

. .



Computer Hacking Forensic Investigator v11

CLASSROOM LAB SETUP GUIDE

EC-Council Official Curricula

Table of Contents

Classroom Setup Instructions: CHFIv11	4
Classroom Requirements	5
Hardware	6
Software	6
Classroom Connectivity	7
Configuration	7
Setup Document Overview	7
Training Room Environment	8
Instructor Computer	8
Student Workstations	9
Room Environment	11
Classroom Configuration	11
Computer Names	12
Network Topology	12
CHFI VM Setup on Instructor and Student Machines	13
Instructor Acceptance	13
Firewall Settings	13
Blackboard	14
Setup Checklist	14
Instructor Acceptance	15
Assistance	15
Detailed Setup Instructions - Configuration Tasks (CT)	16
CT#1: Install the Host Operating System	16
CT#2: Copy the Host Operating System Files	16
CT#3: Install WinRAR on the Host Operating System	16
CT#4: Download the ISO File	17
CT#5: Install VMware Workstation Pro on the Host Machine	17
CT#6: Configure a Virtual Network in VMware Virtual Network Editor	19
CT#7: Install Windows Virtual Machines in VMware	24
CT#8: Configure the Internet Explorer (IE) Enhanced Security Configuration in Windows Se 2022 Virtual Machine	rver 46

CT#9: Install .NET Framework in Windows Server 2022 Virtual Machine	48
CT#10: Install the Ubuntu Suspect and Ubuntu Forensics Virtual Machines in VMware	54
CT#11: Turn the Windows Defender Firewall Off on all Windows Virtual Machines	71
CT#12: Configure Windows Components on all Windows Virtual Machines	89
CT#13: Install WinRAR on the Windows Server 2022 Virtual Machine	93
CT#14: Install MS Office on the Windows Server 2022 Virtual Machine	93
CT#15: Create a Partition in the Windows Server 2022 Virtual Machine	94
CT#16: Download CHFI Tools on the Windows Server 2022 Virtual Machine	99
CT#17: Share and Map the CHFI-Tools Folder to the Windows Virtual Machines	100
CT#18: Share and Map the CHFI-Tools Folder to the Ubuntu Virtual Machines	115
CT#19: Create a Forensic Disk (F:) and Volume (G:) in Windows 11 and Delete Volume (G) for Investigation Purpose	119
CT#20: Install Adobe Acrobat Reader DC on all Windows Virtual Machines	131
CT#21: Install WinRAR on the Windows 11 Virtual Machine	131
СТ#22: Install Notepad++ on all Windows Virtual Machines	132
CT#23: Install Web Browsers on all Windows Virtual Machines	132
CT#24: Install WinPCap on all Windows Virtual Machines	132
CT#25: Configure File Explorer on all Windows Virtual Machines	133
CT#26: Install the Java Runtime Environment on the Windows Virtual Machines	134
CT#27: Turn Off Screen Savers on all Windows Virtual Machines	135
CT#28: Ping Test Among all Virtual Machines	137
CT#29: Disable DEP in Windows Server 2022 Virtual Machine	139
CT#30: Install PuT*TY in Windows Server 2022 Virtual Machine	139
CT#31: Take Snapshots of the Virtual Machines	140

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.

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 \times 6 feet (1 m \times 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:
 - o Ergonomic desk and chair
 - o Power outlet
 - o Network jack
 - $\circ~$ LCD projector with a minimum resolution of 740 \times 1280 pixels and all connecting cables
- Student station (per student):
 - o Ergonomic chair
 - Workstation with a minimum horizontal workspace of 9 square feet (3 feet \times 3 feet)
 - o One power outlet
 - o One network jack

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

- 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)
 - o Microsoft Windows 11 Enterprise or Professional (64-bit) with full patches applied
 - o Microsoft Windows Server 2022 Standard Edition (64-bit) with full patches applied
 - o 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.

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 <u>CT#4</u> 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 <u>CT#16</u> in the Configuration Tasks section).
- Install VMware Workstation Pro on the host machine (see <u>CT#5</u> in the Configuration Tasks section).
- Configure a virtual network in the VMware Virtual Network Editor (see <u>CT#6</u> in the Configuration Tasks Section).
- Install guest operating systems (Windows Server 2022 and Windows 11) on VMware Workstation (see <u>CT#7</u> in the Configuration Tasks section).
- Configure the Internet Explorer Enhanced Security Configuration (see <u>CT#8</u> in the Configuration Tasks section).
- Run the IP protocol.
- Install guest operating systems (Ubuntu Suspect and Ubuntu Forensics) on VMware Workstation (see <u>CT#10</u> in the Configuration Tasks section).
- Turn off the firewall on all Windows virtual machines (see <u>CT#11</u> in the Configuration Tasks section).

- Install Windows components in all the Windows virtual machines (see <u>CT#12</u> in the Configuration Tasks section).
- Install WinRAR and MS Office on the Windows 11 virtual machine (see <u>CT#13</u> and <u>CT#14</u> in the Configuration Tasks section).
- Create a partition in the Windows Server 2022 virtual machine (see <u>CT#15</u> in the Configuration Tasks section).
- Have CHFI Tools shared as the Z: drive on the Windows and Ubuntu machines (mapping the Z: drive) (see <u>CT#17</u> and <u>CT#18</u> 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 <u>CT#19</u>)
- Install Adobe Acrobat Reader DC on all Windows virtual machines (see <u>CT#20</u> in the Configuration Tasks section).
- Install WinRAR on the Windows Server 2022 (see <u>CT#21</u> 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 <u>CT#22</u>, <u>CT#23</u>, and <u>CT#24</u> in the Configuration Tasks section).
- Have Windows Explorer set to show all files, file types, and extensions (see <u>CT#25</u> in the Configuration Tasks section).
- Install Java Runtime Environment on all the Windows virtual machines (see <u>CT#26</u> in the Configuration Tasks section).
- Turn off screen savers on the Windows virtual machines (see <u>CT#27</u> in the Configuration Tasks section).
- Conduct a ping test between all the machines in your network (see <u>CT#28</u> in the Configuration Tasks section).
- Disable DEP in Windows Server 2022 Virtual Machine (see <u>CT#29</u>)
- Install PuTTY in Windows Server 2022 Virtual Machine (see <u>CT#30</u>)
- Take snapshots of the virtual machines (see <u>CT#31</u> 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 <u>CT#4</u> 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 <u>CT#16</u> in the Configuration Tasks section).

- Install VMware Workstation Pro on the host machine (see <u>CT#5</u> in the Configuration Tasks section).
- Configure a virtual network in the VMware Virtual Network Editor (see <u>CT#6</u> in the Configuration Tasks Section).
- Install guest operating systems (Windows Server 2022 and Windows 11) on VMware Workstation (see <u>CT#7</u> in the Configuration Tasks section).
- Configure the Internet Explorer Enhanced Security Configuration (see <u>CT#8</u> in the Configuration Tasks section).
- Run the IP protocol.
- Install guest operating systems (Ubuntu Suspect and Ubuntu Forensics) on VMware Workstation (see <u>CT#10</u> in the Configuration Tasks section).
- Turn off the firewall on all Windows virtual machines (see <u>CT#11</u> in the Configuration Tasks section).
- Install Windows components in all Windows virtual machines (see <u>CT#12</u> in the Configuration Tasks section).
- Install WinRAR and MS Office on the Windows 11 virtual machine (see <u>CT#13</u> and <u>CT#14</u> in the Configuration Tasks section).
- Create a partition in the Windows 11 virtual machine (see <u>CT#15</u> in the Configuration Tasks section).
- Have CHFI Tools shared as the Z: drive on the Windows and Ubuntu machines (mapping the Z: drive) (see <u>CT#17</u> and <u>CT#18</u> 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 <u>CT#20</u> 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 <u>CT#22</u>, <u>CT#23</u>, and <u>CT#24</u> in the Configuration Tasks section).
- Have Windows Explorer set to show all files, file types, and extensions (see <u>CT#25</u> in the Configuration Tasks section).
- Install Java Runtime Environment on all the Windows virtual machines (see <u>CT#26</u> in the Configuration Tasks section).
- Turn off screen savers on the Windows virtual machines (see <u>CT#27</u> in the Configuration Tasks section).
- Conduct a ping test between all the machines in your network (see <u>CT#28</u> in the Configuration Tasks section).

- Disable DEP in Windows Server 2022 Virtual Machine (see <u>CT#29</u>)
- Install PuTTY in Windows Server 2022 Virtual Machine (see <u>CT#30</u>)
- Take snapshots of the virtual machines (see <u>CT#31</u> 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 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.

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.

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.

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.

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.winrar.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** popup 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]

CT#4: Download the ISO File

- 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 <u>https://www.vmware.com/in/products/workstation-pro/workstation-pro-evaluation.html</u>.

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.

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

🞲 VMware Workstation Pro Setup - 🗆 🗙
Custom Setup Select the installation destination and any additional features.
Install to: C:\Program Files (x86)\VMware\VMware Workstation\ Change
Enhanced Keyboard Driver (a reboot will be required to use this feature) This feature requires 10MB on your host drive.
Back Next Cancel

- 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]

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.

😟 Virtual I	Network Edi	itor			×
Name	Туре	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.98.0
VMnet8	NAT	NAT	Connected	Enabled	192, 168, 109,0
			Add Network	Remove Netv	vork Rename Network
	rmation		, addite the state of the state	center e ricer	Tenane Recordinaria
Bridged	d (connect Vi	Ms directly to the external netv	vork)		
Bridge	d to:	,			Automatic Settings
Contrage					· Automate occurgs
NAT (s	hared host's	IP address with VMs)			NAT Settings
O Host-o	nly (connect	VMs internally in a private net	work)		
Conne	ct a host virt	ual adapter to this network			
Host v	irtual adapte	er name: VMware Network Adap	oter VMnet8		
🗹 Use loo	al DHCP serv	vice to distribute IP address to	VMs		DHCP Settings
Subnet IP:	: 192 . 168	3.109.0 Subnet mas	k: 255.255.255.0	0	
		Administrator privileges are req	uired to modify the net	work configur	ation. Change Settings
Restore De	faults	mport Export	OK Ca	ncel	Apply Help

- 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....

👲 Virtual I	Network Edi	tor				×
Name	Туре	External Connection	Host Connection	DHCP	Subnet Address	
VMnet0	Bridged	Auto-bridging	-	-	-	
VMnet1	Host-only	-	Connected	Enabled	192.168.98.0	
VMnet8	NAT	NAT	Connected	Enabled	10.10.1.0	
Add Network Remove Network Rename Network						
Bridge	d tot	is directly to the external networ	K)		Automatic Sattings	. 1
 NAT (s Host-o 	hared host's	IP address with VMs) VMs internally in a private netwo	k)	(4 NAT Settings	
Connect a host virtual adapter to this network Host virtual adapter name: VMware Network Adapter VMnet8 Use local DHCP service to distribute IP address to VMs DHCP Settings						
Subnet IP: 10 . 10 . 1 . 0 2 Subnet mask: 255 . 255 . 255 . 0 3						
Restore De	faults	nport Export	OK Ca	ancel	Apply Help	

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

NAT Settings	×				
Network: vmnet8 Subnet IP: 10.10.1.0 Subnet mask: 255.255.255.0 Gateway IP: 10 . 10 . 1 . 1					
Host Port Type Virtual Machine IP Address Description Add Remove Properties					
Advanced Allow active FTP Allow any Organizationally Unique Identifier UDP timeout (in seconds): 30 Image: Config port:					
Enable IPv6 IPv6 prefix: fd15:4ba5:5a2b:1008::/64 DNS Settings NetBIOS Settings					
OK Cancel Help					

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

👲 Virtual N	Vetwork Edi	tor				×
Name	Туре	External Connection	Host Connection	DHCP	Subnet Address	
VMnet0	Bridged	Auto-bridging	-	-	-	
VMnet1	Host-only	-	Connected	Enabled	192.168.98.0	
VMnet8	NAT	NAT	Connected	Enabled	10.10.1.0	
Add Network Remove Network Rename Network VMnet Information Open in the second sec						k
Bridged to: Automatic V Automatic Settings						
<u>NAT</u> (shared host's IP address with VMs) NAT <u>S</u> ettings						
O <u>H</u> ost-or	nly (connect	VMs internally in a private networ	k)			
✓ Connect a host virtual adapter to this network Host virtual adapter name: VMware Network Adapter VMnet8 ✓ Use local DHCP service to distribute IP address to VMs DHCP Settings Subnet IP: 10 . 10 . 1 . 0 Subnet IP: 10 . 10 . 1 . 0						
Restore Defaults Import Export OK Cancel Apply Help						

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.

DHCP Settings					×
Network:	vmnet8				
Subnet IP: Subnet mask:	10.10.1.0 255.255.255.0				
Starting IP address:	10 . 10 . 1	. 3			
Ending IP address:	10 . 10 . 1	. 254			
Broadcast address:	10.10.1.255				
	Days:	Hours:		Minutes:	
Default lease time:	1	0	▲ ▼	30	•
Max lease time:	0	2	▲ ▼	0	•
	OK		Cancel	Hel	2

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

👲 Virtual N	Network Edi	tor			×
Name VMnet0 VMnet1 VMnet8	Type Bridged Host-only NAT	External Connection Auto-bridging - NAT	Host Connection - Connected Connected	DHCP - Enabled Enabled	Subnet Address - 192.168.98.0 10.10.1.0
- VMnet Info O <u>B</u> ridged Bridged	rmation d (connect VI d to: Autom	A Ms directly to the external netwo	add N <u>e</u> twork I	Rem <u>o</u> ve Netw	vork Rename Network
● <u>N</u> AT (sl	hared host's nly (connect	IP address with VMs) VMs internally in a private netwo	ork)		NAT <u>S</u> ettings
 ✓ Connect a host virtual adapter to this network Host virtual adapter name: VMware Network Adapter VMnet8 ✓ Use local DHCP service to distribute IP address to VMs DHCP Settings Subnet IP: 10 . 10 . 1 . 0 Subnet mask: 255.255.255.0 					
<u>R</u> estore De	faults Ir	npor <u>t</u> Export	ОК Са	ancel	<u>A</u> pply Help

[Back to Configuration Task Outline]

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.

New Virtual Machine Wizard		×
Guest Operating System Installation A virtual machine is like a physical computer; it ne system. How will you install the guest operating s	eds an ope system?	rating
Install from:		
O Installer disc:		
No drives available	\sim	
O Installer disc image file (iso):		
	~	Browse
• I will install the operating system later.		
The virtual machine will be created with a blank har	d disk.	
Help < Back	Next >	Cancel

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**.

