





Certified Threat Intelligence Analyst v2

CLASSROOM LAB SETUP GUIDE

EC-Council Official Curricula

Table of Contents

Classroom Setup Instructions: CTIAv2	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	
Classroom Configuration	
Computer Names	
Network Topology	
CTIA VM Setup on Instructor and Student Machines	
Instructor Acceptance	
Firewall Settings	
Blackboard	14
Setup Checklist	14
Instructor Acceptance	
Assistance	
Detailed Setup Instructions - Configuration Tasks (CT)	
CT#1: Install the Host Operating System	
CT#2: Copy the Host Operating System Files	
CT#3: Install WinRAR on Host Operating System	
CT#4: Download the ISO File	
CT#5: Install VMware Workstation Pro on Host Machine	
CT#6: Configure a Virtual Network in VMware Virtual Network Editor	
CT#7: Install Windows 11 Virtual Machine in VMware	24
CT#8: Create a Partition in the Windows 11 Virtual Machine	

CT#9: Install Parrot Security Virtual Machine in VMware	51
CT#10: Turn Off Windows Defender Firewall on the Windows 11 Virtual Machine	.64
CT#11: Configure Windows Components on the Windows 11 Virtual Machine	.82
CT#12: Install WinRAR on the Windows 11 Virtual Machine	.86
CT#13: Install MS Office on the Windows 11 Virtual Machine	.86
CT#14: Download CTIA Tools on the Windows 11 Virtual Machine	.86
CT#15: Adding .NET Framework in the Windows 11 Virtual Machine	.87
CT#16: Install Java Runtime Environment and Java Development Kit in the Windows 11 Virtual Machine	.87
CT#17: Share and Map CTIA-Tools Folder to Parrot Security Virtual Machine	.88
CT#18: Install Adobe Acrobat Reader DC on the Windows 11 Virtual Machine	.93
CT#19: Install Web Browsers on the Windows 11 Virtual Machine	.94
CT#20: Install WinPcap on the Windows 11 Virtual Machine	.94
CT#21: Turn Off Screen Savers on the Windows 11 Virtual Machine	.94
CT#22: Ping Test Among Both Virtual Machines	.97
CT#23: Take Snapshots of Virtual Machines	.99

Classroom Setup Instructions: CTIAv2

This document contains setup instructions for the EC-Council Certified Threat Intelligence Analyst (CTIA) 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 threat intelligence methodology, which includes collection, analysis, reporting, and dissemination of intelligence. 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.

Certified Threat Intelligence Analyst and CTIA 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 Certified Threat Intelligence Analyst (CTIA) 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 8 GB or more RAM
- Hard disk, 500 GB 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
- CTIA 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: Microsoft Edge, Firefox, and Chrome
- WinPcap driver
- Microsoft Office 2016 or Open Office
- Java Runtime Environment v8u391 or later version

- Java Development Kit v8u171 or later version
- 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 all patches applied
 - o Parrot Security 5.0 Electric Ara (64 bit) with all patches applied

Note: All the above-mentioned tools, except the Windows operating system (Windows 11) and Parrot Security, are available in the CTIA Tools downloads from the Aspen portal.

Classroom Connectivity

As this class teaches network attack 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 CTIA 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 500 GB free disk space, a minimum of 8 GB RAM (16 GB recommended), 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 500 GB free disk space, a minimum of 8 GB RAM (16 GB recommended), 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 CTIA Tools from Aspen to the E:\CTIA-Tools folder on your hard drive for easy access (see <u>CT#14</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 11) on VMware Workstation (see <u>CT#7</u> in the Configuration Tasks section).
- Create a partition in the Windows 11 virtual machine (see <u>CT#8</u> in the Configuration Tasks section).
- Install guest operating system (Parrot Security) on VMware Workstation (see <u>CT#9</u>, in the Configuration Tasks section).
- Turn off the firewall on the Window 11 virtual machine (see <u>CT#10</u> in the Configuration Tasks section).

