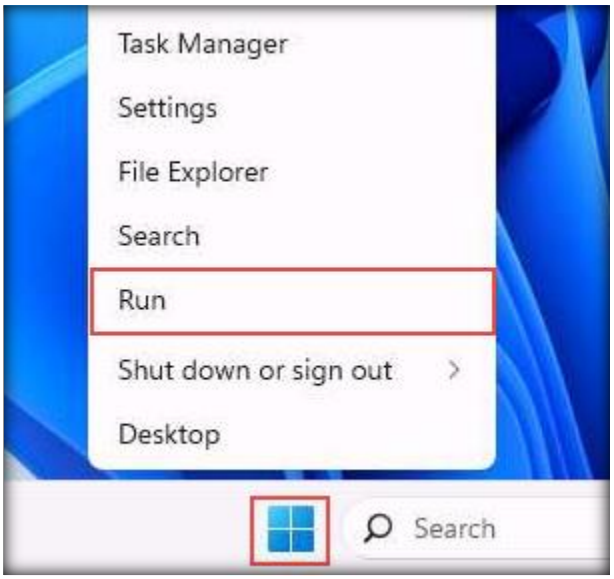


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. When the **Windows Defender Firewall with Advanced Security on Local Computer Properties** window appears, in the **Domain Profile** tab, choose **Off** from the **Firewall state** drop-down list. Then, navigate to the **Private Profile** and **Public Profile** tabs and ensure that the **Firewall state** is **Off**. Click **Apply** and then **OK**.

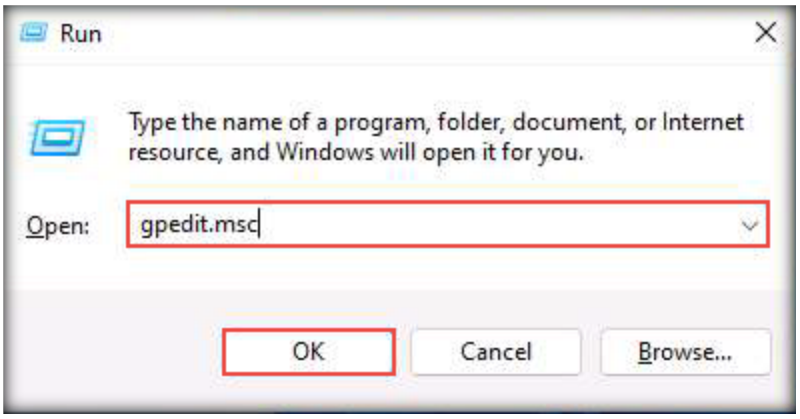


10. Close all windows.
11. Right-click the **Windows** icon in the lower section of the screen and click **Run**.



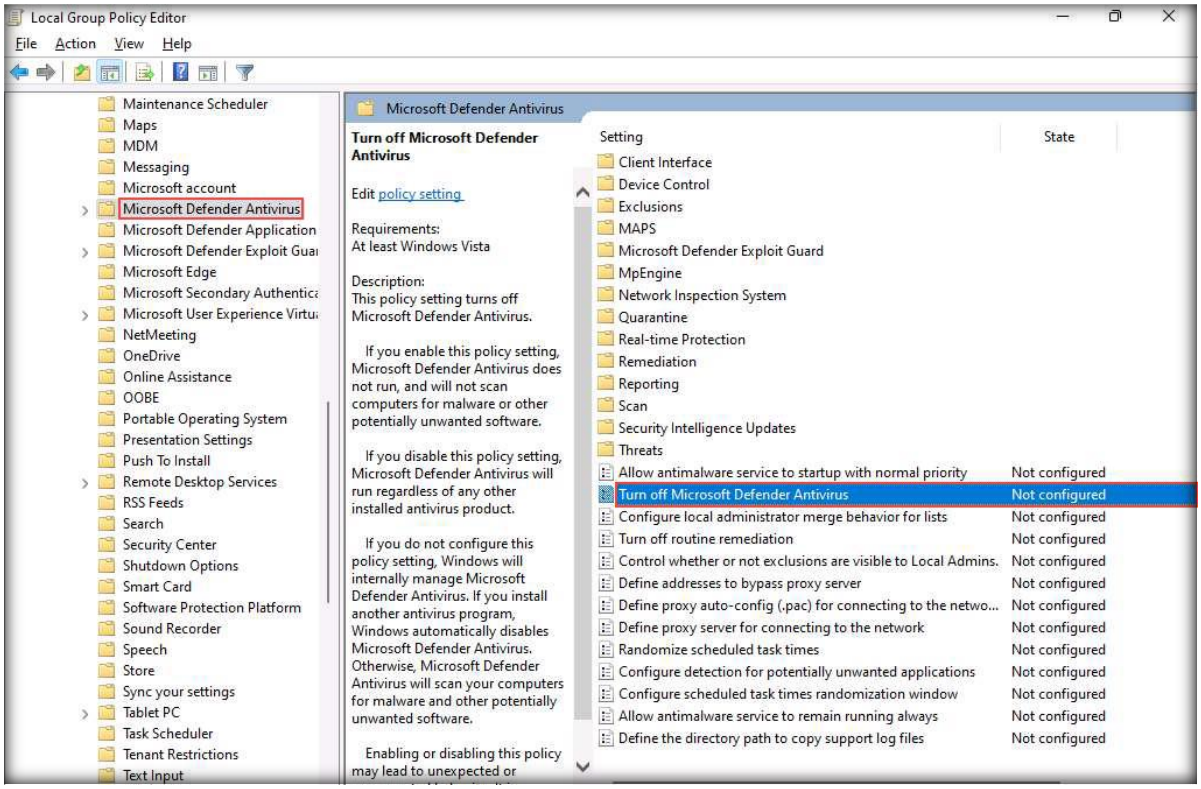
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **Run** window appears. Type **gpedit.msc** and click **OK**.



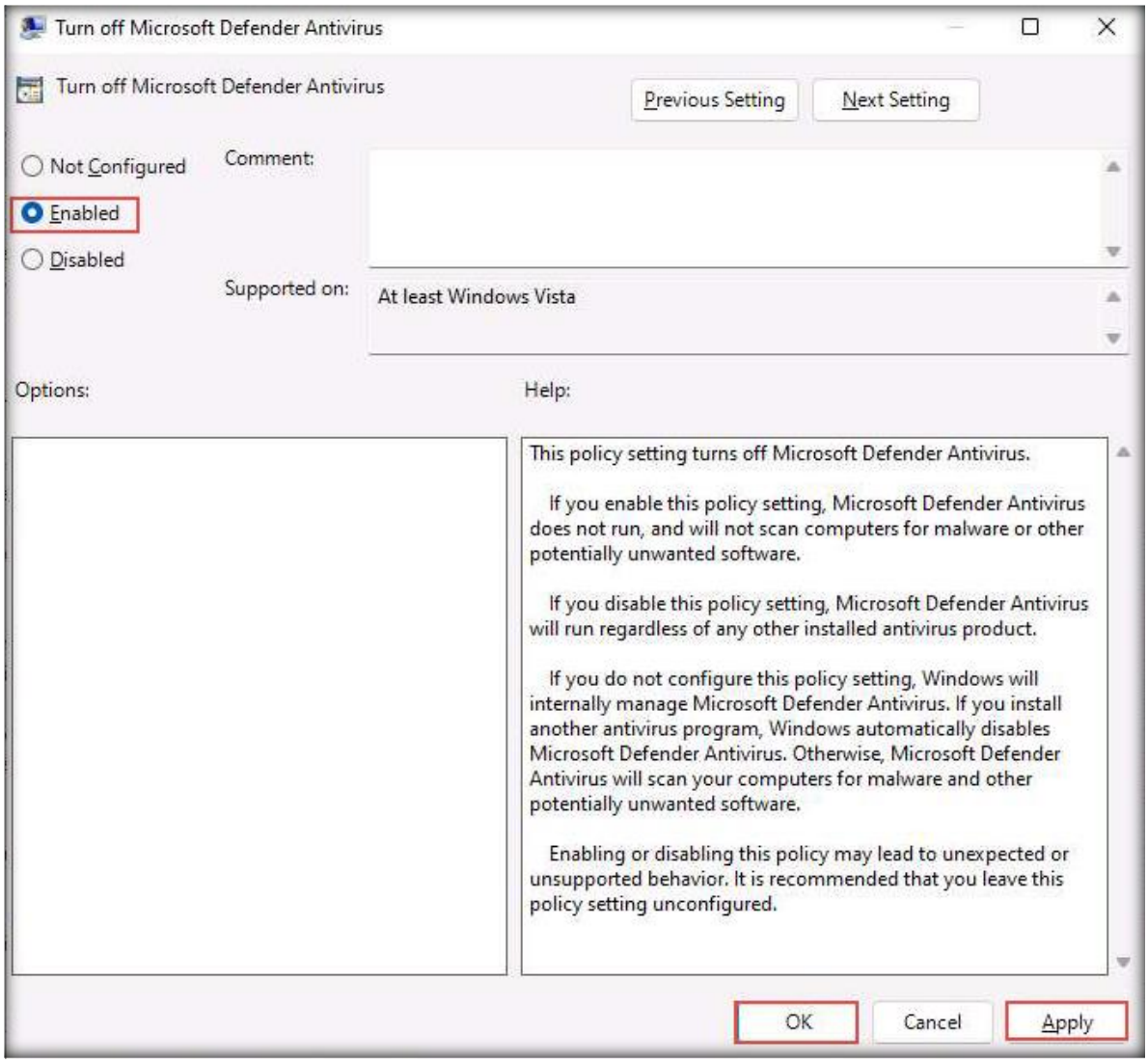
13. The **Local Group Policy Editor** window appears. In the left-hand pane, navigate to **Local Computer Policy → Computer Configuration → Administrative Templates → Windows Components → Microsoft Defender Antivirus**. Double-click the **Turn off Microsoft Defender Antivirus** policy in the right-hand pane of the window, as shown in the screenshot below.

Note: If you are using an older version of **Windows**, you might see a **Windows Defender Antivirus** folder instead of **Microsoft Defender Antivirus**.



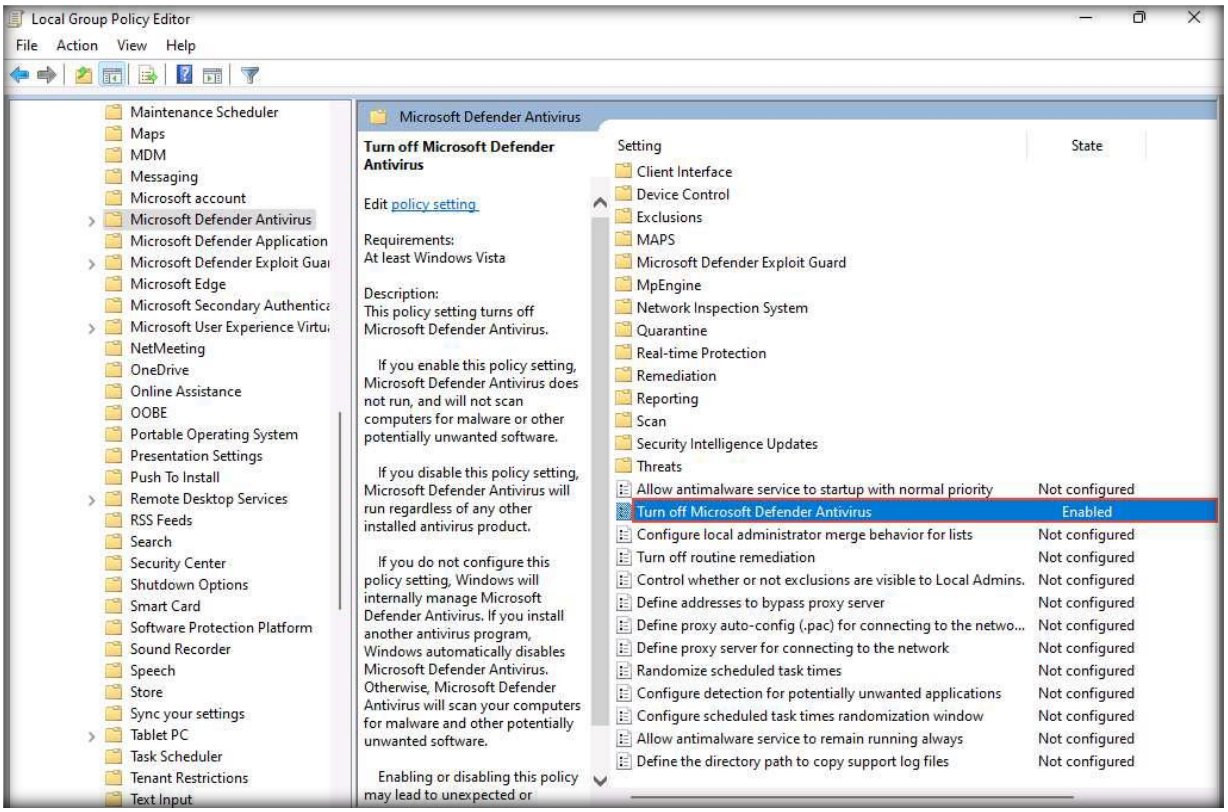
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

14. When the **Turn off Microsoft Defender Antivirus** window appears, select the **Enabled** radio button, click **Apply**, and then click **OK** to turn off **Microsoft Defender Antivirus**.

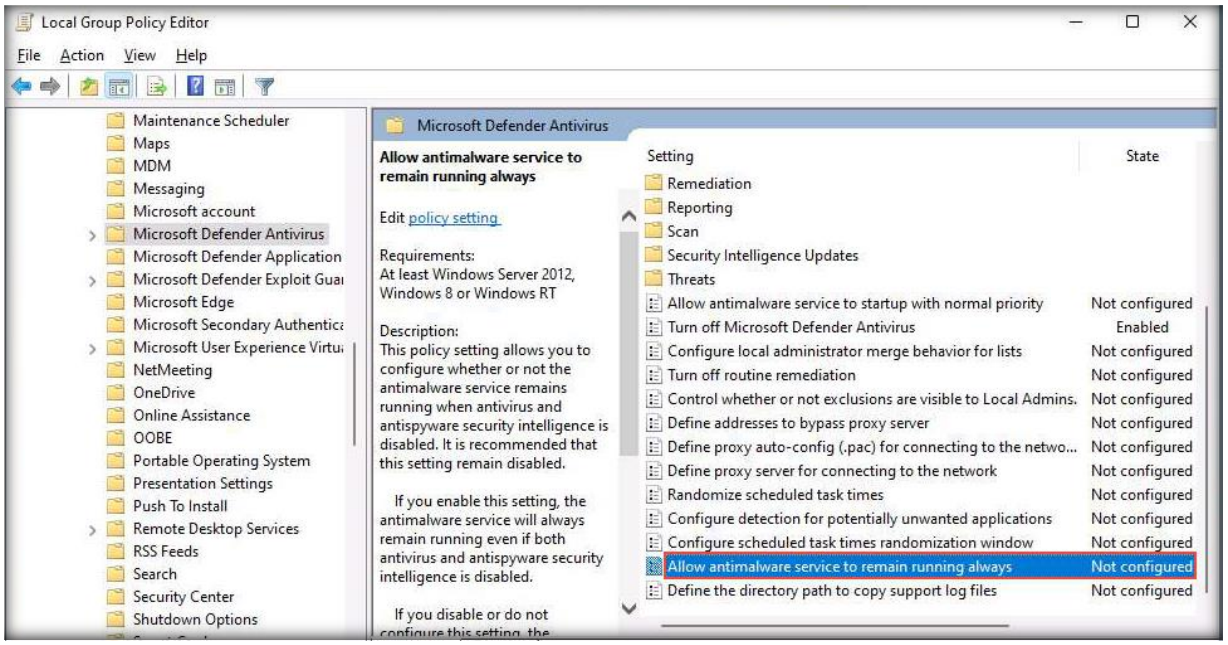


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

15. **Microsoft Defender Antivirus** is turned off.

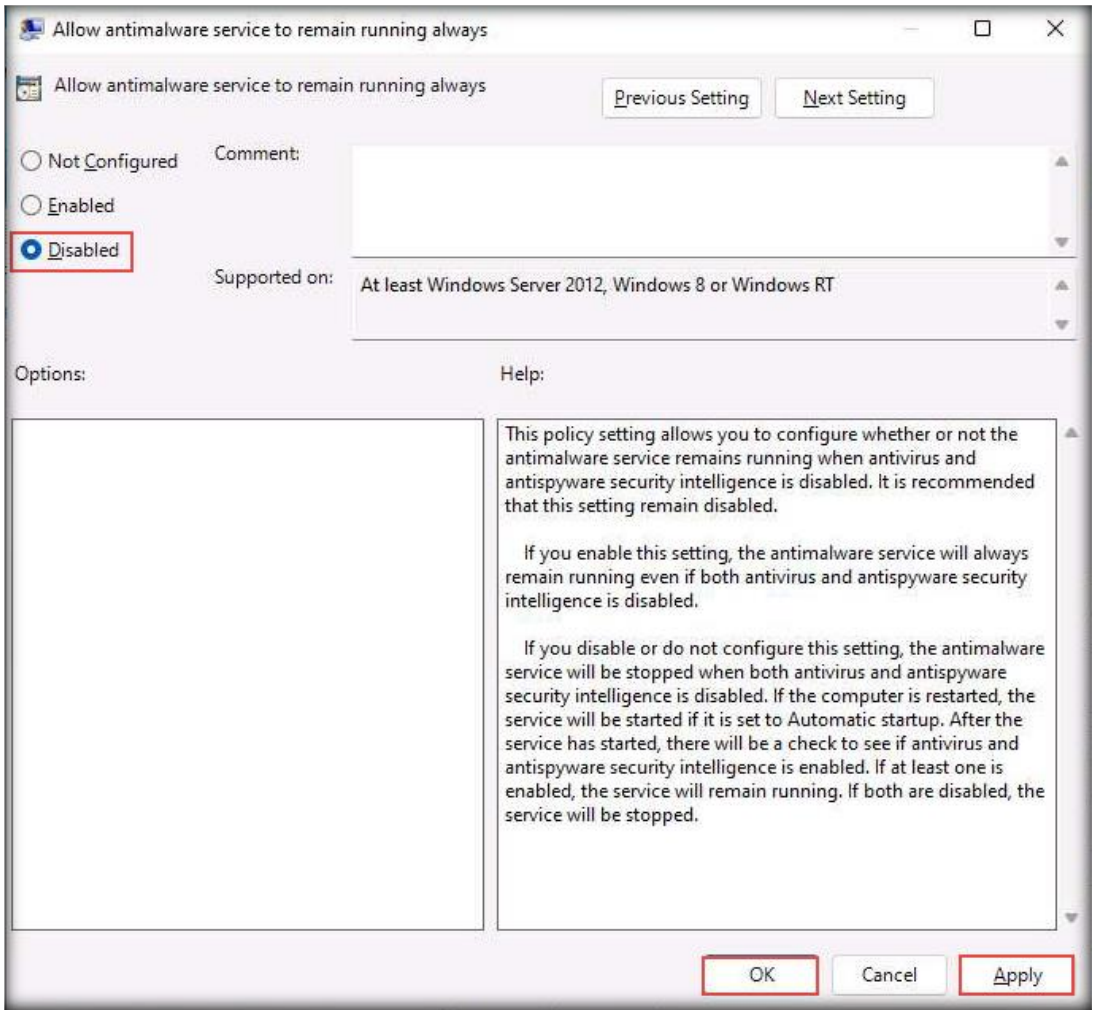


16. In the **Local Group Policy Editor** window, double-click **Allow antimalware service to remain running always**.



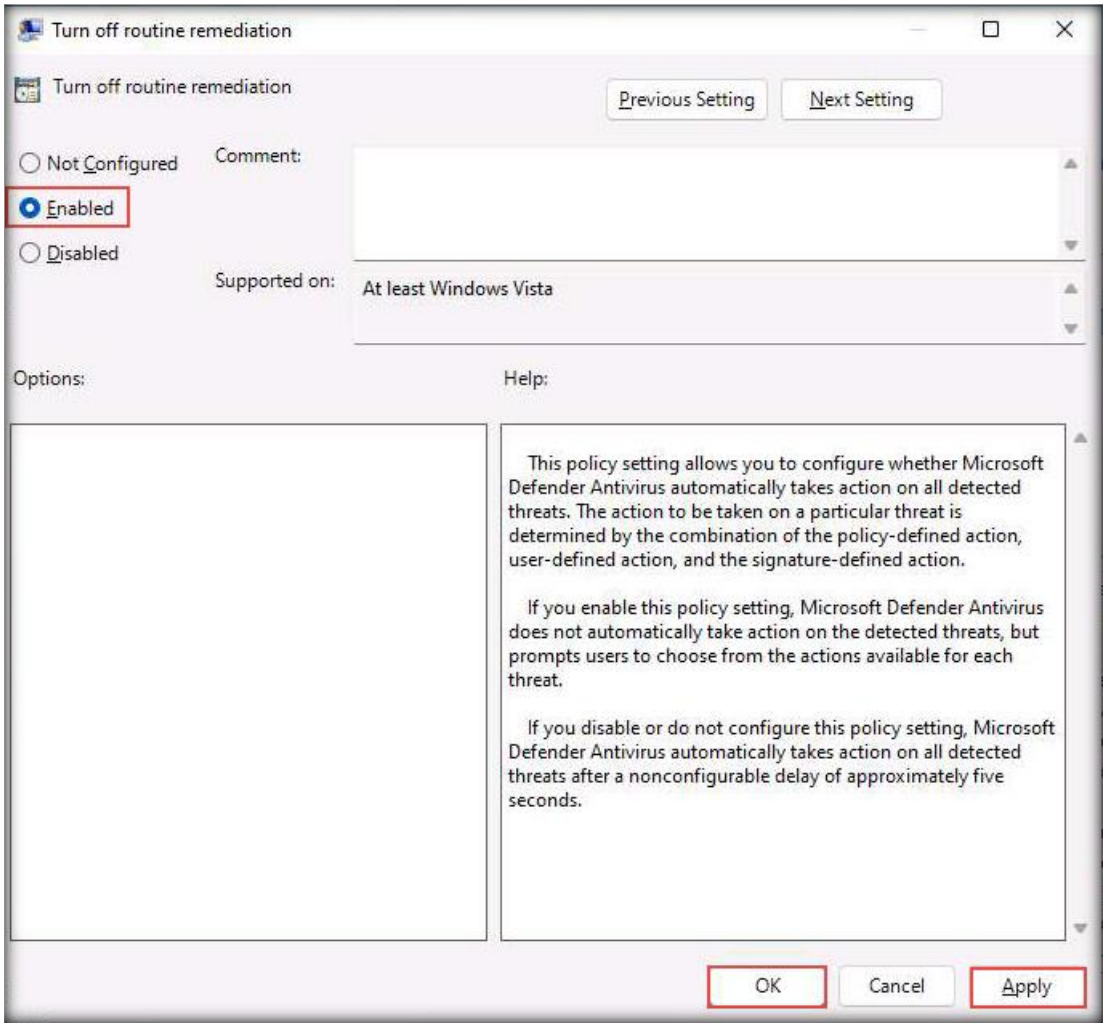
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. When the **Allow antimalware service to remain running always** window appears, select the **Disabled** radio button. Click **Apply** and then **OK**.



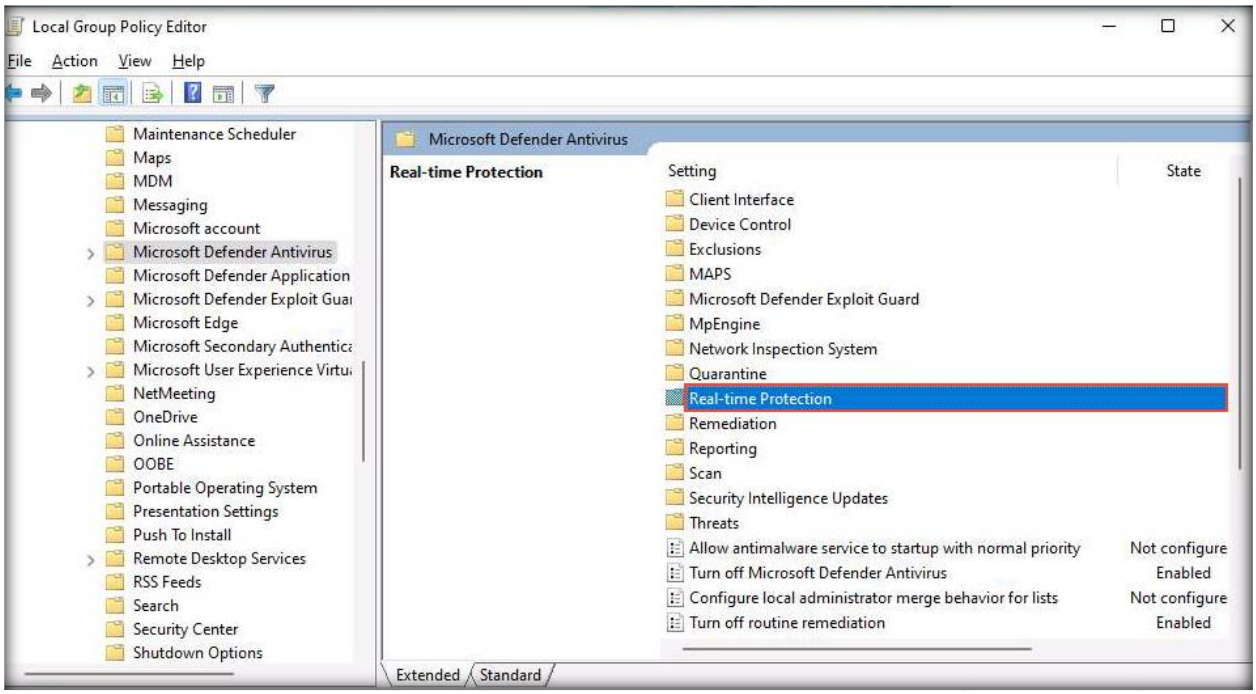
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. In the **Local Group Policy Editor** window, double-click **Turn off routing remediation**.
19. When the **Turn off routing remediation** window appears, select the **Enabled** radio button. Click **Apply** and then **OK**.

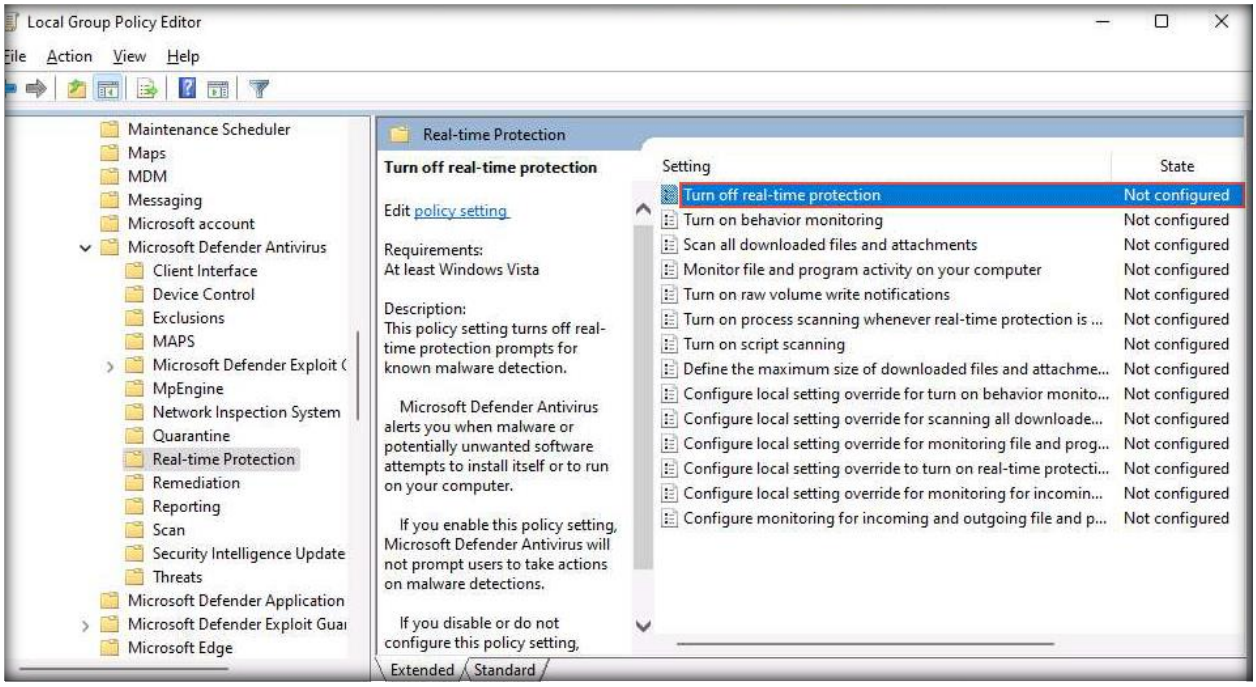


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

20. In the **Local Group Policy Editor** window, double-click the **Real-time Protection** folder.

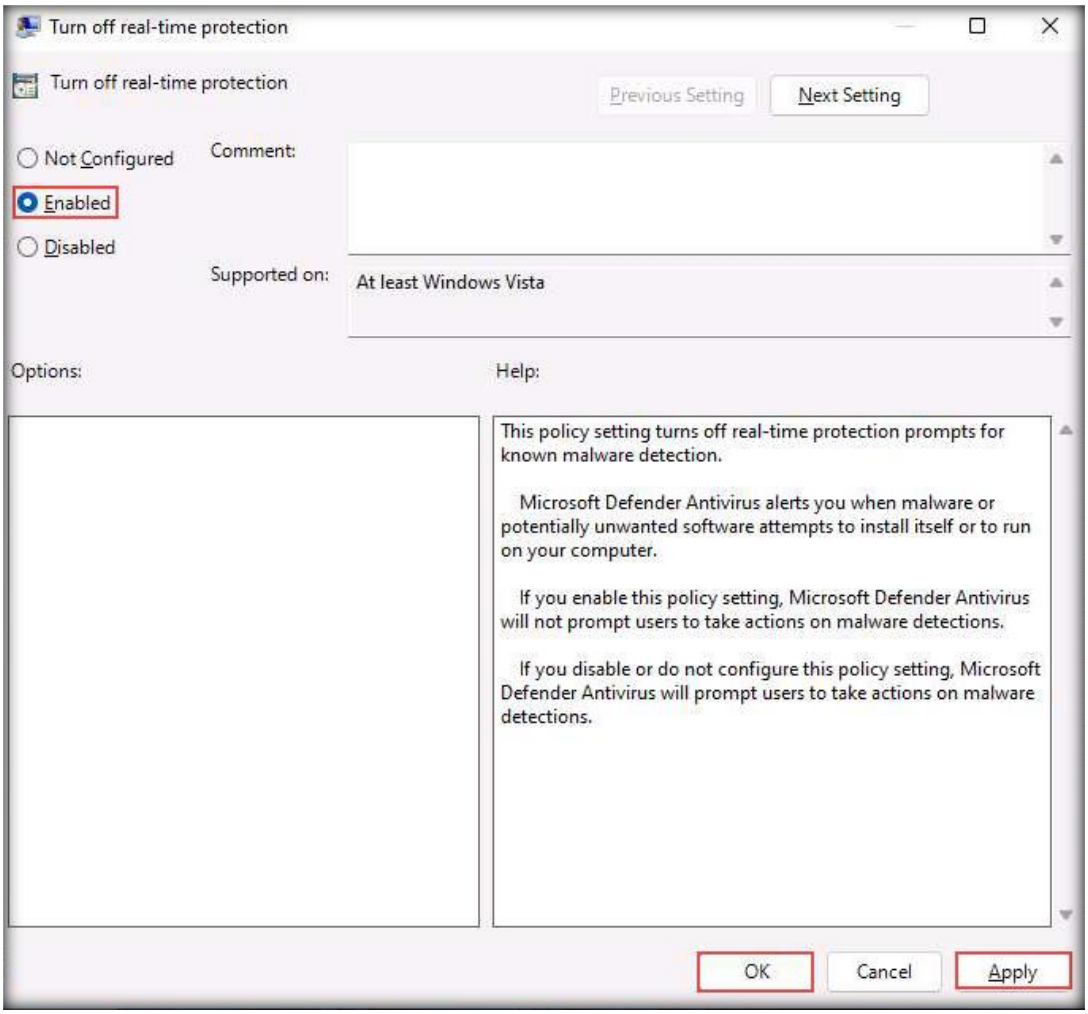


21. In the **Real-time Protection** window, double-click **Turn off real-time protection**.

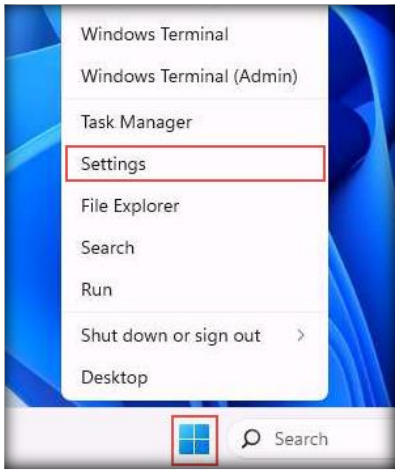


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

22. When the **Turn off real-time protection** window appears, select the **Enabled** radio button. Click **Apply** and then **OK**.