New Virtual Machine Wizard	×
Select a Guest Operating System Which operating system will be installed on this virtual machine?	
Guest operating system Microsoft <u>Windows</u> Linux VMware ES <u>X</u> Other	
Version Windows Server 2019	~
Heip < <u>B</u> ack <u>N</u> ext > C	ancei

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.

New Virtual Machine Wizard			×
Name the Virtual Machine			
What name would you like	to use for this vir	tual machine?	
Virtual machine name:			
Windows Server 2022			
Location:			
1 Carol Descention of the	Windows	Server 2022	Browse
	< Back	Next >	Cancel

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.

New Virtual Machine Wizard X
Specify Disk Capacity How large do you want this disk to be?
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine. Maximum disk gize (GB): 300 300 Recommended size for Windows Server 2016: 60 GB Store virtual disk as a single file Split virtual disk into <u>multiple files</u> Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

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

v Virtual Machin	e Wizard			
Ready to Create Click Finish to Server 2016.	Virtual Mac create the vir	hine tual machine. T	hen you can inst	all Windows
he virtual machine	will be create	ed with the follow	wing settings:	
Name:	Windows Se	erver 2022		
Location:	1.000			
Version:	Workstation	15.x		
Operating System:	Windows Se	erver 2016		
Hard Disk:	300 GB			
Memory:	2048 MB			
Network Adapter:	NAT			
Other Devices:	2 CPU cores	, CD/DVD, USB	Controller, Printe	r, Sound C.
<u>C</u> ustomize Hardw	are			
		< <u>B</u> ack	Finish	Cancel

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.

Hardware				×
Device Memory Conservations Network Adapter Sound Card Printer Display	Summary 2 GB 2 NAT Present Auto detect Present Auto detect Auto detect	Device status Connected Connect at power gn Ouse physical drive: Auto detect @ Use ISO image file: 	· · ·	Browse Adyanced
			Close	Help

- 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.



- 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**.

Virtual Machine Settings	5					×
Hardware Options						
Virtual Machine Settings Hardware Options Settings Su General Wi Power Shared Folders Dis Shared Folders Dis Support AutoProtect Dis Guest Isolation CACcess Control No WWare Tools Tir VNC Connections Dis Unity Appliance View Pautologin No Advanced De	s ummary findows Server 2022 isabled isabled ot encrypted ime sync off isabled ot available efault/Default	Process priorities Input grabbed: Input ungrabbed: The default setting Settings Gather debugging Disable memor Log virtual mad Enable Templa Gather verbose Clean up disks Enable VBS (Vi Firmware type A Changing firm operating syst DISS UEFI Enable gecu File locations Configuration: Log: (N	Default Default gs are specified information: y page trimmi chine progress te mode (to be e USB debuggir after shutting rtualization Ba mware might ca tem to become ure boot	d in Edit Default ng periodic e used fo ng inform down thi ised Secu ause the e unboota	> Preferences > ally or cloning) nation s virtual machinurity) support installed guest able. Windows Serve	 Priority. e
			0	К	Cancel	Help

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



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**.

Microsoft Server Operating System Setup	
Language to install: English (United States) Time and currency format: English (United States)	
Enter your language and other preferences and click "Next" to continue.	
Microsoft Corporation. All rights reserved.	Next

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

Microsoft Server Operating System Setup	
Install now	
<u>R</u> epair your computer	
Microsoft Corporation. All rights reserved.	

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

Operating system	Architecture	Date modified
/indows Server 2022 Standard	х64	And Description
/indows Server 2022 Standard (Desktop Experience)	x64	
/indows Server 2022 Datacenter	х64	and the second
indens server este sourcenter (sestiop experience)		
scription: is option installs the full Windows graphical environment,	, consuming extra di	ive space. It can be
ful if you want to use the Windows desktop or have an ap	p <mark>p that requires it.</mark>	

- 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.

-	G Microsoft Server Operating System Setup
	Which type of installation do you want?
	Upgrade: Install Microsoft Server Operating System and keep files, settings, and applications
	The files, settings, and applications are moved to the new operating system with this option. This option is only available when a supported version of the operating system is already running on the computer.
	<u>Custom: Install Microsoft Server Operating System only (advanced)</u> The files, settings, and applications aren't moved to the new operating system with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

- 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.

Installing Microsoft Server Operating System Status Copying Microsoft Server Operating System files Getting files ready for installation (3%) Installing features Installing updates Finishing up	/stem Setup
Status Copying Microsoft Server Operating System files Getting files ready for installation (3%) Installing features Installing updates Finishing up	er Operating System
Copying Microsoft Server Operating System files Getting files ready for installation (3%) Installing features Installing updates Finishing up	
	perating System files allation (3%)

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**.

<u>U</u> ser name	Administrator			
Password	•••••			
<u>R</u> eenter password		Ŷ		

Lab Setup Guide Page 33

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

23. The machine storts and the lock screen appears; click the Send Ctrl+Alt+Del to this virtual

machine icon	n () from the menu bar.
📴 Windows Server 2022 - VMware Wo	rkstation – 🗆 🗙
<u>Eile E</u> dit <u>V</u> iew V <u>M</u> <u>T</u> abs <u>H</u> elp	
Library X	Home X IF Windows Server 2022 X
My Computer My Computer Mindows Server 2022 Shared VMs	

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.

Try Windows Admin Cen	ter and Azure Arc today
Instead of Server Manager, built into the Azure portal to Azure.	you can use Azure Arc and the new Windows Admin Center manage individual servers and clusters-on-premises and in
With Azure Arc you can see across clouds. You can also lifecycle of your server with	cure and govern Windows Server at scale-on-premises and o automate operations and apply best practices across the Azure Automanage.
Get more info at	aka.ms/ManageWindowsServer

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**.

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.

Settings		- 🗆 X				
命 Home	About					
Find a setting	Your PC is monitored and protected.					
System	indows Security					
🖵 Display	Device specifications					
	Device name	WIN-4G1P1GEL9JQ				
다》) Sound	Processor	Intel(R) Xeon(R) Gold 6262V CPU @ 1.90GHz 1.90 GHz				
Notifications & actions	Installed RAM	16.0 GB				
	Device ID	F8E87299-4673-457D-A06D-88A5EF7D3F20				
2) Focus assist	Product ID	00454-10000-00001-AA217				
(h) Baurar & alasa	System type	64-bit operating system, x64-based processor				
O Power & sleep	Pen and touch	No pen or touch input is available for this display				
📼 Storage	Сору					
년 Tablet	Rename this F	c				
甘 Multitasking	Windows si	pecifications				
Projecting to this PC	Edition	Windows Server 2022 Standard				

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

Rename your PC	
Rename your PC You can use a combination of letters, hyphens, and numbers.	
Current PC name: WIN-4G1P1GEL9JQ	
Server2022 ×	
	Next Cancel

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

Rename your PC	Choose a reason that best describes why you to shut down this computer	ı want
Rename your PC	Other (Unplanned)	~
After you restart, your PC name	Co	ntinue
	Restart now	Restart later

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.

Network and Sharing	Center			- 0	×
← → × ↑ 🔽 «	Network and Internet > Network and Sharing Center	~	Ō	Search Control Panel	P
Control Panel Home Change adapter settir	View your basic network informa View your active networks	ition and se	et up o	connections	
Change advanced sha settings	aring Unidentified network Public network	4	Access t Connect	ype: No network access ions: 🚇 Ethernet	
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.

and the second states			
vetworking			
Connect using:			
Microsoft Hyper	r-V Network Adapter		
. Les and the second se		Conf	igure
This connection uses	the following items:		
Client for Mic	crosoft Networks		~
🗹 😨 File and Print	ter Sharing for Microsof	t Networks	
🗹 🐙 QoS Packet	Scheduler		
Internet Prote	ocol Version 4 (TCP/IP	v4)	
1. 1. 2. 11	twork Adaptor Multiplay	or Protocol	
Microsoft Ne	awork Adapter Multiples	101 1 1010 001	
Microsoft Ne	DP Protocol Driver		
Microsoft Ne	DP Protocol Driver ocol Version 6 (TCP/IP	v6)	~
Image: A second se	DP Protocol Driver ocol Version 6 (TCP/IP	v6)	~
Li ⊥ Microsoft Ne ✓ ⊥ Microsoft LLI ✓ ⊥ Internet Prote < Install	Uninstall	v6) P <u>r</u> op	> eties
Install	Uninstall	v6) P <u>rop</u>	> erties
Install	DP Protocol Driver ocol Version 6 (TCP/IP Uninstall	v6) P <u>rop</u>	erties
Internet Prote Install Description Transmission Contr wide area network	DP Protocol Driver ocol Version 6 (TCP/IP Uninstall ol Protocol/Internet Pro protocol that provides o	v6) <u>Prop</u> stocol. The d	erties lefault on
Install Description Transmission Contr wide area network across diverse inter	DP Protocol Driver ocol Version 6 (TCP/IP Uninstall ol Protocol/Internet Pro protocol that provides o rconnected networks.	v6) P <u>rop</u> stocol. The d	erties lefault on
Install Description Transmission Contra wide area network across diverse inter	DP Protocol Driver ocol Version 6 (TCP/IP Uninstall ol Protocol/Internet Pro protocol that provides o rconnected networks.	v6) P <u>rop</u> stocol. The d	erties lefault on
Internet Prote Install Description Transmission Contra wide area network across diverse inter	DP Protocol Driver ocol Version 6 (TCP/IP Uninstall ol Protocol/Internet Pro protocol that provides o reconnected networks.	v6) Prop tocol. The d	erties lefault on

- 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**.

Internet Protocol Version 4 (TC	P/IPv4) Properties X
General	
You can get IP settings assigne this capability. Otherwise, you for the appropriate IP settings	ed automatically if your network supports need to ask your network administrator omatically
• Use the following IP addre	ess:
IP address:	10 . 10 . 1 . 22
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 10 . 1 . 1
Obtain DNS server addres	ss automatically ver addresses:
Preferred DNS server:	8.8.8.8
Alternate DNS server:	
Validate settings upon ex	kit Ad <u>v</u> anced
	OK Cancel

- 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 \rightarrow Server Manager Properties.

Dashboard Local Server	WELCOME TO SERV	ER MANAGER	Remove Roles and Features Add Servers Create Server Group
All Servers		1 Configure this local server	Server Manager Properties
	QUICK START	2 Add roles and features	
	WHAT'S NEW	3 Add other servers to manage	
		 Connect this server to cloud services 	
	LEARNI MORE		Hide

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.

← Settings	– – ×
	Windows Update *Some settings are managed by your organization (View policies) No updates available We'll continue to check daily for newer updates.
📿 Windows Update	Check for updates
凸 Delivery Optimization	*We'll automatically download and install updates, except on metered connections (where charges may apply). In that case, we'll
Windows Security	automatically download only those updates required to keep Windows running smoothly.
P Troubleshoot	Pause updates for 7 days
츠 Recovery	Visit Advanced options to change the pause period
⊘ Activation	Change active hours Currently 8:00 AM to 5:00 PM
1 For developers	See update history See updates installed on your device

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

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





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

Virtual Machine Settings	5					×
Hardware Options						
Device Memory Processors Hard Disk (SCSI) CD/DVD (SATA) Network Adapter USB Controller USB Controller USB Controller Display	Summary 2 GB 2 250 GB Using file NAT Present Auto detect Present Auto detect	 <u>R</u> emove	Device status ☐ Connected ☑ Connect at power on ⓒ iJse physical drive: Auto detect ○ Use ISO image file:			✓ Browse Advanced
				ОК	Cancel	Help

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.

🕂 Registry Editor					
File Edit View Favorites Help					
Computer\HKEY_LOCAL_MACHINE\SY	STEM\Setup				
Computer KKEY_CLASSES_ROOT KKEY_CURRENT_USER KKEY_CURRENT_USER KKEY_LOCAL_MACHINE KKEY_LOCAL_MACHINE KKEY_LOCAL_MACHINE KKEY_LOCAL_MACHINE CURTY CONTROLOTION CURTATION CURTATIO	Name (Default) (Default) (CmdLine FactoryPreInstall DoLoaderPath Respecialize RestartSetup Setup Type SystemSetupInP WorkingDirectory	Type REG_SZ REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_SZ	Data (value noi winpeshl. 0x0000000 0x0000000 0x0000000 0x0000000	t set) exe D1 (1) D0 (0) D0 (0) D1 (1) ws\panther	
> Softwi Expand		ev			
> HKEY_USER: Find > HKEY_CURR	Si	tring Value			
Delete	B	inary Value			
Rename	D	WORD (32-bit) Value	:		
Export	Q	WORD (64-bit) Value	:		

Lab Setup Guide Page 42

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**.

🔡 Registry Editor				
File Edit View Favorites Help				
Computer\HKEY_LOCAL_MACHINE\SYS	TEM\Setup\LabConfig			
> 📩 HardwareConfig	Name	Туре	Data	
> Keyboard Layout MountedDevices	ab) (Default)	REG_SZ	(value not set)	
> C ResourceManager				
Select				
🗸 🚞 Setup				
> Cart AllowStart				
Pid				
SETUPCL				
> Software				
HKEY_CURRENT_CONFIG				

• Right-click anywhere in the right-pane and navigate to New \rightarrow DWORD (32-bit) Value.

👫 Registry Editor				
File Edit View Favorites Help				
Computer\HKEY_LOCAL_MACHINE\SYS	TEM\Setup\LabConfig			
	Name (Default) New	Type REG_SZ	Data (value not set) Key String Value Binary Value DWORD (32-bit) Value QWORD (64-bit) Value Multi-String Value Expandable String Value	
HKEY_CURRENT_CONFIG				

- 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.

File Edit View Favorites Help	
Computer\HKEY_LOCAL_MACHINE\SYSTEM\Setup\LabConfig	
> HardwareConfig > Keyboard Layout MountedDevices > ResourceManager RNG Select > AllowStart Pid Setup > AllowStart > SetUPCL LabConfig > Software WPA > HKEY_USERS > HKEY_CURRENT_CONFIG	

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

🎬 Registry Editor				
File Edit View Favorites Help				
Computer\HKEY_LOCAL_MACHINE\SYS	TEM\Setup\LabConfig			
> 📩 HardwareConfig	Name	Туре	Data	
> Keyboard Layout	(Default)	REG_SZ	(value not set)	
ResourceManager	BypassCPUCheck	REG_DWORD	0x00000001 (1)	
RNG	BypassTPMCheck	REG_DWORD	0x00000001 (1)	
Select	BypassRAMCheck	REG_DWORD	0x00000001 (1)	
🗸 🚞 Setup	BypassSecureBootCheck	REG_DWORD	0x00000001 (1)	
> 📥 AllowStart				
Pid				
Software				
WPA				
> 🚞 HKEY_USERS				
> THEY_CURRENT_CONFIG				

- 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.
- After completing the installation, Is this the right country or region? wizard appears. Select your country and click Yes.
- Similarly, select the preferred keyboard layout (here, **US**) in the next wizard and click **Yes**.