- Install Windows components in the Windows 11 virtual machine (see <u>CT#11</u> in the Configuration Tasks section).
- Install WinRAR and MS Office on the Windows 11 virtual machine (see <u>CT#12</u> and <u>CT#13</u> in the Configuration Tasks section).
- Have CTIA Tools shared as the E: drive on the Windows and Parrot Security machines (mapping the E: drive) (see <u>CT#17</u> in the Configuration Tasks section).
- Install Adobe Acrobat Reader DC on the Windows 11 virtual machine (see <u>CT#18</u> in the Configuration Tasks section).
- Install Web Browsers and WinPcap in the Windows 11 virtual machine (all software can be found in the Lab Prerequisites directory in the E:\CTIA-Tools folder) (see <u>CT#19</u>, and <u>CT#20</u> in the Configuration Tasks section).
- Install .NET Framework on the Windows 11 virtual machine (see <u>CT#15</u> in the Configuration Tasks section).
- Install Java Runtime Environment and Java Development Kit on the Windows 11 virtual machine (see <u>CT#16</u> in the Configuration Tasks section).
- Turn off screen savers on the Windows 11 virtual machine (see <u>CT#21</u> in the Configuration Tasks section).
- Conduct a ping test between both the virtual machines in the network (see <u>CT#22</u> in the Configuration Tasks section).
- Take snapshots of the virtual machines (see <u>CT#23</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 CTIA Tools from Aspen to the E:\CTIA-Tools folder on your hard drive for easy access (see <u>CT#14</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 11) on VMware Workstation (see <u>CT#7</u> in the Configuration Tasks section).
- Create a partition in the Windows 11 virtual machine (see <u>CT#8</u> in the Configuration Tasks section).

- Install guest operating system (Parrot Security) on VMware Workstation (see <u>CT#9</u>, in the Configuration Tasks section).
- Turn off the firewall on the Windows 11 virtual machine (see <u>CT#10</u> in the Configuration Tasks section).
- Install Windows components in the Windows 11 virtual machine (see <u>CT#11</u> in the Configuration Tasks section).
- Install WinRAR and MS Office on the Windows 11 virtual machine (see <u>CT#12</u> and <u>CT#13</u> in the Configuration Tasks section).
- Have CTIA Tools shared as the E: drive on the Windows and Parrot Security machines (mapping the E: drive) (see <u>CT#17</u> in the Configuration Tasks section).
- Install Adobe Acrobat Reader DC on the Windows 11 virtual machine (see <u>CT#18</u> in the Configuration Tasks section).
- Install Web Browsers and WinPcap in the Windows 11 virtual machine (all software can be found in the Lab Prerequisites directory in the E:\CTIA-Tools folder) (see <u>CT#19</u>, and <u>CT#20</u> in the Configuration Tasks section).
- Install .NET Framework on the Windows 11 virtual machine (see <u>CT#15</u> in the Configuration Tasks section).
- Install Java Runtime Environment and Java Development Kit on the Windows 11 virtual machine (see <u>CT#16</u> in the Configuration Tasks section).
- Turn off screen savers on the Windows 11 virtual machine (see <u>CT#21</u> in the Configuration Tasks section).
- Conduct a ping test between both the virtual machines in the network (see <u>CT#22</u> in the Configuration Tasks section).
- Take snapshots of the virtual machines (see <u>CT#23</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 CTIASTUDENT1, CTIASTUDENT2, CTIASTUDENT3. 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 10.0.0/24 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 they are based on the threat intelligence tools discussed in the trainer slides. The instructors are encouraged to demonstrate and guide the students on the use of threat intelligence tools. Please feel free to include your own exercises.

CTIA 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 CTIA tools are on the computer in the CTIA-Tools folder in the 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 check 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 500 GB or more of free disk space.

Verify whether you can successfully boot the Windows 11 and Parrot Security virtual machines using VMware Workstation.
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 CTIAv2 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 technical contact (system administrator) for the facility 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 CTIA 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 one extended logical partition (D:\ of 200 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 Host Operating System

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

Note: Download the latest version of WinRAR compatible with your host operating system from the official website (Here, we consider Windows to be the host OS).

- 2. Double-click on the **.exe** setup file to begin the installation. If a **User Account Control** 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 **CTIAv2 ISO.zip** file from the right-hand pane to download the ISO files for the Parrot Security operating system.
- 3. Navigate to the location where you downloaded the **CTIAv2 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 Host Machine

- 1. In your host system, navigate to the location where you have extracted the CTIAv2 ISO.zip file and then to CTIAv2 ISO\VMware Workstation Pro.
- 2. Double-click the file VMware-workstation-full-15.5.1-15018445.exe.

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

Note: If you decide to download the latest version, the screenshots in your lab environment might differ from those shown in this guide.