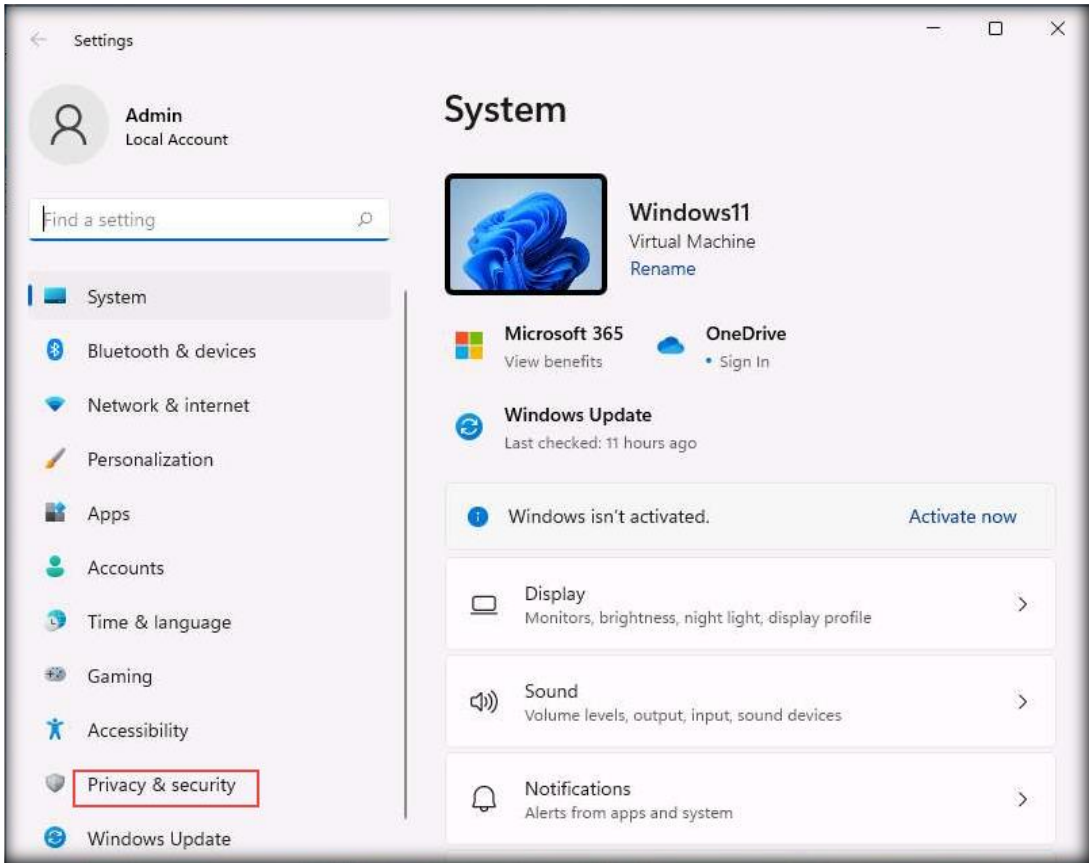
23. Close all windows.
24. Right-click the **Windows** button in the lower-left corner of the screen and click **Settings**.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

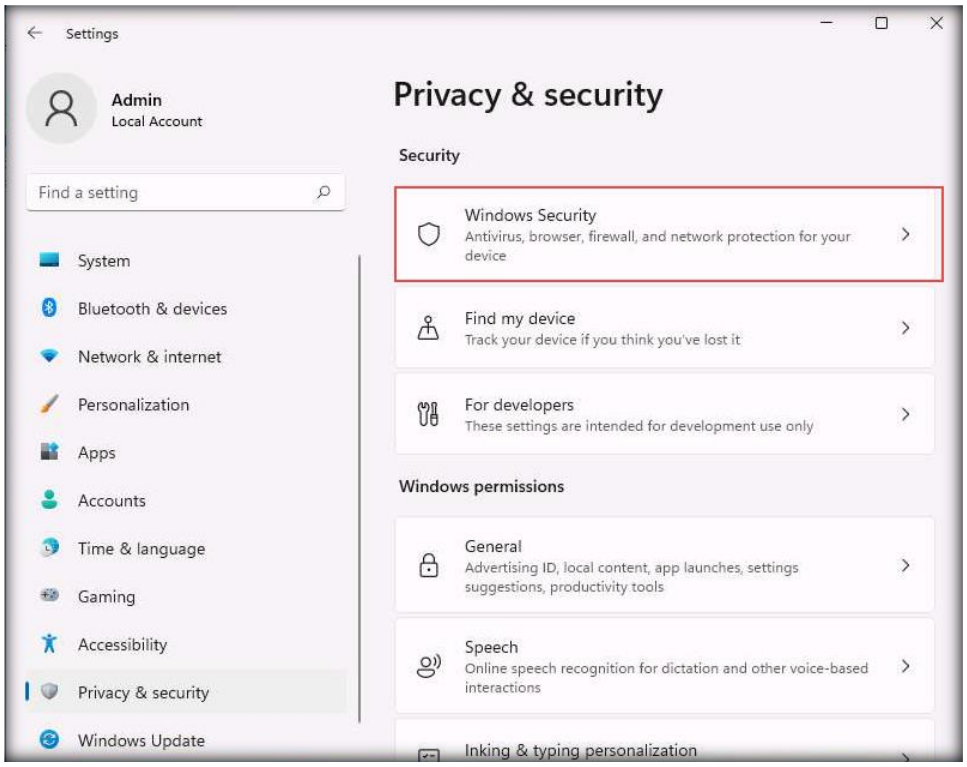
25. In the **Settings** window, click **Privacy & security** from the left-hand pane.

    Note: In **Windows Server 2022** machine, the **Windows Security** option is present in **Update & Security** section.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

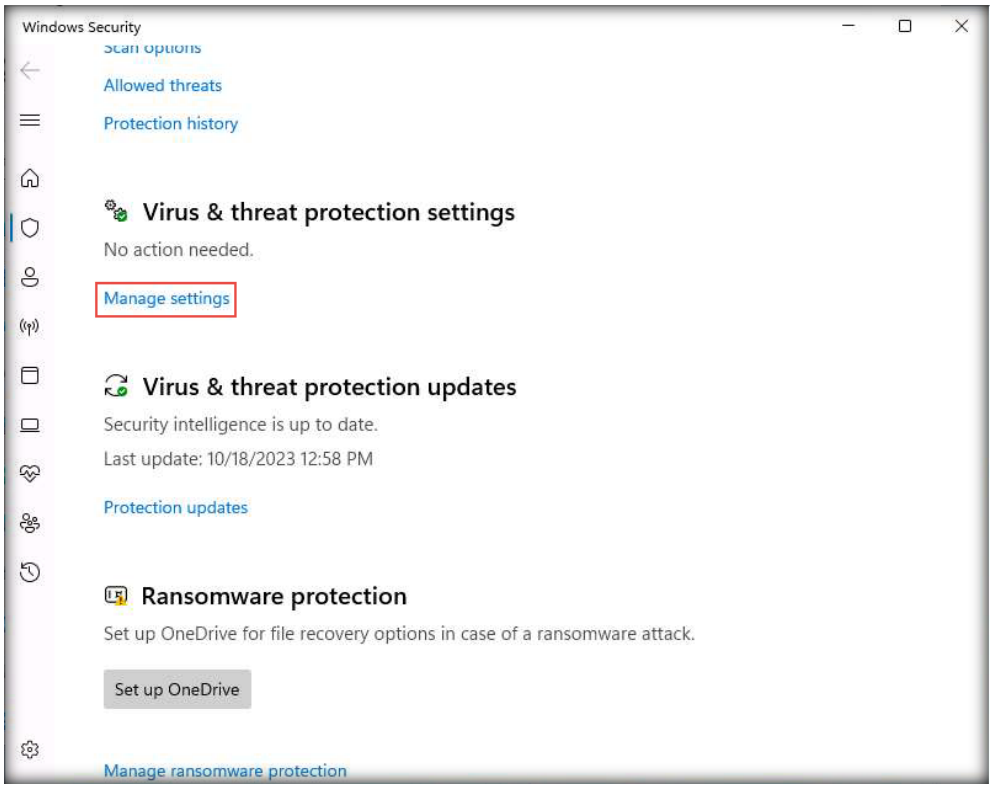
26. The **Privacy & security** settings appear in the right-hand pane. Then, click the **Windows Security** option.



27. In the **Windows Security** window, click **Virus & threat protection**.

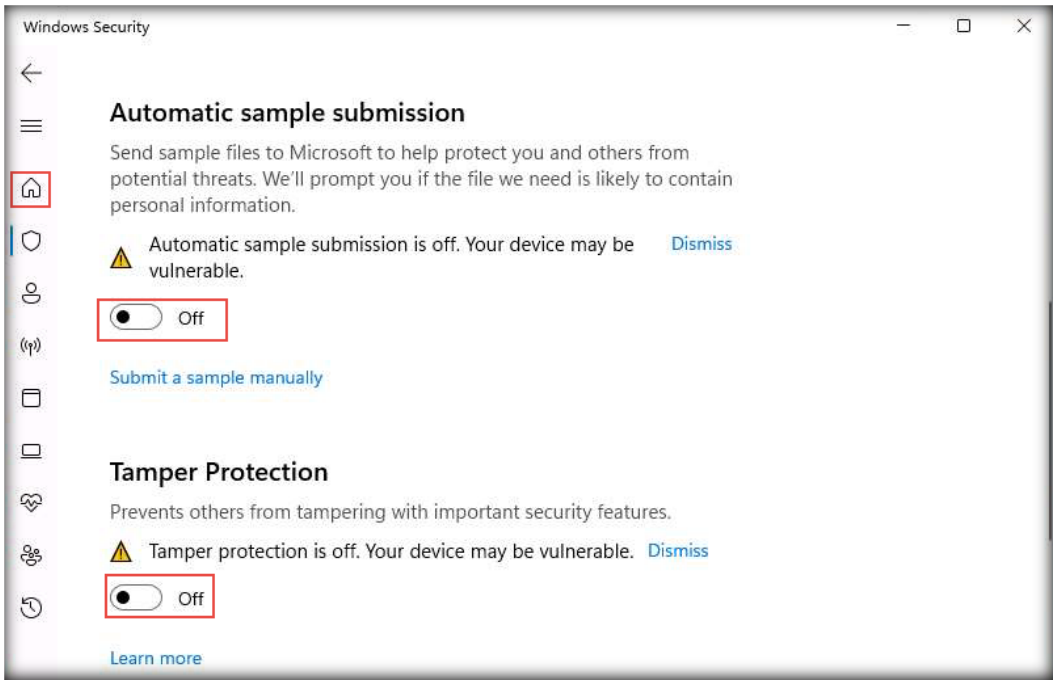
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

28. On the **Virus & threat protection** page, click **Manage settings** under **Virus & threat protection settings**.



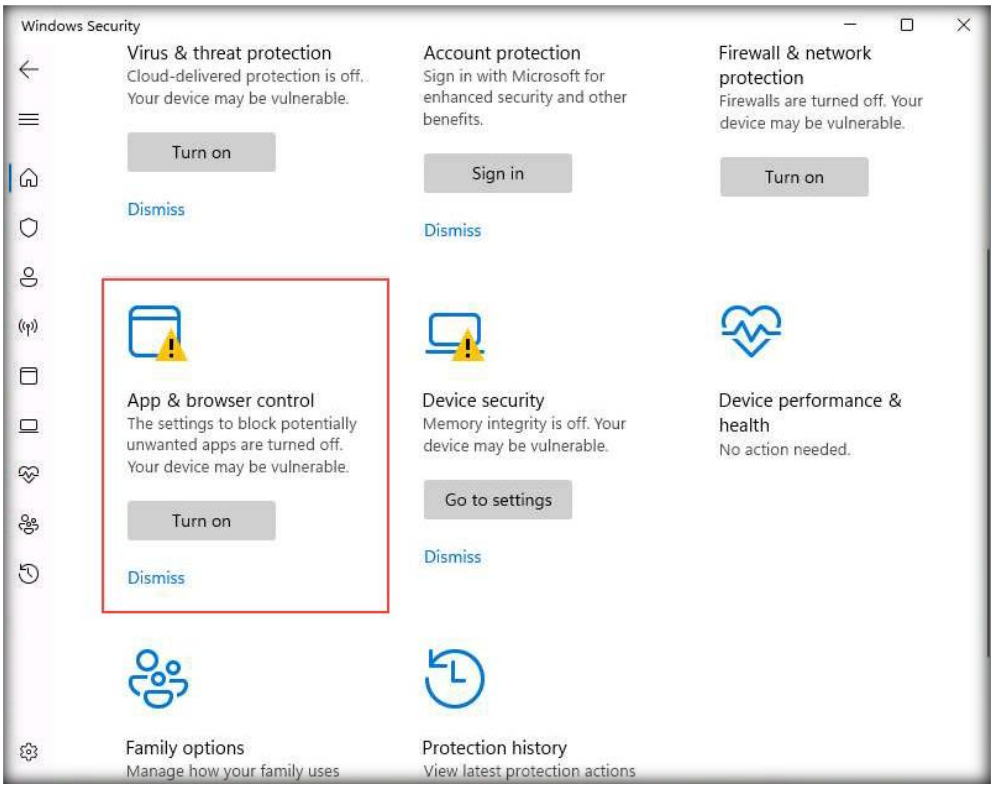
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

29. When the **Virus & threat protection settings** page appears, turn off **Real-time protection**, **Cloud-delivered protection**, **Automatic sample submission**, and **Tamper Protection**. If a **User Account Control** pop-up window appears, click **Yes**. After turning off the above-mentioned items, click the **Home** icon in the left menu bar.

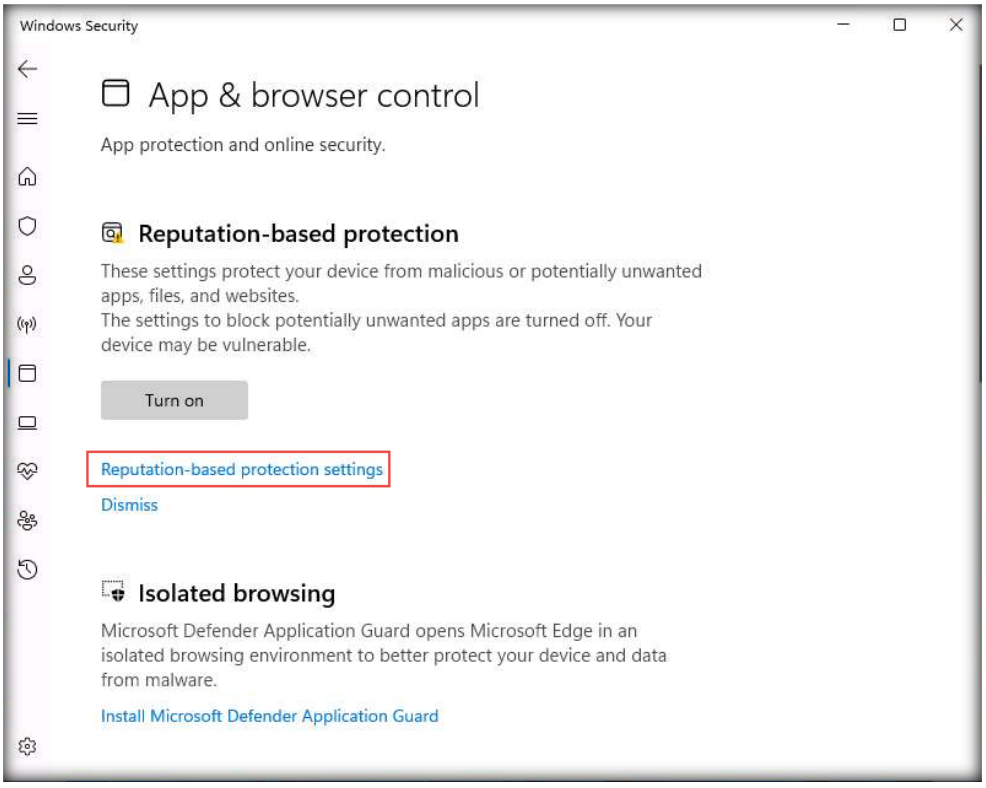


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

30. Next, click **App & browser control** in the **Windows Security** window.



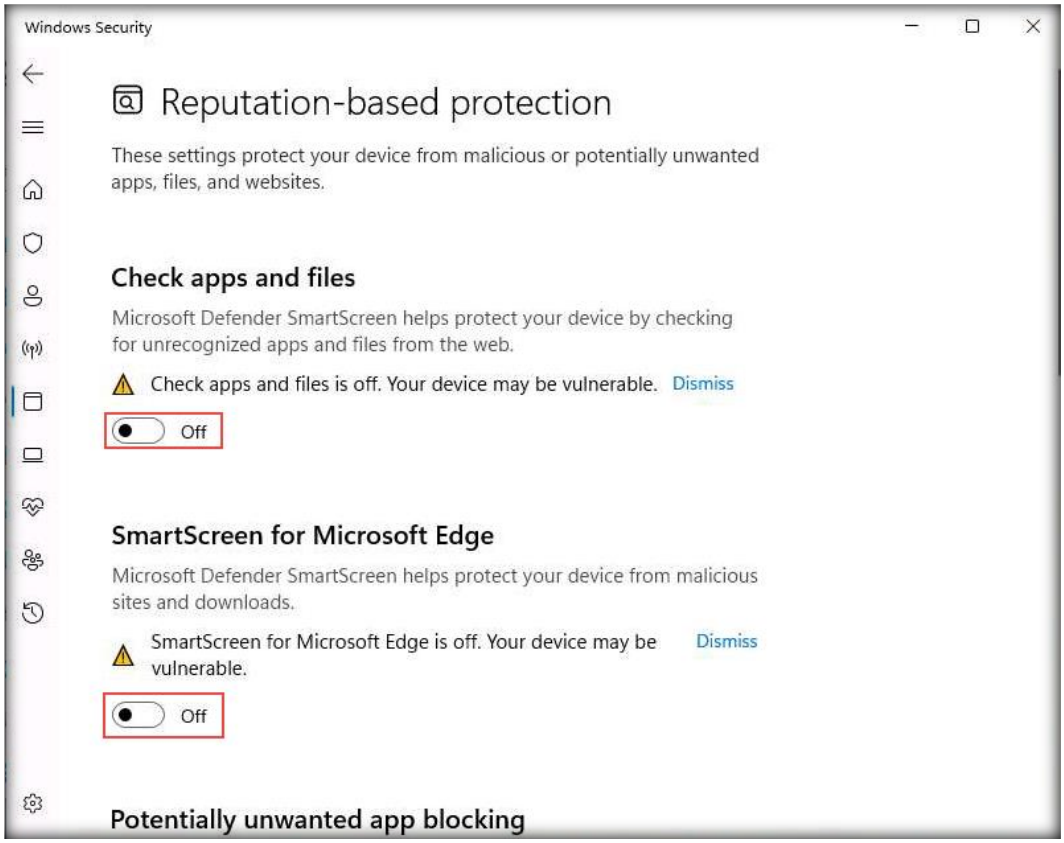
31. In the **App & browser control** page, click the **Reputation-based protection settings** link under **Reputation-based protection**.



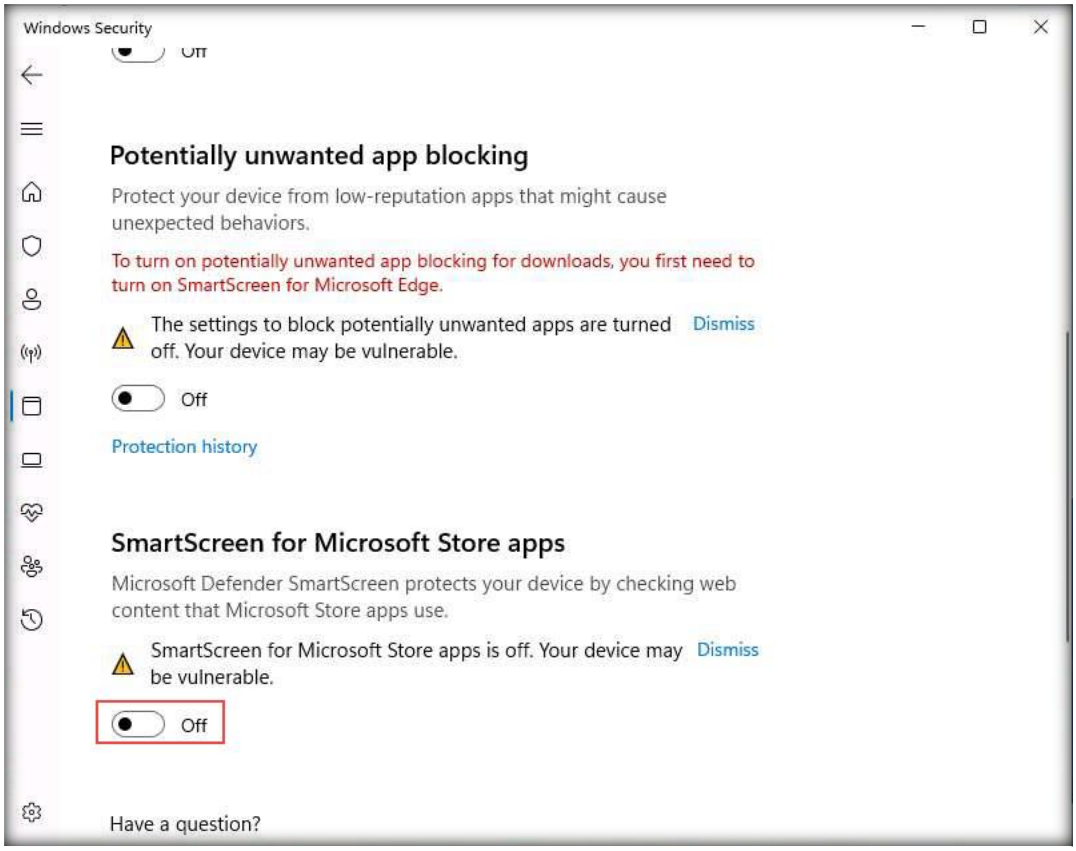
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

32. The **Reputation-based protection** page appears. Select the **Off** radio buttons under **Check apps and files**, **SmartScreen for Microsoft Edge**, and **SmartScreen for Microsoft Store apps**. If a **User Account Control** pop-up window appears, click **Yes**.

    Note: If you are unable to turn off the **SmartScreen for Microsoft Edge** radio button, leave the setting for **SmartScreen for Microsoft Edge** radio button as it is, and continue with the setup.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



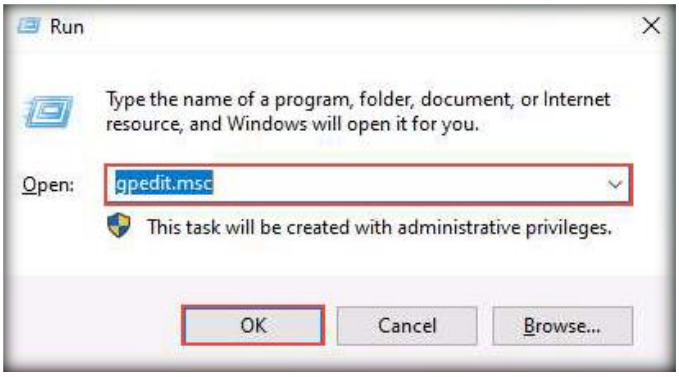
33. Close all windows.
34. Similarly, follow the above steps to turn off the Windows Defender Firewall on all Windows virtual machines (Windows Server 2022).

[Back to Configuration Task Outline]

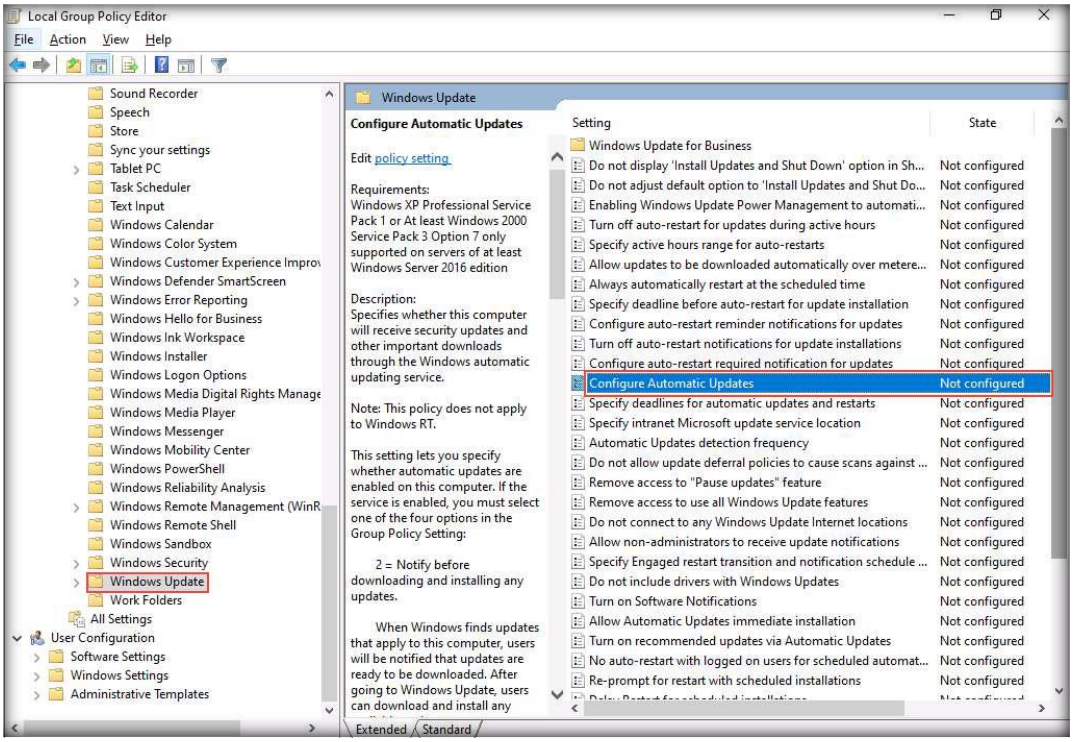
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#12: Configure Windows Components on all Windows Virtual Machines

1. Log in to the **Windows Server 2022** virtual machine. Right-click on **Start** and click **Run**.
2. The **Run** window appears; type **gpedit.msc** and click **OK**.

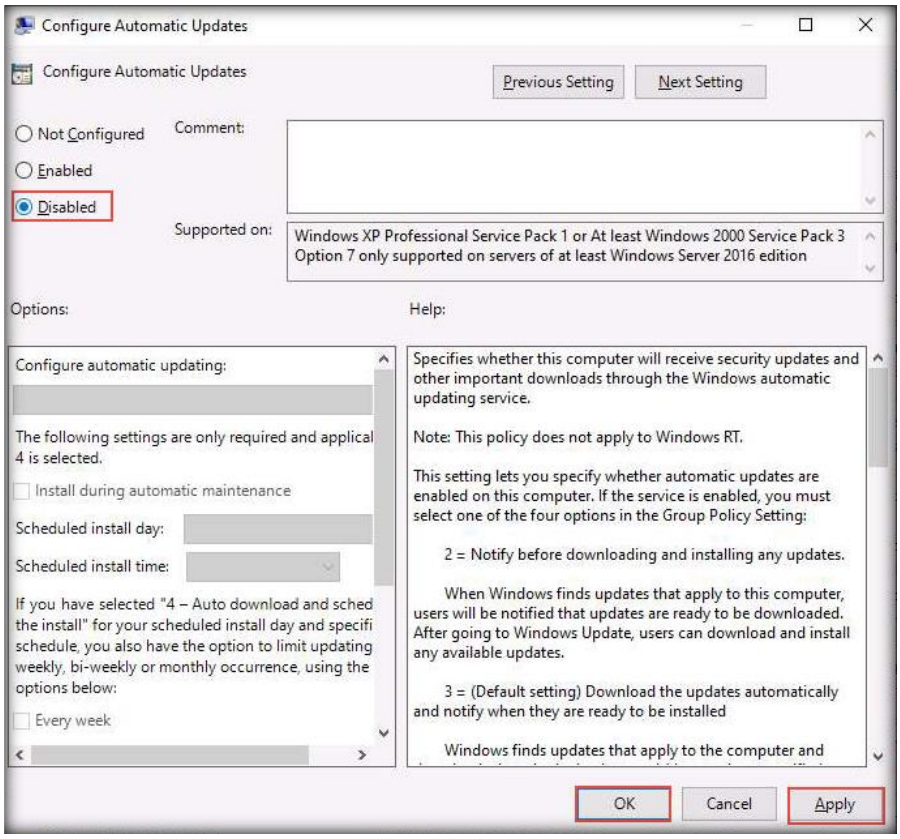


3. The **Local Group Policy Editor** window appears; expand **Administrative Templates** under **Computer Configuration** in the left pane.
4. In **Administrative Templates**, expand **Windows Components**, scroll down, click **Windows Update** in the left pane, and double-click **Configure Automatic Updates** in the right-hand pane, as shown in the screenshot below.



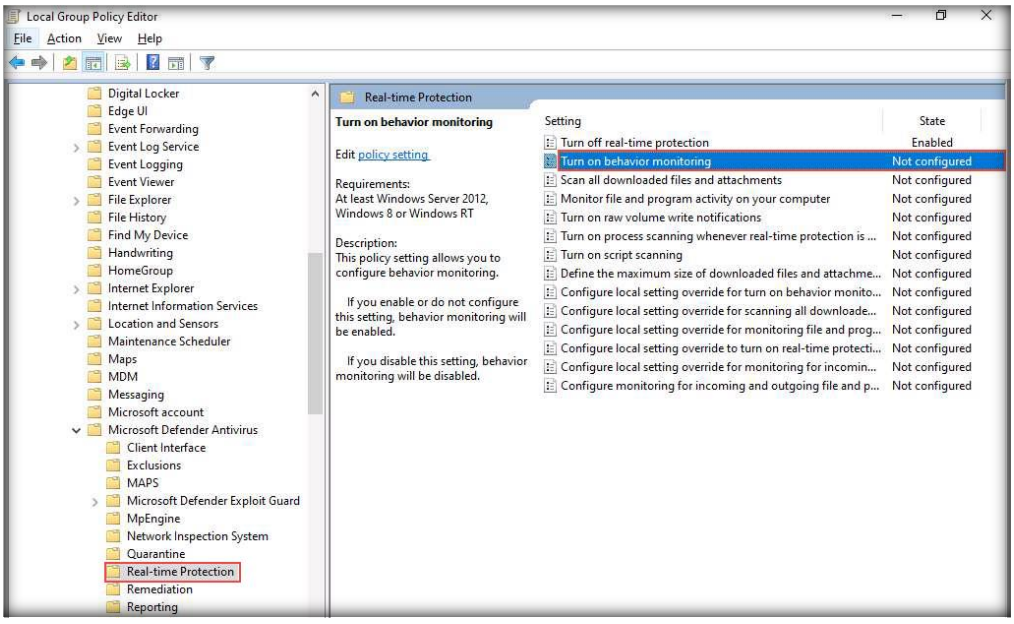
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The **Configure Automatic Updates** window appears; select the **Disabled** radio button. Click **Apply** and then **OK**.