- 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**.
- o 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]

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.

Server Manager				- 0
😧 🔹 Server Ma	nager • Local Ser	ver	• 🗷 🚩 Manage	<u>T</u> ools <u>V</u> iew <u>H</u> el
Dashboard	PROPERTIES For Server2022			TASKS 🔻
Local Server All Servers File and Storage Services D	Computer name Workgroup	Server2022 WORKGROUP	Last installed updates Windows Update Last checked for updates	Today at 11:37 PM Download updates c Today at 11:38 PM
	Microsoft Defender Firewall Remote management Remote Desiton	Private: On Enabled Disabled	Microsoft Defender Antivirus Feedback & Diagnostics	Real-Time Protection Settings
	NIC Teaming Ethernet Azure Arc Management	Disabled 10.10.1.22, IPv6 enabled Disabled	Time zone Product ID	(UTC-08:00) Pacific T Not activated
	Operating system version Hardware information	Microsoft Windows Server 2022 Standard Microsoft Corporation Virtual Machine	Processors Installed memory (RAM)	Intel(R) Xeon(R) Gole 16 GB

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.

Internet Explorer Enhanced Security Configuration	×
Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.	
Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.	
<u>A</u> dministrators:	
On (Recommended)	
I Off	
Users:	
On (Recommended)	
I ODff	
More about Internet Explorer Enhanced Security Configuration	
OK Cance	1

7. The IE Enhanced Security Configuration will be Off.

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

💺 Server Manager			– 0 ×
Server Ma	anager • Local Server	- (🕄 🚩 Manage Iools View Help
III Dashboard	PROPERTIES For Server2022		TASKS
Local Server All Servers File and Storage Services	Server2022 WORKGROUP	Last installed updates Windows Update Last checked for updates	Today at 11:37 PM Download updates only, using Windows Update Today at 11:38 PM
	ill Private: On Enabled Disabled Disabled	Microsoft Defender Antivirus Feedback & Diagnostics IE Enhanced Security Configuration Time zone	Real-Time Protection: On Settings Off (UTC-08:00) Pacific Time (US & Canada)
	10.10.1.22, IPv6 enabled Disabled	Product ID	Not activated

[Back to Configuration Task Outline]

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.

🖾 Server Manager					(—)	
Server M	lanager • Dashb	poard	• © 🖡	<u>M</u> anage	<u>T</u> ools <u>V</u> iew	<u>H</u> elp
Dashboard Local Server All Servers File and Storage Services	WELCOME TO SERVE	Configure this loca Configure this loca Add roles and featur Add other servers to Create a server grou S Connect this server	Il server res o manage up to cloud services		н	ide

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

Add Roles and Features Wizard	-		×
Before you begin	DESTIN	ATION SER Server2	VER 022
Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	This wizard helps you install roles, role services, or features. You determine which roles, rol features to install based on the computing needs of your organization, such as sharing do hosting a website. To remove roles, role services, or features: Start the Remove Roles and Features Wizard Before you continue, verify that the following tasks have been completed: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The most current security updates from Windows Update are installed If you must verify that any of the preceding prerequisites have been completed, close the complete the steps, and then run the wizard again. To continue, click Next.	e services cuments, wizard,	, or or
	Skip this page by default		
	< Previous Next > Install	Cance	el

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.

1				DESTINA	TION SER	VEF
elect destination	on server				Server2	:02
Before You Begin	Select a server or a	virtual hard dis <mark>k</mark> on whic	h to install roles and features.			
Installation Type	Select a server f	rom the server pool				
Server Selection	O Select a virtual h	nard disk				
Server Roles	Server Pool					
Features						
	Filter:					
	Name	IP Address	Operating System			_
	Server2022	10 10 1 22	Microsoft Windows Server 2	022 Standard		
	1 Computation forum	d				
	This page shows see and that have been newly-added server	u rvers that are running Wi added by using the Add 's from which data collec	ndows Server 2012 or a newer re Servers command in Server Mai tion is still incomplete are not sh	elease of Windo nager. Offline s nown,	ows Serv ervers ar	/er, nd

6. Server Roles section will appear; click Next.

elect server ro	les	DESTINATION SERVER Server2022
Before You Begin Installation Type Server Selection	Select one or more roles to install on the selected server. Roles Active Directory Certificate Services	Description Active Directory Certificate Services
Server Roles Features Confirmation Results	 Active Directory Domain Services Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server Fax Server File and Storage Services (1 of 12 installed) Host Guardian Service Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Access Remote Activation Services Volume Activation Services Web Server (IIS) Windows Server Update Services 	(AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

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.



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.



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

elect role servi	ices	DESTINATION SERVER Server2022
Before You Begin Installation Type	Select the role services to install for Web Server (IIS) Role services	Description
Server Selection Server Roles Features Web Server Role (IIS) Role Services		Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to
Confirmation Results	 HTTP Redirection WebDAV Publishing Health and Diagnostics HTTP Logging Custom Logging Logging Tools ODBC Logging Request Monitor Tracing Performance Static Content Compression Dynamic Content Compression 	create Web-based applications.
	2 3	

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





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.

1	DECTIN		D
nstallation prog	ress	Server2022	2
	View installation progress		
Installation Type	1 Feature installation		
	Installation started on Server2022		
	NET Framework 3.5 Features	1	~
	.NET Framework 3.5 (includes .NET 2.0 and 3.0)		
	.NET Framework 4.8 Features		
	ASP.NET 4.8		
Results	WCF Services		
	Message Queuing (MSMQ) Activation		
	Named Pipe Activation		
	TCP Activation		
	Message Queuing		
	Marcana Olianing Samirae		Y
	You can close this wizard without interrupting running tasks. View task progress or	open this	
	page again by clicking Notifications in the command bar, and then lask Details.		
	Export configuration settings		

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

[Back to Configuration Task Outline]



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.

New Vistoral Marshine Missard	\sim
	^
Guest Operating System Installation	
A virtual machine is like a physical computer; it needs an operating	
system. How will you install the guest operating system?	
Install from:	
◯ Installer <u>d</u> isc:	
No drives available	
Installer disc image file (iso):	
	_
ubuntu-22.04-di v B <u>r</u> owse	
Ubuntu 64-bit 22.04 detected.	
To use Easy Install, insert the first disc of the set.	
○ I will ingtall the operating system later.	
The virtual machine will be created with a blank hard disk.	
Help < <u>B</u> ack <u>Next</u> > Cancel	

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.

New Virtual Machine Wizard	×
Name the Virtual Machine What name would you like to use for this virtual machine?	
Virtual machine name:	
Ubuntu Suspect	
Location:	
Ubuntu Suspect	B <u>r</u> owse
The default location can be changed at Edit > Preferences.	
< <u>B</u> ack <u>N</u> ext >	Cancel

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.

New Virtual	Machine Wizard			×
Specify Die How la	sk Capacity Irge do you want this	s disk to be?		
The virtual ma computer's phy applications, fi Maximum disk Recommended	chine's hard disk is s (sical disk. These file les, and data to your gize (GB): I size for Ubuntu 64- al disk as a single file disk into <u>m</u> ultiple file disk makes it easie but may reduce perfo	tored as one or a(s) start small a virtual machine. 50.0 • bit: 20 GB es er to move the virtual primance with vertices	more files on the nd become large rtual machine to y large disks.	e host r as you add another
Help		< <u>B</u> ack	<u>N</u> ext >	Cancel

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

New Virtual Machin	e Wizard	×
Ready to Create Click Finish to 64-bit.	Virtual Machine create the virtual machine and start installing Ubuntu	
The virtual machine	will be created with the following settings:	
Name:	Ubuntu Suspect	
Location:	Ubuntu Suspect	
Version:	Workstation 15.x	
Operating System:	Ubuntu 64-bit	
Hard Disk:	50 GB	
Memory:	2048 MB	
Network Adapter:	NAT	
Other Devices:	CD/DVD, USB Controller, Printer, Sound Card	
<u>C</u> ustomize Hardw	are	
Power on this vir	tual machine after creation	
	< <u>B</u> ack Finish Can	cel

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

gnu gi	NUB version 2.06	
₩Try or Install Ubuntu Ubuntu (safe graphics) UBM install (for маnufacturers) Test мемогу		
Use the ↑ and ↓ keys to selec Press enter to boot the selec before booting or 'c' for a c The highlighted entry will be e:	t which entry is highlighted. ted 05, 'e' to edit the commands command-line. æcuted automatically in 16s.	

English		
Español		•
Esperanto		
Euskara		
Français		
Gaeilge		
Galego		
Hrvatski		
Íslenska		
Italiano	Try Ubuntu	Install Ubuntu
Kurdî		
Latviski	You can try Ubuntu without making a	any changes to your computer directly from this CD
Lietuviškai	Too can by oboned without making t	any changes to your compater, an easy nom this es.
Magyar	Or if you're ready, you can install Ub	ountu alongside (or instead of) your current operating
Nederlands	system. This shouldn't take too long	g.
No localization (UTF-8)		
Norsk bokmål		

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.

	Install				
Keyboard layout					
Choose your keyboard layout:					
English (Australian) English (Cameroon) English (Ghana) English (Nigeria) English (South Africa) English (UK) English (UK) Esperanto Estonian Faroese Filipino Finnish French	En En En En En En En En	glish (US) glish (US) - CH glish (US) - En glish (US) - En	erokee glish (Colema glish (Colema glish (Colema glish (Dvorak glish (Dvorak glish (Dvorak glish (Dvorak glish (Dvorak glish (Noraa glish (Norma glish (US, Syn	ak) ak-DH ISO) ak-DH) (; (; alt. intl.) (; alt. intl., with dea (; left-handed) (; right-handed) (; right-handed) (; osh) () n) nbolic)	d keys)
Type here to test your keyboard					
Detect Keyboard Layout					
			Ouit	Back	Continue

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.

Undates and other software	
opudes and other software	
What apps would you like to install to start with?	
O Normal installation	
Web browser, utilities, office software, games, and media players.	
O Minimal installation	
Web browser and basic utilities.	
Other options	
Download updates while installing Ubuntu	
Not available because there is no Internet connection.	
Install third-party software for graphics and Wi-Fi bardware and additional media formats	
This software is subject to license terms included with its desumentation. Some is proprietary	
This solume is subject to license terms included with its documentation. Some is proprietary.	
<u>Q</u> uit <u>B</u> ac	k Continue

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

Install	×
Installation type	
This computer currently has no detected operating systems. What would you like to do?	
O Erase disk and install Ubuntu	
Warning: This will delete all your programs, documents, photos, music, and any other files in all operating systems.	
Advanced features None selected	
You can create or resize partitions yourself, or choose multiple partitions for Ubuntu.	
Quit Back Install No	w
$\bullet \bullet \bullet \bullet \bullet \circ \circ$	

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

Write the changes to disks?		×
If you continue, the changes listed below will be written to the disks. further changes manually.	Otherwise, you will	be able to make
The partition tables of the following devices are changed: SCSI3 (0,0,0) (sda)		
The following partitions are going to be formatted: partition #2 of SCSI3 (0,0,0) (sda) as ESP partition #3 of SCSI3 (0,0,0) (sda) as ext4		
	Go Back	Continue

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

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.

	Install	
Who are you?		
Your name: Your computer's name: Pick a username: Choose a password: Confirm your password:	james james-Virtual-Machine The name it uses when it talks to other computers. james Short password Log in automatically Require my password to log in	
	Use Active Directory You'll enter domain and other details in the next step.	Back Continue

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.

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.

		A
4 »)		0
4	Wired Connected	~
	Turn Off	
	Wired Settings	
Φ	Balanced	>
Ø	Settings	
0	Lock	
ധ	Power Off / Log Out	>

Lab Setup Guide Page 62

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

Q Settings =	Network	
③ Network		
Bluetooth	Wired	+
Background	Connected - 10000 Mb/s	
P Appearance	VPN	+
♣ Notifications	Not set up	Ľ.
Q Search		

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.

<u>C</u> ancel	Wired		Apply
Details Identi	ity IPv4 IPv6 Sec	urity	
IPv <u>4</u> Method	O Automatic (DHCP)	O Link-Loc	al Only
2	Manual O Manual	🔘 Disable	
	 Shared to other computing 	ters	
Addresses	0		
Addresses Address	3 Netmask	Gateway	_
Addresses Address 10.10.1.8	3 Netmask 255.255.255.0	Gateway	Ē
Addresses Address 10.10.1.8	3 Netmask 255.255.255.0	Gateway 10.10.1.1	1
Addresses Address 10.10.1.8	3 Netmask 255.255.255.0	Gateway 10.10.1.1	1
Addresses Address 10.10.1.8 DNS	3 Netmask 255.255.255.0	Gateway 10.10.1.1 Automa	atic C
Addresses Address 10.10.1.8 DNS 8.8.8.8.8.8.4.4	3 Netmask 255.255.255.0	Gateway 10.10.1.1 Automa	atic

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



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.

To install or remove	software, you need to
authe	enticate.
	-
-	0
ja	mes
and the second se	۲

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

Software Updater	(_) (×
Installing updates	
	Cancel
Downloading linux-firmware > Details	

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

	Software Updater	1
The computer needs to	o restart to finish installing up	dates.
		-

30. Click the **Show Applications** (iii) 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.

Q termina		Ø
	> Terminal	

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.

Activitie	s 🗈 Terminal			
6				
٥	F	james@james-Virtual-Machine: ~	Q = -	- ×
	james@james-Virtual-M	achine: \$ []		
0				
Â				
?	All Windows >			
>_	New Window Preferences			
	Add to Favorites			
	Quit			
8				

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.



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.

Ħ	james@james-Virtual-Machine: ~	Q	III			×
james@james-Virtual-Ma [sudo] password for ja Reading package lists Building dependency to Reading state informa The following NEW pack net-tools 0 upgraded, 1 newly in Need to get 204 kB of After this operation, Get:1 http://us.archig git20181103.0eebece-10 Fetched 204 kB in 0s Selecting previously of (Reading database Preparing to unpack . Unpacking net-tools (Setting up net-tools (chine: \$ sudo apt-get install net- ames: Done ree Done tion Done kages will be installed: nstalled, 0 to remove and 2 not upg archives. 819 kB of additional disk space wi ve.ubuntu.com/ubuntu jammy/main amd ubuntu5 [204 kB] (443 kB/s) unselected package net-tools. 198772 files and directories curre /net-tools_1.60+git20181103.0eebe 1.60+git20181103.0eebece-1ubuntu5) (1.60+git20181103.0eebece-1ubuntu5) or man-db (2.10.2-1)	raded. ll be 64 net ntly i ce-1ub 	used. -tool nstal untu5	s amd led.) _amd6	64 1. 4.det	60+)

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.