3. A User Account Control pop-up window appears. Click Yes.

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

Note: After the system reboots, double-click the file VMware-workstation-full-15.5.1-15018445.exe.

- 4. VMware Workstation Pro initializes; in the installation wizard, click Next.
- 5. Accept the user agreement and click **Next**.
- 6. In the Custom Setup wizard, check the Enhanced Keyboard Driver option and click Next.
- 7. Follow the wizard-driven installation steps to install VMware Workstation Pro using the default settings.

记 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	
		A	Add Network	Remove Netv	vork Rename Net	work
-VMnet Info	ormation					
Bridged	d (connect Vi	Ms directly to the external netwo	ork)			
Bridge	d to:				 Automatic Setting 	gs
🔍 NAT (s	hared host's	IP address with VMs)			NAT Settings.	
O Host-o	nly (connect	VMs internally in a private netw	ork)			_
Conne	ct a host virt	ual adapter to this network				_
Host v	irtual adapte	r name: VMware Network Adapt	ter VMnet8			
✓ Use loc	al DHCP serv	vice to distribute IP address to V	Ms		DHCP Settings	
Subnet IP:	192 . 168	. 109 . 0 Subnet mask	255 . 255 . 255 .	D		
		Administrator privileges are requ	ired to modify the net	work configur	ration. 📢 Change S	ettings
Restore De	faults	mport Export	ОК Са	incel	Apply H	elp

- 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	
104-c+ T=6			Add Network	Remove Netv	vork Rename Netw	ork
	ormation d (connect VI	Vs directly to the external netw	uork)			
Bridge	d to: Autom	atic	URY .		 Automatic Settings 	s
🖲 NAT (s	NAT (shared host's IP address with VMs)					
O Host-o	nly (connect	VMs internally in a private netw	vork)			
Conne Host v	Connect a host virtual adapter to this network Host virtual adapter name: VMware Network Adapter VMnet8					
Subnet IP	Use local DHCP service to distribute IP address to VMs DHCP Settings Subnet IP: 10 . 10 . 1 . 0 2 Subnet IP: 10 . 10 . 1 . 0 2					
Restore De	faults	mport Export	OK Ca	ancel	Apply Hel	p

6. The NAT Settings window appears; enter 10.10.1.2 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 Port Forwarding	
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 Config port: 0 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 I	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	
	ormation	Ad	d N <u>e</u> twork F	lem <u>o</u> ve Netv	vork Rename Nety	<u>v</u> ork
◯ <u>B</u> ridged	○ Bridged (connect VMs directly to the external network)					
Bridged to: Automatic Automatic Automatic Settings				js		
<u>NAT</u> (shared host's IP address with VMs) NAT <u>Settings</u>						
O Host-o	nly (connect	VMs internally in a private networ	k)			
 ✓ Connect a host <u>virtual adapter to this network</u> Host virtual adapter name: VMware Network Adapter VMnet8 ✓ Use local <u>D</u>HCP service to distribute IP address to VMs DHCP Settings Subnet <u>I</u>P: 10 . 10 . 1 . 0 Subnet <u>mask</u>: 255 . 255 . 255 . 0 						
<u>R</u> estore De	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:	0 🗘 30	•
Max lease time:		•
	OK Cancel Help	

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

😟 Virtual I	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 Bridgeo Bridge	ormation d (connect VI d to: Autom	As directly to the external netw	Add N <u>e</u> twork	Rem <u>o</u> ve Netw	vork Rename Network ✓ Automatic Settings
● <u>N</u> AT (sl	<u>NAT</u> (shared host's IP address with VMs) NAT <u>Settings</u> NAT <u>Settings</u>				
✓ 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					
<u>R</u> estore De	faults Ir	npor <u>t</u> Export	OK Ca	incel	<u>A</u> pply Help

[Back to Configuration Task Outline]

CT#7: Install Windows 11 Virtual Machine in VMware

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 11) and click Next.

New Virtual Machine Wizard				×
Guest Operating System Insta A virtual machine is like a physi system. How will you install the	llation cal computer; i guest operati	t needs an ope ng system?	erating	
Install from:				
O Installer disc:				
No drives available		\sim		
O Installer disc image file (iso):				
			Province	. 1
		~	browse	1
 I will install the operating system 	later.			
The virtual machine will be create	ed with a blank	hard 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 10 x64 is selected under Version. Click Next.