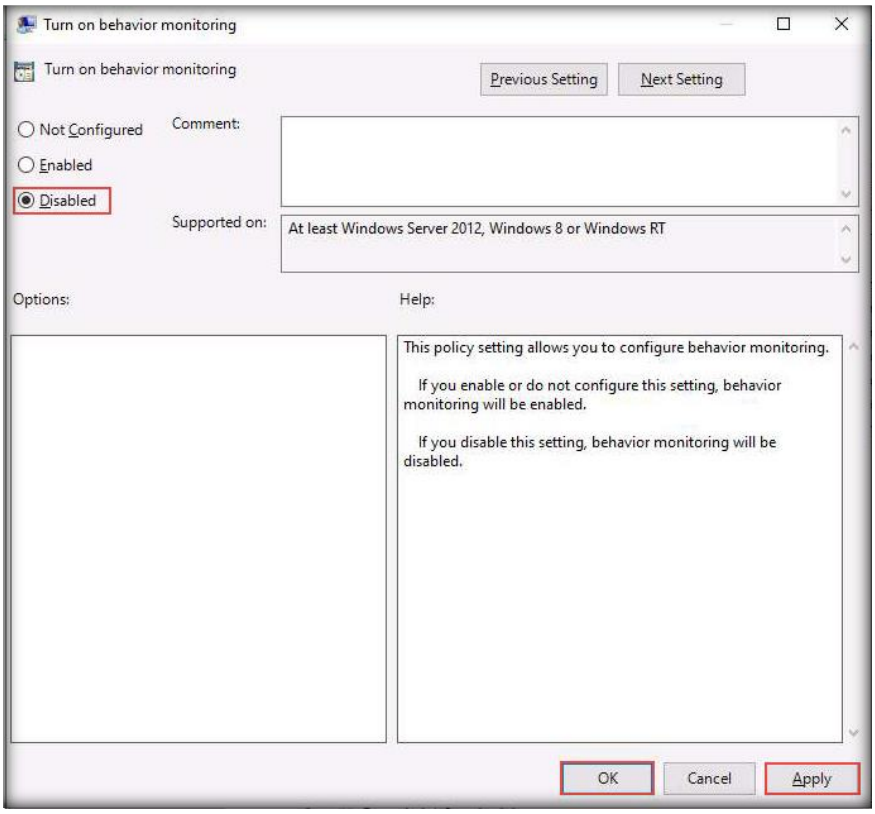
6. In the left-hand pane, navigate to **Local Computer Policy → Computer Configuration → Administrative Templates → Windows Components → Windows Defender Antivirus → Real-time Protection**.

7. Double-click the **Turn on behavior monitoring** setting to configure its settings.

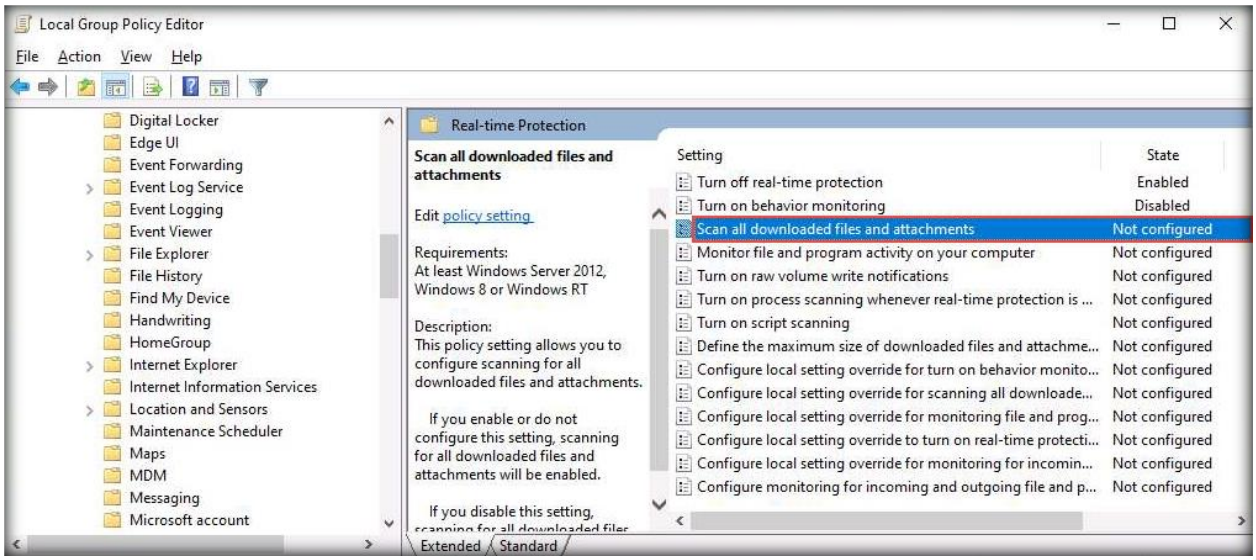


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **Turn on behavior monitoring** window appears. Select the **Disabled** radio button. Click **Apply** and then **OK**.

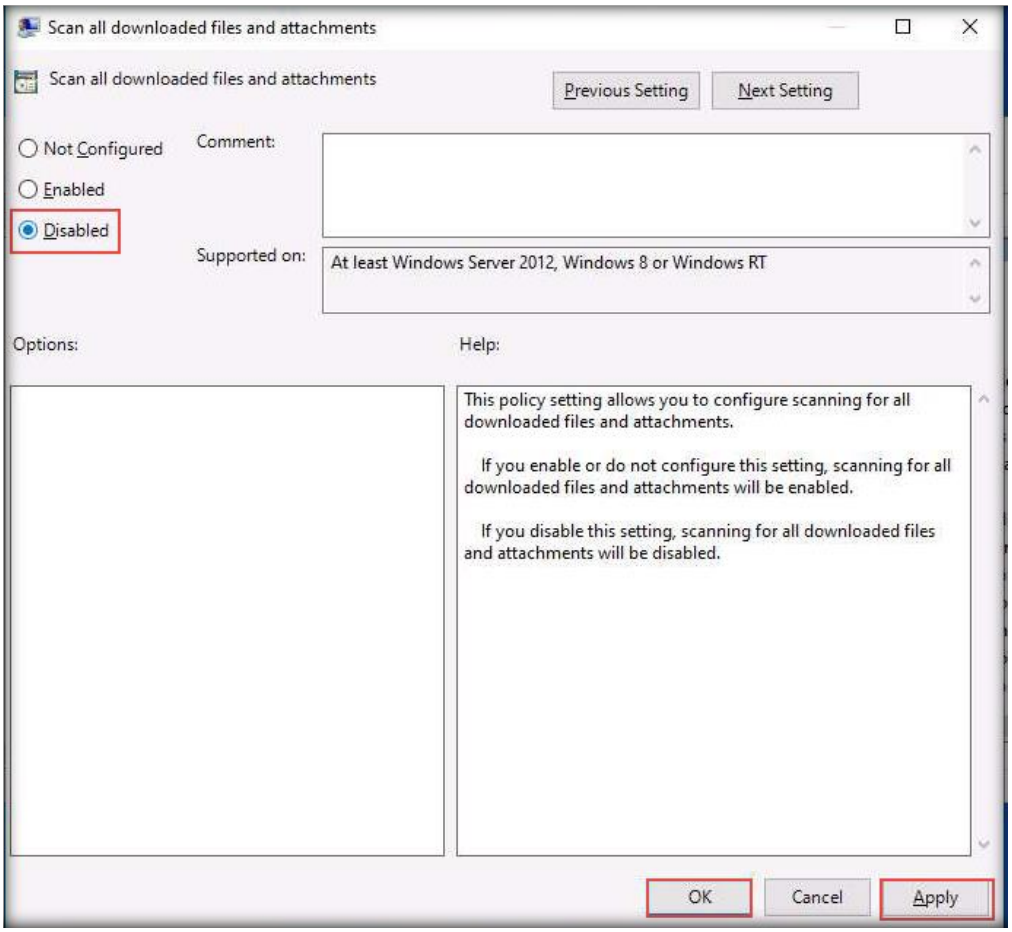


9. Double-click the **Scan all downloaded files and attachments** setting, as shown in the screenshot below.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Scan all downloaded files and attachments** window appears. Select the **Disabled** radio button. Click **Apply** and then **OK**.



11. Similarly, follow the above steps to configure Windows components on the **Windows 11** virtual machine.

Note: For the **Windows 11** virtual machine, in **Windows Update** settings, double-click **Manage end user experience** in the right-hand pane. In the **Manage end user** experience window, **Configure Automatic Updates** in the right-hand pane.

[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#13: Install WinRAR on the Windows Server 2022 Virtual Machine

1. Log in to the **Windows Server 2022** virtual machine with the credentials **Administrator** and **Pa$$w0rd**.
2. Download the latest version of **WinRAR** from the official WinRAR website (**https://www.rarlab.com/download.htm**).

   Note: Download the 64-bit version of **WinRAR**.
3. Double-click on the **winrar-x64-624.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
4. The **WinRAR** setup window appears; click **Install**.
5. Complete the installation by choosing the default settings throughout the installation process.
6. After completing the installation, the **installation location of WinRAR files** window opens automatically; close the window.

[Back to Configuration Task Outline]

CT#14: Install MS Office on the Windows Server 2022 Virtual Machine

1. Download the latest version of **MS Office** from the official Microsoft website (**https://www.microsoft.com**).

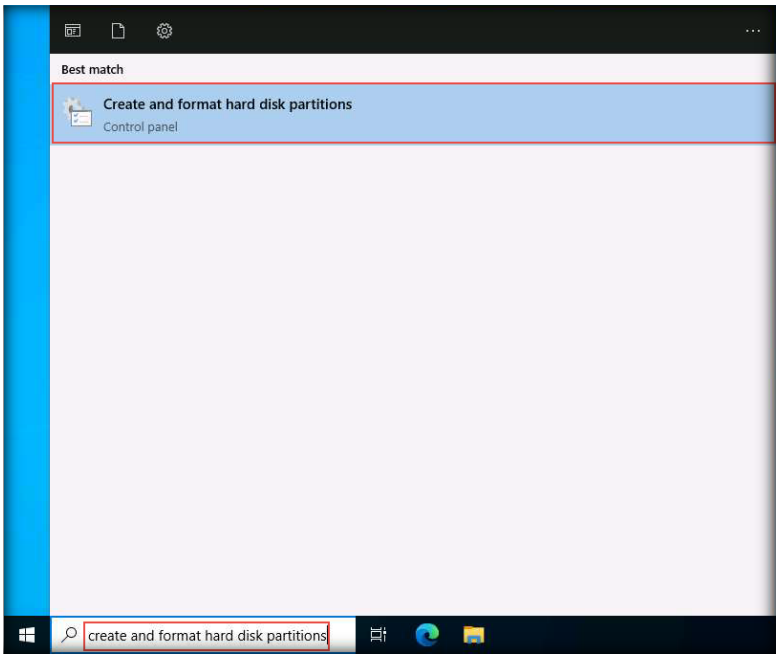
   Note: Download the 64-bit version of **MS Office**.
2. Double-click on the setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
3. Accept the license terms and complete the installation by choosing the default settings throughout the installation process.

[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

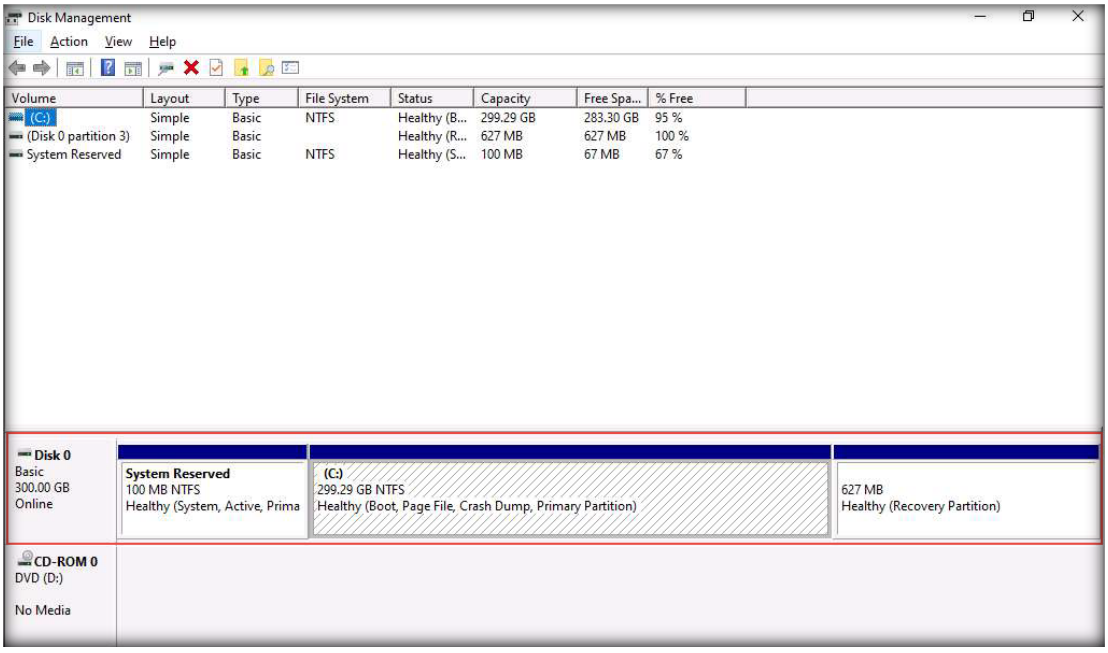
CT#15: Create a Partition in the Windows Server 2022 Virtual Machine

1. In the search bar, type **create and format hard disk partitions** and select **Create and format hard disk partitions** from the search result.



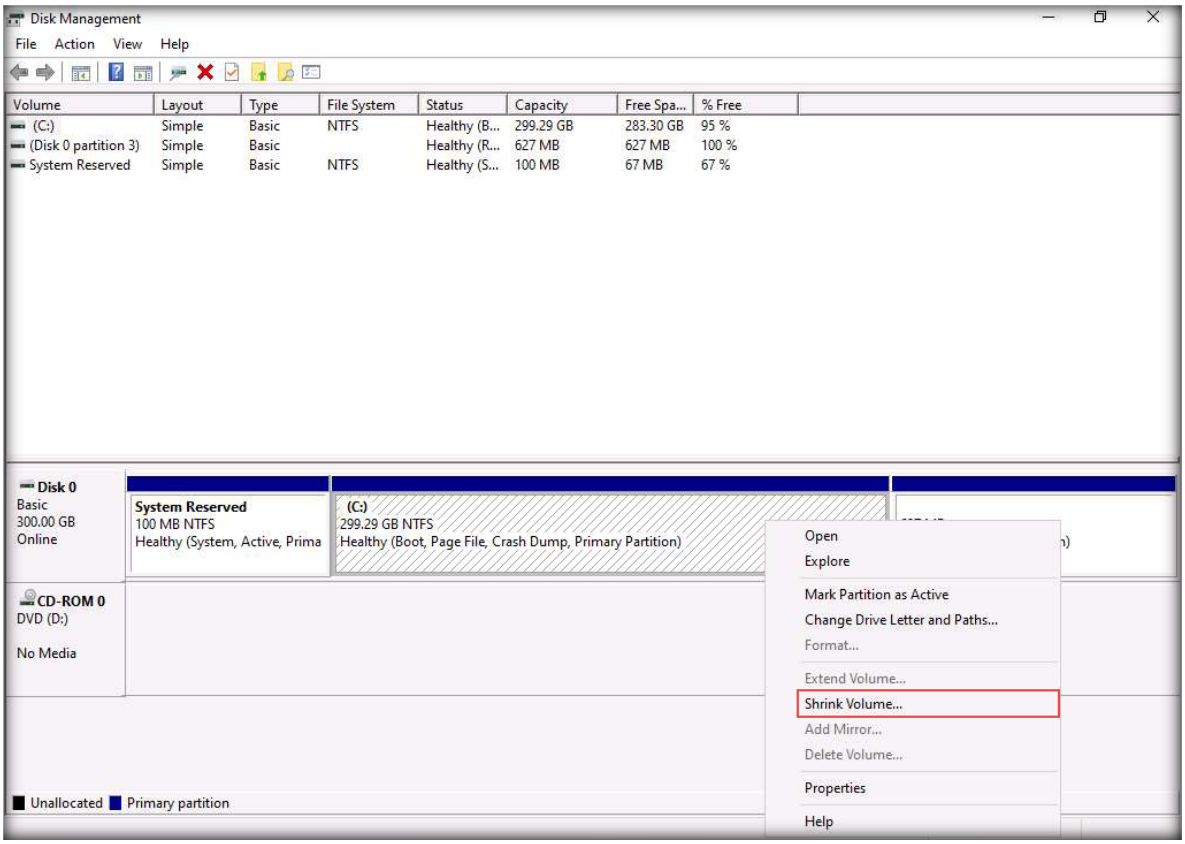
2. This will display the current disk partition, as shown in the screenshot below.

   Note: While creating the Windows Server 2022 virtual machine, we allocated a disk space of **300 GB**. Here, we will create the partitions **C:** and **E:** with a disk space of **50 GB** and **250 GB**, respectively.

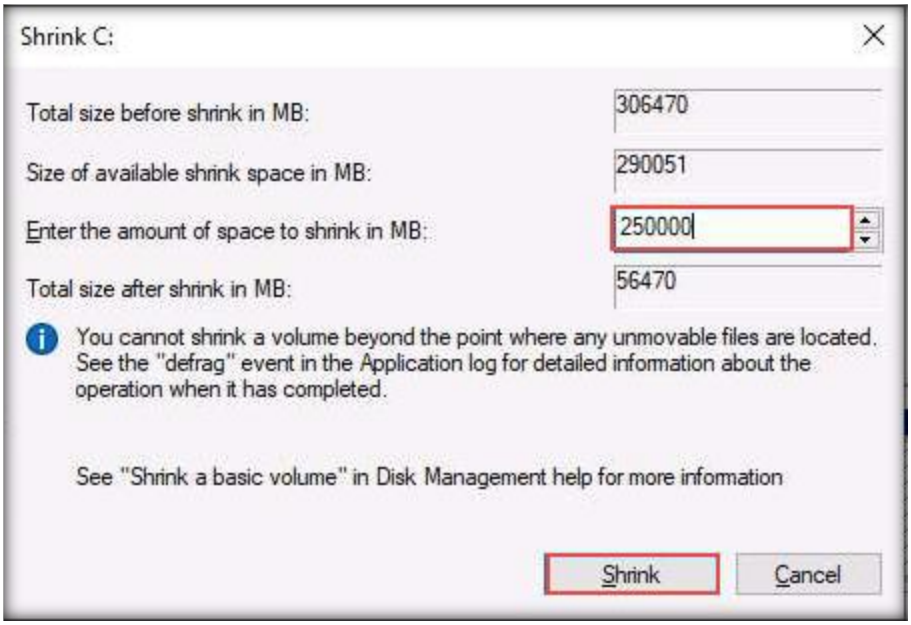


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Select the drive from the middle pane (here, **C:**). Right-click the selected drive and click **Shrink Volume...**.

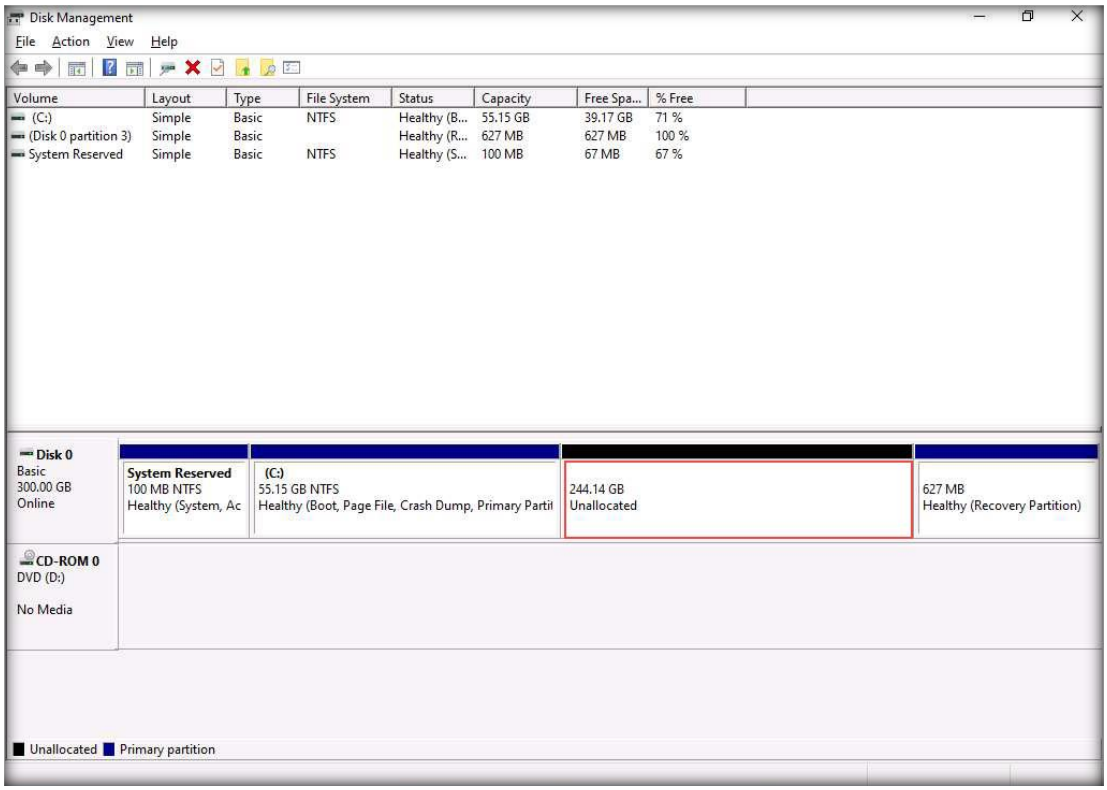


4. A **Shrink C:** window appears showing available shrink space. Enter **250000** (i.e., 250 GB) in the **Enter the amount of space to shrink in MB:** field and click **Shrink**.

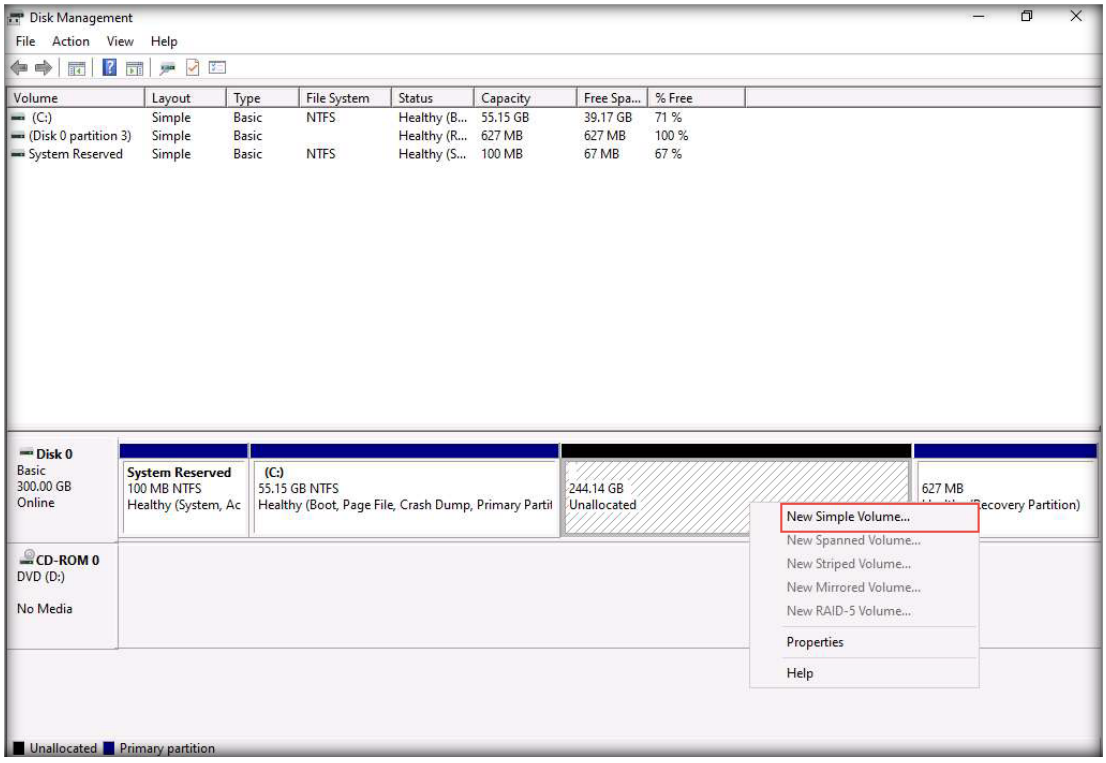


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The **Disk Management** window will display the newly created unallocated disk partition in the middle pane, as shown in the screenshot below.

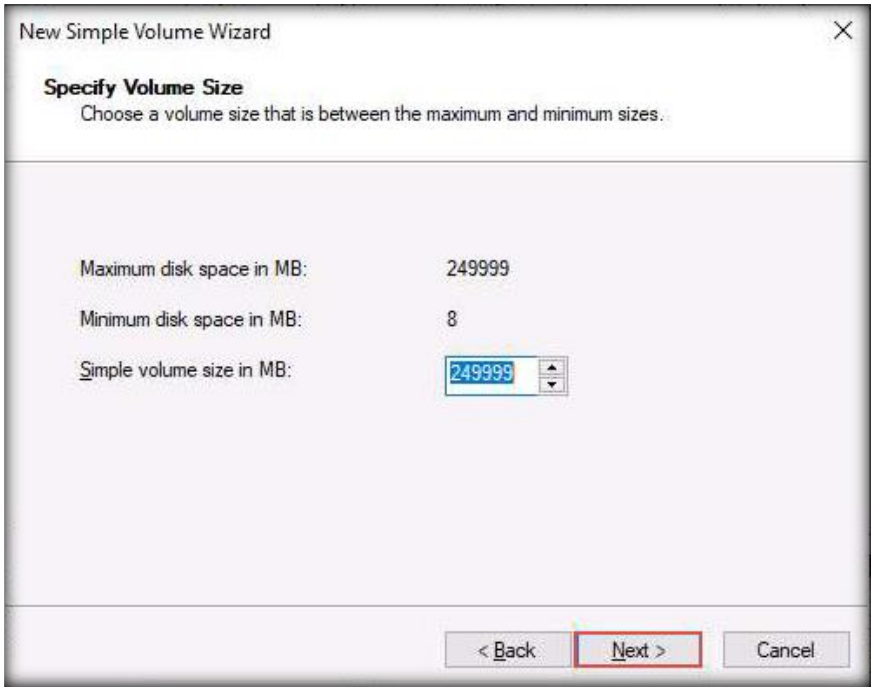


6. Select the **Unallocated** drive from the middle pane, right-click the selected drive, and click **New Simple Volume...**.



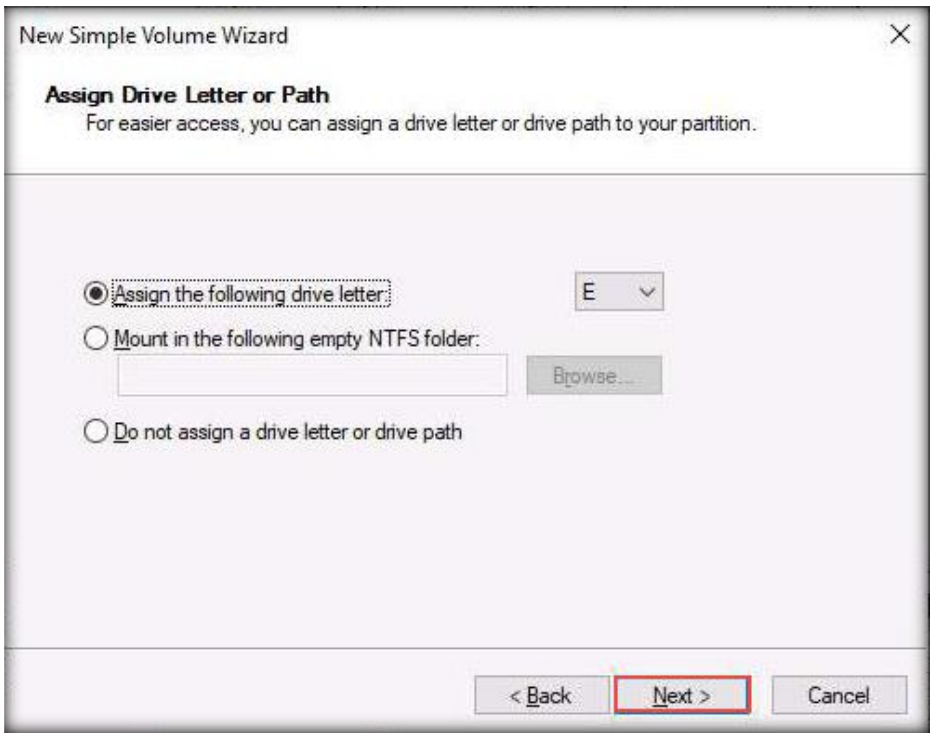
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **New Simple Volume Wizard** window appears; click **Next**.
8. In the **Specify Volume Size** wizard, leave the default settings and click **Next**.



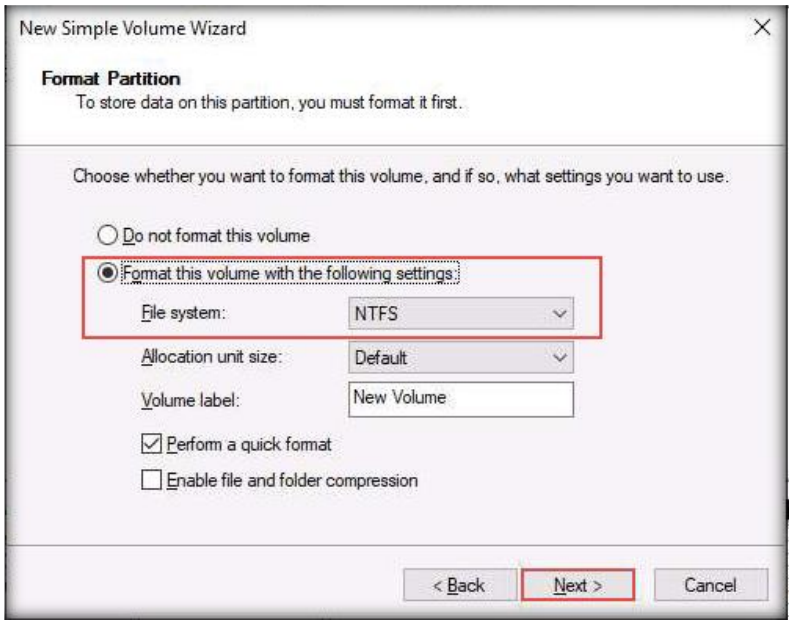
9. In the **Assign Drive Letter or Path** wizard, the **E** letter is selected by default in the **Assign the following drive letter** field; click **Next**.

   Note: If a letter other than **E** is selected in the **Assign the following drive letter** field, click on the drop-down menu and select **E**.