FT.	james@james-Virtual-Machine: ~	Q	W.			×
james eth0:	<pre>@james-Virtual-Machine: \$ ifconfig flags=4163<up,broadcast,running,multicast> mtu 15 inet 10.10.1.8 netmask 255.255.255.0 broadcast inet6 fe80::b02c:1a1c:bbbf:81e9 prefixlen 64 s ether 02:15:5d:41:ca:cf txqueuelen 1000 (Ether RX packets 404 bytes 413583 (413.5 KB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 306 bytes 53956 (53.9 KB) TX errors 0 dropped 0 overruns 0 carrier 0 co</up,broadcast,running,multicast></pre>	500 10.10 scopeid net)	.1.25 0x20 ns 0	5 <link:< td=""><td>></td><td></td></link:<>	>	
lo: f	<pre>lags=73<up,loopback,running> mtu 65536 inet 127.0.0.1 netmask 255.0.0.0 inet6 ::1 prefixlen 128 scopeid 0x10<host> loop txqueuelen 1000 (Local Loopback) RX packets 170 bytes 16014 (16.0 KB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 170 bytes 16014 (16.0 KB) TX errors 0 dropped 0 overruns 0 carrier 0 co</host></up,loopback,running></pre>	ollisio	ns O			
james PING 64 by 64 by 64 by	<pre>@james-Virtual-Machine:-\$ ping www.eccouncil.org www.eccouncil.org (104.18.9.180) 56(84) bytes of da tes from 104.18.9.180 (104.18.9.180): icmp_seq=1 tt tes from 104.18.9.180 (104.18.9.180): icmp_seq=2 tt tes from 104.18.9.180 (104.18.9.180): icmp_seq=3 tt</pre>	ita. :l=58 t :l=58 t :l=58 t	ime=1 ime=7 ime=3	2.3 m .64 m .73 m	5 5 5	

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.

F	james@james-Virt	:ual-Machine: ~	Q				×
james@james-Virt Reading package	ual-Machine:~\$ sudo apt in lists Done	stall git					
Building depender	ncy tree Done						
Reading state in	formation Done						
The following ad git-man liberry	ditional packages will be or-perl	installed:					
Suggested package	es:						
git-daemon-run git-cvs git-me	git-daemon-sysvinit git diawiki git-svn	-doc git-email	git-g	ui git	tk git	tweb	
The following NE	W packages will be install berror-perl	.ed:					
0 upgraded, 3 new	wlv installed. 0 to remove	and 2 not upor	aded.				
Need to get 4.14	7 kB of archives.						
After this opera	tion, 21.0 MB of additiona	l disk space wi	ll be	used.			
Do you want to co	ontinue? [Y/n] Y						
Get:1 http://us.	archive.ubuntu.com/ubuntu	jammy/main amd6	i4 lib	error	perl	all	0.1
7029-1 [26.5 kB]							
Get:2 http://us.	archive.ubuntu.com/ubuntu	jammy-updates/m	nain an	nd64 g	git-ma	an al	l 1
:2.34.1-1ubuntu1	.10 [954 kB]						
Get:3 http://us.	archive.ubuntu.com/ubuntu	jammy-updates/m	nain a	nd64 g	git an	md64	1:2
.34.1-1ubuntu1.1	0 [3,166 kB]						
Fetched 4,147 kB	in 1s (4,996 kB/s)						
Selecting previo	usly unselected package li	berror-perl.					
(Reading databas	e 198821 files and dir	ectories currer	itly i	nstall	led.)		

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.

F	james@james-Virtual-Machine: ~	Q				×
james@james-Vir Reading package Building depend Reading state i The following p libpython2-st python-pkg-re	tual-Machine:-\$ sudo apt install python3 lists Done ency tree Done nformation Done ackages were automatically installed and dlib libpython2.7-minimal libpython2.7-s sources python-setuptools python2 python	-pip are no tdlib 2-minim	o long nal py	er re thon2	quire .7	ed:
Use 'sudo apt a The following a javascript-co libjs-undersc python3-distu Suggested packa	utoremove' to remove them. dditional packages will be installed: mmon libexpat1-dev libjs-jquery libjs-sp ore libpython3-dev libpython3.10-dev pyt tils python3-setuptools python3-wheel py ges:	hinxdoc hon3-de thon3.1	: :v :0-dev	zlib	1g-de	₽V
The following p python-pip The following N javascript-co libjs-undersc python3-distu python3.10-de	ackages will be REMOVED: IEW packages will be installed: IMMon libexpat1-dev libjs-jquery libjs-sp ore libpython3-dev libpython3.10-dev pyt itils python3-pip python3-setuptools pyth ev zlib1g-dev	hinxdoo hon3-de on3-whe	: v el			

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]

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.



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

Windows Defender Firewall			- 0	×	
🗧 🔶 👻 🛧 🔐 🖉 🖉 Syst	em and Secu > Windows Defender Firewall	~ C	Search Control Panel	p	
Control Panel Home	Help protect your PC with Windo	ows Defender Fir	ewall		
Allow an app or feature through Windows Defender	PC through the Internet or a network.	nt hackers of maliciou	is software from gaining access to y	ou	
Firewall Change notification settings	Private networks		Not connected	×	
Turn Windows Defender Firewall on or off	Guest or public networks	3	Connected	^	
Restore defaults	Networks in public places such as airports	or coffee shops			
Advanced settings	Windows Defender Firewall state:	On			
Troubleshoot my network	Incoming connections: Block all connections to apps that are not on the list of allowed apps				
	Active public networks:	T Netwo	rk 2		
	Notification state:	Notify me w blocks a nev	hen Windows Defender Firewall v app		
See also					
Security and Maintenance					
Network and Sharing Center					

 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.

Customize Settings			
- → × ↑	🔗 « Windows Defender Firew » Customize Settings 🛛 🗸 📿	Search Control Panel	م
Cust	omize settings for each type of network		
You c	an modify the firewall settings for each type of network that you use.		
Privat	te network settings		
	Turn on Windows Defender Firewall		
	Block all incoming connections, including those in the list of allowed ap	ops	
	Notify me when Windows Defender Firewall blocks a new app		
8	Turn off Windows Defender Firewall (not recommended)		
Publi	c network settings		
	Turn on Windows Defender Firewall		
	Block all incoming connections, including those in the list of allowed ap	ops	
	Notify me when Windows Defender Firewall blocks a new app		
	Turn off Windows Defender Firewall (not recommended)		
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.



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.

domain.	enavior for when a compu			its corpor	ale
	<u>F</u> irewall state:	Off			~
	Inbound connections		Block (default)	×.
	Outbound connection	IS:	Allow (d	default)	×
	Protected network co	nnections		Customi	ze
Settings					
1	Specify settings that con Defender Firewall behav	trol Windo ior.	ws	<u>C</u> ustomi:	ze
Logging					
	Specify logging settings troubleshooting.	for		Customi	ze

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

lask Manager	
Settings	
File Explorer	
Search	
Run	
Shut down or sign out >	
Deskton	

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.

J Local Group Policy Editor			- 0	×
<u>File Action View Help</u>				
Maintenance Scheduler	📋 Microsoft Defender Antivirus			
Maps MDM Messaging Microsoft account Microsoft Defender Antivirus Microsoft Defender Application Microsoft Defender Exploit Guai Microsoft Edge Microsoft Secondary Authenticc Microsoft User Experience Virtu: NetMeeting OnEDrive Online Assistance OOBE Portable Operating System Presentation Settings	Turn off Microsoft Defender Antivirus Edit <u>policy setting</u> Requirements: At least Windows Vista Description: This policy setting turns off Microsoft Defender Antivirus. If you enable this policy setting, Microsoft Defender Antivirus does not run, and will not scan computers for malware or other potentially unwanted software. If you disable this policy setting.	Setting Client Interface Device Control Exclusions MAPS Microsoft Defender Exploit Guard MpEngine Network Inspection System Quarantine Real-time Protection Remediation Reporting Scan Scan Scurity Intelligence Updates Threats	State	
 Remote Desktop Services RSS Feeds Search Security Center Shutdown Options Smart Card Software Protection Platform Sound Recorder Speech Store Sync your settings Tablet PC Task Scheduler Tenant Restrictions Tenant Restrictions 	Microsoft Defender Antivirus will run regardless of any other installed antivirus product. If you do not configure this policy setting, Windows will internally manage Microsoft Defender Antivirus. If you install another antivirus program, Windows automatically disables Microsoft Defender Antivirus. Otherwise, Microsoft Defender Antivirus will scan your computers for malware and other potentially unwanted software. Enabling or disabling this policy may lead to unexpected or	Allow antimalware service to startup with normal priority Turn off Microsoft Defender Antivirus Configure local administrator merge behavior for lists Turn off routine remediation Control whether or not exclusions are visible to Local Admins. Define addresses to bypass proxy server Define proxy auto-config (,pac) for connecting to the network. Randomize scheduled task times Configure detection for potentially unwanted applications Configure scheduled task times randomization window Allow antimalware service to remain running always Define the directory path to copy support log files	Not configured Not configured	

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.

Turn off Microsoft Defender Antivir	us – D 🗙	
Turn off Microsoft Defender Antivir	us <u>P</u> revious Setting <u>N</u> ext Setting	
O Not <u>Configured</u> Comment:		
<u>Disabled</u>		
Supported on:	At least Windows Vista	h.
Options:	Help:	
	 This policy setting turns off Microsoft Defender Antivirus. If you enable this policy setting, Microsoft Defender Antivirus does not run, and will not scan computers for malware or other potentially unwanted software. If you disable this policy setting, Microsoft Defender Antivirus will run regardless of any other installed antivirus product. If you do not configure this policy setting, Windows will internally manage Microsoft Defender Antivirus. If you install another antivirus program, Windows automatically disables Microsoft Defender Antivirus. Otherwise, Microsoft Defender Antivirus will scan your computers for malware and other potentially unwanted software. Enabling or disabling this policy may lead to unexpected or unsupported behavior. It is recommended that you leave this policy setting unconfigured. 	•
	OK Cancel <u>A</u> pply	ן

15. Microsoft Defender Antivirus is turned off.



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

Local Group Policy Editor		-	
<u>File Action View Help</u>			
🗢 🔿 🔁 📰 🔒 🛛 🖬 🛛 🍸			
Maintenance Scheduler Maps MDM Messaging Microsoft account Microsoft Defender Antivirus Microsoft Defender Application Microsoft Defender Exploit Guai Microsoft Edge Microsoft Secondary Authentica Microsoft User Experience Virtus NetMeeting OneDrive Online Assistance OOBE Portable Operating System Presentation Settings	Microsoft Defender Antivirus Allow antimalware service to remain running always Edit <u>policy setting</u> . Requirements: At least Windows Server 2012, Windows 8 or Windows RT Description: This policy setting allows you to configure whether or not the antimalware service remains running when antivirus and antispyware security intelligence is disabled. It is recommended that this setting remain disabled.	Setting Remediation Security Intelligence Updates Scan Security Intelligence Updates Allow antimalware service to startup with normal priority Allow antimalware service to startup with normal priority Configure local administrator merge behavior for lists Turn off routine remediation Control whether or not exclusions are visible to Local Admins. Define addresses to bypass proxy server Define proxy auto-config (.pac) for connecting to the netwo Define proxy server for connecting to the network	State State Not configured Enabled Not configured Not configured Not configured Not configured Not configured
 Push To Install Remote Desktop Services RSS Feeds Courts 	If you enable this setting, the antimalware service will always remain running even if both antivirus and antispyware security	Annoomize scheduled task times Configure detection for potentially unwanted applications Configure scheduled task times randomization window Allow antimalware service to remain running always	Not configured Not configured Not configured
 Security Center Shutdown Options 	Intelligence is disabled.	E Define the directory path to copy support log files	Not configured

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

Allow antimalwa	re service to remai	n running always		-		×
Allow antimalwa	re service to remai	n running always	Previous Setting	Next Setting		
O Not <u>C</u> onfigured	Comment:					
<u>Disabled</u>						v
	Supported on:	At least Windows Server	2012, Windows 8 or Wind	ows RT		* *
Options:		Help:				
		This pol antimal antispy that this If you remain intellige If you service security service antispy enablec service	icy setting allows you to ware service remains run ware security intelligence s setting remain disabled. I enable this setting, the a running even if both anti ence is disabled. I disable or do not config will be stopped when bot rintelligence is disabled. I will be started if it is set to has started, there will be a ware security intelligence I, the service will remain r will be stopped.	configure whether or ning when antivirus a is disabled. It is recor intimalware service w virus and antispyware ure this setting, the a h antivirus and antisp f the computer is rest o Automatic startup. / a check to see if antiv is enabled. If at least unning. If both are di	not the nd mmended iill always e security ntimalwar yyware tarted, the After the irus and one is isabled, th	e :
			ОК	Cancel	Appl	у

- 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.

Turn off routine remediation	- O X
Turn off routine remediation	Previous Setting <u>N</u> ext Setting
 Not <u>Configured</u> Comment: <u>Enabled</u> 	
O <u>D</u> isabled Supported on:	At least Windows Vista
Options:	Help:
	This policy setting allows you to configure whether Microsoft Defender Antivirus automatically takes action on all detected threats. The action to be taken on a particular threat is determined by the combination of the policy-defined action, user-defined action, and the signature-defined action. If you enable this policy setting, Microsoft Defender Antivirus does not automatically take action on the detected threats, but prompts users to choose from the actions available for each threat. If you disable or do not configure this policy setting, Microsoft Defender Antivirus automatically takes action on all detected threats after a nonconfigurable delay of approximately five seconds.
	OK Cancel Apply



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.



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

Turn off real-time protection	— 🗆 X
Turn off real-time protection	Previous Setting Next Setting
○ Not <u>C</u> onfigured Comment:	
<u>D</u> isabled Supported on:	
	At least Windows Vista
Options:	Help:
	This policy setting turns off real-time protection prompts for known malware detection. Microsoft Defender Antivirus alerts you when malware or potentially unwanted software attempts to install itself or to run on your computer. If you enable this policy setting, Microsoft Defender Antivirus will not prompt users to take actions on malware detections. If you disable or do not configure this policy setting, Microsoft Defender Antivirus will prompt users to take actions on malware detections.
	OK Cancel Apply

23. Close all windows.

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

Windows Terminal (Admin)
Task Manager
Settings
File Explorer
Search
Run
Shut down or sign out
Desktop

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.



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.



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



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 abovementioned items, click the Home icon in the left menu bar.





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.



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.





- 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]



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.