New Virtual Machine Wizard			×
Select a Guest Operating Sy Which operating system w	stem ill be installed on	this virtual mac	hine?
Guest operating system			
VMware ESX Other			
Version			
Windows 10 x64			~
	c De els	Nexts	Consul
неір	< Back	Next >	Cancel

5. The Name the Virtual Machine wizard appears; type Windows 11 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	\times
Name the Virtual Machine What name would you like to use for this virtual machine?	
Virtual machine name:	
Windows 11	
Location:	
\Windows Browse	
The default location can be changed at Edit > Preferences.	
< Back Next > Cance	el

Certified Threat Intelligence Analyst Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

6. The Specify Disk Capacity wizard appears. Leave the Maximum disk size (GB) to default (i.e., 80 GB, recommended), select the Store virtual disk as a single file radio button, and click Next.

New Virtual Machine Wizard			×
Specify Disk Capacity How large do you want this di	sk to be?		
The virtual machine's hard disk is stor computer's physical disk. These file(s) applications, files, and data to your vir Maximum disk size (GB): 80 Recommended size for Windows 10 x Store virtual disk as a single file Store virtual disk into multiple files Split virtual disk into multiple files Splitting the disk makes it easier to computer but may reduce perform	ed as one or of start small an tual machine. 0 54: 60 GB 54: 60 GB	more files on the nd become large tual machine to y large disks.	e host er as you add another
Help	< Back	Next >	Cancel

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

Ready to Create Virtual Machine Click Finish to create the virtual machine. Then you can install Windows 10 x64. The virtual machine will be created with the following settings: Name: Windows 11 Location: \Windows 10 Version: Workstation 15.x Operating System: Windows 10 x64	
The virtual machine will be created with the following settings: Name: Windows 11 Location: \Windows 11 Version: Workstation 15.x Operating System: Windows 10 x64	
Name: Windows 11 Location: \Wi. Version: Workstation 15.x Operating System: Windows 10 x64	
Location: \Wi. Version: Workstation 15.x Operating System: Windows 10 x64	••
Version: Workstation 15.x Operating System: Windows 10 x64	
Operating System: Windows 10 x64	
Hard Disk: 80 GB	
Memory: 2048 MB	
Network Adapter: NAT	
Other Devices: 2 CPU cores, CD/DVD, USB Controller, Printer, Sound C	

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 11 ISO file. Click Close.

Hardware	×
Device Summary Memory 2 GB Processors 2 New CD/DVD (SATA) Auto detect Network Adapter NAT Sound Card Auto detect Printer Present Display Auto detect Printer Present Display Auto detect	Device status Connected Connection Use physical drive: Muto detect Use ISO image file: Moves Advanced
	ciose help

9. In the Ready to Create Virtual Machine wizard, click Finish.



10. The Windows 11 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**.



14. Click the Power on this virtual machine option to launch the Windows 11 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**.

🖆 Windows Setup	- • •
Windows	
Languag <u>e</u> to install: English (United States)	_
Time and currency format: English (United States)	•
Keyboard or input method: US	•
Enter your language and other preferences and click "Next" to continue.	
Microsoft Corporation. All rights reserved.	<u>N</u> ext

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

🖆 Windows Setup		- • •
	. Windows [.]	
	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 11 Pro and click Next.

		10 7 (2021
Windows 11 Education	x64	12/7/2021
Windows 11 Education N	x64	12/7/2021
Windows 11 Enterprise	x64	12/7/2021
Windows 11 Enterprise N	x64	12/7/2021
Windows 11 Pro	хб4	12/7/2021
Windows 11 Pro N	хб4	12/7/2021
Windows 11 Pro Education	хб4	12/7/2021
escription: /indows 11 Pro		

18. 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.



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

👫 Registry Editor				
File Edit View Favorites Help				
Computer\HKEY_LOCAL_MACHINE\SYS	STEM\Setup			
File Edit View Favorites Help Computer\HKEY_LOCAL_MACHINE\SYS Computer HKEY_CLASSES_ROOT HKEY_CLASSES_ROOT HKEY_CURRENT_USER HKEY_LOCAL_MACHINE SAM SECURITY SOFTWARE SOFTWARE ControlSet001 CurrentControlSet DriverDatabase HardwareConfig Keyboard Layout MountedDevices ResourceManager RNG Select Softw Keypand New	TEM\Setup Name (Default) (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) D0 (0) D1 (1) vs\panther
> HKEY_USER: Find	St	trina Value		
> HKEY_CURR Delete	Bi	inary Value		
Rename	D	WORD (32-bit) Value		
Export	Q	WORD (64-bit) Value		

• A new key has been created, rename it as **LabConfig** and press **Enter**.