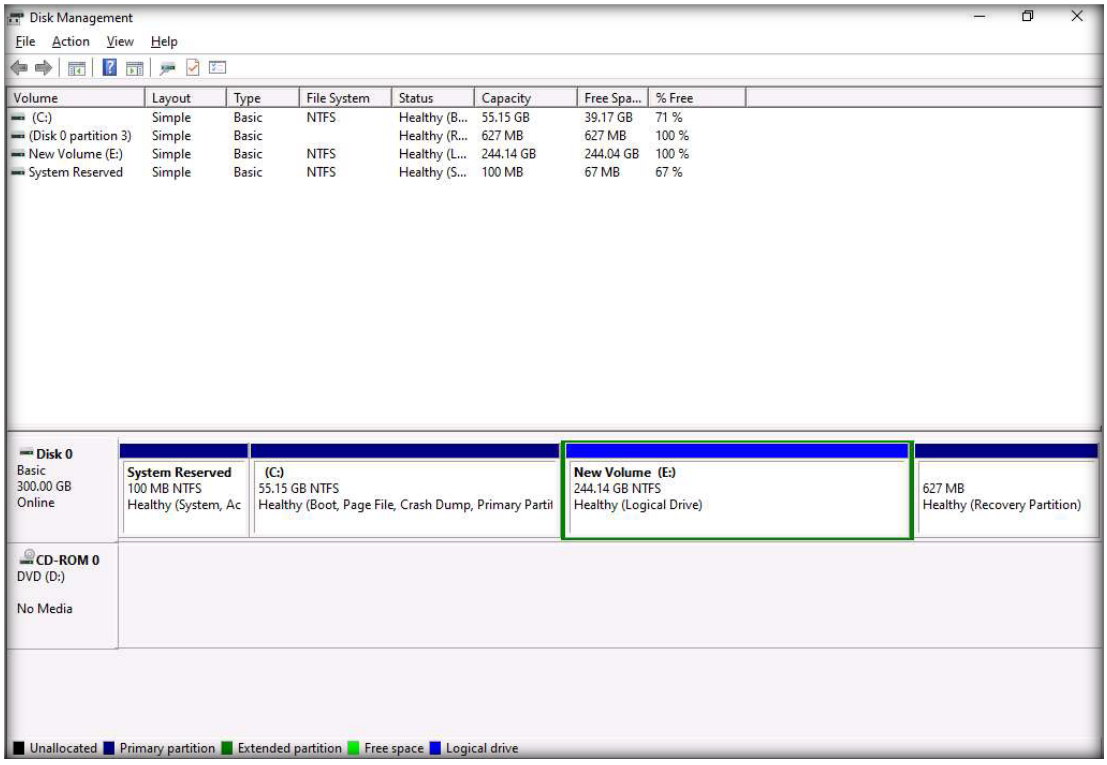


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. In the **Format Partition** wizard, **NTFS** is the file system selected by default to format the volume; click **Next**.



11. In the next wizard, click **Finish**.
12. The **Computer Management** window displays the newly created disk partition in the middle pane, as shown in the screenshot below.



13. Close all windows and restart the **Windows Server 2022** virtual machine.

[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#16: Download CHFI Tools on the Windows Server 2022 Virtual Machine

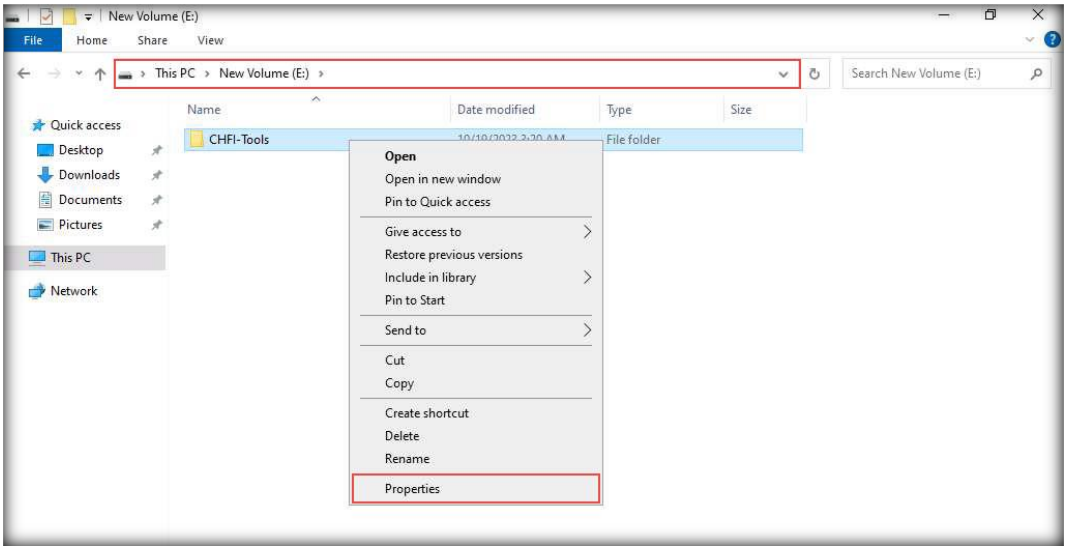
1. Log in to the **Windows Server 2022** virtual machine with the credentials **Administrator** and **Pa$$w0rd**.
2. Create a folder on drive **E:** named **CHFI-Tools**.
3. Log in to your **Aspen** account (you will see your course listed under **My Courses**). Click the **TRAINING** button under the course to access the e-Courseware, Lab Manuals, and tools in the **Training** area. → Click the **Download Tools** tab in the left-hand pane.
4. Click the module names in the right-hand pane (except **CHFIv11 ISO.zip**) and download all the **CHFI Tools** files to the **E:\CHFI-Tools** folder.
5. Right-click the .zip files in the **E:\CHFI-Tools** folder and select the **Extract Here** option.

[Back to Configuration Task Outline]

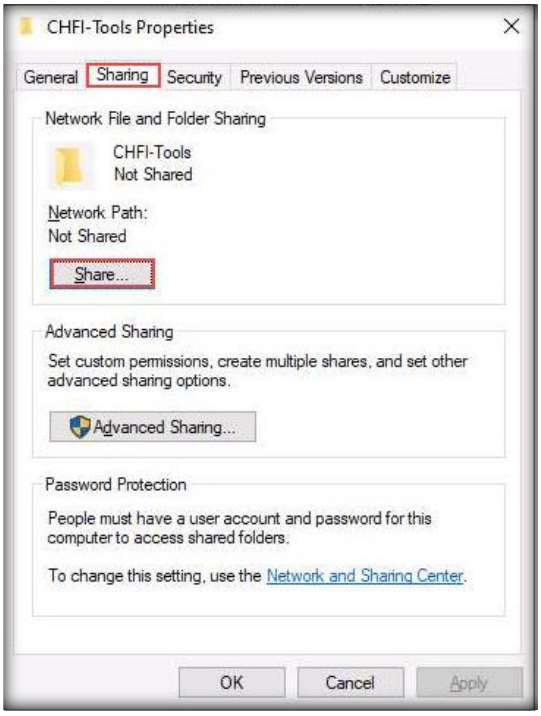
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#17: Share and Map the CHFI-Tools Folder to the Windows Virtual Machines

1. Log in to the **Windows Server 2022** virtual machine with the credentials **Administrator** and **Pa$$w0rd**.
2. Open a **File Explorer** window, navigate to the **E:** drive, right-click on the **CHFI-Tools** folder, and select **Properties** from the context menu.

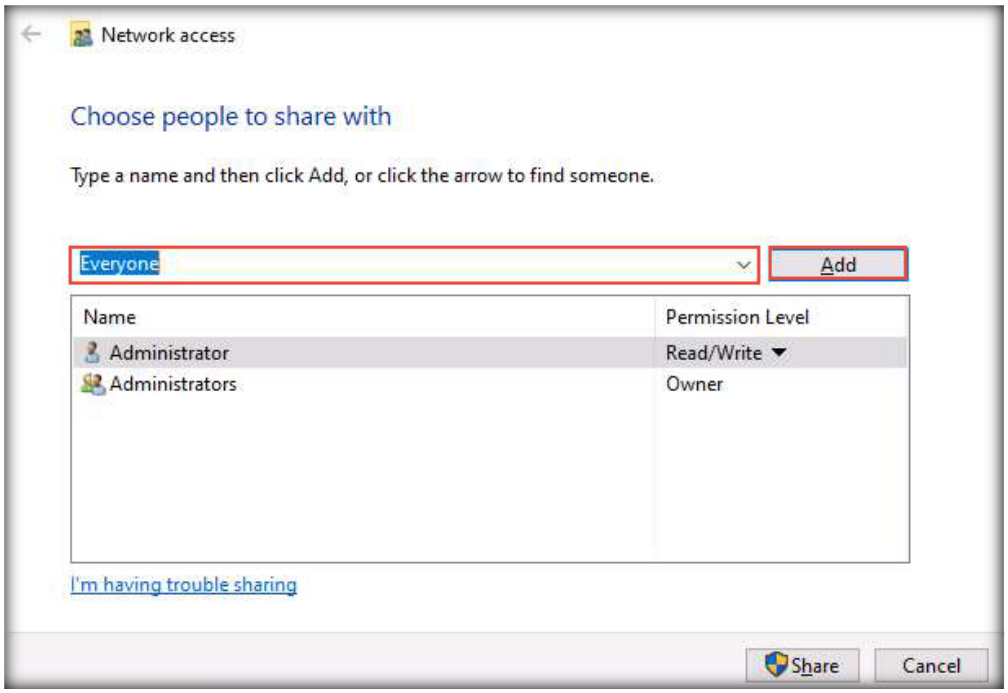


3. Select the **Sharing** tab from the **CHFI-Tools Properties** window to modify and display the current shared folder settings.
4. Click the **Share...** button to access the **File Sharing** options.

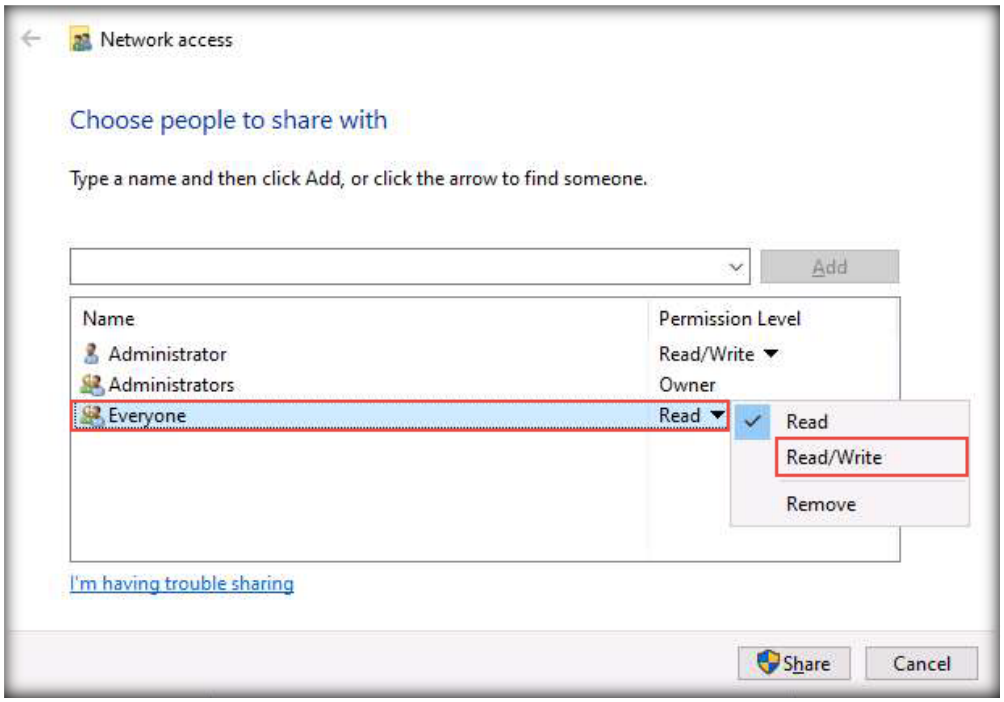


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. In the **File Sharing** wizard, select **Everyone** from the drop-down list and click **Add**.

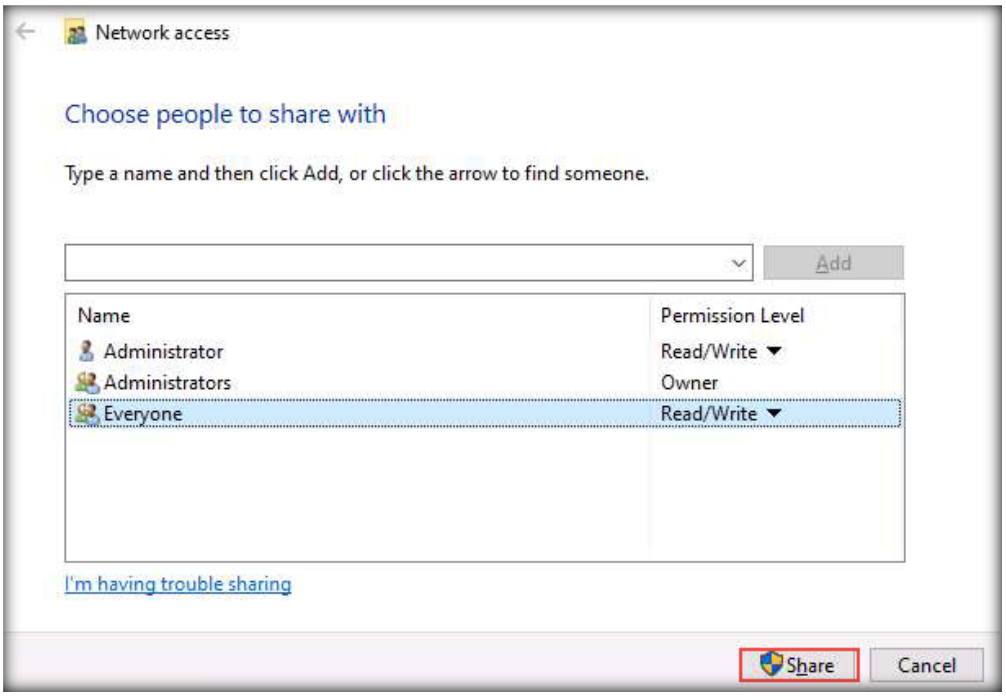


6. For the newly added users (**Everyone**), click the **Read** drop-down menu and click **Read/Write**.



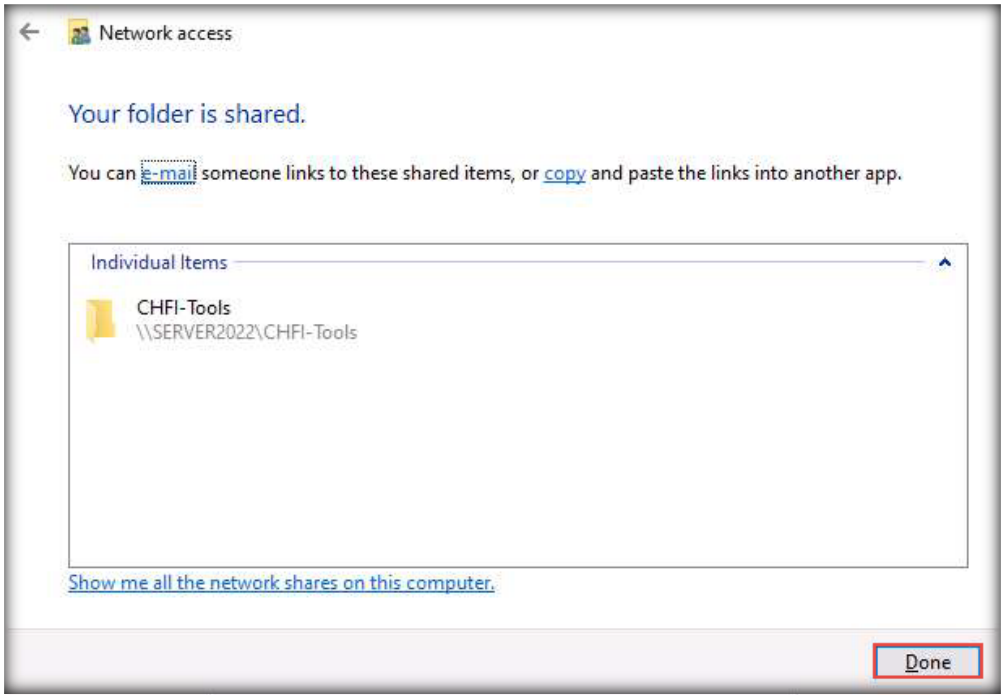
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Click **Share** to begin sharing with the added users.



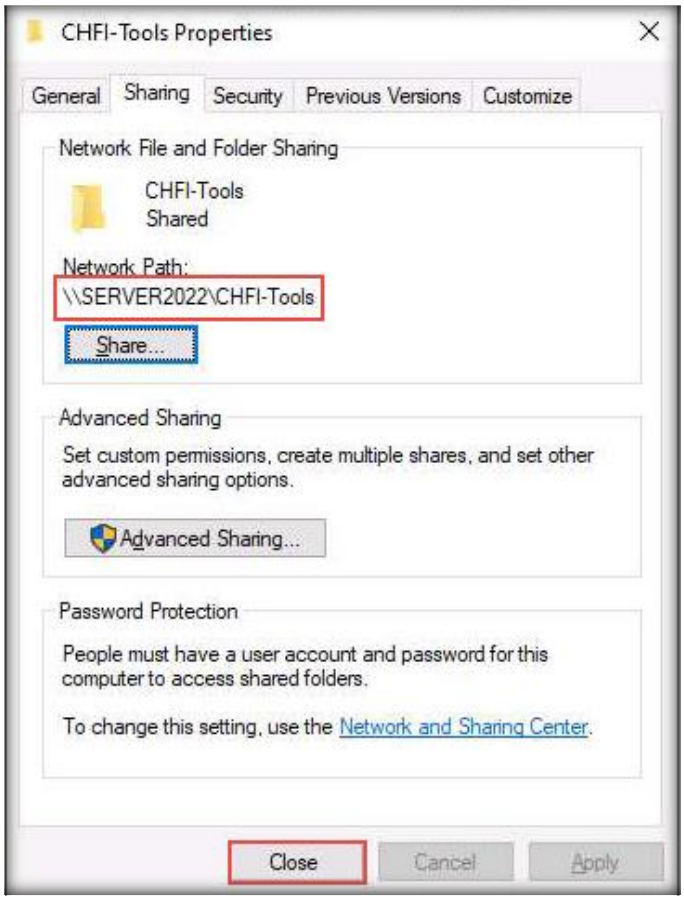
8. Click **Done** on the confirmation page of the **File Sharing** wizard.

   Note: If the **Do you want to change the settings for these items?** window appears, click **Change Settings**.

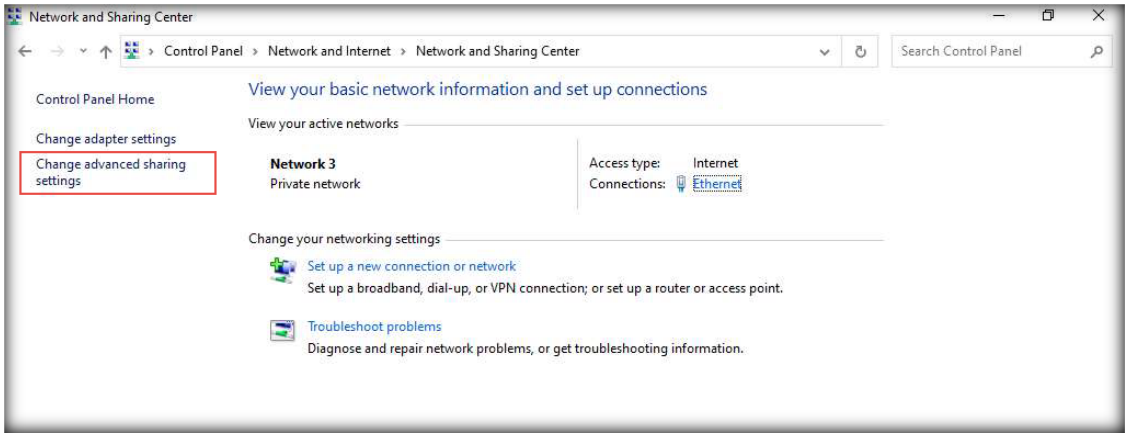


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Close the **CHFI-Tools Properties** window.

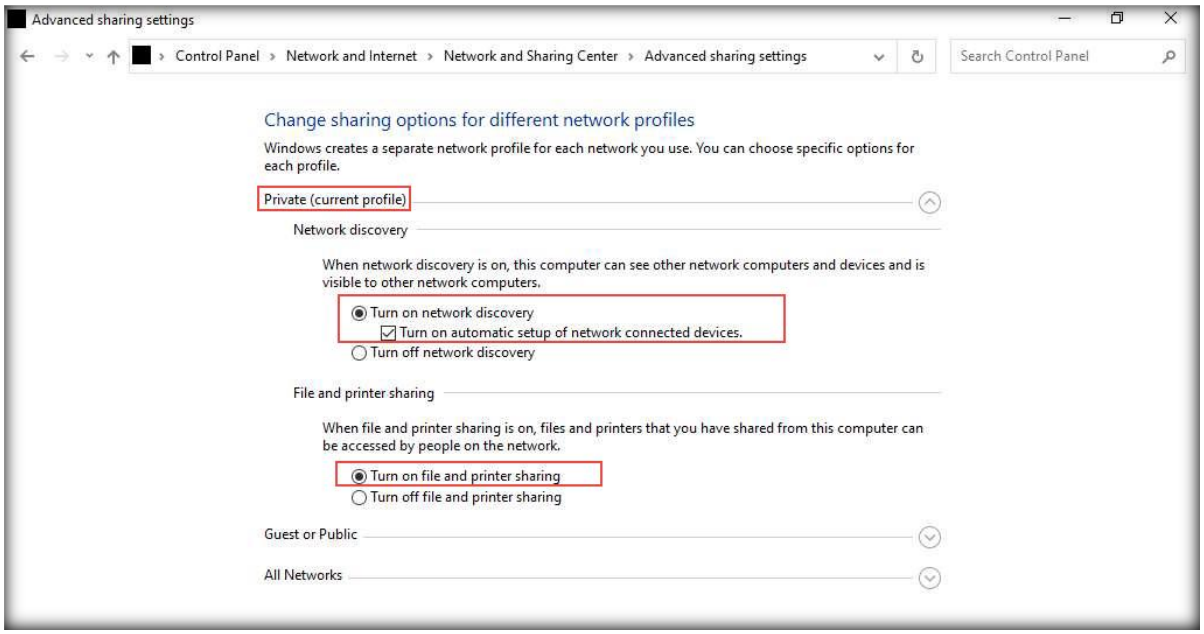


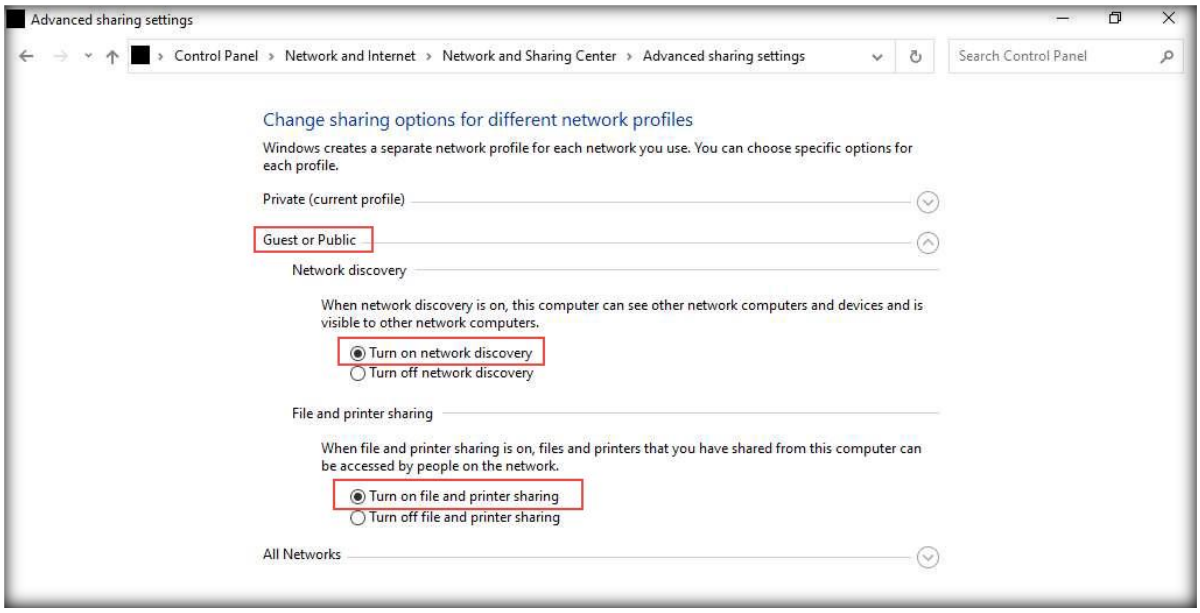
10. Open **Network and Sharing Center** by navigating to **Control Panel** → **Network and Internet** → **Network and Sharing Center**.
11. In the **Network and Sharing Center** window, click the **Change advanced sharing settings** link in the left pane.



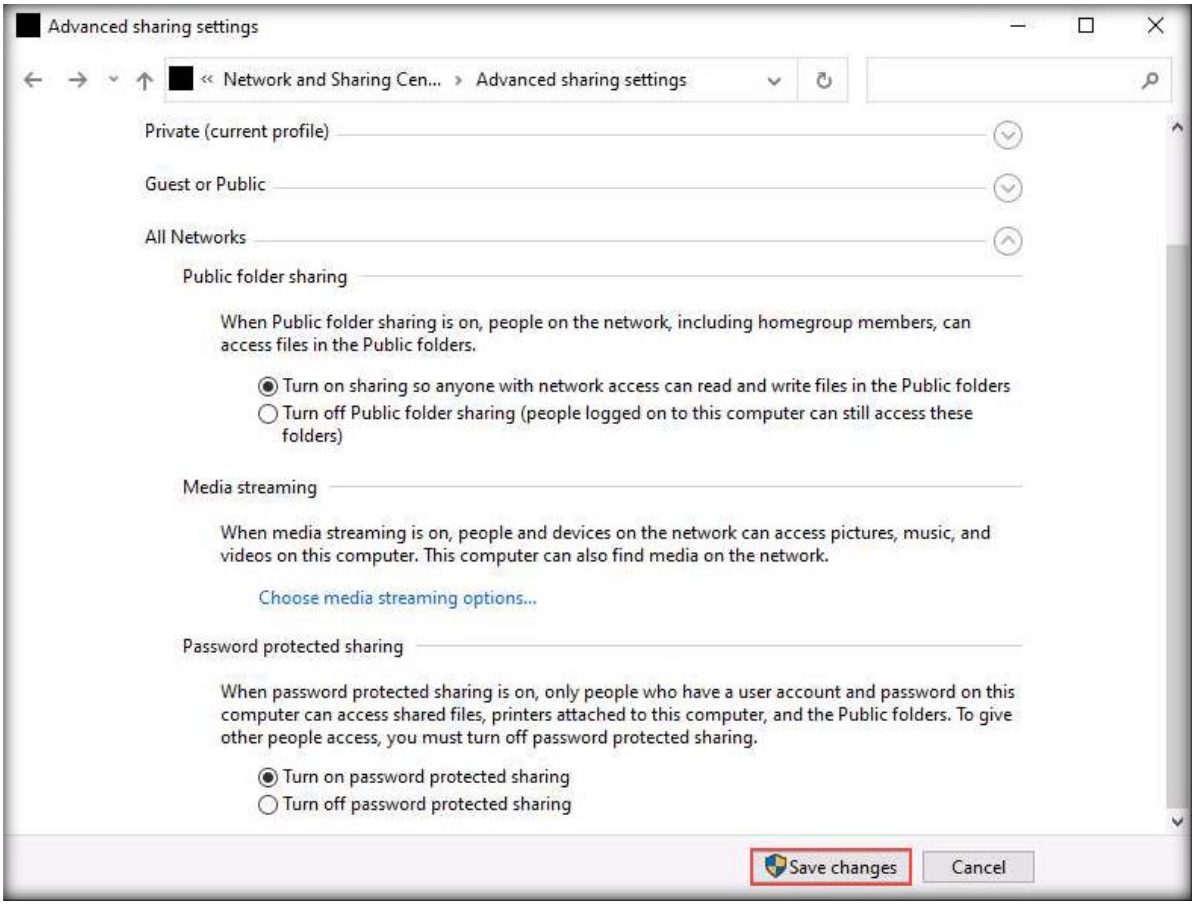
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. In the **Advanced sharing settings** window, turn on network discovery as well as file and printer sharing under **Private (current profile)**, **Guest or Public**, and **All Networks**, as shown in the screenshots below, and click **Save changes**.





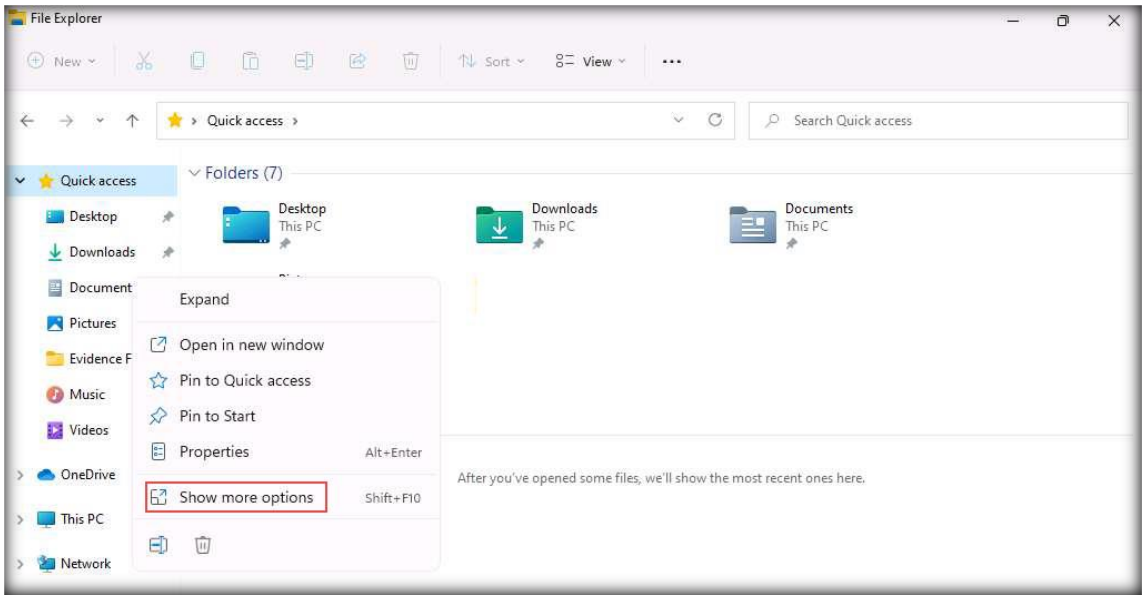
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



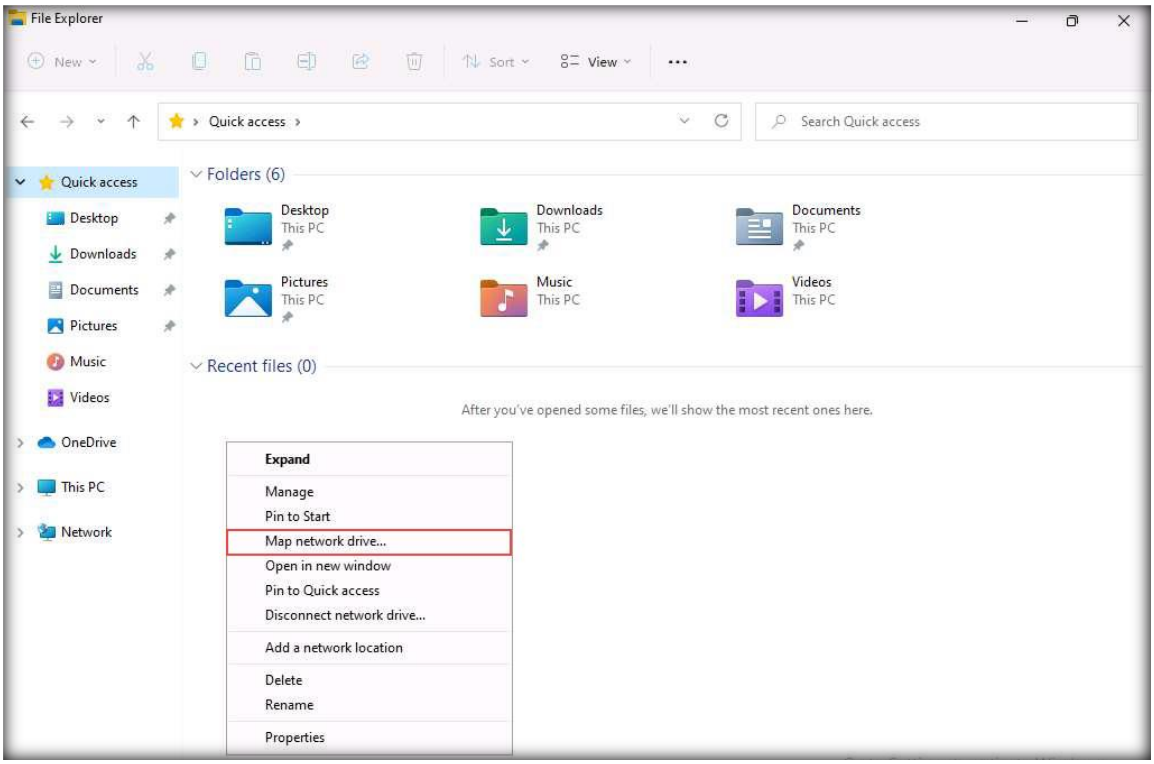
13. Close the **Network and Sharing Center** window.
14. Log in to the **Windows 11** virtual machine with the credentials **Admin** and **Pa$$w0rd**.
15. Open the **Network and Sharing Center** and click the **Change advanced sharing settings** link in the left pane.
16. In the **Advanced sharing settings** window, turn on network discovery as well as file and printer sharing under **Private**, **Guest or Public (current profile)**, and **All Networks**. Then, click **Save changes**.