Local Group Policy Editor Eile Action View Help			- 0	×
 Sound Recorder Speech Store Store Store Store Store Tablet PC Task Scheduler Text Input Windows Calendar Windows Color System Windows Color System Windows Defender SmartScreen Windows Hello for Business Windows Intaller Windows Intaller 	Windows Update Configure Automatic Updates Edit policy setting Requirements: Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3 Option 7 only supported on servers of at least Windows Server 2016 edition Description: Specifies whether this computer will receive security updates and other important downloads through the Windows utomatic	Setting Windows Update for Business Do not display 'Install Updates and Shut Down' option in Sh Do not adjust default Option to 'Install Updates and Shut Down' Enabling Windows Update Power Management to automati Turn off auto-restart for updates during active hours Specify active hours range for auto-restarts Allow updates to be downloaded automatically over metere Always automatically restart at the scheduled time Specify dealline before auto-restart for update installation Configure auto-restart reminder notifications for updates Turn off auto-restart reminder notification for updates	State Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured	
 Windows Logon Options Windows Media Digital Rights Manage Windows Media Player Windows Media Player Windows Media Player Windows Media Player Windows Reliability Center Windows Remote Shell Windows Remote Shell Windows Sandbox Windows Sandbox Windows Supdate Windows Update Work Folders Windows Settings Software Settings Windows Settings Mindows Settings Mindows Settings Mindows Settings Windows Settings Windows Settings Windows Settings 	updating service. Note: This policy does not apply to Windows RT. This setting lets you specify whether automatic updates are enabled on thic computer, if the service is enabled, you must select one of the four options in the Group Policy Setting: 2 = Notify before downloading and installing any updates. When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any	Compare sub-result required nonincation to updates Compare Automatic Updates Specify deadlines for automatic update service location Automatic Updates detection frequency Do not allow update deferral policies to cause scans against Remove access to "Pause updates" feature Remove access to use all Windows Update Internet locations Allow non-administrators to receive update notifications Specify Engaged restart transition and notification schedule Do not include drivers with Windows Updates Turn on Software Notifications Allow Automatic Updates immediate installation Turn on recommended updates via Automatic Updates No auto-restart with logged on users for scheduled automat Re-prompt for restart with scheduled installations Specify Internet for scheduled installations	Not configured Not configured	>

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



- 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.



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.



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

Scan all downloaded files and attac	hments				×
Scan all downloaded files and attac	hments	Previous Setting	Next Setting		
○ Not <u>C</u> onfigured Comment:					^
) <u>E</u> nabled					
Disabled Supported on:	At least Windows Server	2012, Windows 8 or Windov	vs RT		°
)ptions:	Help:				
	This poi downlo lf you downlo If you and atta	licy setting allows you to co aded files and attachments I enable or do not configure aded files and attachments I disable this setting, scanni achments will be disabled.	nfigure scanning fo e this setting, scann will be enabled. ing for all download	or all ing for al led files	H.
		ОК	Cancel	Арр	ly

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]

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]

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.

፼ <u></u> <u> </u>
Best match
Create and format hard disk partitions Control panel
🔎 create and format hard disk partitions 🛛 🗮 💽 🥫

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.

T Disk Managemen	Help								- 6	7	×
	11 🥦 🗙 🖟] 🔒 📙 🖂									
Volume	Layout	Туре	File System	Status	Capacity	Free Spa	% Free				-
(C:)	Simple	Basic	NTFS	Healthy (B	299.29 GB	283.30 GB	95 %				
- (Disk 0 partition 3)	Simple	Basic		Healthy (R	627 MB	627 MB	100 %				
— yinin kente	Simple	bure		ricencity (2.2			0,10				
Disk 0 Basic 300.00 GB	System Reserv 00 MB NTFS	ed	(C:) 299.29 GB N	ITFS	ante Dama Dai			627 MB			
CD-ROM 0 DVD (D:)	Healthy (System	n, Active, Prima	Healthy (Bo	ot, Page File, Cr	ash Dump, Prir	nary Partition)		Healthy (Recovery Parti	ition)		_
No Media											

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

📅 Disk Managen	ient								-	٥	×
File Action \	'iew Help										
(+ - + 💼 🚺	🗖 🕅 🏓 🗯 🗱	2 🛃 🎜 🖸]								
Volume	Layout	Туре	File System	Status	Capacity	Free Spa	% Free				-
= (C:)	Simple	Basic	NTFS	Healthy (B	299.29 GB	283.30 GB	95 %				
🛥 (Disk 0 partitio	n 3) Simple	Basic	1000	Healthy (R	627 MB	627 MB	100 %				
- System Reserv	ed Simple	Basic	NTFS	Healthy (S	100 MB	67 MB	67 %				
- Disk 0											
Basic 300.00 GB	System Reserve	/ed	(C:) 200 20 GB N	ITES							
Online	Healthy (Syster	n, Active, Prim	a Healthy (Bo	ot, Page File, Cr	rash Dump, Prir	nary Partition)		Open Explore	(ר		
CD-ROM 0								Mark Partition as Active			
DVD (D:)								Change Drive Letter and Paths			
No Media								Format			
								Extend Volume			
								Shrink Volume			
								Add Mirror			
								Delete Volume			
Unallocated	Primary partition							Properties			
- successed	Pertition	S									1

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.

Shrink C:	×
Total size before shrink in MB:	306470
Size of available shrink space in MB:	290051
Enter the amount of space to shrink in MB;	250000
Total size after shrink in MB:	56470
You cannot shrink a volume beyond the point v See the "defrag" event in the Application log fo operation when it has completed.	where any unmovable files are located. or detailed information about the
See "Shrink a basic volume" in Disk Managem	ent help for more information
	Shrink Cancel

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

📅 Disk Managemen	t							- 0 ×
<u>File</u> <u>Action</u> <u>Viev</u>	w <u>H</u> elp							
(+ +) 🖬 🛛	🇊 🗯 🗶 📝	🔒 😡 🛛						
Volume	Layout	Туре	File System	Status	Capacity	Free Spa	% Free	
- (C:)	Simple	Basic	NTFS	Healthy (B	55.15 GB	39.17 GB	71 %	
- (Disk 0 partition 3)) Simple	Basic	672860	Healthy (R	627 MB	627 MB	100 %	
- System Reserved	Simple	Basic	NIFS	Healthy (S	100 MB	67 MB	67 %	
- Disk 0 Basic	System Recenzed	((-)						
300.00 GB Online	100 MB NTFS Healthy (System, A	55.15 c Healt	GB NTFS hy (Boot, Page Fil	e, Crash Dump,	Primary Partil	244.14 GB Unallocated		627 MB Healthy (Recovery Partition)
CD-ROM 0 DVD (D:)								
No Media								
-								
Unallocated P	rimary partition							

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

		1									
		1	ſ	-				1			
/olume	Layout	Туре	File System	Status	Capacity	Free Spa	% Free				
(C:)	Simple	Basic	NTFS	Healthy (B	55.15 GB	39.17 GB	71 %				
(Disk 0 partition	3) Simple	Basic	LUTTO .	Healthy (R	627 MB	627 MB	100 %				
Disk 0 asic 00.00 GB Inline	System Reserve 100 MB NTFS Healthy (System,	d (C:) 55.1 Ac Heal	5 GB NTFS thy (Boot, Page Fi	ile, Crash Dump,	, Primary Partil	244.14 GB Unallocated		New Simple Volur	627 M	1B	ition
Disk 0 Basic 00.00 GB Dnline	System Reserve 100 MB NTFS Healthy (System,	d (C:) 55.1 Ac Heal	5 5 GB NTFS Ithy (Boot, Page Fi	ile, Crash Dump,	Primary Partil	244.14 GB Unallocated		New Simple Volur New Spanned Vol	627 M me	18 Decovery Parti	ition
Disk 0 Jasic 300.00 GB Online CD-ROM 0 DCD.(0)	<mark>System Reserve</mark> 100 MB NTFS Healthy (System,	d (C:) 55,11 Ac Heal	5 GB NTFS thy (Boot, Page Fi	ile, Crash Dump,	Primary Partit	244.14 GB Unallocated		New Simple Volur New Spanned Vol New Striped Volu	627 M me Iume me	18 Tecovery Parti	ition
Disk 0 lasic 00.00 GB Inline CD-ROM 0 IVD (D:)	System Reserve 100 MB NTFS Healthy (System,	d (C:) 55.1 Ac Heal) 5 GB NIFS thy (Boot, Page Fi	ile, Crash Dump,	, Primary Partil	244.14 GB Unallocated		New Simple Volur New Spanned Vol New Striped Volu New Mirrored Vol	627 M me lume me	18 Becovery Parti	ition
Disk 0 asic D0.00 GB inline CD-ROM 0 VD (D:) Io Media	System Reserve 100 MB NTFS Healthy (System,	d (C:) 55.1 Heal) 5 GB NTFS tthy (Boot, Page Fi	ile, Crash Dump,	, Primary Partit	244.14 GB Unallocated		New Simple Volur New Spanned Vol New Striped Volu New Mirrored Vol New RAID-5 Volu	627 M me uume me uume	18 ecovery Parti	ition
Disk 0 Jasic 00.00 GB Online CD-ROM 0 VVD (D:) Vo Media	System Reserve 100 MB NTFS Healthy (System,	d (C:) 55.1 Heal) 5 GB NTFS tthy (Boot, Page Fi	ile, Crash Dump,	. Primary Partil	244.14 GB Unallocated		New Simple Volur New Spanned Vol New Striped Volur New Mirrored Vol New RAID-5 Volur Properties	627 M me me me me	1B ecovery Parti	ition

Lab Setup Guide Page 96

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.

New Simple Volume Wizard	×
Specify Volume Size	
Choose a volume size that is betwee	n the maximum and minimum sizes.
Maximum disk space in MB:	249999
Minimum disk space in MB:	8
<u>S</u> imple volume size in MB:	249999
	< Back Next > Cancel

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**.

New Simple Volume Wizard	×
Assign Drive Letter or Path	
For easier access, you can assign a drive letter or drive path to your partition.	
Assign the following drive letter	
<u>M</u> ount in the following empty NTFS folder:	
Browse	
O Do not assign a drive letter or drive path	
< <u>B</u> ack Next> (Cancel

Lab Setup Guide Page 97

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.

New Si	mple Volume Wizard			×
For	nat Partition To store data on this partition, yo	u must format it <mark>first</mark> .		
)	Choose whether you want to fom	nat this volume, and if s	o, what settings you war	it to use.
	O Do not format this volume			
	Format this volume with the	e following settings:		
	<u>Hie system:</u>	NIFS	~	
	Allocation unit size:	Default	~	
	<u>V</u> olume label:	New Volume		
	Perform a quick form	at		
	Enable file and folde	r compression		
-				
		< <u>B</u> ack	<u>N</u> ext >	Cancel

- 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.

📪 Disk Managem	ent							-	đ	×
<u>File Action V</u>	iew <u>H</u> elp									
🗇 🏟 📅 🛛 😰	🛅 🏓 🗹									
Volume	Layout	Туре	File System	Status	Capacity	Free Spa	% Free			_
- (C:)	Simple	Basic	NTFS	Healthy (B	55.15 GB	39.17 GB	71 %			
- (Disk 0 partition	a 3) Simple	Basic		Healthy (R	627 MB	627 MB	100 %			
- New Volume (E	:) Simple	Basic	NTFS	Healthy (L	244.14 GB	244.04 GB	100 %			
- System Reserve	d Simple	Basic	NTFS	Healthy (S	100 MB	67 MB	67 %			
	1									
- Disk 0										
- Disk 0 Basic	System Reserv	ed (C:)				New Volume	• (E:)			_
- Disk 0 Basic 300.00 GB Opline	System Reserv 100 MB NTFS	ed (C:) 55.15	GB NTFS	ile Creek Durre	Duine an Dentil	New Volume 244.14 GB NT	e (E:) FS	 627 MB		
- Disk 0 Basic 300.00 GB Online	System Reserv 100 MB NTFS Healthy (System	ed (C:) 55.15 h, Ac Heal	GB NTFS thy (Boot, Page Fi	ile, Crash Dump,	Primary Partif	New Volume 244.14 GB NT Healthy (Log	• (E:) FS ical Drive)	 627 MB Healthy (Red	covery Part	tition)
- Disk 0 Basic 300.00 GB Online	System Reserv 100 MB NTFS Healthy (System	ed (C:) 55.15 Heal	GB NTFS thy (Boot, Page Fi	ile, Crash Dump,	Primary Partif	New Volume 244.14 GB NT Healthy (Log	e (E:) FS ical Drive)	627 MB Healthy (Re	covery Part	tition)
- Disk 0 Basic 300.00 GB Online	System Reserv 100 MB NTFS Healthy (System	ed (C:) 55.15 Heal	GB NTFS thy (Boot, Page Fi	ile, Crash Dump,	Primary Partit	New Volume 244,14 GB NT Healthy (Log	e (E:) FS ical Drive)	627 MB Healthy (Re	covery Part	tition)
Disk 0 Basic 300.00 GB Online CD-ROM 0 DVD (D:)	System Reserv 100 MB NTFS Healthy (System	ed (C:) 55.15 Heal	GB NTFS thy (Boot, Page F	ile, Crash Dump,	Primary Partil	New Volume 244.14 GB NT Healthy (Log	e (E:) FS ical Drive)	627 MB Healthy (Ree	covery Part	iition)
Disk 0 Basic 300.00 GB Online CD-ROM 0 DVD (D2)	System Reserv 100 MB NTFS Healthy (System	ed (C:) 55.15 Heal	GB NTFS thy (Boot, Page F	ile, Crash Dump,	Primary Partil	New Volume 244.14 GB NT Healthy (Log	e (E-) FS ical Drive)	627 MB Healthy (Re	covery Part	tition)
Disk 0 Basic 300.00 GB Online CD-ROM 0 DVD (D:) No Media	System Reserv 100 MB NTFS Healthy (System	ed (C:) 55,15 , Ac Heat	GB NTFS hy (Boot, Page Fi	ile, Crash Dump,	Primary Partil	New Volume 244.14 GB NT Healthy (Log	e (E:) FS ical Drive)	627 M8 Healthy (Re	covery Part	tition)
Disk 0 Basic 300.00 GB Online CD-ROM 0 DVD (D:) No Media	System Reserv 100 MB NTF5 Healthy (System	ed (C:) 55.15 Heat	GB NTFS thy (Boot, Page Fi	ile, Crash Dump,	Primary Partil	New Volum 244.14 GB NT Healthy (Log	e (E:) FS ical Drive)	627 MB Healthy (Re	covery Part	tition)
Disk 0 Basic 300.00 GB Online CD-ROM 0 DVD (D:) No Media	System Reserv 100 MB NTFS Healthy (System	ed (C:) 55.15 Heat	GB NTFS thy (Boot, Page Fi	ile, Crash Dump,	Primary Partil	New Volume 244.14 GB NT Healthy (Log	• (E:) FS ical Drive)	627 MB Healthy (Re	covery Part	tition)
Disk 0 Basic 300.00 GB Online CD-ROM 0 DVD (D:) No Media	System Reserv 100 MB NTFS Healthy (System	ed (C:) 55.15 Heat	GB NTFS ihy (Boot, Page Fi	ile, Crash Dump,	Primary Partit	New Volume 244.14 GB NT Healthy (Log	e (E:) FS ical Drive)	627 MB Healthy (Re	covery Part	tition)
Disk 0 Basic 300.00 GB Online CD-ROM 0 DVD (D:) No Media	System Reserv 100 MB NTFS Healthy (System	ed (C.) 55.15 h, Ac	GB NTFS thy (Boot, Page Fi	ile, Crash Dump,	Primary Partif	New Volum 244.14 GB NT Healthy (Log	e (E:) FS ical Drive)	627 M8 Healthy (Re	covery Part	tition)
Disk 0 Basic 300.00 GB Online CD-ROM 0 DVD (D:) No Media	System Reserv 100 MB NTFS Healthy (System	ed (C:) 55.15 Heat	GB NTFS thy (Boot, Page F	ile, Crash Dump,	Primary Partil	New Volum 244.14 GB NT Healthy (Log	a (E:) FS ical Drive)	627 MB Healthy (Re	covery Part	tition)
Disk 0 Basic 300.00 GB Online CD-ROM 0 DVD (D:) No Media Unallocated	System Reserv 100 MB NTFS Healthy (System	ed (C:) 55.15 Heal	GB NTFS thy (Boot, Page F	ile, Crash Dump,	Primary Partit	New Volum 244.14 GB NT Healthy (Log	e (E:) FS ical Drive)	627 MB Healthy (Re	covery Part	tition)

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

[Back to Configuration Task Outline]

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]

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.