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Open the **File Explorer** window, right-click **This PC** in the left-hand pane, and click **Show more options**.

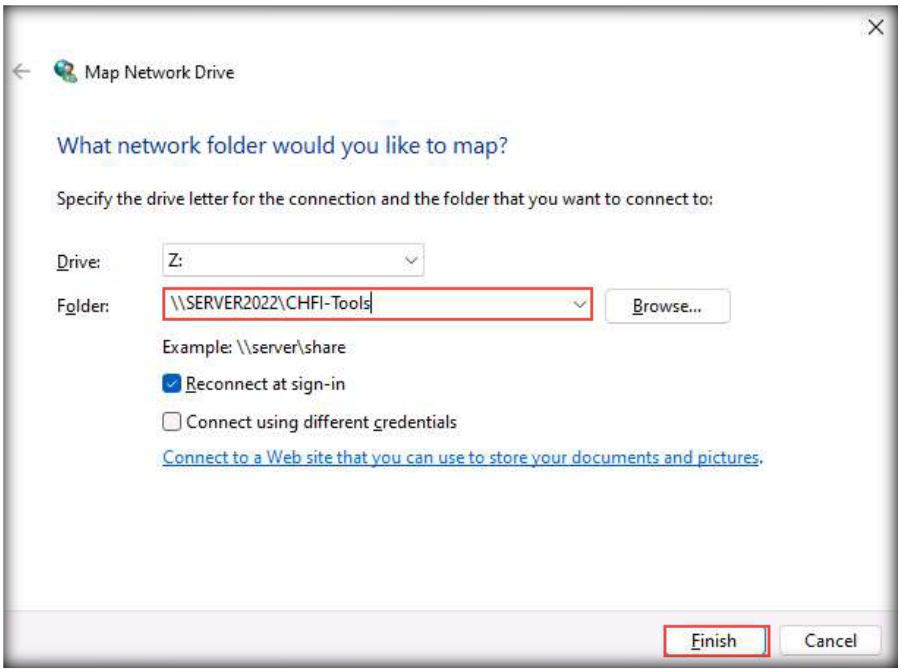


18. From the options, click **Map network drive...**.

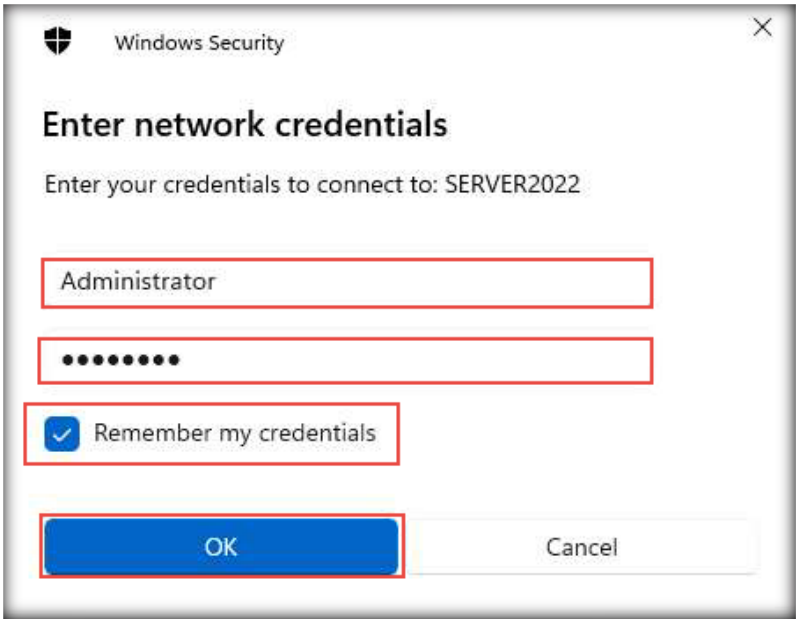


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

19. In the **Map Network Drive** window, specify the **Drive** letter as **Z:**. In the **Folder** field, enter **\\SERVER2022\CHFI-Tools**. Click **Finish**.

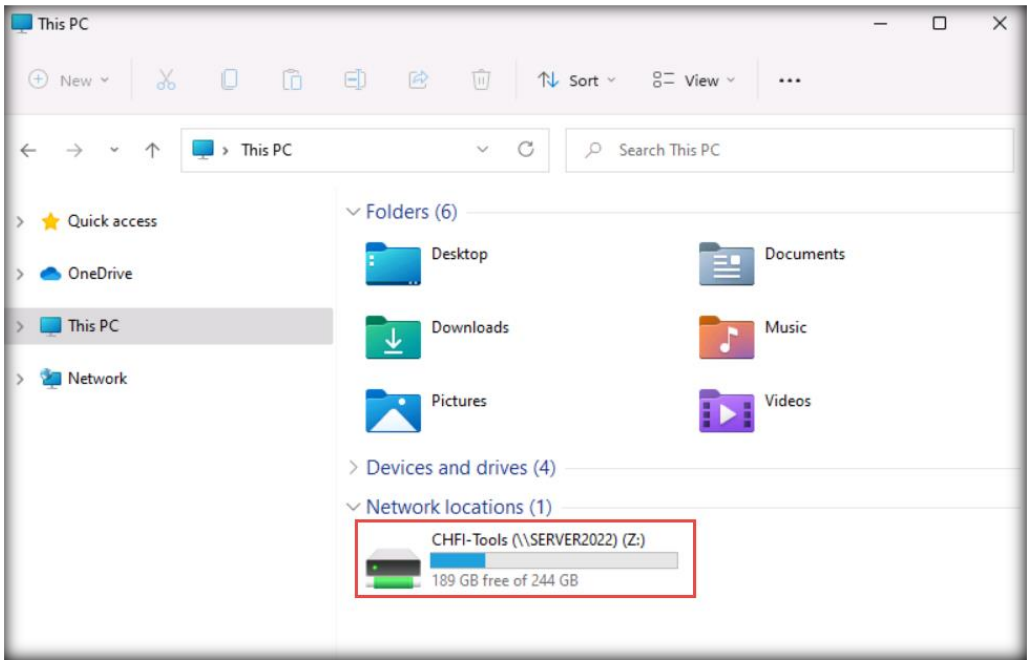


20. The **Enter network credentials** pop-up window appears; enter the credentials of the Windows Server 2022 virtual machine (**Administrator** and **Pa$$w0rd**). Check the **Remember my credentials** checkbox and click **OK**.

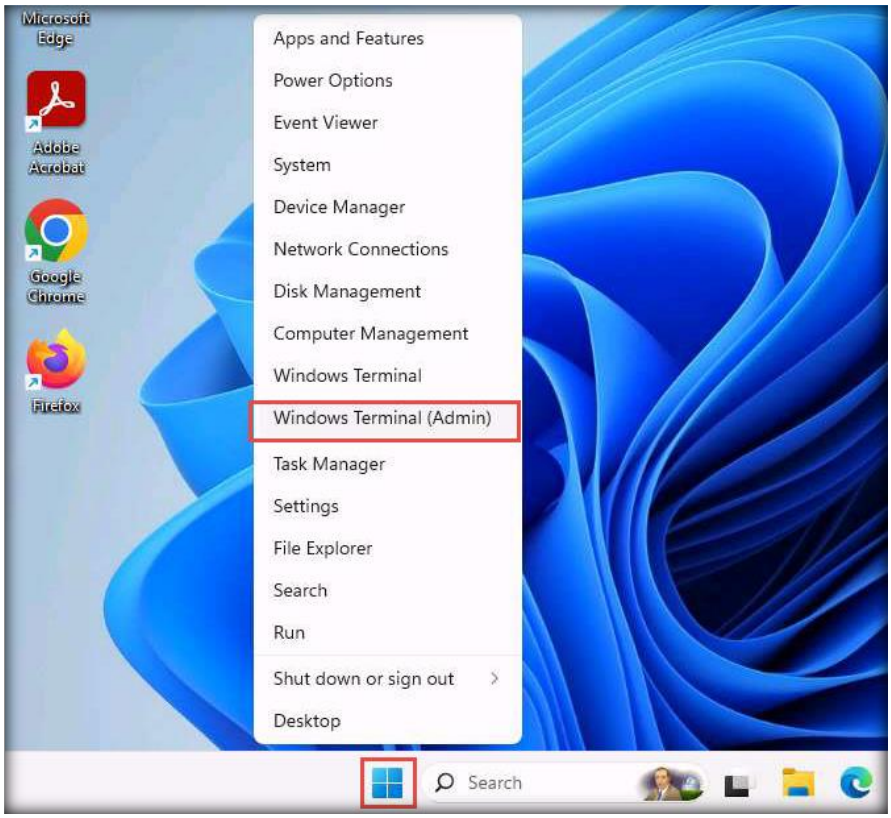


Computer Hacking Forensic Investigator Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Now, the **Shared Folder** can be viewed in **Windows Explorer**.



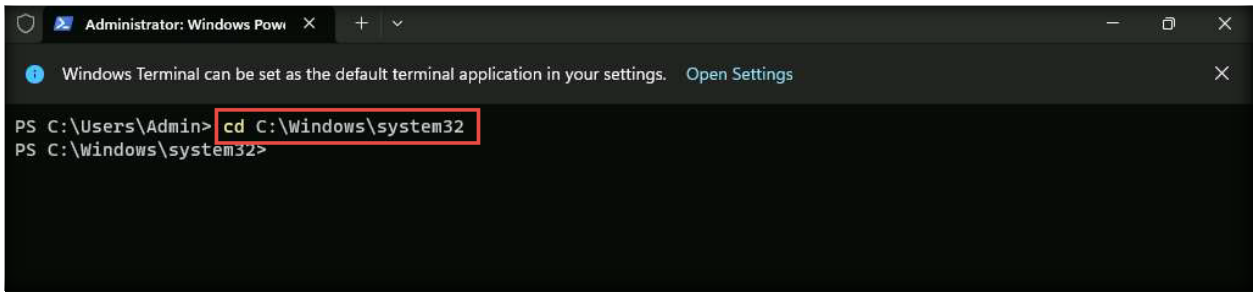
22. We shall attach alternate data stream files to two text files using Windows PowerShell. To launch Windows PowerShell as Administrator, right-click on the **Windows** icon and select **Windows Terminal (Admin)**.



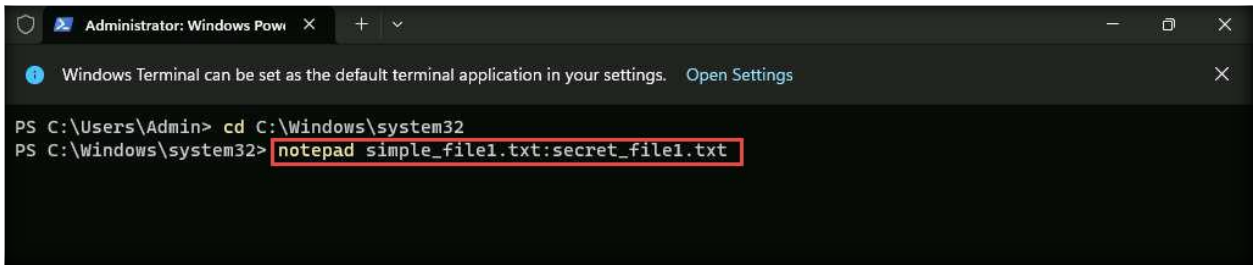
Note: If a **User Account Control** pop-up appears, click **Yes**

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Navigate to **C:\Windows\system32 location**.

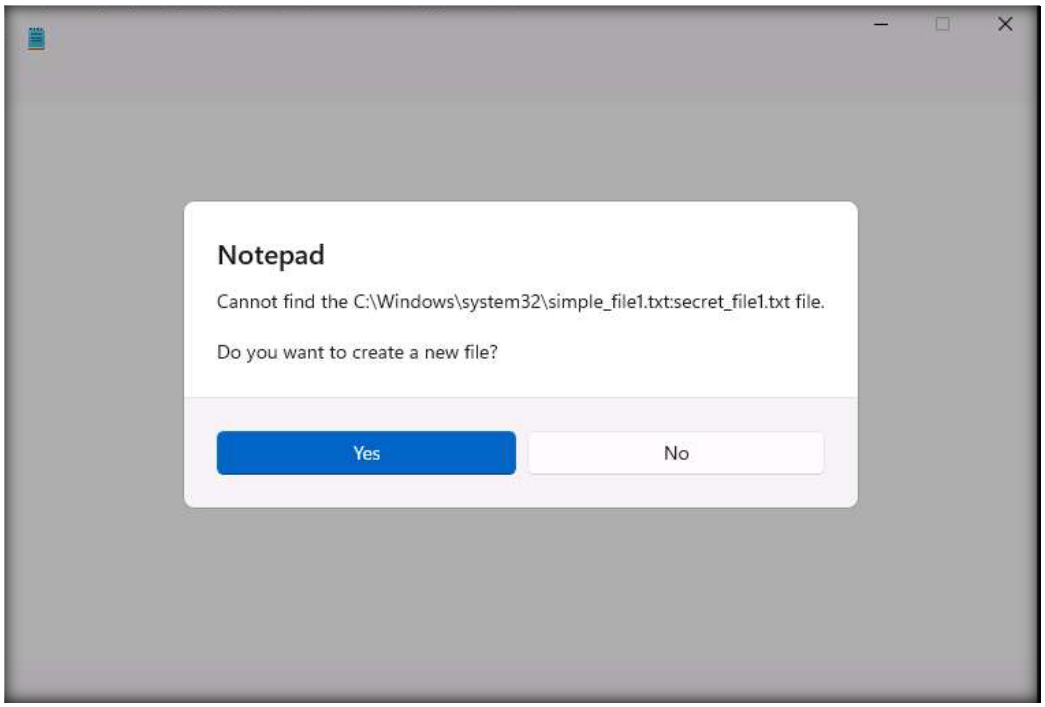


24. Our next task is to attach a stream named **secret_file1.txt** to a text file **simple_file1.txt**



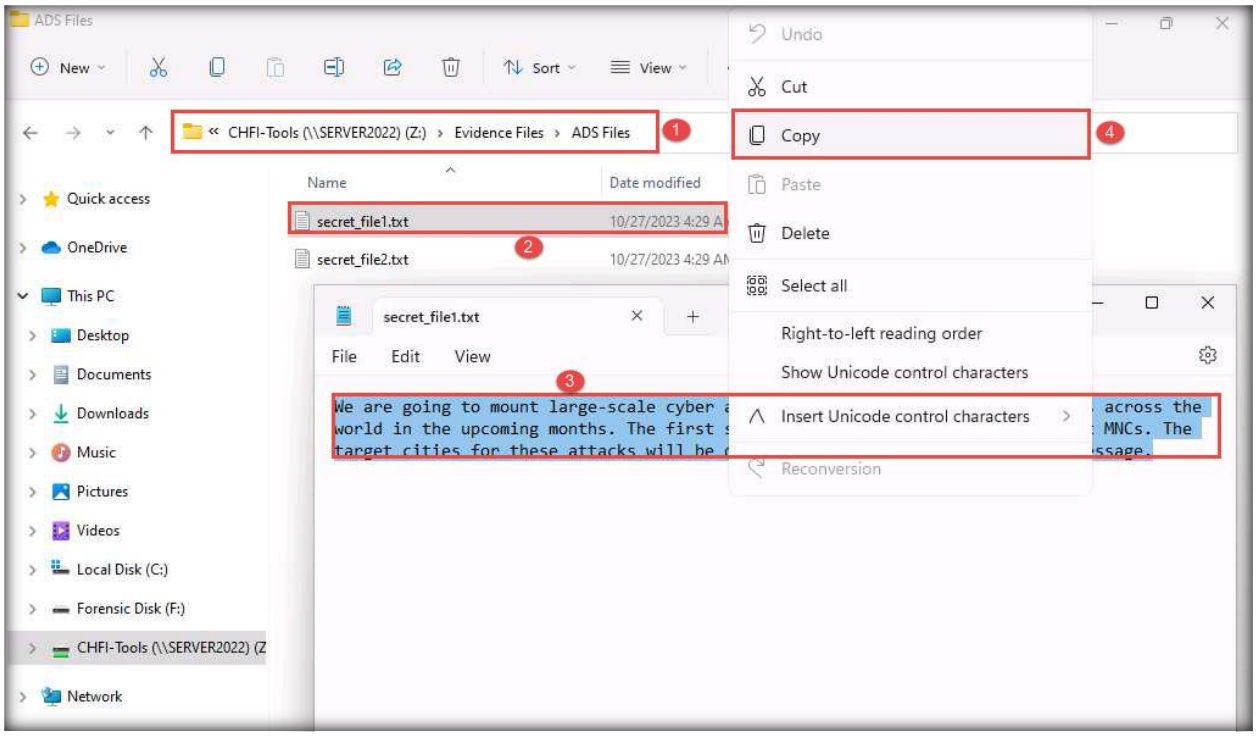
25. By issuing this command, we are creating a text file named **simple_file1.txt** and attaching it to a stream named **secret.file1.txt.**

26. A **Notepad** pop-up will appear; click **Yes** to create the new file

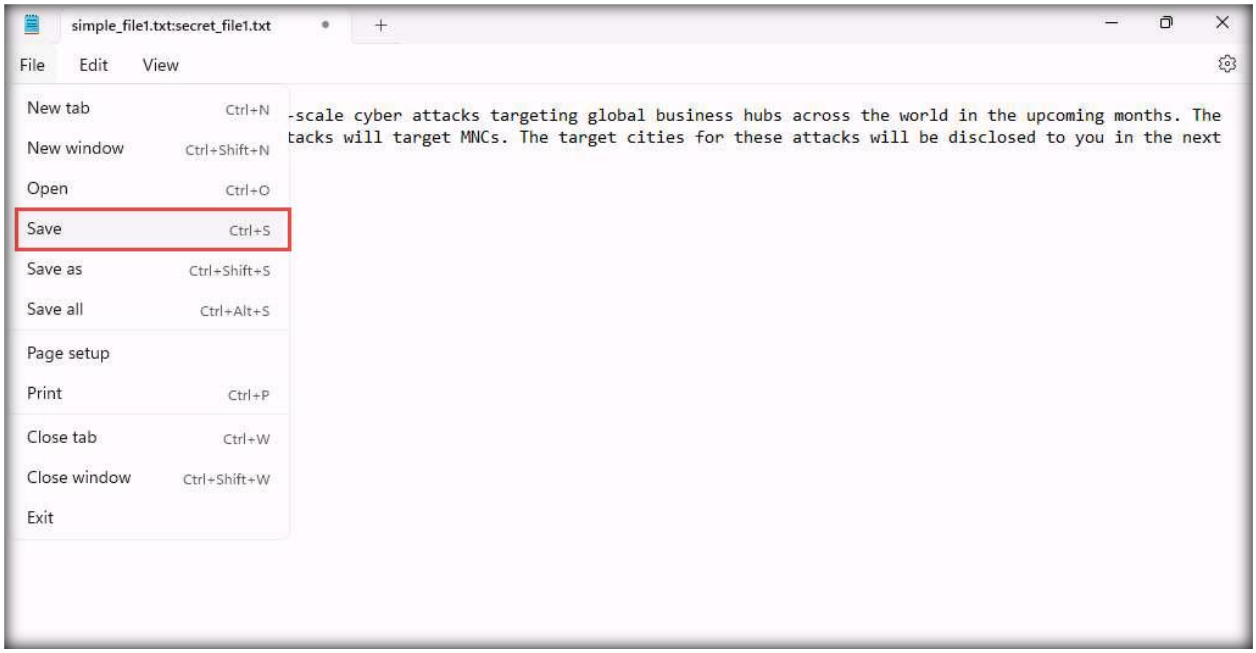


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. An empty stream file will appear; navigate to **Z:\ Evidence Files\ADS Files**, open the text file **secret_file1.txt**, and copy its contents.



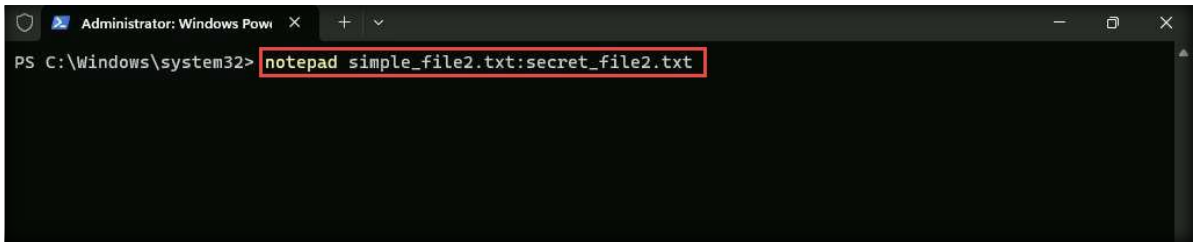
28. Switch back to the stream file, **paste** the copied contents, and **save** the file.



29. Now, this data is stored in the stream file, while the **simple_file1.txt** file looks empty. Close both the stream file and the **secret_file1.txt** file opened from the **ADS Files** folder.

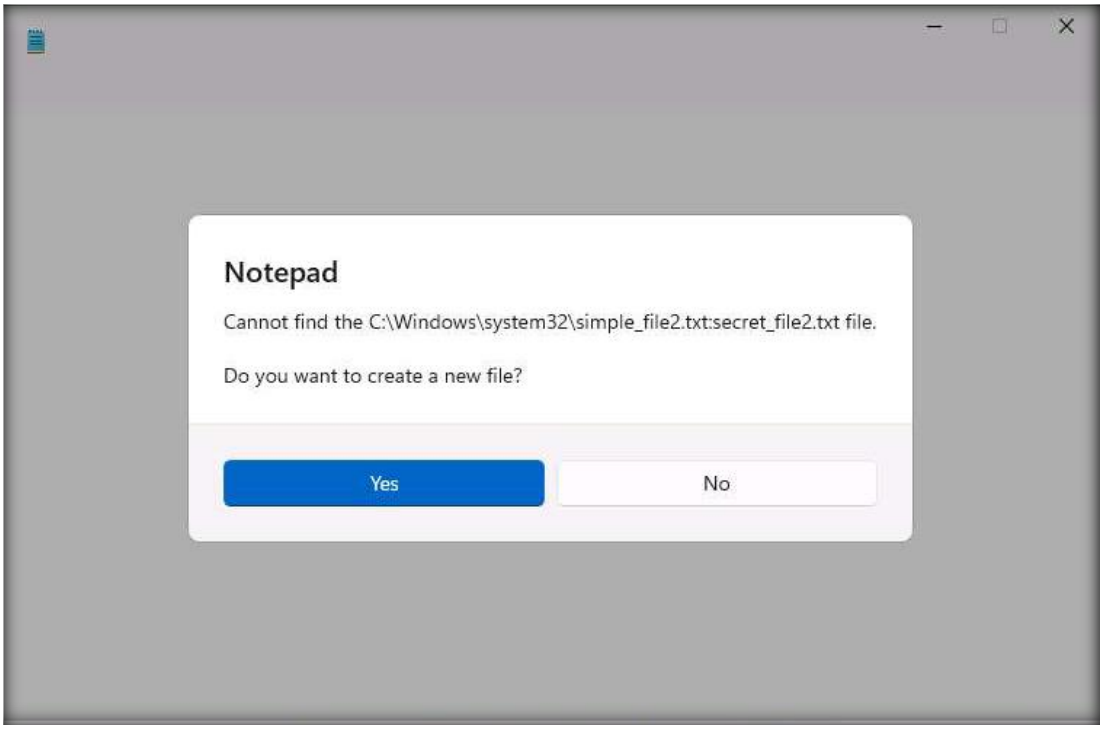
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

30. Our next task is to attach a stream named **secret_file2.txt** to a text file **simple_file2.txt.**



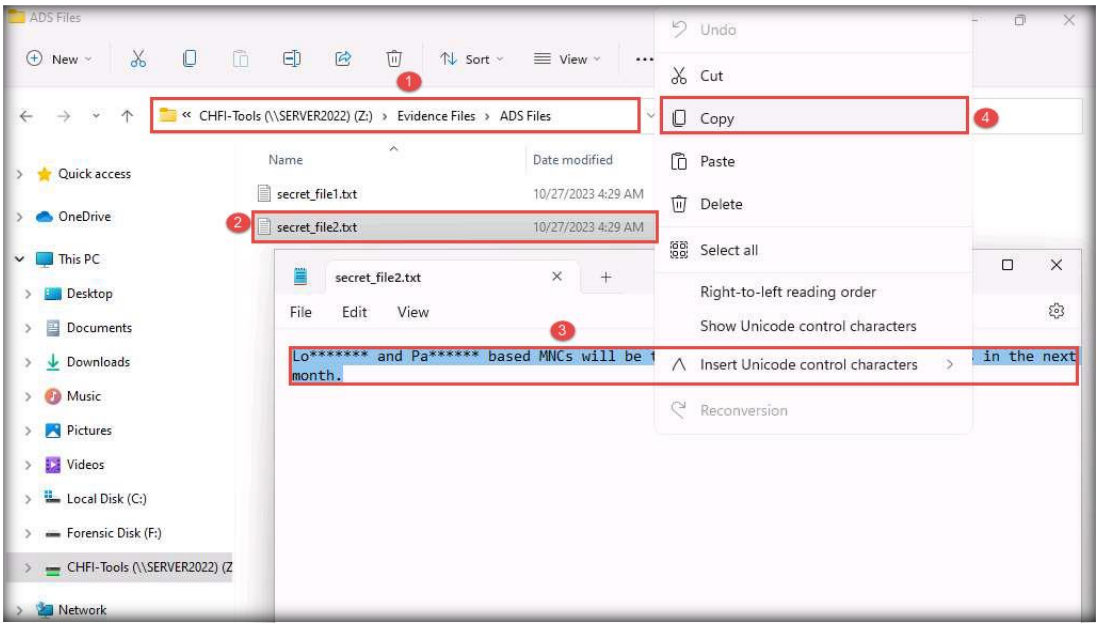
31. By issuing this command, we are creating a text file named **simple_file2.txt** and attaching it to a stream named **secret.file2.txt.**

32. A **Notepad** pop-up will appear; click **Yes** to create the new file.

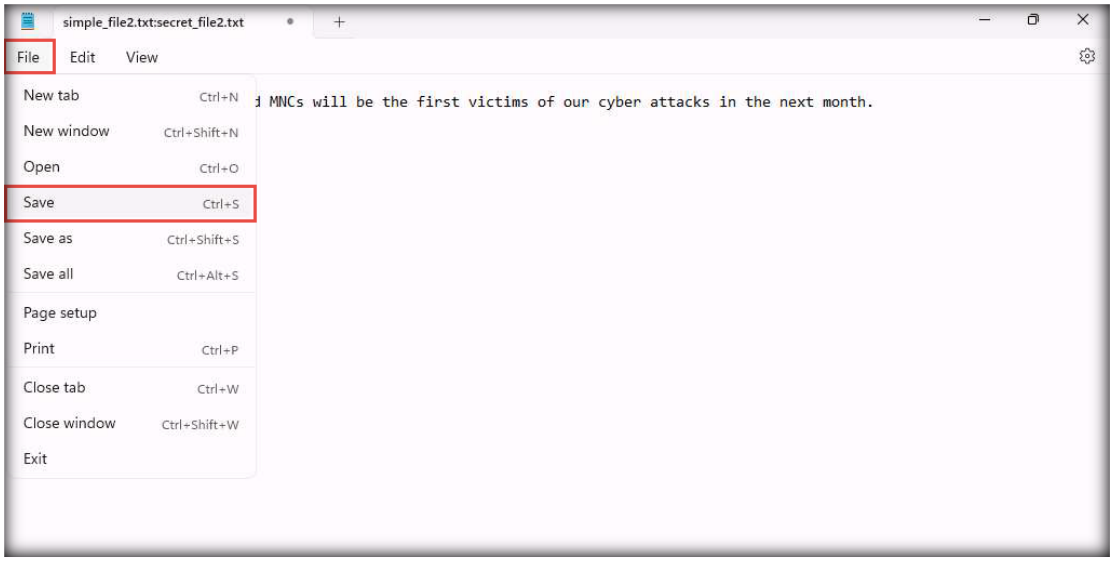


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

33. An empty stream file will appear; navigate to **Z:\ Evidence Files\ADS Files**, open the text file **secret_file2.txt**, and copy its contents.



34. Switch back to the stream file, **paste** its contents and **save** the file.

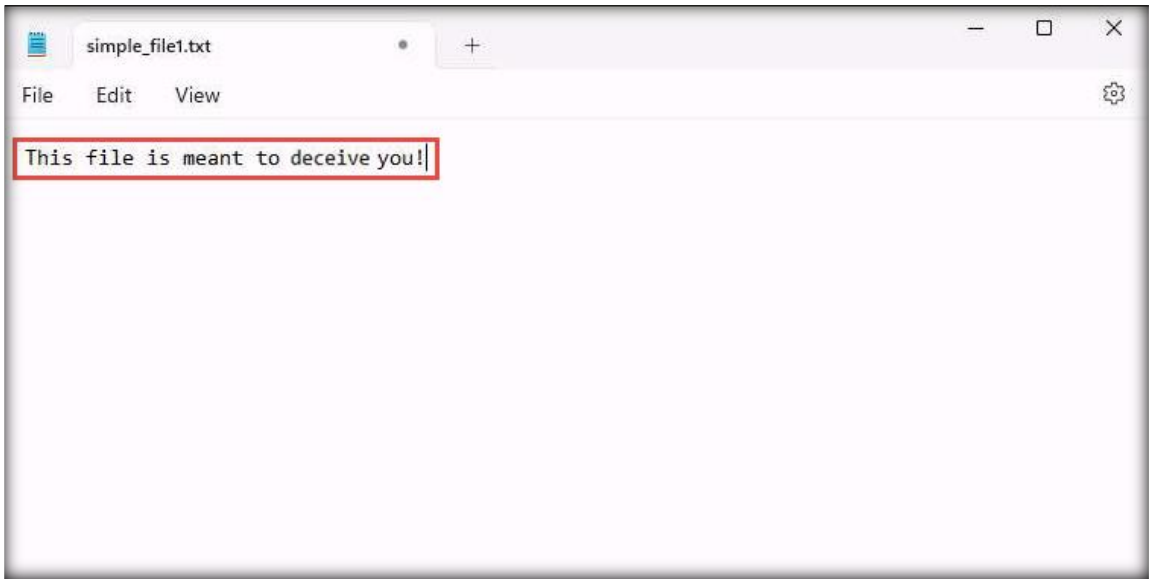


35. Now, this data is stored in the stream file, while the **simple_file2.txt** file looks empty. Close the stream file and the **secret_file2.txt** file opened from the **ADS Files** folder.