CHFI	-Tools Pro	operties			×
ieneral	Sharing	Security	Previous Versions	Customize	
Netwo Netwo Not S	ork File and CHFI- Not Sh ork Path: Shared	d Folder Sh Tools nared	aring		
Advar Set c advar	hare Inced Shari ustom perm nced shari Advance	ng nissions, cr ng options. d Sharing	eate multiple shares	s, and set other	
Passv Peop comp To ch	vord Protec le must har uter to acc nange this	ction ve a user a cess shared setting, use	iccount and passwo d folders. e the <u>Network and S</u>	ord for this Sharing Center.	
		0	IK Cano	el App	N

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

- 📓 Network access	
Choose people to share with	
Type a name and then click Add, or click the an	row to find someone.
Everyone	<u>∼</u> <u>A</u> dd
Name	Permission Level
🔏 Administrator	Read/Write 💌
Administrators	Owner
I'm having trouble sharing	
	Share Cancel

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

Choose people to share with				
Type a name and then click Add, or click the arrow to find	someone.			
		~	Add	
Name	Permissi	on Le	evel	1
🙎 Administrator	Read/Wr	ite		
Administrators	Owner			
🤽 Everyone	Read 🔻	~	Read	
			Read/Wr	ite
			Remove	
'm having trouble sharing				

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

pe a name and then click Add, or click the	arrow to find someone.
	∼ <u>A</u> dd
Name	Permission Level
🙎 Administrator	Read/Write 🔻
Administrators	Owner
Everyone	Read/Write 🔻

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.

2 Network access	
Your folder is shared.	
You can <u>e-mail</u> someone links to these shared items, or <u>copy</u> and paste the links into another app.	
Individual Items	^
CHFI-Tools \\SERVER2022\CHFI-Tools	
Show me all the network shares on this computer.	
	ne

9. Close the CHFI-Tools Properties window.

CHFI	-Tools Pro	operties			×
General	Sharing	Security	Previous Versions	Customize	
Netwo	ork File and	l Folder Sł	naring		
	CHFI-	Fools H			
Netwo	ork Path:				
\\SE	RVER202	2\CHFI-To	ols		
<u></u>	hare				
Advar	nced Shari	na			
Set ci advar	ustom pern nced shari	nissions, ci ng options	reate multiple shares	, and set other	
6	Advance	d Sharing.			
Passw	vord Protec	ction			
Peopl	e must ha uter to acc	ve a user a cess share	account and passwo d folders.	rd for this	
To ch	ange this	setting, us	e the <u>Network and S</u>	haring Center.	
		Cle	ose Cance	App.	ly.

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



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.

Advanced sharing settings	-	ð X
\leftrightarrow \rightarrow \checkmark \Uparrow \blacksquare > Control	ol Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings 🗸 🧿 Search Control Panel	م
	Change sharing options for different network profiles Windows creates a separate network profile for each network you use. You can choose specific options for each profile. Private (current profile) Network discovery When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. Turn on network discovery Turn on network discovery Tile and printer sharing When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network. Turn off le and printer sharing Turn off lie and printer sharing Guest or Public	
	Guest or Public	
	All Networks	
Advanced sharing settings		ō ×
Advanced sharing settings ← → → ↑ ■ → Contr	ol Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings v 👌 Search Control Pane	۵ × ۶
Advanced sharing settings ← → → ↑ ▲ > Contr	ol Panel → Network and Internet → Network and Sharing Center → Advanced sharing settings v ♂ Search Control Pane Change sharing options for different network profiles	א ס ק
Advanced sharing settings ← → → ↑ ■ > Contr	ol Panel → Network and Internet → Network and Sharing Center → Advanced sharing settings v ♂ Search Control Pane Change sharing options for different network profiles Windows creates a separate network profile for each network you use. You can choose specific options for each profile.	ס X א
Advanced sharing settings ← → ← ↑ ■ > Contr	DI Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings Image: Search Control Panel Change sharing options for different network profiles Windows creates a separate network profile for each network you use. You can choose specific options for each profile. Private (current profile) Image: Search Control Panel Image	۵ X م
Advanced sharing settings ← → → ↑ ▲ → Contr	bil Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings Image: Search Control Panel Change sharing options for different network profiles Windows creates a separate network profile for each network you use. You can choose specific options for each profile. Private (current profile) Image: Search Control Panel Imag	D X
Advanced sharing settings ← → → ↑ ▲ → Contr	bil Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings Image: Search Control Panel Change sharing options for different network profiles Windows creates a separate network profile for each network you use. You can choose specific options for each profile. Private (current profile) Guest or Public Image: Search Control Panel 	X 10 م
Advanced sharing settings ← → → ↑ ■ > Contr	bil Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings Search Control Panel Change sharing options for different network profiles Windows creates a separate network profile for each network you use. You can choose specific options for each profile. Private (current profile) Guest or Public Network discovery 	X ات م
Advanced sharing settings ← → ← ↑ ■ > Contr	bil Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings change sharing options for different network profiles Windows creates a separate network profile for each network you use. You can choose specific options for each profile. Private (current profile) Guest or Public Network discovery When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.	۵ X م
Advanced sharing settings ← → ← ↑ ■ > Contr	bil Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings change sharing options for different network profiles Windows creates a separate network profile for each network you use. You can choose specific options for each profile. Private (current profile) Guest or Public Network discovery When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.	۵ X م
Advanced sharing settings ← → → ↑ ■ > Contr	bil Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings Change sharing options for different network profiles Windows creates a separate network profile for each network you use. You can choose specific options for each profile. Private (current profile) Guest or Public Network discovery When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. Image: Turn on network discovery Turn off network discovery	X ات م
Advanced sharing settings ← → → ↑ ■ > Contr	bil Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings Change sharing options for different network profiles Windows creates a separate network profile for each network you use. You can choose specific options for each profile. Private (current profile) Guest or Public Network discovery When network discovery is on, this computer can see other network computers and devices and is visible to other network discovery Turn on network discovery Turn off network discovery File and printer sharing When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network. Turn on file and printer sharing	X ات م
Advanced sharing settings ← → → ↑ ■ > Contr	bl Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings Change sharing options for different network profiles Windows creates a separate network profile for each network you use. You can choose specific options for each profile. Private (current profile) Guest or Public Network discovery When network discovery is on, this computer can see other network computers and devices and is visible to other network discovery Turn on network discovery Turn off network discovery File and printer sharing When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network. I urn on file and printer sharing O turn off leand printer sharing	X ال م

Advanced sharing settings	<u></u>	×
$\leftarrow \rightarrow \checkmark \uparrow$ 🗖 « Network and Sharing Cen » Advanced sharing settings 🗸 👌		Q
Private (current profile)		-
Guest or Public	$ \odot$	
All Networks		
Public folder sharing		
When Public folder sharing is on, people on the network, including homegroup memb access files in the Public folders.	ers, can	
Turn on sharing so anyone with network access can read and write files in the P	ublic folders	
 Turn off Public folder sharing (people logged on to this computer can still acce folders) 	ss these	
Media streaming		
When media streaming is on, people and devices on the network can access pictures, r videos on this computer. This computer can also find media on the network.	nusic, and	
Choose media streaming options		
3		
Password protected sharing	?	
Password protected sharing When password protected sharing is on, only people who have a user account and pass computer can access shared files, printers attached to this computer, and the Public fo other people access, you must turn off password protected sharing.	word on this ders. To give	
Password protected sharing When password protected sharing is on, only people who have a user account and pass computer can access shared files, printers attached to this computer, and the Public fo other people access, you must turn off password protected sharing.	word on this ders. To give	

- 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.

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

File Explorer	K 0 6 0 0		View ~ ···		- 0	>
→ • ↑	📌 > Quick access >		~ C	, Search Quick access		
🐈 Quick access	V Folders (7)					
🛄 Desktop 🞍 Downloads	Desktop This PC	This PC	ads	This PC		
Document	Expand					
Evidence F	Open in new window Pin to Quick access					
1 Music 1 Videos	☆ Pin to Start					
🌰 OneDrive	Properties A	After you've opened	some files, we'll show the mo	ost recent ones here,		
This PC	E) Ū					

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

Tile Explorer				- 0 ×
🕀 New ~ 🔥		11. Sort ~ 8= View ~ ···		
$\leftarrow \rightarrow \ \cdot \ \uparrow$	🚖 🔸 Quick access 🔹	~	C Search Quick access	
✓ ★ Quick access	v Folders (6)			
🛅 Desktop 🛓 Downloads	Desktop This PC	Downloads This PC	Documents This PC	
Documents Pictures	Pictures This PC	This PC	Videos This PC	
🕖 Music	✓ Recent files (0)			
Videos		After you've opened some files, we'll sho	w the most recent ones here.	
> 📥 OneDrive	Expand			
This PC	Manage Pin to Start			
> 🦢 Network	Map network drive			
	Open in new window			
	Pin to Quick access			
	Disconnect network drive			
	Add a network location			
	Delete Rename			
	Properties			

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

What n	etwork folder would you like to map?	
Constitute	a drive latter for the compatible and the folder that you want to compate the	
specify th	le drive letter for the connection and the folder that you want to connect to:	
Drive:	Z: ~	
F <u>o</u> lder:	\\SERVER2022\CHFI-Tools	
	Example: \\server\share	
	<u>Reconnect at sign-in</u>	
	Connect using different <u>c</u> redentials	
	Connect to a Web site that you can use to store your documents and pictures.	

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.

3
SERVER2022
Cancel

🖵 This PC		
⊕ New ~ 🛛 🔏 🔲 🙃	E]	8- View ~ •••
\leftarrow \rightarrow \checkmark \uparrow \blacksquare > This PC	~ C > ~	Search This PC
> 🐈 Quick access	✓ Folders (6) Desktop	Documents
> 📮 This PC	Downloads	Music
> 🖆 Network	Pictures	Videos
	> Devices and drives (4)	
	~ Network locations (1)	
	CHFI-Tools (\\SERVER2022) 189 GB free of 244 GB	(Z:)

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
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

	<u>-1</u> 1	/ㅁ\	×
Notepad Cannot find the C:\Windows\system32\simple_file1.txt:secret_file1.txt file. Do you want to create a new file?			
Yes No			

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.

ADS Files			9	Undo		- 0 X
⊕ New ~ 🔏 🔲 🛅	E] 🖄 🗍 î↓ Sort	✓ ■ View ✓	%	Cut		
← → ∽ ↑ 🛅 « CHFI-Tool	s (\\SERVER2022) (Z:) > Evidence Files >	ADS Files	Ø	Сору		4
> 🖕 Quick access	Name	Date modified	ſ	Paste		
> 📥 OneDrive	secret_file1.txt	10/27/2023 4:29 A	⑩	Delete		
🗸 🛄 This PC	secret_file2.txt	10/2//2023 4:29 AM	100) 100)	Select all		- п х
> Desktop	File Edit View	× +		Right-to-left reading order		\$
 Documents University Downloads 	We are going to mount la world in the upcoming mo	3 arge-scale cyber a onths. The first s	\wedge	Insert Unicode control characters	>	across the MNCs. The
> 🕖 Music > 🛃 Pictures	target cities for these	attacks will be c	9	Reconversion		ssage.
> 🚺 Videos						
> 🖳 Local Disk (C:)						
> 🕳 Forensic Disk (F:)						
CHFI-Tools (\\SERVER2022) (Z						
> 🛬 Network						

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

simple_file1.txt:secret_file1	txt • + - O X
File Edit View	¢
New tab Ctrl	$^{ m N}$ -scale cyber attacks targeting global business hubs across the world in the upcoming months. The
New window Ctrl+Shift	tacks will target MNCs. The target cities for these attacks will be disclosed to you in the next \sim
Open Ctrl	.0
Save Ctr	+5
Save as Ctrl+Shift	+5
Save all Ctrl+Alt	-S
Page setup	
Print Ctrl	+P
Close tab Ctrl-	w
Close window Ctrl+Shift-	w
Exit	

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.

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.

	-	×
Notepad		
Cannot find the C:\Windows\system32\simple_file2.txt:secret_file2.txt file.		
Do you want to create a new file?		
Yes No		

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.