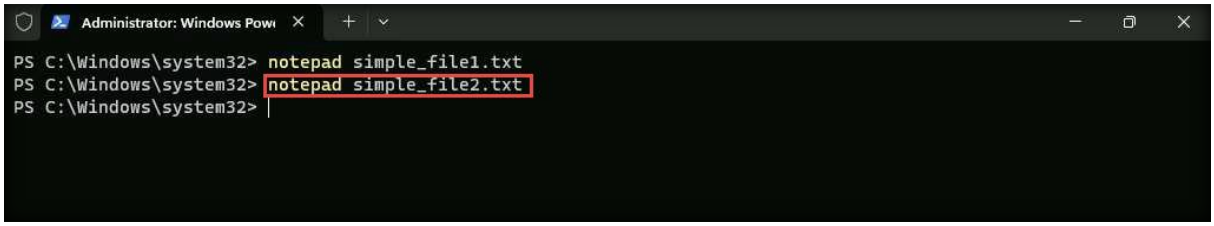
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

36. We shall now write some text in **simple_file1.txt** and **simple_file2.txt** files and save them. To edit the text file **simple_file1.txt**, type the command notepad **simple_file1.txt** in Windows PowerShell and press **Enter**.

37. **simple_file1.txt** will open in **Notepad**; write some text in it. In this context, the text written is "**This file is meant to deceive you!**" Save the file and close it.

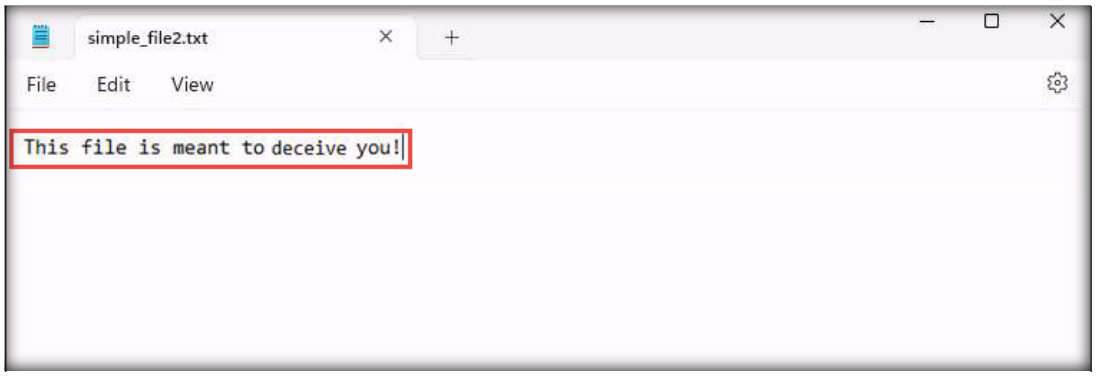


38. We shall now edit the text file **simple_file2.txt**. To edit, type the command notepad **simple_file2.txt** in Windows PowerShell and press **Enter**.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

39. **simple_file2.txt** will open in Notepad; write some text in it. In this context, the text written is, "**This file is meant to deceive you!**" Save the file and close it.



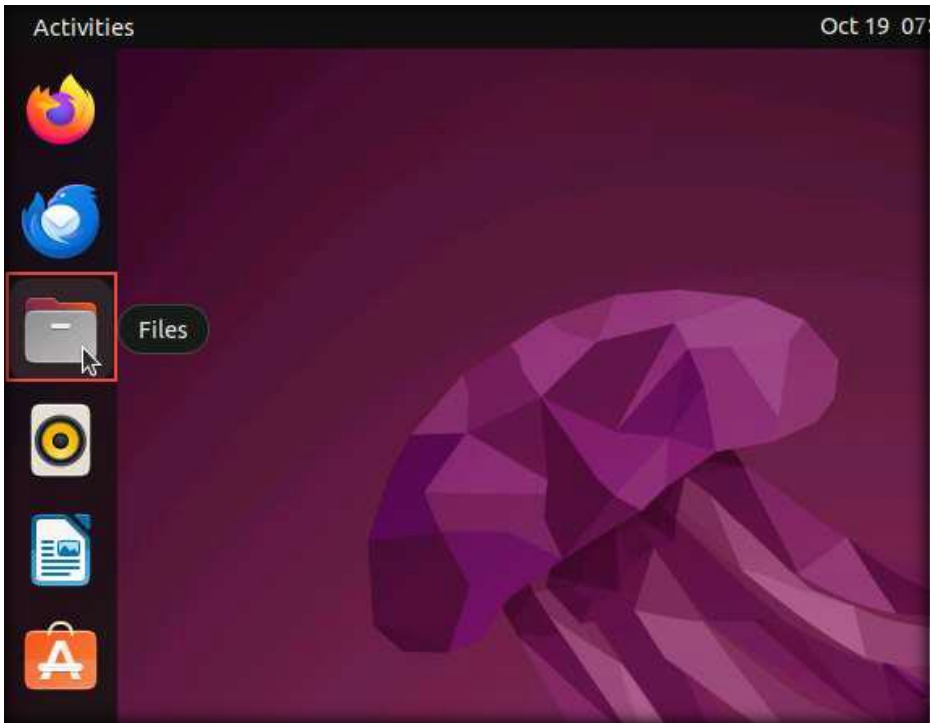
40. You will understand how to recover the deleted files and how to recover data from the hidden streams (from the above text files) in the lab exercises
41. Shut down the virtual machine.

[Back to Configuration Task Outline]

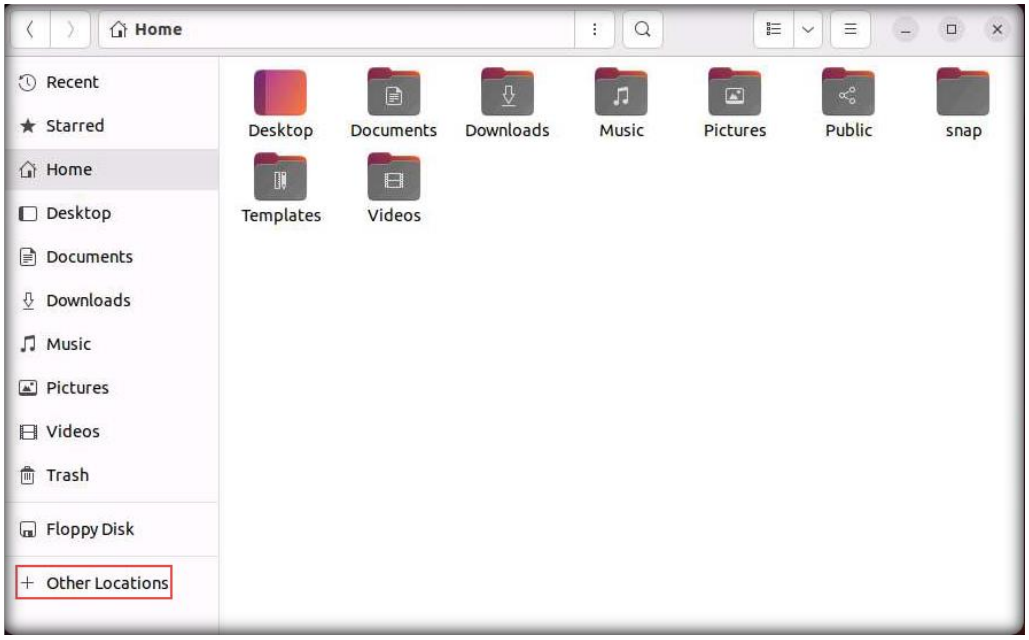
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#18: Share and Map the CHFI-Tools Folder to the Ubuntu Virtual Machines

1. In the **Ubuntu Suspect** machine, click the **Files** icon in the Launcher panel to launch the **File Manager**.

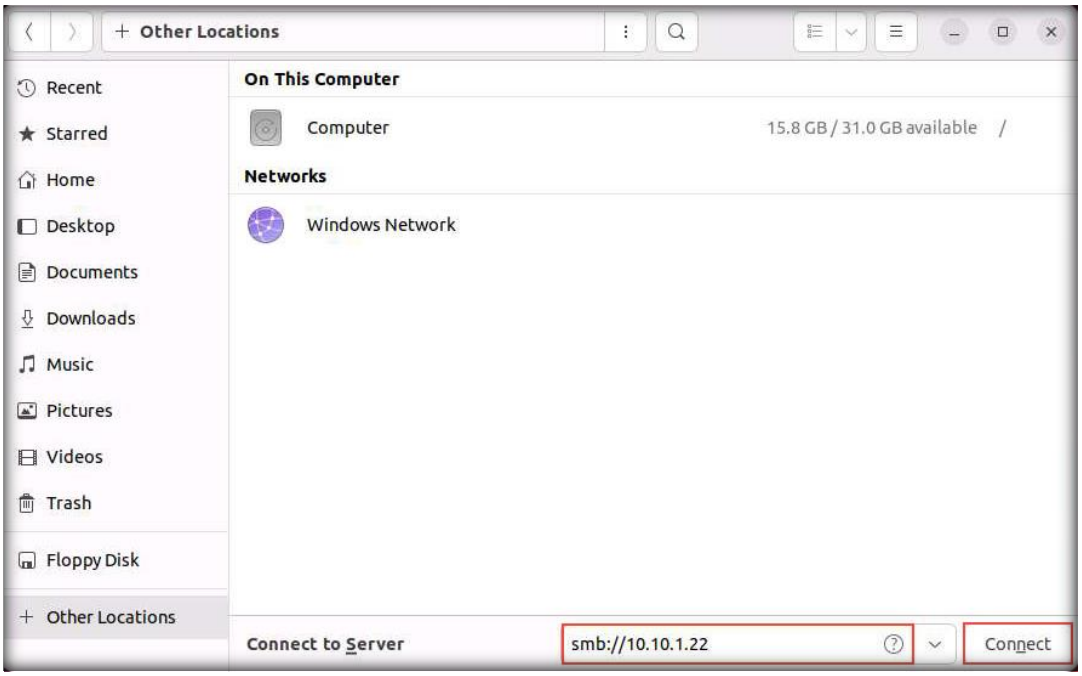


2. A file manager window will appear, pointing to the **Home** directory. Click on **+ Other Locations**.

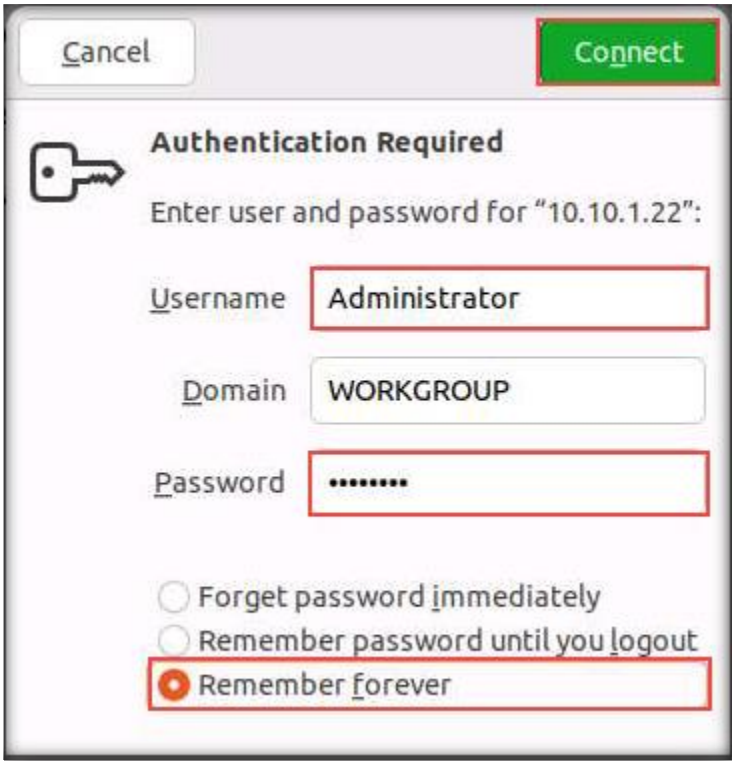


Computer Hacking Forensic Investigator Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. In the **Connect to Server** field, type **smb://10.10.1.22** and click **Connect**. Here, we are accessing the **CHFI-Tools** folder that is located in **Windows Server 2022**.

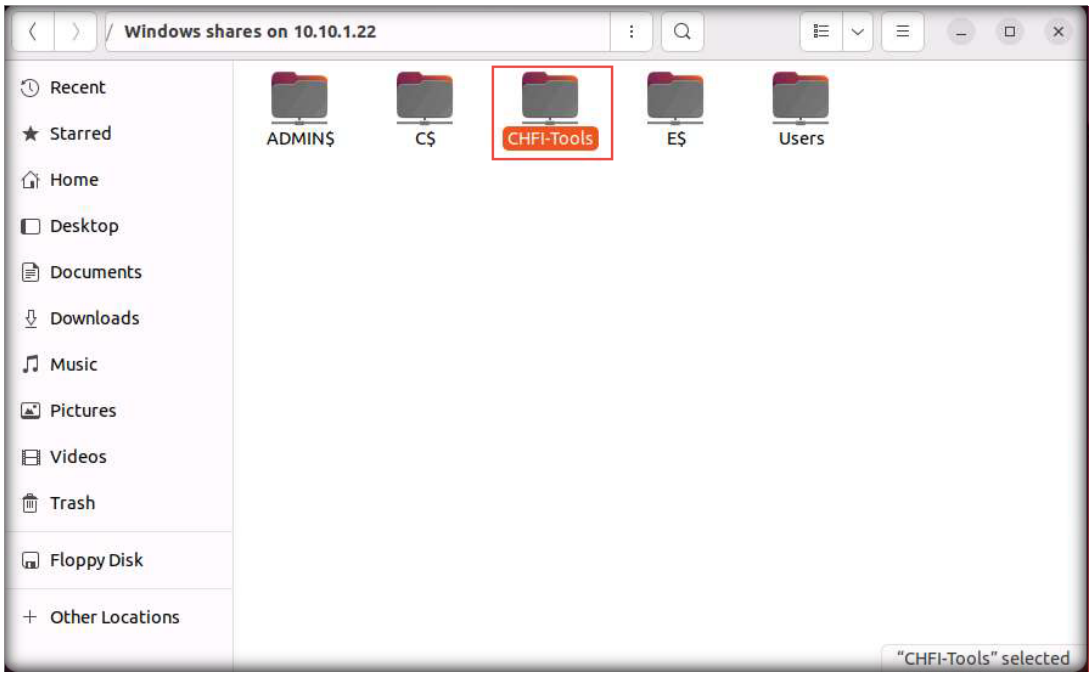


4. If a window appears asking to enter the credentials of Windows Server 2022, type **Administrator** in the **Username** field, leave the **Domain** field set to **WORKGROUP**, enter the password **Pa$$w0rd** in the Password field, select Remember forever radio button, and click Connect.

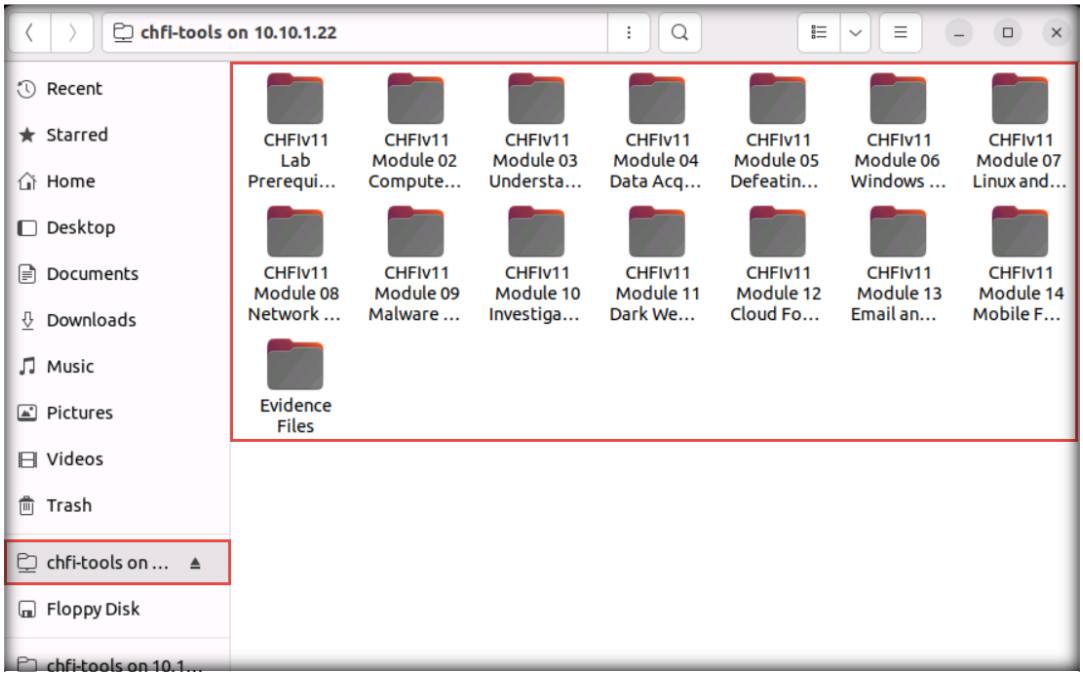


Computer Hacking Forensic Investigator Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. All the shared folders of **Windows Server 2022** appear in a new window. Double-click on **CHFI-Tools** shared folder.

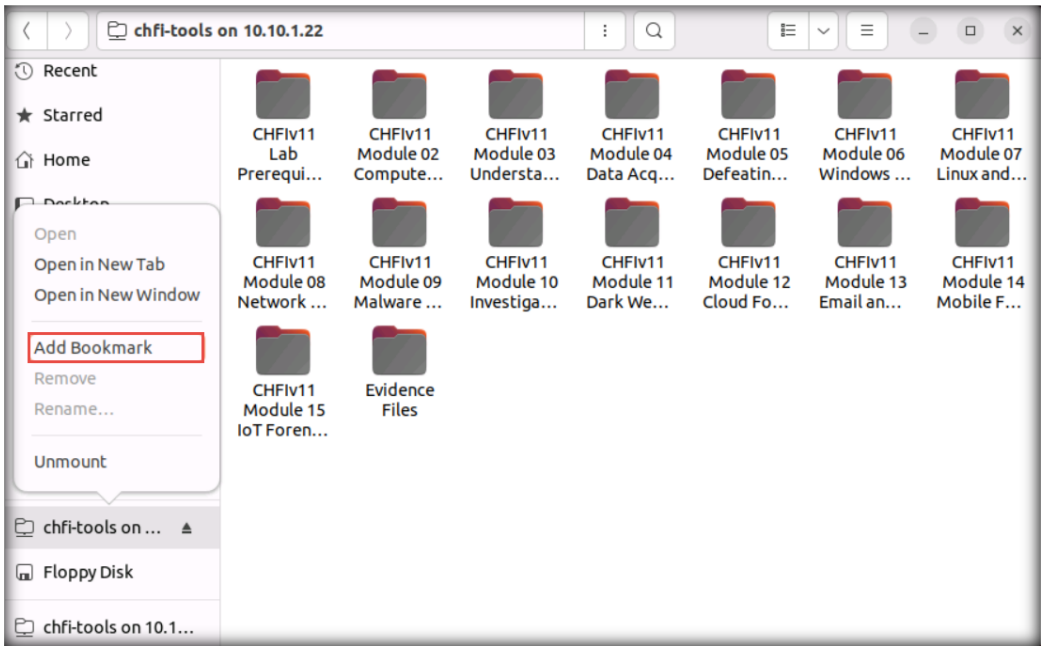


6. This will automatically mount the shared folder and display all the contents of the folder, as shown in the following screenshot:

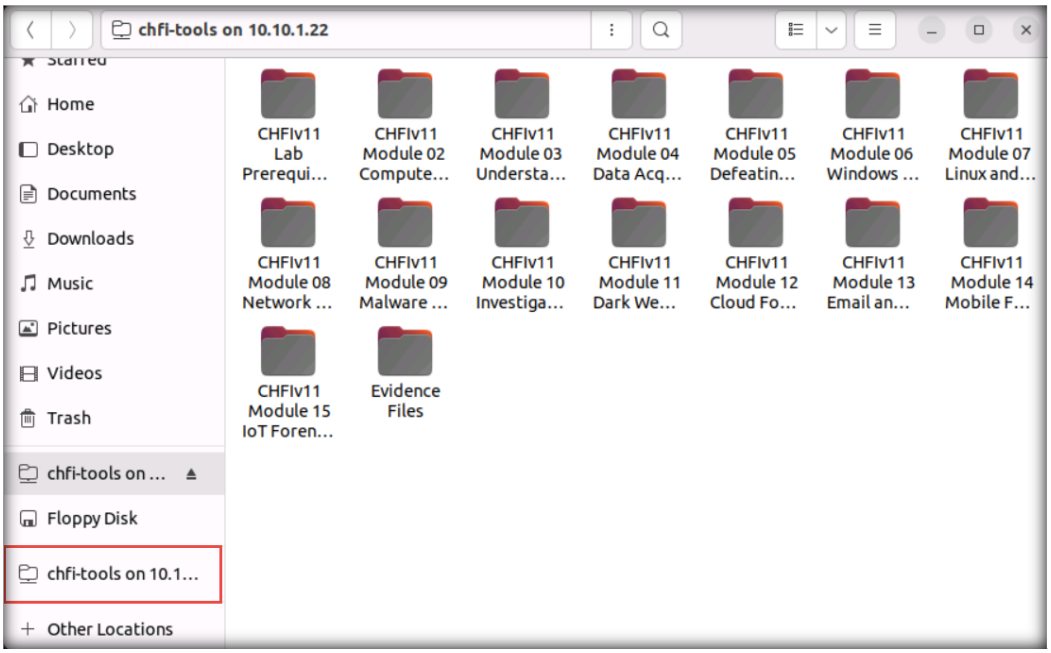


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Now, right-click on the mounted **chfi-tools** directory and click **Add Bookmark** in the context menu to create a bookmark for easily accessing the tools while practicing the labs.



8. The bookmarked folder will be visible in the left pane, as shown in the following screenshot:



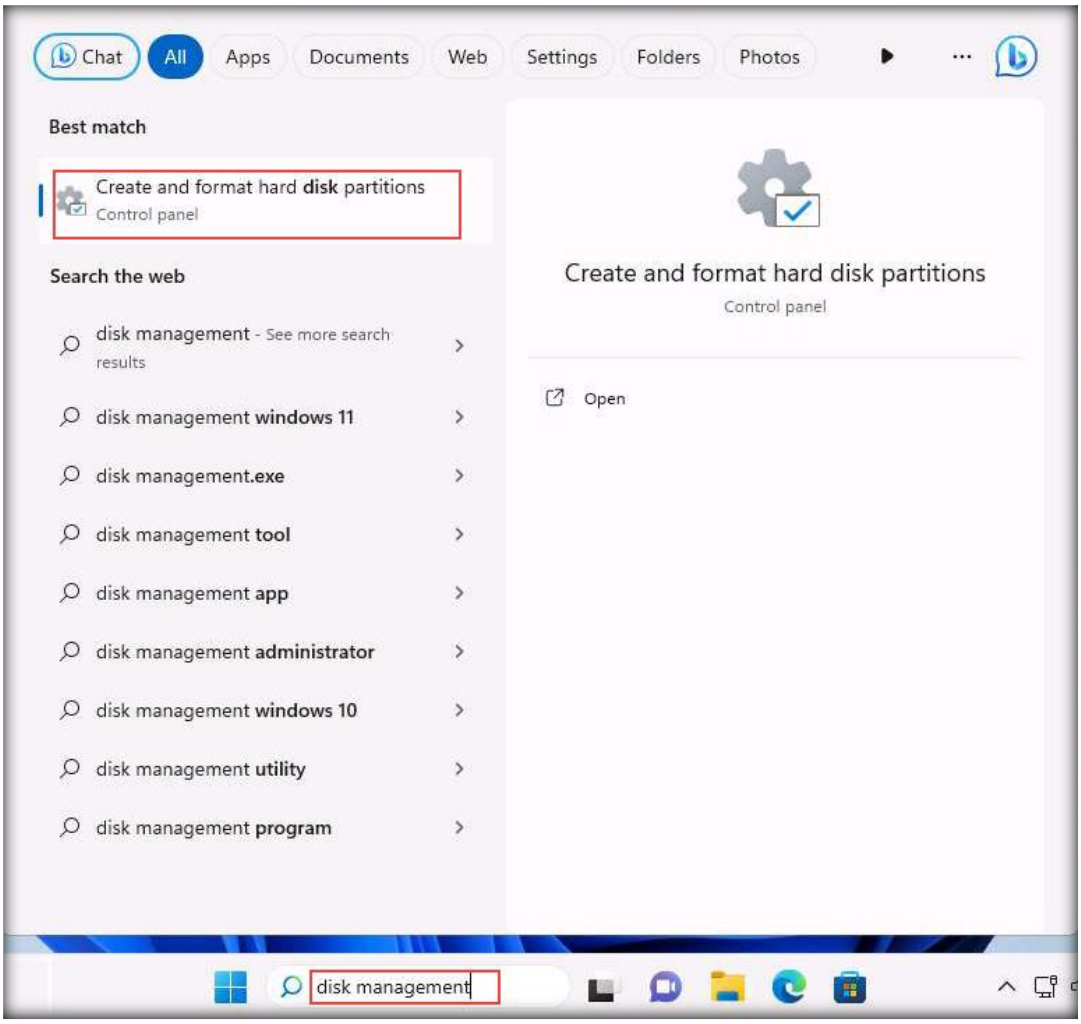
9. Follow the same steps in the **Ubuntu Forensics** machine demonstrated above to map the CHFI-Tools folder.

[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

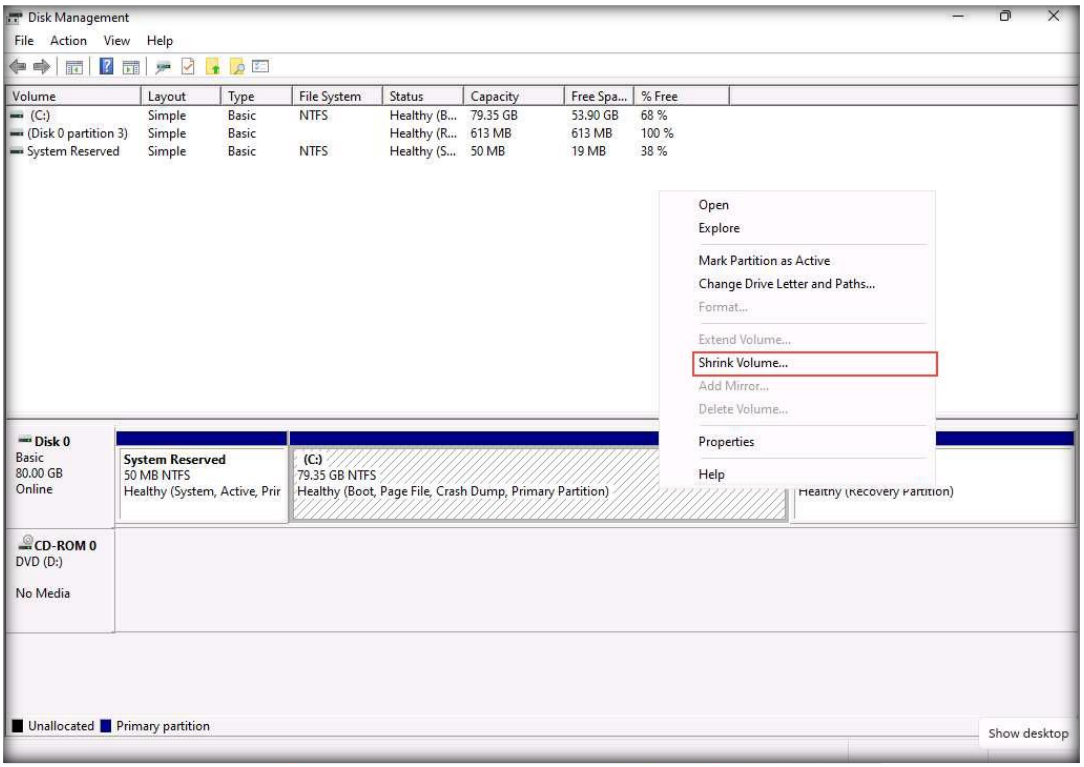
CT#19: Create a Forensic Disk (F:) and Volume (G:) in Windows 11 and Delete Volume (G) for Investigation Purpose

1. In the **Windows 11** machine, type **disk management** in the **Search bar** and press **Enter**.

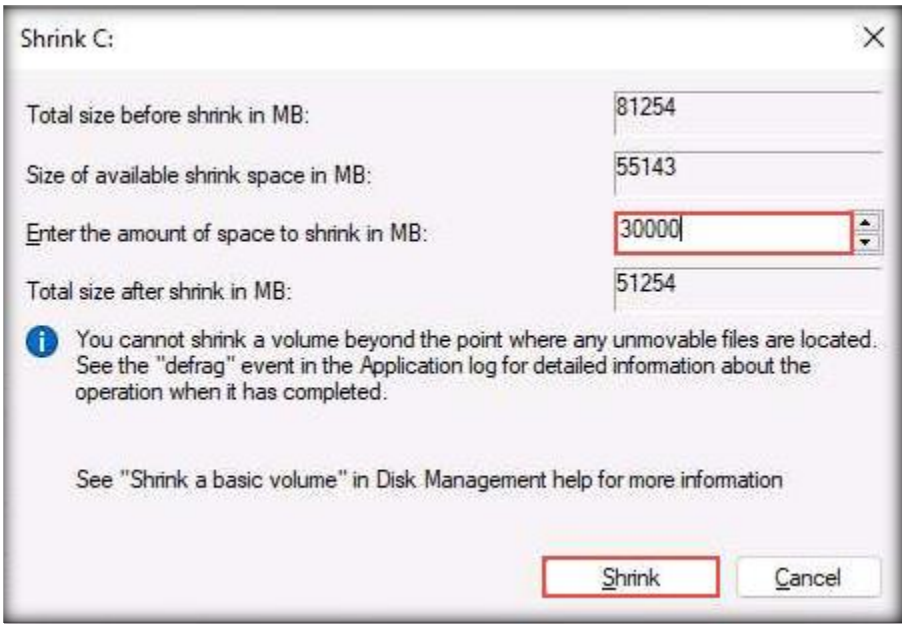


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. **Disk Management** window appears, select the drive from the middle pane (here, **C:**). Right-click the selected drive and click **Shrink Volume...**.

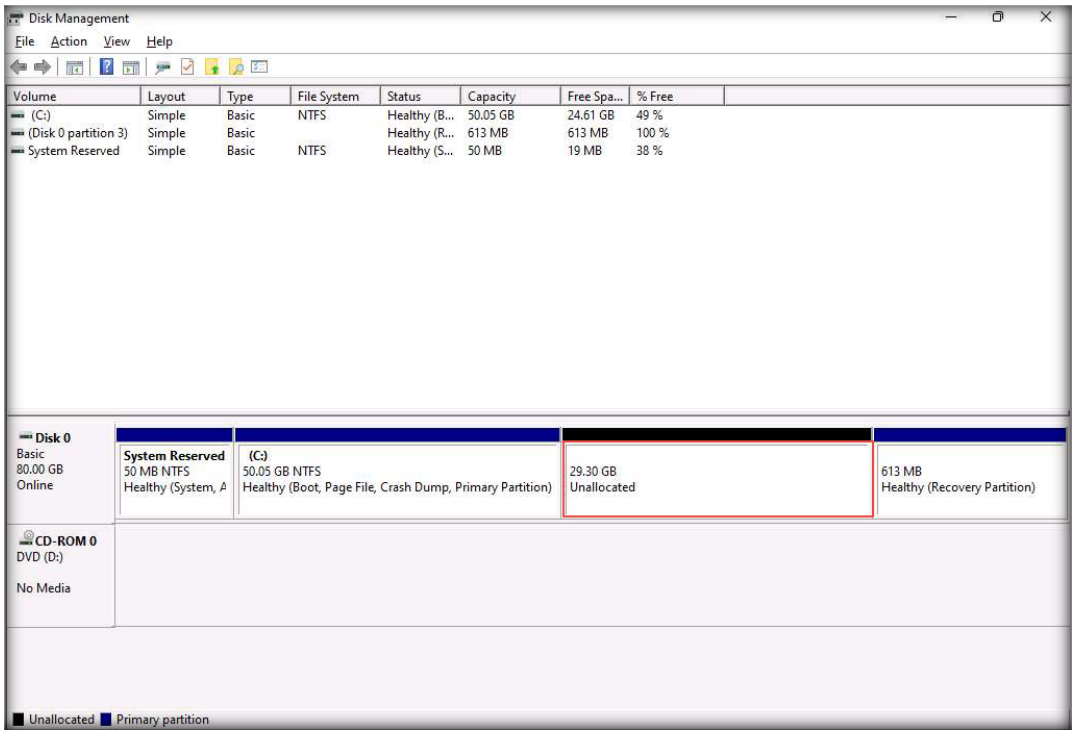


3. A **Shrink C:** window appears showing available shrink space. Enter **30000** (i.e., **30 GB**) in the **Enter the amount of space to shrink in MB:** field and click **Shrink**.

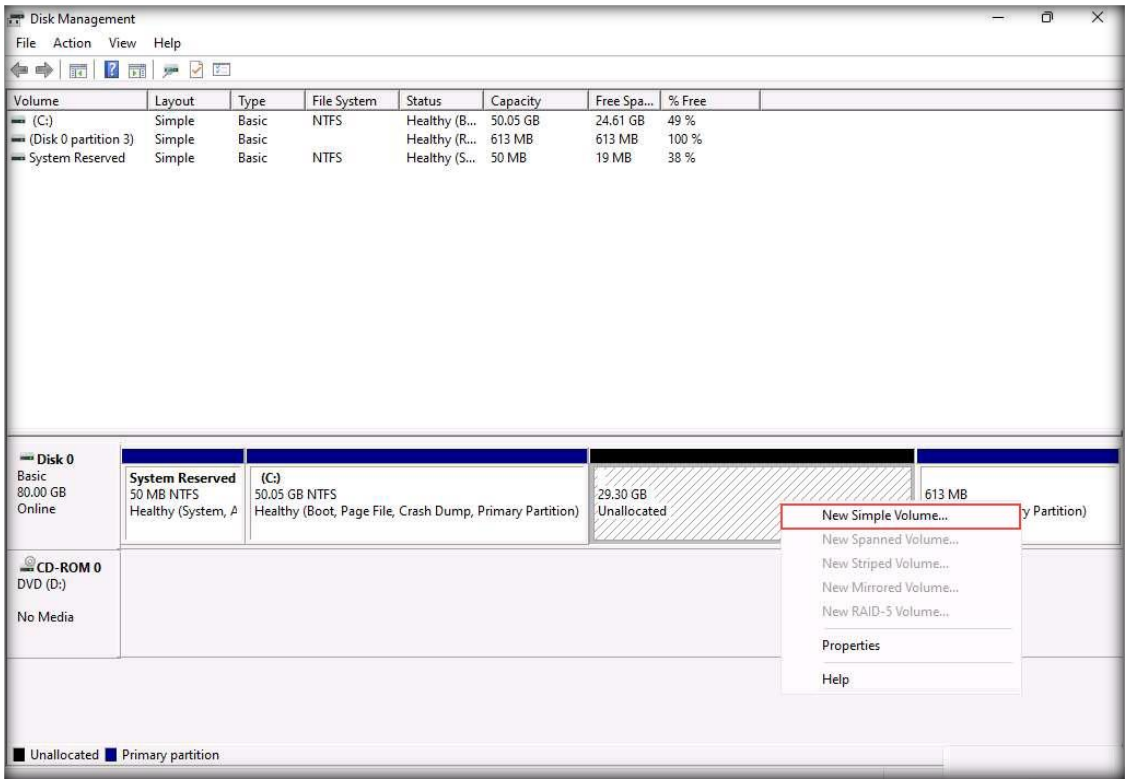


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. The **Disk Management** window will display the newly created unallocated disk partition in the middle pane, as shown in the screenshot below.



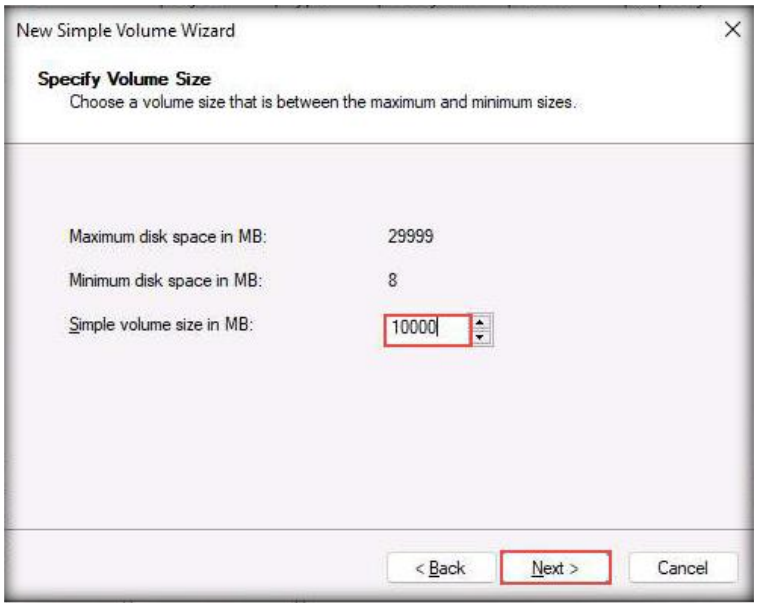
5. Select the **Unallocated** space, right-click the selected drive, and click **New Simple Volume...**.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

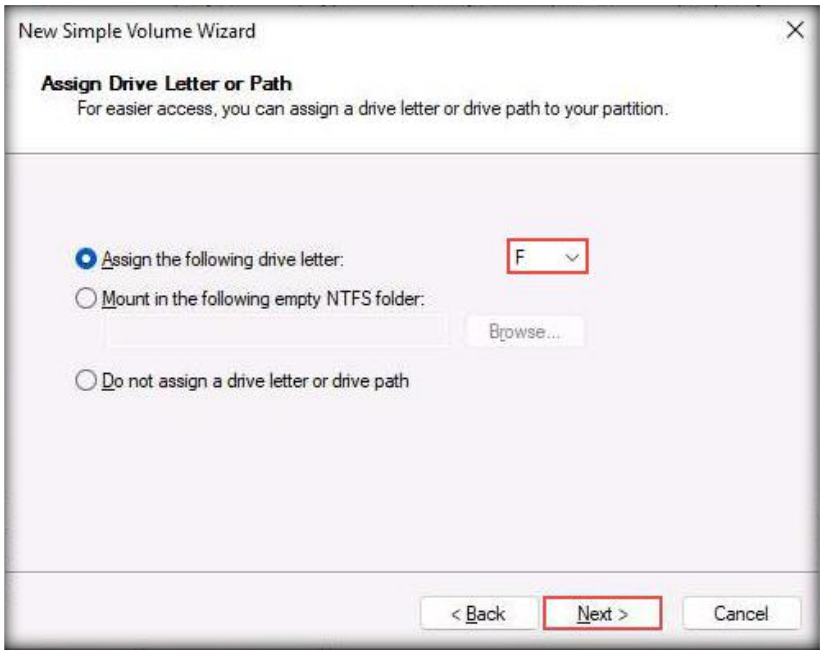
6. A **new Simple Volume Wizard** appears, click **Next**.

7. **Specify Volume Size** section of the wizard will appear; set the volume size as **10000 MB (**i.e., **10 GB)** and click **NextV**

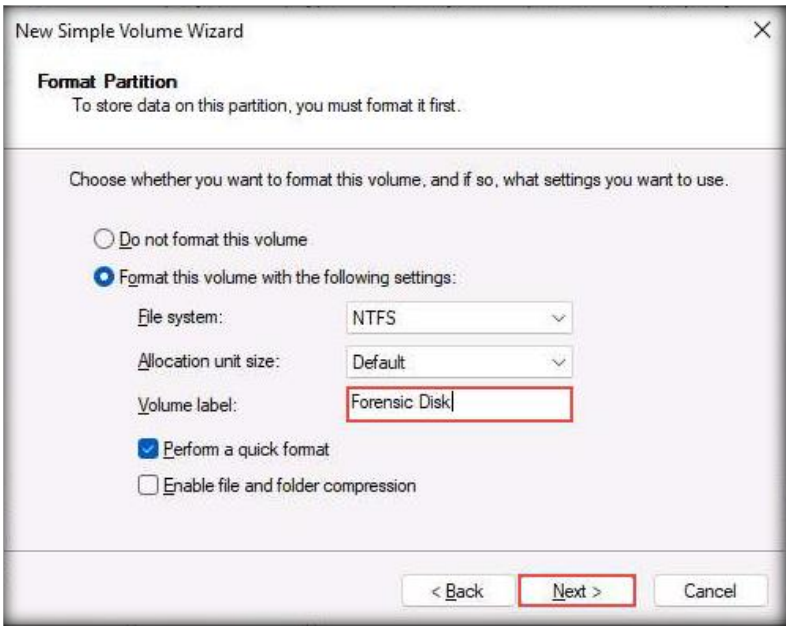


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. **Assign Drive Letter or Path** section of the wizard will appear; assign the drive letter and click **Next**. Here, we have assigned the drive letter as **F**. This might vary in your lab environment.

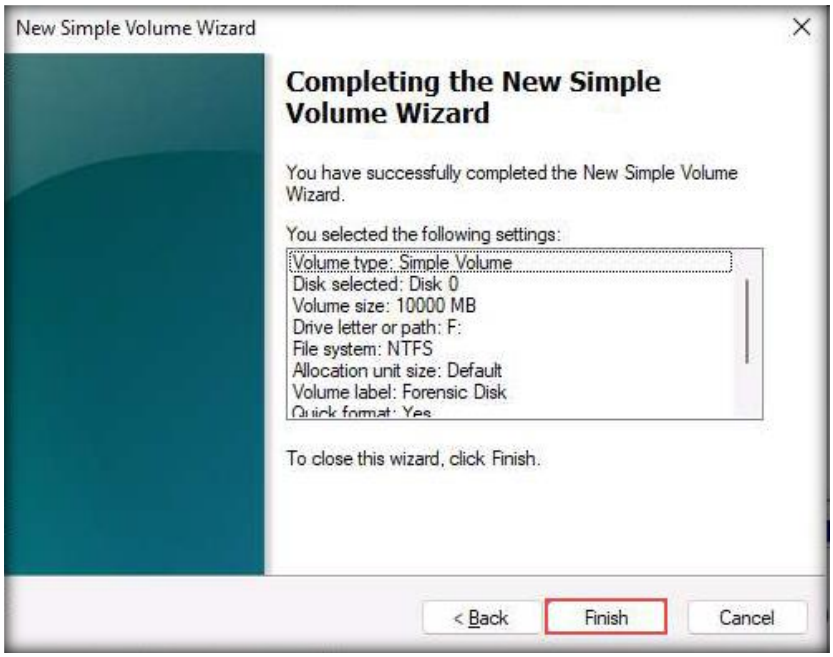


9. In the **Format Partition** section, leave the **File system** and **Allocation unit size** options set to default; enter the **Volume label** as **Forensic Disk** and click **Next**.



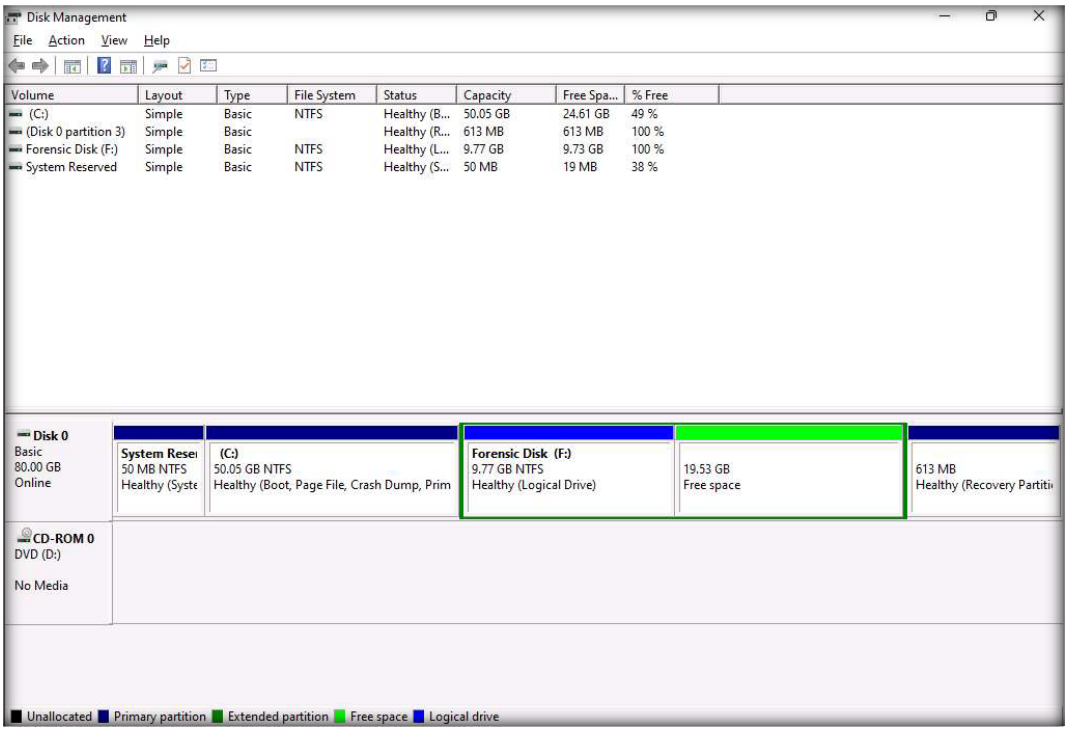
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

10. In the final step of the wizard, click **Finish**.



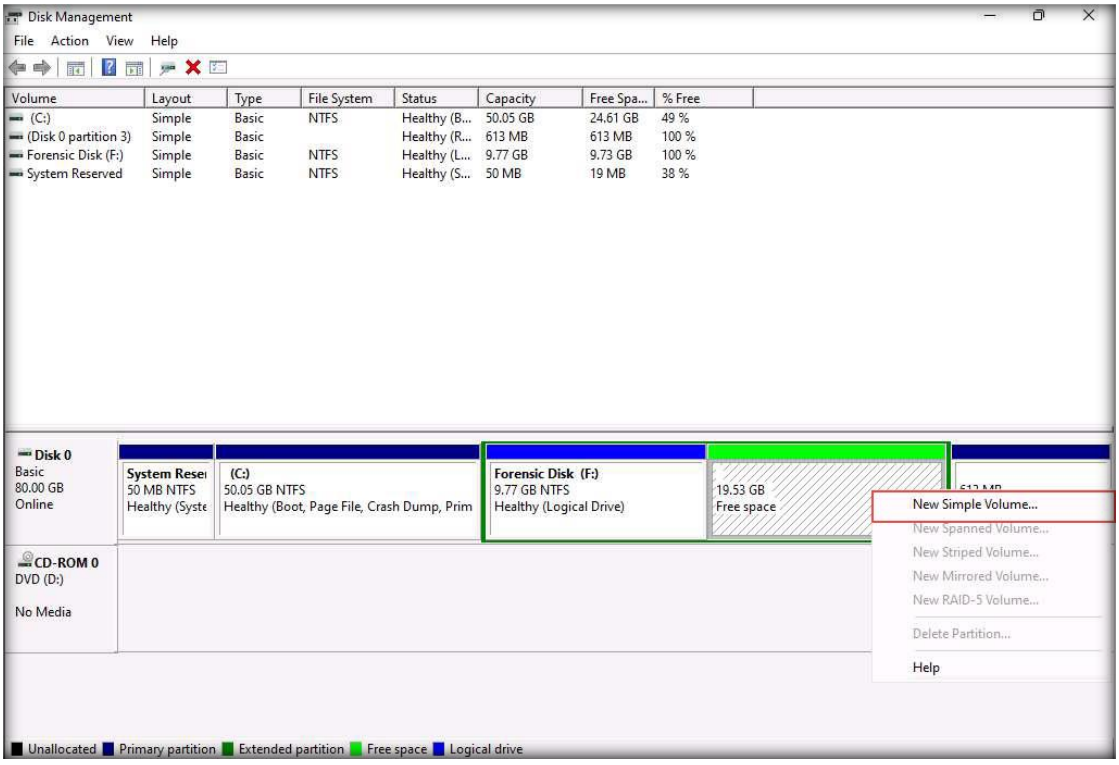
Note: If the **Microsoft Windows** pop-up appears asking to format the disk, click **Format disk**. Later, the **Format [Disk Name]** window will appear; leave the options set to default and click **Start** to begin formatting the disk. Before the formatting begins, **Format [Disk Name]** pop-up will appear, displaying a warning message. Click **OK** to initiate the formatting. Upon completion, another pop-up appears stating that the format is complete. Click **OK** to close the pop-up.

11. Now, a new drive named **Forensic Disk** is created under the **Disk 0** section.



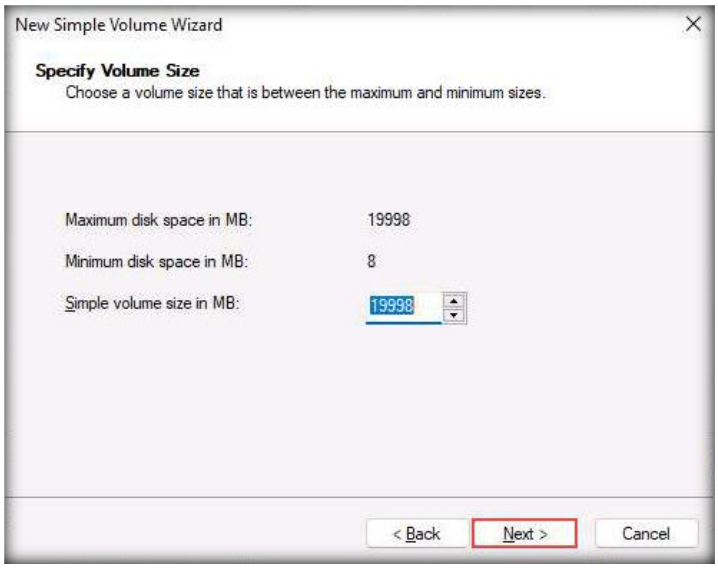
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The purpose of creating this volume is to use it in the labs to demonstrate forensic image acquisition of Windows 11 (Disk 0) and store the image in this Forensic Disk (F:) volume.
13. Open **Disk Management** again, where you can see a **~2 GB** unallocated space. Right-click on this space and select **New Simple Volume...**.



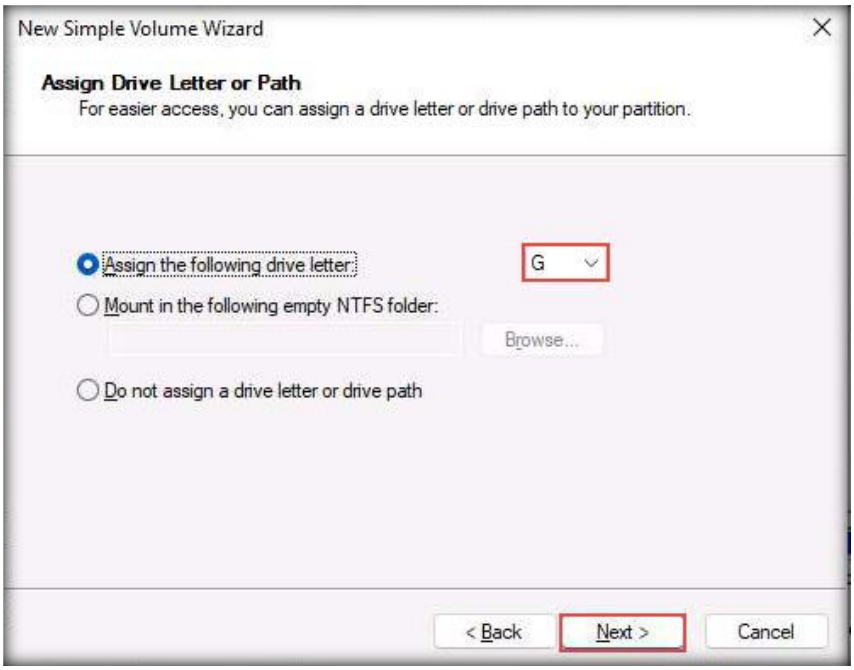
14. A **new Simple Volume Wizard** will appear; click **Next**.
15. **Specify Volume Size** section of the wizard will appear; leave the volume size as default here, **19998 MB (~2 GB)** (leave the size to the default), and click **Next**.

    Note: The size remaining in the disk might vary when you perform the lab.

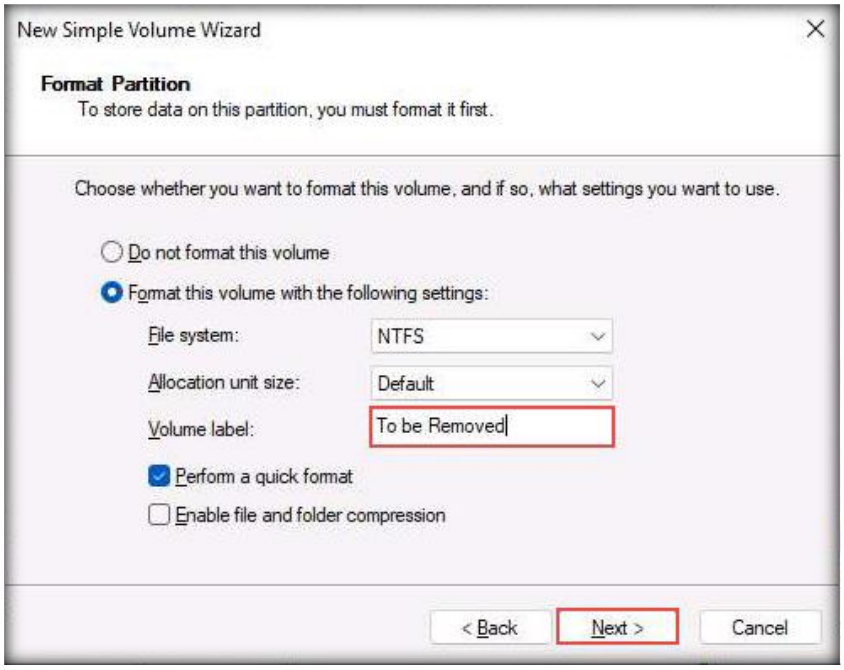


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

16. **Assign Drive Letter or Path** section of the wizard will appear; assign the drive letter and click **Next**. Here, we have assigned the drive letter as **G**. This might vary in your lab environment.

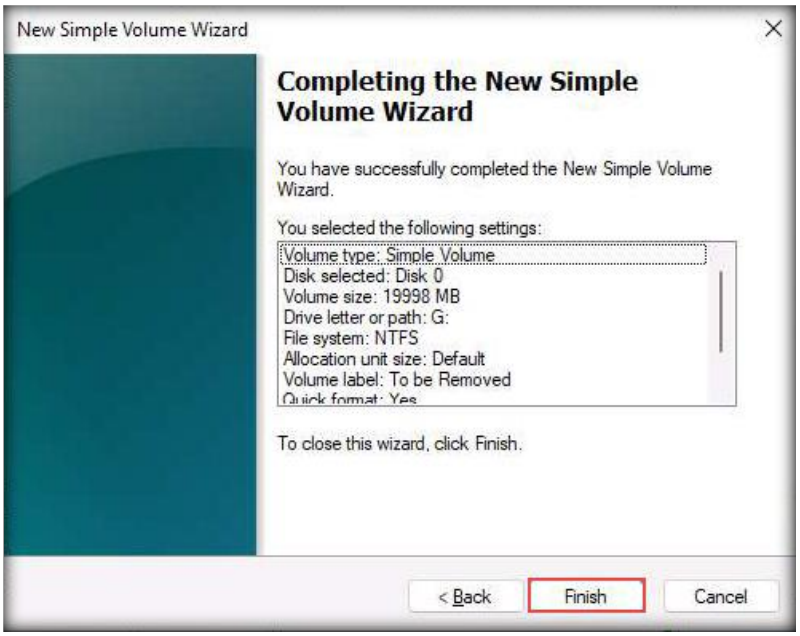


17. In the **Format Partition** section, leave the **File system** and **Allocation unit size** options set to default; enter the volume label as **To be Removed** and click **Next**.



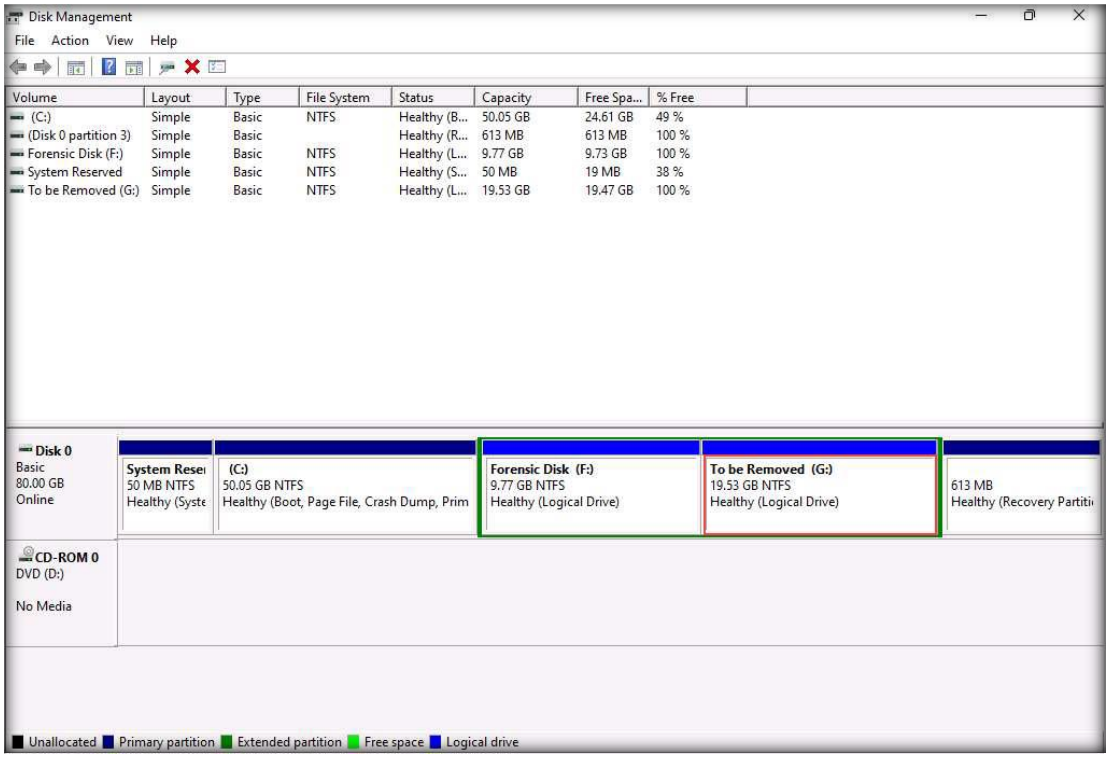
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

18. In the final step of the wizard, click **Finish**.



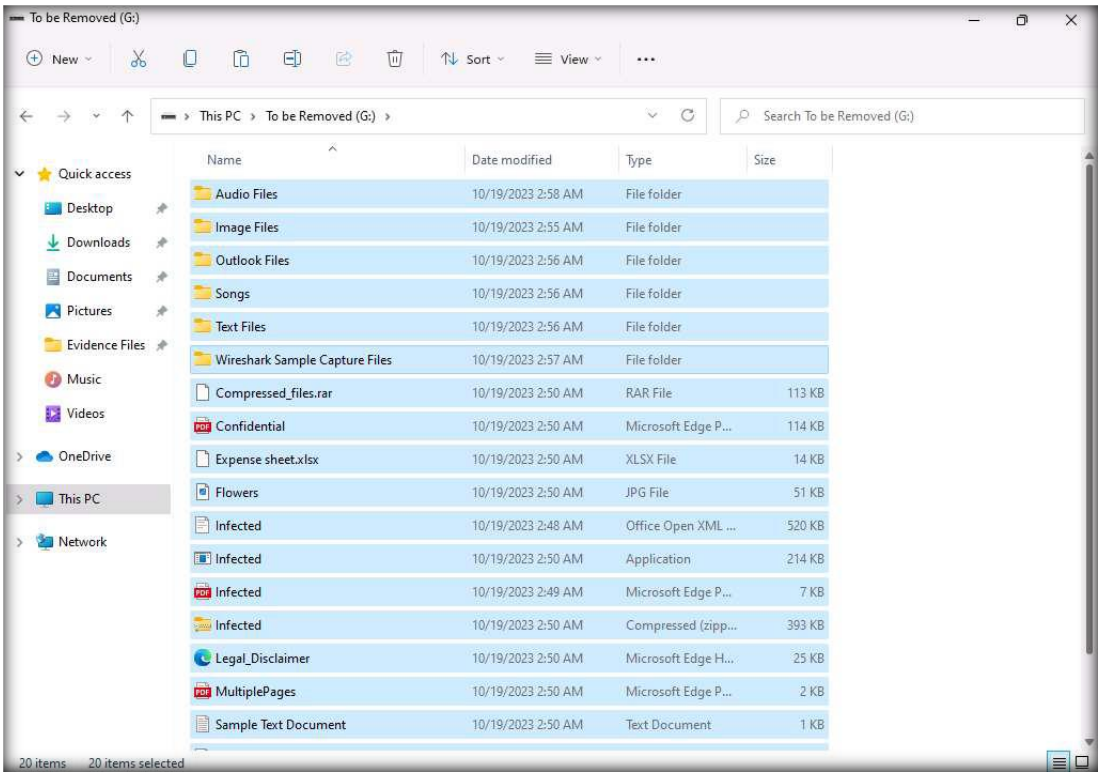
Note: If a **Microsoft Windows** pop-up appears asking to format the disk, click **Format disk**. Later, the **Format [Disk Name]** window will appear; leave the options set to default and click **Start** to begin formatting the disk. Before the formatting begins, **Format [Disk Name]** pop-up will appear, displaying a warning message. Click **OK** to initiate the formatting. Upon completion, another pop-up appears stating that the format is complete. Click **OK** to close the pop-up.