ADS Files			9	Undo		- 0	×
⊕ New ~ 🔏 📮 🛅	E] @ ₪ ↑↓ Sort ①	~ ≣ View ~ ···	%	Cut			
← → → ↑ ¹ CHFI-Too	Is (\\SERVER2022) (Z:) \rightarrow Evidence Files \rightarrow	ADS Files \sim	O	Сору		4	
> 🖕 Quick access	Name	Date modified	Ô	Paste			
> OneDrive	secret_file1.txt	10/27/2023 4:29 AM	⑩	Delete			
✓	secret_hile2.txt	10/27/2023 4:29 AM	(00) (00)	Select all			×
> 🛄 Desktop	secret_file2.txt	× +		Right-to-left reading order			6
> Documents	File Edit View	3		Show Unicode control characters			205
> 🛓 Downloads	Lo******* and Pa****** b month.	based MNCs will be 1	\wedge	Insert Unicode control characters	>	in the	next
> 👩 Music			C	Reconversion			
> 🔀 Pictures							
> 🔝 Videos							
> 🏪 Local Disk (C:)							
> 🕳 Forensic Disk (F:)							
> CHFI-Tools (\\SERVER2022) (Z							
> 🎦 Network							_

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

simple_file2.tx	tt:secret_file2.txt	• + -	O	×
File Edit Vie	w			63
New tab	Ctrl+N	J MNCs will be the first victims of our cyber attacks in the next month.		
New window	Ctrl+Shift+N			
Open	Ctrl+O			
Save	Ctrl+S			
Save as	Ctrl+Shift+S			
Save all	Ctrl+Alt+S			
Page setup				
Print	Ctrl+P			
Close tab	Ctrl+W			
Close window	Ctrl+Shift+W			
Exit				

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.

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.

📕 sir	ple_file1.txt	• +		-	×
File E	dit View				¢
This fi	le is meant to deceive	you!			

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**.





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.

	simple_f	ile2.txt		×	+	-	×
File	Edit	View					ŵ
This	file is	s meant	to deceive	you!			

- 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.

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.

< > ☐ Home				: Q	目	> Ξ (.	-) (¤) (x
③ Recent★ Starred	Desktop	Documents	Downloads	Music	Pictures	Public	snap
∰ Home	<u>I</u> II	B					
Desktop	Templates	Videos					
Documents							
Downloads							
Л Music							
Pictures							
□ Videos							
💼 Trash							
🝙 Floppy Disk							
+ Other Locations							

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.

$\langle \rangle$ + Other L	ocations	: Q		0		×
① Recent	On This Computer					
* Starred	Computer		15.8 GB / 31.0 GB ava	ilable	/	
습 Home	Networks					_
Desktop	Windows Network					
Documents						
Downloads						
♫ Music						
Pictures						
日 Videos						
🛅 Trash						
🝙 Floppy Disk						
+ Other Locations						_
	Connect to Server	smb://10.10.1.22	0	~	Con <u>n</u> e	ect

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.

Authentica Enter user a Jsername	nd password for "10.10.1.22":
Enter user a <u>J</u> sername	nd password for "10.10.1.22":
Jsername	
	Administrator
<u>D</u> omain	WORKGROUP
<u>P</u> assword	
🔿 Forget p	bassword <u>i</u> mmediately
Remem	ber password until you logout
O Rememi	ber <u>f</u> orever
	Domain Password Forget p Rememi

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

〈 〉 / Windows share	res on 10.10. <mark>1</mark> .2	2		: Q	IE ~			×
C Recent								
* Starred	ADMIN\$	C\$	CHFI-Tools	E\$	Users			
슈 Home								
Desktop								
Documents								
<u>⊕</u> Downloads								
🎵 Music								
Pictures								
🖽 Videos								
💼 Trash								
🝙 Floppy Disk								
+ Other Locations								
						"CHFI-Too	ols" s <mark>e</mark> le	cted

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

Chfi-tools of the second se	on 10.10.1.22			: Q	E	~ ≡ .	- • ×
🕚 Recent							
★ Starred	CHFlv11	CHFIv11 Module 02	CHFIv11 Module 03	CHFIv11 Module 04	CHFIv11 Module 05	CHFIv11 Module 06	CHFIv11 Module 07
습 Home	Prerequi	Compute	Understa	Data Acq	Defeatin	Windows	Linux and
🖸 Desktop							
Documents	CHFIv11 Module 08	CHFIv11 Module 09	CHFIv11 Module 10	CHFIv11 Module 11	CHFIv11 Module 12	CHFIv11 Module 13	CHFIv11 Module 14
$\underline{\oplus}$ Downloads	Network	Malware	Investiga	Dark We	Cloud Fo	Email an	Mobile F
♫ Music							
Pictures	Evidence Files						
🖽 Videos							
💼 Trash							
跓 chfi-tools on 🔺							
🖬 Floppy Disk							
C chfi-tools on 10.1							

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.

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.

	Create and format hard disk partition Control panel	s	
Sear	ch the web		Create and format hard disk partitions
Q	disk management - See more search results	>	Control panel
Q	disk management windows 11	>	🖸 Open
Q	disk management .exe	>	
Q	disk management tool	>	
Q	disk management app	>	
Q	disk management administrator	>	
Q	disk management windows 10	>	
Q	disk management utility	>	
Q	disk management program	>	



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

Volume	Layout	Type	File System	Status	Capacity	Free Spa	% Free		
 (C:) (Disk 0 partition System Reserved 	Simple Simple Simple	Basic Basic Basic	NTFS	Healthy (B Healthy (R Healthy (S	79.35 GB 613 MB 50 MB	53.90 GB 613 MB 19 MB	68 % 100 % 38 %	Open	
								Explore Mark Partition as Active Change Drive Letter and Paths Format Extend Volume Shrink Volume Add Mirror Delete Volume	
- Disk 0 Basic 80.00 GB Online	System Reser 50 MB NTFS Healthy (Syste	ved m, Active, Prir	(C:) 79.35 GB NTFS Healthy (Boot	. Page File, Cras	h Dump, Primar	y Partition)		Properties Help Heartny (kecovery Partition)	
CD-ROM 0 DVD (D:) No Media			1						

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.

Shrink C:	×
Total size before shrink in MB:	81254
Size of available shrink space in MB:	55143
Enter the amount of space to shrink in MB:	30000
Total size after shrink in MB:	51254
You cannot shrink a volume beyond the po See the "defrag" event in the Application lo operation when it has completed.	oint where any unmovable files are located. og for detailed information about the
See "Shrink a basic volume" in Disk Mana	gement help for more information

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

	ent							- 0
<u>File Action V</u> i	iew <u>H</u> elp							
🔶 🔿 📰 👔	📼 💌 🖻 🖡	<u>,</u>						
Volume	Layout	Type F	File System	Status	Capacity	Free Spa	% Free	
- (C:)	Simple	Basic M	NTFS	Healthy (B	50.05 GB	24.61 GB	49 %	
- (Disk 0 partition	n 3) Simple	Basic	1750	Healthy (R	613 MB	613 MB	100 %	
- System Reserve	d Simple I	Basic P	NIFS	Healthy (S	50 MB	19 MB	38 %	
						2		
- Disk 0								
Disk 0 Basic 80.00 GB	System Reserved	(C:)	TTEC			20.20 CP		 613 MP
Disk 0 Basic 80.00 GB Online	System Reserved 50 MB NTFS Healthy (System, A	(C:) 50.05 GB N Healthy (Bo	ITFS oot, Page File, C	rash Dump, F	Primary Partition)	29.30 GB Unallocate	d	 613 MB Healthy (Recovery Partition)
Disk 0 Basic 80.00 GB Online	System Reserved 50 MB NTFS Healthy (System, A	(C:) 50.05 GB N Healthy (Bo	ITFS oot, Page File, C	rash Dump, F	Primary Partition)	29.30 GB Unallocate	d	 613 MB Healthy (Recovery Partition)
Disk 0 Basic 80.00 GB Online	System Reserved 50 MB NTFS Healthy (System, A	(C:) 50.05 GB N Healthy (Bo	ITFS oot, Page File, C	rash Dump, F	Primary Partition)	29.30 GB Unallocate	d	613 MB Healthy (Recovery Partition)
Disk 0 Basic 80.00 GB Online	System Reserved 50 MB NTFS Healthy (System, A	(C:) 50.05 GB N Healthy (Bo	ITFS oot, Page File, C	Trash Dump, F	Primary Partition)	29.30 GB Unallocate	d	613 MB Healthy (Recovery Partition)
Disk 0 Basic 80.00 GB Online	System Reserved 50 MB NTFS Healthy (System, A	(C:) 50.05 GB N Healthy (Bo	ITFS oot, Page File, C	Trash Dump, F	Primary Partition)	29.30 GB Unallocate	d	613 MB Healthy (Recovery Partition)
Disk 0 Basic 80.00 GB Online DVD (D:) No Media	System Reserved 50 MB NTFS Healthy (System, A	(C:) 50.05 GB N Healthy (Bo	ITFS oot, Page File, C	irash Dump, F	Primary Partition)	29.30 GB Unallocate	d	613 MB Healthy (Recovery Partition)
Disk 0 Basic 80.00 GB Online CD-ROM 0 DVD (D:) No Media	System Reserved 50 MB NTFS Healthy (System, A	(C:) 50.05 GB N Healthy (Bo	ITFS oot, Page File, C	irash Dump, F	Primary Partition)	29.30 GB Unallocate	d	 613 MB Healthy (Recovery Partition)
Disk 0 Basic 80.00 GB Online CD-ROM 0 DVD (D:) No Media	System Reserved 50 MB NTFS Healthy (System, A	(C:) 50.05 GB N Healthy (Bo	ITFS oot, Page File, C	Trash Dump, F	Primary Partition)	29.30 GB Unallocate	d	613 MB Healthy (Recovery Partition)
Disk 0 Basic Boxic CD-ROM 0 DVD (D:) No Media	System Reserved 50 MB NTFS Healthy (System, A	(C:) 50.05 GB N Healthy (Bo	ITFS coot, Page File, C	ïrəsh Dump, F	Primary Partition)	29.30 GB Unallocate	d	613 MB Healthy (Recovery Partition)
Disk 0 Basic 80.00 GB Online CD-ROM 0 DVD (D:) No Media	System Reserved 50 MB NTFS Healthy (System, A	(C.) 50.05 GB N Healthy (Br	ITFS oot, Page File, C	Trash Dump, F	Primary Partition)	29.30 GB Unallocate	d	613 MB Healthy (Recovery Partition)
Disk 0 Basic 80.00 GB Online CD-ROM 0 DVD (D-) No Media	System Reserved 50 MB NTFS Healthy (System, A	(C:) 50.05 GB N Healthy (Br	ITFS oot, Page File, C	Trash Dump, F	Primary Partition)	29.30 GB Unallocate	d	613 MB Healthy (Recovery Partition)

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

Disk Managem	ent							8	- 0	
e Action V	iew Help									_
🔿 🕅 🖬										
olume	Layout 1	Type File System	Status	Capacity	Free Spa	% Free				
(C:)	Simple E	Basic NTFS	Healthy (B	50.05 GB	24,61 GB	49 %				
(Disk 0 partition	3) Simple E	Basic	Healthy (R	613 MB	613 MB	100 %				
System Reserve	d Simple E	Sasic NTES	Healthy (S	20 MB	19 MB	38 %				
Disk 0										
asic 0.00 GB	System Reserved	(C:) 50.05 GB NTES			29 30 GB			613 MB		
nline	Healthy (System, A	Healthy (Boot, Page File	e, Crash Dump, F	rimary Partition)	Unallocate	d ////////////////////////////////////	New Simple V	olume	y Partitio	n)
							New Seanned	Volume		
3					-		New Spanned			-
CD-ROM 0							New Striped v	olume		
10 (0:)							New Mirrored	Volume		
o Media							New RAID-5 V	olume		
							Properties			
							Help			

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

Specify Volume Size Choose a volume size that is betwee	en the maximum and minimum sizes.
Maximum disk space in MB: Minimum disk space in MB: <u>S</u> imple volume size in MB:	29999 8 10000
	< Back Next > Cancel

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.

New Simple Volume Wizard	×
Assign Drive Letter or Path For easier access, you can assign a drive letter	or drive path to your partition.
Assign the following drive letter: <u>Mount in the following empty NTFS folder:</u>	F v
O Do not assign a drive letter or drive path	
	< <u>B</u> ack <u>N</u> ext > Cancel

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.

New Simple Volume Wizard			×
Format Partition			
To store data on this partition, yo	u must format it first.		
Choose whether you want to fom	nat this volume, and if s	o, what settings you wa	nt to use.
O Do not format this volume			
• Format this volume with the	e following settings:		
<u>F</u> ile system:	NTFS	~	
<u>Allocation unit size:</u>	Default	~	
<u>V</u> olume label:	Forensic Disk		
Seriom a quick form	at		
Enable file and folde	r compression		
	< <u>B</u> ack	<u>N</u> ext >	Cancel

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

Completing the New Simple Volume Wizard	
You have successfully completed the New Simple Volume Wizard.	
Volume type: Simple Volume Disk selected: Disk 0 Volume size: 10000 MB Drive letter or path: F: File system: NTFS Allocation unit size: Default Volume label: Forensic Disk Quick format: Yes	
To close this 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.

	Layout	Type	File System	Status	Capacity	Free Spa	% Free	1	
(C:)	Simple	Basic	NTFS	Healthy (B	50.05 GB	24.61 GB	49 %		
(Disk 0 partition	3) Simple	Basic		Healthy (R	613 MB	613 MB	100 %		
Forensic Disk (F:) Simple	Basic	NTFS	Healthy (L	9.77 GB	9.73 GB	100 %		
System Reserved	d Simple	Basic	NTFS	Healthy (S	50 MB	19 MB	38 %		
- Disk 0					Enropeic Die	L. (E.)		10.52.50	1.111
Disk 0 Basic 00.00 GB Dnline	System Resei 50 MB NTFS Healthy (Syste	(C:) 50.05 GB N Healthy (Be	TFS pot, Page File, Cra	sh Dump, Prim	9.77 GB NTF9 Healthy (Log	ical Drive)		Free space	613 MB Healthy (Recovery Partit
Disk 0 Basic 80.00 GB Online CD-ROM 0 DVD (D:)	System Reset 50 MB NTFS Healthy (Syste	(C:) 50.05 GB N Healthy (Be	TFS pot, Page File, Cra	sh Dump, Prim	9.77 GB NTFS Healthy (Log	ical Drive)		Free space	613 MB Healthy (Recovery Partit
Disk 0 Basic Basic Control Co	System Reset 50 MB NTFS Healthy (Syste	(C:) 50.05 GB N Healthy (Be	TFS bot, Page File, Cra	sh Dump, Prim	9.77 GB NTFS Healthy (Log	ical Drive)		Free space	613 MB Healthy (Recovery Partit

- 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....