19. Now, you can observe a new drive named **To be Removed** created under the **Disk 0** section.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

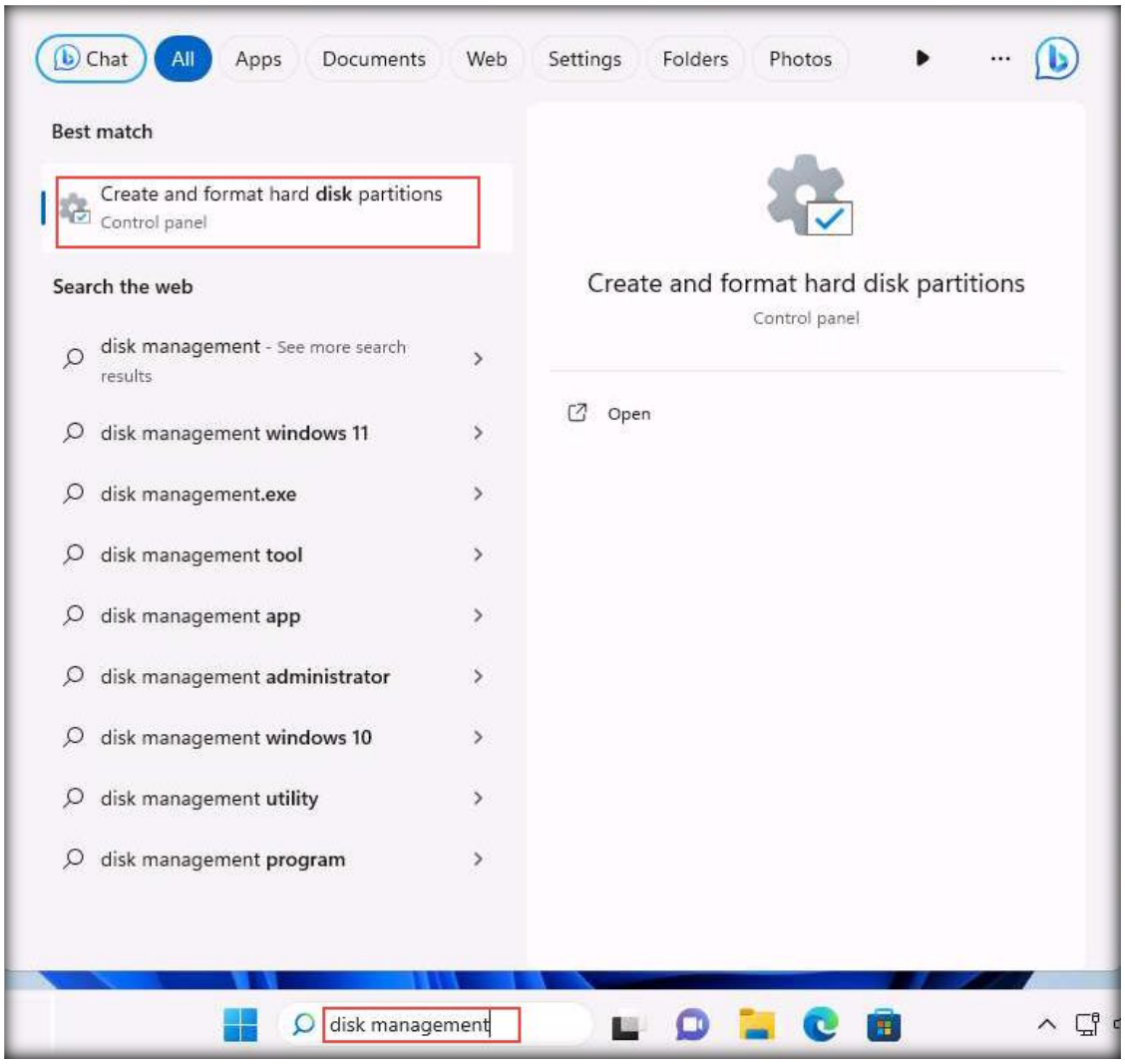
20. Close the **Disk Management** window.
21. The **G:** (To be Removed) window pops up on the screen. Now, we shall copy some folders and files from **Z:\Evidence Files** and paste them in **G:**. The folders should be **Audio Files**, **Image Files**, **Outlook Files**, **Songs**, **Text Files**, and **Wireshark Sample Capture Files**. The files should be **Compressed_files.rar**, **Confidential.pdf**, **Expense sheet.xlsx**, **Flowers.jpg**, **Legal_Disclaimer.htm**, **MultiplePages.pdf**, **Sample Text Document.txt**, **Tutorial.pptx**, **Sample_1.docx**, and **Sample_2.docx**.



22. Close the window.

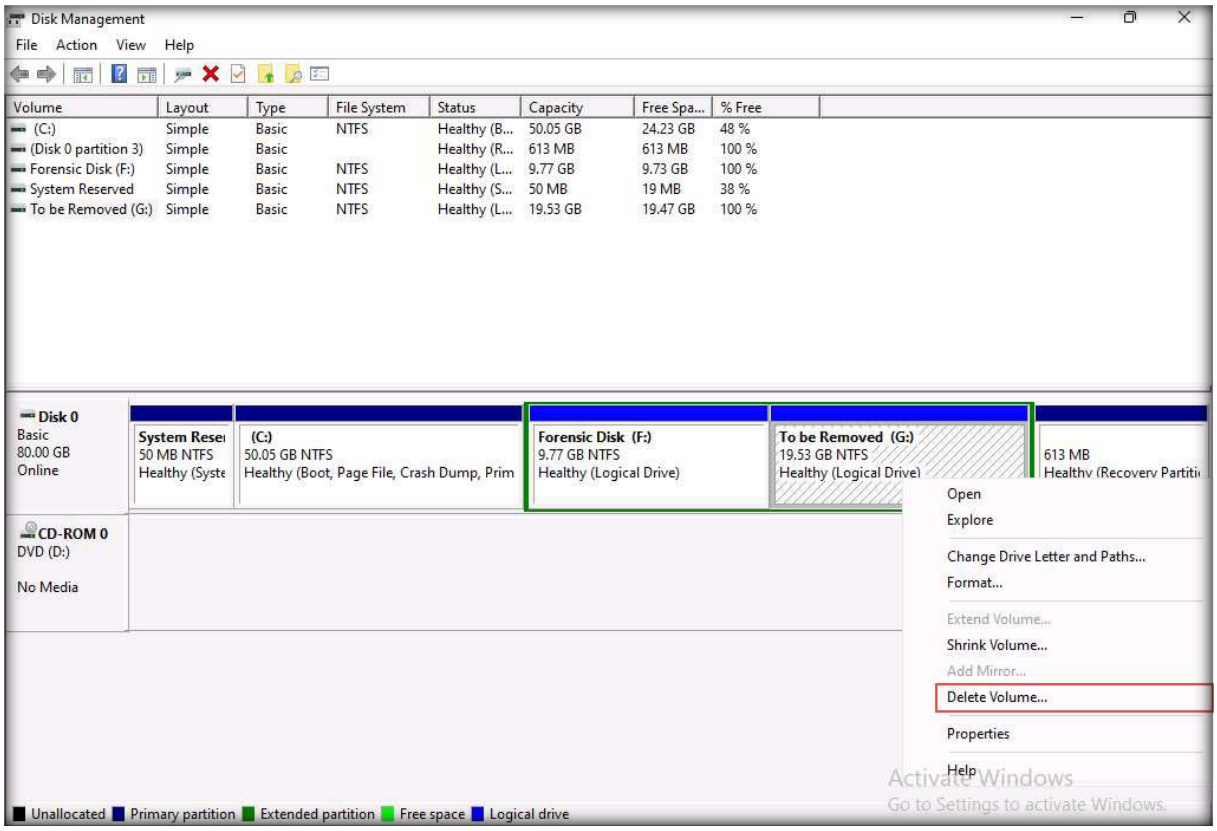
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Now, delete this partition from **Disk Management**. To do so, type **disk management** in the **Windows Search bar** and press **Enter** to launch **Disk Management**.



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

24. **Disk Management** window will appear; right-click on the **To be Removed (G:)** disk and click **Delete Volume...** from the context menu.



25. The purpose of removing the disk is to demonstrate a lab for recovering data from the deleted partition.

[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#20: Install Adobe Acrobat Reader DC on all Windows Virtual Machines

1. Log in to the **Windows 11** virtual machine with the credentials **Admin** and **Pa$$w0rd**.
2. Open a **File Explorer** window and navigate to the **Z:\CHFI-Tools\CHFIv11 Lab Prerequisites\Adobe Reader** folder.
3. Alternatively, you may download the latest version of **Adobe Acrobat Reader DC** from the official Adobe website.
4. Double-click the **Reader_Install_Setup.exe** file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
5. Follow the **wizard-driven** installation steps and complete the installation by choosing the default options throughout. After the installation has completed, close all windows.
6. In the same manner, install the application on the **Windows Server 2022** virtual machine.

   Note: On the **Windows Server 2022** virtual machines, navigate to the **E:\CHFIv11 Lab Prerequisites\Adobe Reader** folder to access the **Adobe Reader** setup file.

[Back to Configuration Task Outline]

CT#21: Install WinRAR on the Windows 11 Virtual Machine

1. Log in to the **Windows 11** virtual machine using the credentials **Admin** and **Pa$$w0rd**.

   Note: Ensure that the **Windows Server 2022** virtual machine is also running.
2. Navigate to the **Z:\CHFIv11 Lab Prerequisites\WinRAR** folder.
3. Alternatively, you may download the latest version of **WinRAR** from the official website.
4. Double-click on the **winrar-x64-624.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
5. The **WinRAR** setup window appears; click **Install**.
6. Complete the installation by choosing the default options throughout.
7. After completing the installation, the installation location of WinRAR opens automatically in a **File Explorer** window. Close the window.
8. In the same manner, install the application on **Windows Server 2022**.

[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#22: Install Notepad++ on all Windows Virtual Machines

1. On the **Windows Server 2022** virtual machine, navigate to the **E:\CHFI-Tools\CHFIv11 Lab Prerequisites\Notepad++** folder.
2. Alternatively, you may download the latest version of **Notepad++** from the official website.
3. Double-click on the **npp.8.5.8.Installer.x64.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
4. The **Installer Language** window appears. Select **English** and press **OK**.
5. In the **Notepad++** setup window, follow the **wizard-driven** installation steps and complete the installation by choosing the default options throughout. After the installation has completed, uncheck the **Run Notepad++ v8.5.8** box and click **Finish** to close the window.
6. In the same manner, install the application on the **Windows 11** virtual machine.

[Back to Configuration Task Outline]

CT#23: Install Web Browsers on all Windows Virtual Machines

1. On the **Windows Server 2022** virtual machine, navigate to the **E:\CHFI-Tools\CHFIv11 Lab Prerequisites\Web Browsers** folder.
2. Follow the **wizard-driven** installation steps to install the **Google Chrome** and **Mozilla Firefox** web browsers.
3. You can also download the **latest** versions of these web browsers from their respective websites.
4. In the same manner, install the browsers on the **Windows 11** virtual machine.

[Back to Configuration Task Outline]

CT#24: Install WinPCap on all Windows Virtual Machines

1. On the **Windows Server 2022** virtual machine, navigate to the **E:\CHFI-Tools\CHFIv11 Lab Prerequisites\WinPcap** folder.
2. Double-click on the **WinPcap_4_1_3.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
3. Follow the wizard-driven installation steps and complete the installation by choosing the default options throughout.
4. In the same manner, install the application on the **Windows 11** virtual machine.

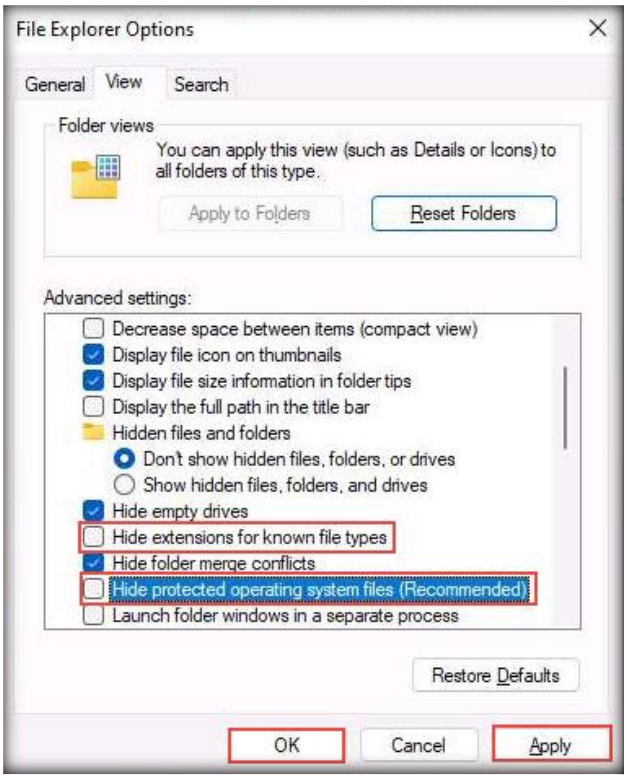
[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#25: Configure File Explorer on all Windows Virtual Machines

1. On the **Windows 11** virtual machine, open the **Control Panel** and select **Small icons** from the **View by:** field in the top-right corner of the window.
2. Click **File Explorer Options**. When the **File Explorer Options** window appears, click the **View** tab.
3. In the **Advanced Settings** section, under **Hidden files and folders**, select **Show hidden files, folder and drives** option, uncheck **Hide** extensions **for known file types**, and uncheck **Hide protected operating system files (Recommended)** (if a **Warning** appears, click **Yes**). Click **Apply** and then click **OK**.

   Note: If a **Warning** pop-up appears, click **Yes**.



4. In the same manner, configure the settings on the **Windows Server 2022** virtual machine.

   Note: In different versions of Windows, the **File Explorer Options** may be named **Folder Options**.

[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#26: Install the Java Runtime Environment on the Windows Virtual Machines

1. Log in to the **Windows Server 2022** virtual machine with the credentials **Administrator** and **Pa$$w0rd**.
2. Navigate to the **E:\CHFIv11 Lab Prerequisites\Java Runtime Environment** folder.
3. Alternatively, you may download the latest version of **Java Runtime Environment** from the official website.
4. Double-click on the **jre-8u391-windows-x64.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
5. The **Java Setup - Welcome** setup window appears; click **Install**.
6. The **Java Setup – Progress** installation window appears, showing the status of the installation process.
7. After completing the installation, close the window.
8. On the **Windows 11** virtual machine, navigate to **Z:\CHFI-Tools\CHFIv11 Lab Prerequisites\Java Runtime Environment**.
9. Double-click on the **jre-8u391-windows-x64.exe** setup file to begin the installation. If a **User Account Control** pop-up window appears, click **Yes**.
10. The **Java Setup - Welcome** setup window appears; click **Install**.
11. The **Java Setup – Progress** installation window appears, showing the status of the installation process.
12. After completing the installation, close the window.

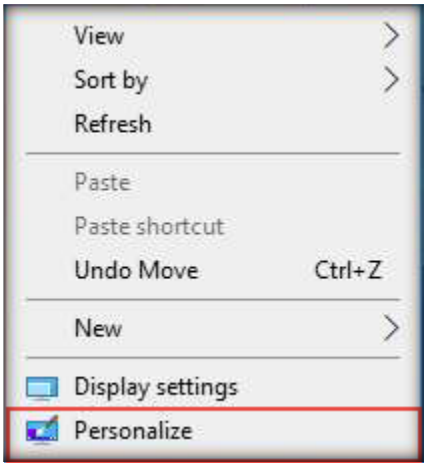
[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

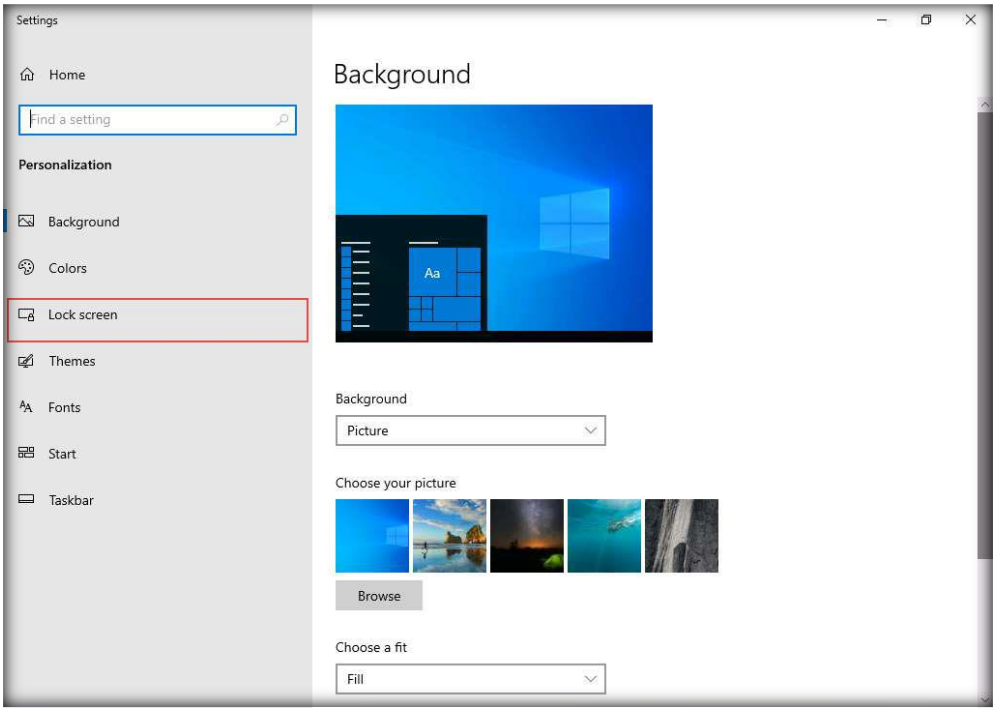
CT#27: Turn Off Screen Savers on all Windows Virtual Machines

Note: Before performing this CT, you must activate the Windows virtual machines.

1. In the **Windows Server 2022** virtual machine, right-click on the **Desktop** and select **Personalize** to open the personalization settings.

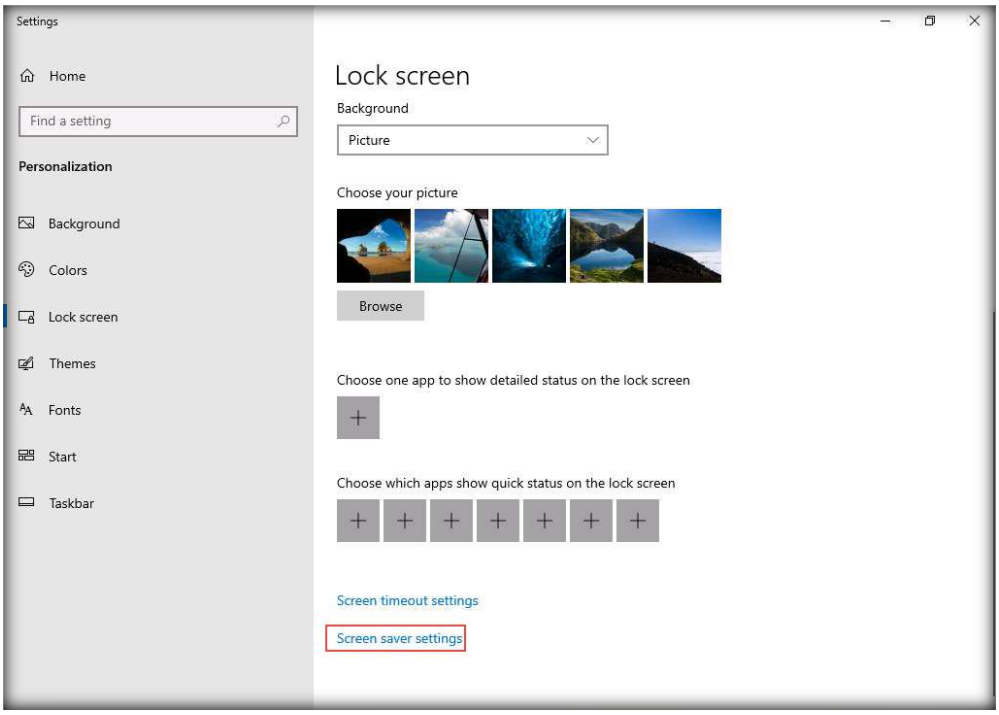


2. In the **Personalization** window scroll down and click **Lock screen** in the right pane.

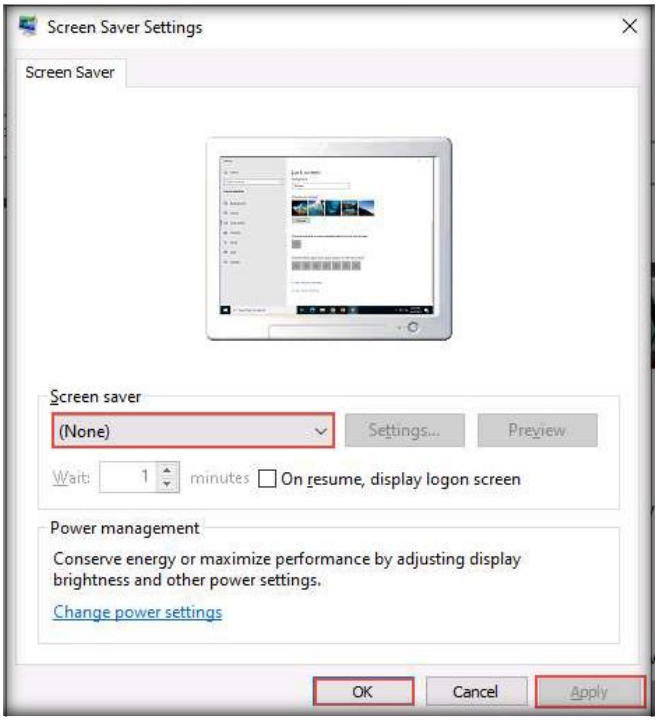


Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The **Lock screen** settings page appears; scroll down and click **Screen saver settings**.



4. The **Screen Saver Settings** window appears; ensure that the **(None)** option is selected from the drop-down list for **Screen saver**. Click **Apply** and then **OK**.



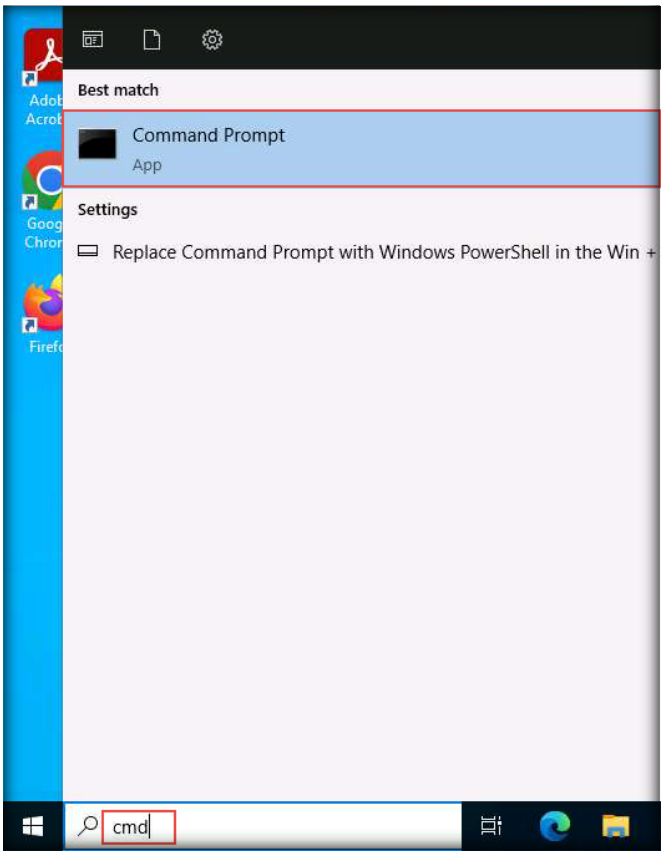
5. Close all windows.
6. Similarly, turn off the screen saver on **Windows 11**.

[Back to Configuration Task Outline]

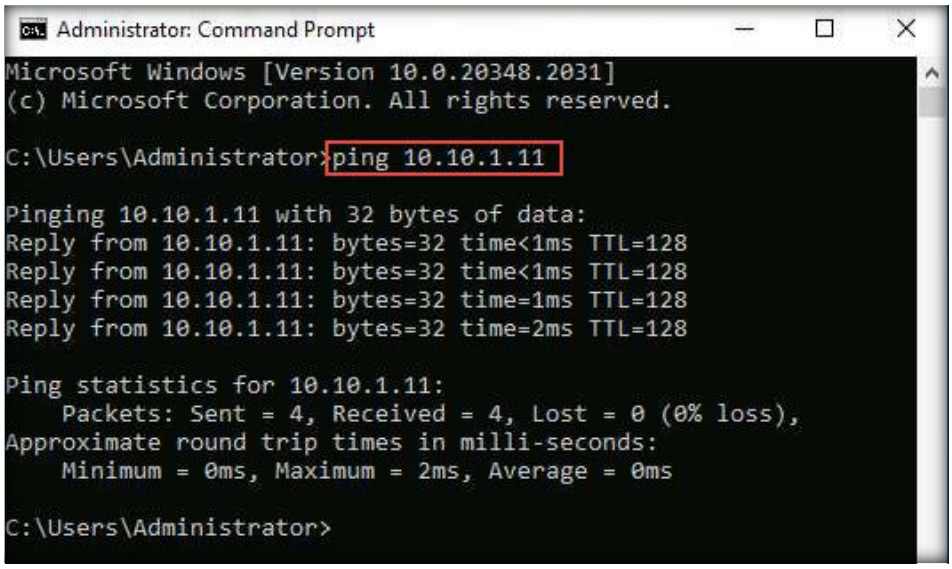
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#28: Ping Test Among all Virtual Machines

1. On the **Windows Server 2022** virtual machine, open a **Command Prompt** window.

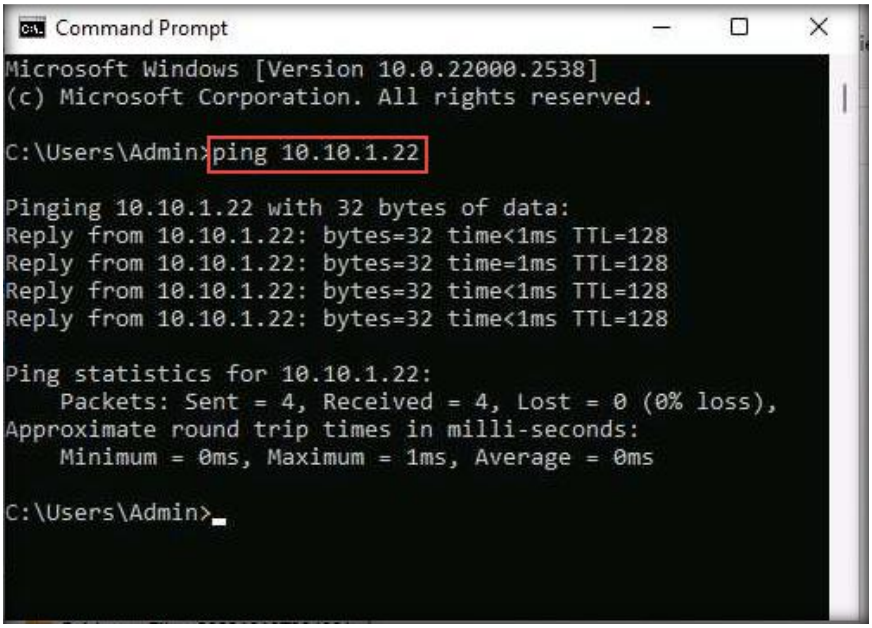


2. Before pinging the virtual machines, ensure that they are running.
3. Check for a reply from the virtual machines. Here, as an example, we are using the **Windows 11** virtual machine with the IP address **10.10.1.11** (this IP address may be different in your lab network).



Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Open the **Command Prompt** in another virtual machine. Here, as an example, we are using the **Windows 11** virtual machine.
5. Here, as an example, we are pinging **Windows Server 2022** from the **Windows 11** machine (the IP address will be different in your lab network).



6. Open **Command Prompt** in one of the virtual machines and execute the command **Ping <IP address of Virtual Machine>**.
7. Repeat the above steps to ping all virtual machines (**Windows 11**, **Windows Server 2022**, **Ubuntu Suspect, and Ubuntu Forensics**).

[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#29: Disable DEP in Windows Server 2022 Virtual Machine

1. Click **Start → Control Panel → System and Security**.
2. In the **System and Security** window, click **System**.
3. Click **Advanced system settings** on the left-pane of the **Control Panel** window.
4. A **System Properties** window will appear.
5. Click the **Advanced** tab and click the **settings** button of the **Performance** section.
6. **Performance Options** window will appear. Click the **Data Execution Prevention** tab.
7. Select the radio button for **Turn on DEP for essential Windows programs and Services only**.
8. Click **Apply** and then click **OK**.
9. Click **OK** to close the System Properties Window and close the **System** window.
10. If the Windows machine prompts you to **reboot** the system for the changes to take effect, reboot the machine.

[Back to Configuration Task Outline]

CT#30: Install PuTTY in Windows Server 2022 Virtual Machine

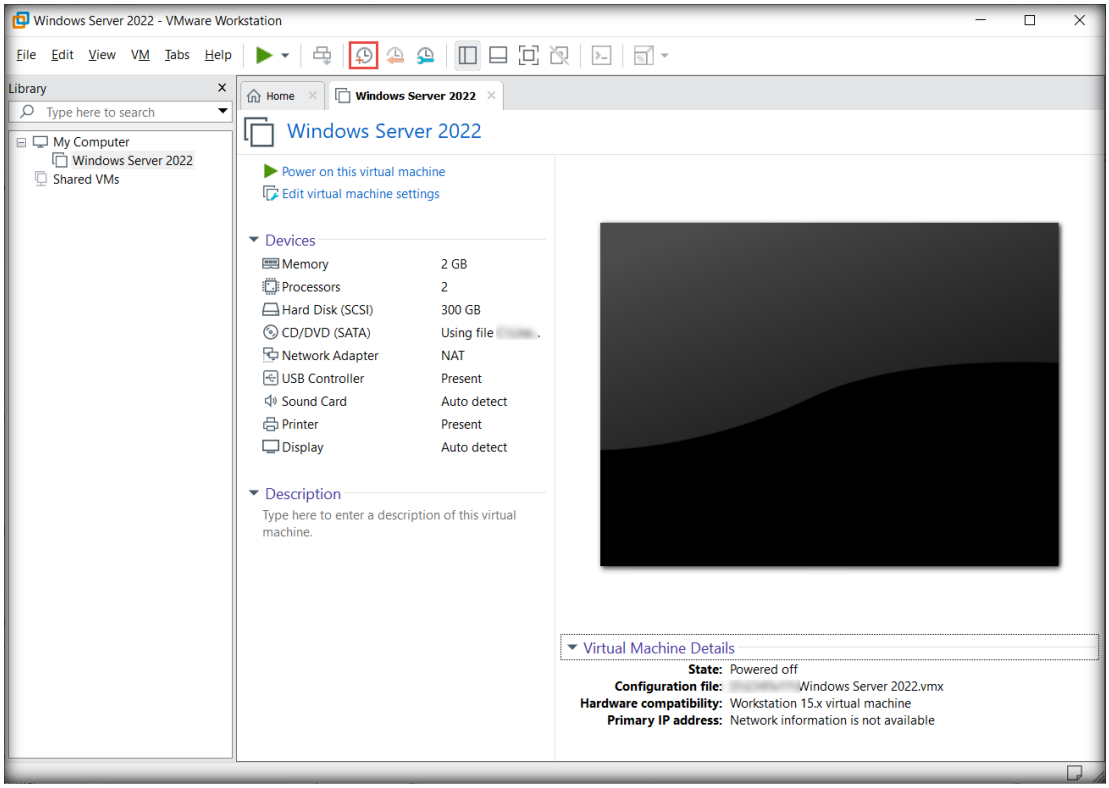
1. Navigate to **C:\CHFI-Tools\CHFIv11 Lab Prerequisites\PuTTY**, or download the file from the **Aspen** portal.
2. **Double**-click **putty-64bit-0.79-installer.msi** to begin the installation.
3. Follow the wizard-driven installation steps and complete the installation by choosing the default settings throughout the process.
4. In the last step of the installation, uncheck the **View README file** option and click **Finish**.

[Back to Configuration Task Outline]

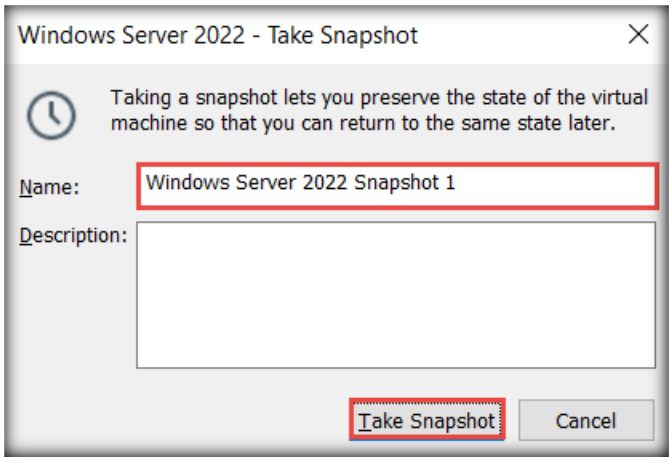
Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

CT#31: Take Snapshots of the Virtual Machines

1. Ensure that all the virtual machines are turned off.
2. In the **VMware Workstation** window, click **Windows Server 2022** in the left pane, and then the **Take a snapshot of this virtual machine** ( ) icon, as the screenshot shows.



3. The **Windows Server 2022 – Take Snapshot** pop-up appears. Type a name for the snapshot in the **Name** field, retain the default description field, and click **Take Snapshot**.



4. Similarly, take snapshots of all the virtual machines once all the CTs have been completed.

[Back to Configuration Task Outline]

Computer Hacking Forensic Investigator Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

End of the Document

EC-Council

Building A Culture Of Security

EC-Council Official Curricula