Volume	Lavout	Type	File System	Status	Canacity	Free Sna	% Free		
- (C:)	Simple	Basic	NTFS	Healthy (B	50.05 GB	24,61 GB	49 %		
- (Disk 0 partition 3	Simple	Basic		Healthy (R	613 MB	613 MB	100 %		
- Forensic Disk (F:)	Simple	Basic	NTFS	Healthy (L	9.77 GB	9.73 GB	100 %		
System Reserved	Simple	Basic	NTFS	Healthy (S	50 MB	19 MB	38 %		
- Disk 0									
Disk 0 Basic 80.00 B	iystem Resei	(C.)			Forensic Disk	(F:)		N 155 750	
Disk 0 Basic 80.00 GB Online	iystem Reser 0 MB NTFS Healthy (Syste	(C:) 50.05 GB N Healthy (B	ITFS oot, Page File, Cra	sh Dump, Prim	Forensic Disk 9.77 GB NTFS Healthy (Logic	(F:) al Drive)		19.53 GB Free space	New Simple Volume
Disk 0 Basic 80.00 GB Online	iystem Rese i 0 MB NTFS Healthy (Syste	(C:) 50.05 GB N Healthy (B	ITFS oot, Page File, Cra	sh Dump, Prim	Forensic Disk 9.77 GB NTFS Healthy (Logic	(F:) al Drive)		19.53 GB Free space	New Simple Volume New Spanned Volume
Disk 0 Basic 80.00 GB Online	i ystem Rese i 0 MB NTFS fealthy (Syste	(C:) 50.05 GB N Healthy (B	ITFS Doot, Page File, Cra	sh Dump, Prim	Forensic Disk 9.77 GB NTFS Healthy (Logic	(F:) al Drive)		19.53 GB Free space	New Simple Volume New Spanned Volume New Striped Volume
Disk 0 Basic 80.00 GB Online CD-ROM 0 DVD (Dc)	iystem Rese i 0 MB NTFS Healthy (Syste	(C:) 50.05 GB N Healthy (B	TFS oot, Page File, Cra	sh Dump, Prim	Forensic Disk 9.77 GB NTFS Healthy (Logic	(F:) al Drive)		19.53 GB Free space	New Simple Volume New Spanned Volume New Striped Volume New Mirrored Volume
Disk 0 Basic 80.00 GB Online CD-ROM 0 DVD (D:) No Media	i ystem Rese i 0 MB NTFS Healthy (Syste	(C:) 50.05 GB N Healthy (B	TFS oot, Page File, Cra	sh Dump, Prim	Forensic Disk 9.77 GB NTFS Healthy (Logic	(F:) al Drive)		19.53 GB Free space	New Simple Volume New Spanned Volume New Striped Volume New Mirrored Volume New RAID-5 Volume
Disk 0 Basic 80.00 GB Online CD-ROM 0 DVD (D:) No Media	i ystem Rese i 0 MB NTFS Healthy (Syste	(C;) 50.05 GB N Healthy (B	ITFS oot, Page File, Cra	sh Dump, Prim	Forensic Disk 9.77 GB NTFS Healthy (Logic	(F-) al Drive)		19.53 GB Free space	New Simple Volume New Spanned Volume New Striped Volume New Mirrored Volume New RAID-5 Volume Delete Partition

- 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.

in the maximum and minimum sizes.
19998
8
19998
////

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.

New Simple Volume Wizard	×
Assign Drive Letter or Path For easier access, you can assign a drive letter	r or drive path to your partition.
 Assign the following drive letter: Mount in the following empty NTFS folder: Do not assign a drive letter or drive path 	G v Browse
	< <u>B</u> ack <u>N</u> ext > Cancel

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.

New Simple Volume Wizard			×
Format Partition To store data on this partition, you	u must format it first.		
Choose whether you want to form	at this volume, and if	so, what settings you wa	int to use.
O Do not format this volume			
• Format this volume with the	e following settings:		
<u>F</u> ile system:	NTFS	~	
Allocation unit size:	Default	~	
<u>V</u> olume label:	To be Removed		
Perform a quick form	at		
Enable file and folder	compression		
	< <u>B</u> ac	< <u>N</u> ext >	Cancel

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

Completing the New Simple Volume Wizard
You have successfully completed the New Simple Volume Wizard. You selected the following settings:
Volume type: Simple Volume Disk selected: Disk 0 Volume size: 19998 MB Drive letter or path: G: File system: NTFS Allocation unit size: Default Volume label: To be Removed Quick format: Yes
To close this wizard, <mark>cl</mark> ick 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.

File Action View	Help	5							
Volume	Lavout	Type	File System	Status	Capacity	Free Spa	% Free	1	
- (C:)	Simple	Basic	NTES	Healthy (B.,	50.05 GB	24.61 GB	49 %		
- (Disk 0 partition 3)	Simple	Basic		Healthy (R.,	613 MB	613 MB	100 %		
- Forensic Disk (F:)	Simple	Basic	NTFS	Healthy (L	9.77 GB	9.73 GB	100 %		
- System Reserved	Simple	Basic	NTFS	Healthy (S	50 MB	19 MB	38 %		
To be Removed (G:)	Simple	Basic	NTFS	Healthy (L	19.53 GB	19.47 GB	100 %		
= Disk 0					1		1		1
Basic Sy 80.00 GB 50 Online H	Stem Rese MB NTFS ealthy (Syste	(C:) 50.05 GB N Healthy (Be	TFS oot, Page File, Cra	ish Dump, Prim	Forensic Di 9.77 GB NTF Healthy (Lo	sk (F:) S gical Drive)		To be Removed (G:) 19.53 GB NTFS Healthy (Logical Drive)	613 MB Healthy (Recovery Partition
CD-ROM 0 DVD (D:)								1	
No Media									

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.

- → · ↑ ,	■ → This PC → To be Removed (G:) →		v C p	Search To be Removed (G:)	
• Ouick accord	Name	Date modified	Туре	Size	
Darlitan d	🔁 Audio Files	10/19/2023 2:58 AM	File folder		
Desktop y	📁 Image Files	10/19/2023 2:55 AM	File folder		
Downloads	📁 Outlook Files	10/19/2023 2:56 AM	File folder		
Documents a	🚬 Songs	10/19/2023 2:56 AM	File folder		
Pictures 🥖	Text Files	10/19/2023 2:56 AM	File folder		
Evidence Files	📁 Wireshark Sample Capture Files	10/19/2023 2:57 AM	File folder		
🕖 Music	Compressed_files.rar	10/19/2023 2:50 AM	RAR File	113 KB	
Videos	Confidential	10/19/2023 2:50 AM	Microsoft Edge P	114 KB	
OneDrive	Expense sheet.xlsx	10/19/2023 2:50 AM	XLSX File	14 KB	
This PC	Flowers	10/19/2023 2:50 AM	JPG File	51 KB	
4	Infected	10/19/2023 2:48 AM	Office Open XML	520 KB	
Metwork	Infected	10/19/2023 2:50 AM	Application	214 KB	
	infected	10/19/2023 2:49 AM	Microsoft Edge P	7 KB	
	👼 Infected	10/19/2023 2:50 AM	Compressed (zipp	393 KB	
	C Legal_Disclaimer	10/19/2023 2:50 AM	Microsoft Edge H	25 KB	
	💼 MultiplePages	10/19/2023 2:50 AM	Microsoft Edge P	2 KB	
	Sample Text Document	10/19/2023 2:50 AM	Text Document	1 KB	

22. Close the window.

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.

Create and format hard disk partition Control panel	S	
Search the web		Create and format hard disk partitions
Ø disk management - See more search results	>	Control panel
Ø disk management windows 11	>	C2 Open
,O disk management.exe	>	
Ø disk management tool	>	
O disk management app	>	
Ø disk management administrator	>	
D disk management windows 10	>	
Ø disk management utility	>	
Ø disk management program	>	

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

Disk Managemen File Action View	t Holp						_			- 0	×
	5 Help	3 🔒 😡	5 c								- 1
Volume	Layout	Type	File System	Status	Capacity	Free Spa	% Free				- 1
- (C:)	Simple	Basic	NTFS	Healthy (B	50.05 GB	24.23 GB	48 %				-
- (Disk 0 partition 3) Simple	Basic		Healthy (R	613 MB	613 MB	100 %				
- Forensic Disk (F:)	Simple	Basic	NTFS	Healthy (L	9.77 GB	9.73 GB	100 %				
- System Reserved	Simple	Basic	NTFS	Healthy (S	50 MB	19 MB	38 %				
To be Removed (0	5:) Simple	Basic	NTFS	Healthy (L	19.53 GB	19.47 GB	100 %				
- Disk 0 Basic 80.00 GB Online	System Rese i 50 MB NTFS Healthy (Syste	(C:) 50.05 GB N Healthy (Be	TFS oot, Page File, Cra	sh Dump, Prim	Forensic Di 9.77 GB NTF Healthy (Lo	sk (F:) S gical Drive)		To be Removed (G:) 19.53 GB NTFS Healthy (Logical Drive)	Open	613 MB Healthy (Recovery	/ Partiti
CD-ROM 0									Explore		
DVD (D:)									Change Drive	Letter and Paths	
No Media									Format		
									Extend Volum	1e	- 1
									Shrink Volum	e	
									Add Mirror		_
									Delete Volum	e	
									Properties		1
								Acti	vallepWind	lows	
		E Catal			of and an			Go to	Settings to a	activate Window	S.
Unallocated	rimary partition	Extende	a partition 📕 Free	e space 📘 Logi	cai drive	_	_		and the second second second		-

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

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**.

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.

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.

General	View	Search					
Folde	er view:	3					
		You can a all folders	apply this vie of this type.	w (such	as Details	or lcons) t	0
-		Apply	to Folders		Reset F	olders)
Adver		tinget					
Auvan		ungs.	a hatwaan it		na nativiou	2	-
	Dicel	ease space	e between it	ems (cor	ipact view	12	
		au file icon	on thumbra	ile			
	Displ	ay file icon av file size i	on thumbna information i	ils n folder t	ins		T
	Displ	ay file icon ay file size i ay the full p	on thumbna information i bath in the tit	ils n folder t le bar	ips		
	Displ Displ Displ Hidd	ay file icon ay file size i ay the full p en files and	on thumbna information i bath in the tit d folders	ils n folde <mark>r t</mark> le bar	ips		
	Displ Displ Displ Hidd	ay file icon ay file size i ay the full p en files and Don't show	on thumbna information i path in the tit folders hidden files,	ils n folder t le bar folders,	ips or <mark>d</mark> rīves		
	Displ	ay file icon ay file size i ay the full p en files and Don't show Show hidde	on thumbna information i path in the tit d folders hidden files, en files, folde	ils n folder t le bar folders, rs, and c	ips or drīves Irives		
	Displ Displ Hidd	ay file icon ay file size i ay the full p en files and Don't show Show hidde empty drive	on thumbna information in both in the tit d folders hidden files, en files, folde es	ils n folder t le bar folders, rs, and c	ips or drīves Irives		
	Displ Displ Hidd O [O S Hide	ay file icon ay file size i ay the full p en files and Don't show Show hidde empty drive extensions	on thumbna information in path in the tit d folders hidden files, en files, folde es s for known f	ils n folder t le bar folders, rs, and c ile types	ips or drives Irives		
	Displ Displ Hidd Hidd Hide Hide	ay file icon ay file size i ay the full p en files and Don't show Show hidde empty drive extensions folder merc	on thumbna information in both in the tit d folders hidden files, an files, folde es s for known fi ge conflicts	ils n folder t le bar folders, rs, and c ile types	ips or drives Irives	and ad	
	Displ Displ Hidd O [Hide Hide Hide Hide	ay file icon ay file size i ay the full p en files and Don't show Show hidde empty drive extensions folder merc protected ch folder w	on thumbna information in both in the tit d folders hidden files, en files, folde es s for known f ge conflicts operating sy vindows in a	ils n folder t le bar folders, rs, and c ile types stem file:	ips or drives Irives (Recommendation	ended)	
	Displ Displ Displ Hidd O [O S Hide Hide Hide Laun	ay file icon ay file size i ay the full p en files and Don't show Show hidde empty drive extensions folder merc protected ch folder w	on thumbna information i both in the tit d folders hidden files, en files, folde es s for known fi ge conflicts operating sy vindows in a	ils n folder t le bar folders, rs, and c ile types stem file separate	ips or drives Irives (Recomments process	nended)	
	Displ Displ Displ Hidd O I O S Hide Hide Hide Hide Laur	ay file icon ay file size i ay the full p en files and Oont show Show hidde empty drive extensions folder merc protected ch folder w	on thumbna information in bath in the tit d folders hidden files, en files, folde es s for known fi ge conflicts operating sy vindows in a	ils n folder t le bar folders, rs, and c ile types stem file separate	ips or drives lrives) s (Recomment e process Rest	rended)	ts
	Displ Displ Displ Hidd Hide Hide Hide Hide Laur	ay file icon ay file size i ay the full p en files and Oont show Show hidde empty drive extensions folder merc protected ch folder w	on thumbna information in bath in the tit d folders hidden files, en files, folde es s for known f ge conflicts operating sy vindows in a	ils n folder t le bar folders, rs, and c ile types stem file separate	ips or drives lrives) s (Recomme e process Rest	iended)	ts

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.

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.

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.

Settings	- 0 ×
ඟි Home	Background
Find a setting	
Personalization	
🖾 Background	
Colors	Aa
Ca Lock screen	
🖆 Themes	
AA Fonts	Background V
器 Start	
🖵 Taskbar	Choose your picture
	Browse
	Choose a fit
	Fill ×

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

Settings		0	×
Home	Lock screen Background Picture		
Personalization			
점 Background 양 Colors			
Ca Lock screen	Browse		
ළු Themes	Choose one app to show detailed status on the lock screen		
A Fonts	+		
器 Start			
🛱 Taskbar	Choose which apps show quick status on the lock screen		
	Screen timeout settings 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.

	ings		
reen Saver			
	an faith ann faith ann an tha ann ann an tha ann ann ann ann ann ann ann ann ann a		
		10	
2		10	
Screen saver	× 5e	tings	Preview
Screen saver (None) Wait: 1	✓ Set	tings	Pre <u>v</u> iew een
Screen saver (None) Wait 1 ÷	✓ Set	tings play logon scr	Pre <u>v</u> iew een
Screen saver (None) Wait: 1 Power managen Conserve energy brightness and d	✓ Set minutes □ On resume, dis nent y or maximize performance by other power settings.	tings play logon scr adjusting disp	Preyiew een olay
Screen saver (None) Wait: 1 ↓ Power managen Conserve energy brightness and o Change power s	Set minutes On resume, dis nent y or maximize performance by other power settings. 	tings play logon scr r adjusting disp	Pre <u>v</u> iew een blay

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

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.
- Check for a reply from the virtual machines. Here, as an example, we are using the Windows

 virtual machine with the IP address 10.10.1.11 (this IP address may be different in your lab network).



- 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).

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

- 1. Click Start \rightarrow Control Panel \rightarrow 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**.

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 $(\overset{(P)}{\frown})$ 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.

Windows Server 2022 - Take Snapshot X	
Taking a snapshot lets you preserve the state of the virtual machine so that you can return to the same state later.	
<u>N</u> ame:	Windows Server 2022 Snapshot 1
Description:	
Take Snapshot Cancel	

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

End of the Document



EC-Council Official Curricula