🎬 Registry Editor				
File Edit View Favorites Help				
Computer\HKEY_LOCAL_MACHINE\SY	STEM\Setup\LabCont	fig		
> 📒 HardwareConfig	Name	Туре	Data	
> Keyboard Layout	(Default)	REG_SZ	(value not set)	
> CRESOURCEManager				
Select				
🗸 🚞 Setup				
> AllowStart				
Pid				
SETUPCL				
Software				
WPA				
> THEY_USERS				
> hKEY_CURRENT_CONFIG				

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

Computer\HKEY_LOCAL_MACHINE\SYSTEM\Setup\LabConfig							
Name Image: A state of the	Type REG_SZ	Key String Valu Binary Valu DWORD (3 QWORD (6 Multi-String Expandable	Data (value not set) e e e 2-bit) Value 2-bit) Value g Value g Value e String Value				
	EM\Setup\LabConfig Name D(Default) New	EM\Setup\LabConfig Name Type (Default) REG_SZ	EM\Setup\LabConfig Name Type [Default] REG_SZ New Key String Valu Binary Valu DWORD (3 QWORD (6 Multi-String Expandable	EM\Setup\LabConfig Name Type Data PEG_SZ (value not set) New Key String Value Binary Value DWORD (32-bit) Value QWORD (64-bit) Value Multi-String Value Expandable String Value			

- Rename the value as **BypassCPUCheck** and press **Enter**.
- Now, right-click BypassCPUCheck value and select Modify... option.

🔡 Registry Editor				
File Edit View Favorites Help				
Computer\HKEY_LOCAL_MACHINE\SYS	TEM\Setup\LabConfig			
 HardwareConfig Keyboard Layout MountedDevices ResourceManager RNG Select Setup AllowStart Pid SETUPCL LabConfig Software WPA HKEY_USERS HKEY_CURRENT_CONFIG 	Name (Default) BypassCPUCheck	Type REG_SZ REG_DWORD Edit DWORD (32-bit) Value name: BypassCPUCheck Value data: 1	Data (value not set) 0x0000000 (0) Value Base O Hexadecimal O Decimal OK Cano	sel

• Edit DWORD (32-bit Value) pop-up appears, change the Value data to 1 and click OK.

• Similarly, create BypassTPMCheck, BypassRAMCheck, and BypassSecureBootCheck values (for each value, set Value data=1).

🎬 Registry Editor				
File Edit View Favorites Help				
Computer\HKEY_LOCAL_MACHINE\SYST	TEM\Setup\LabConfig			
> HardwareConfig > Keyboard Layout MountedDevices > ResourceManager	Name (Default) BypassCPUCheck BypassTPMCheck	Type REG_SZ REG_DWORD REG_DWORD	Data (value not set) 0x00000001 (1) 0x00000001 (1)	
	BypassRAMCheck	REG_DWORD REG_DWORD REG_DWORD	0x00000001 (1) 0x00000001 (1) 0x00000001 (1)	
 Allowstatt Pid SETUPCL LabConfig Software WPA HKEY_USERS 				
> hkey_current_config				

- Now, close all the windows (Registry Editor, Command Prompt and Error window).
- In Windows Setup window, click Yes.
- Click **Install Now** button.
- 19. The Select the operating system you want to install wizard appears again; select Windows 11 Pro and click Next.
- 20. Applicable notices and license terms wizard appears, accept the license terms by clicking on I accept... checkbox and click Next.

0	🔏 Windows Setup	X
	Applicable notices and license terms	
	Your use of this software is subject to the terms and conditions of the license agreement by which you acquired this software. If you are a volume license customer, use of this software is subject to your volume license agreement. You may not use this software if you have not validly acquired a license for the software from Microsoft or its licensed distributors.	
	, I accept the Microsoft Software License Terms. If an organization is licensing it, I am authorized to bind the organization. <u>N</u> ex	:

Lab Setup Guide Page 35

21. In the Which type of installation do you want? wizard, click the Custom: Install Windows only (advanced) option.



- 22. In the Where do you want to install Windows? wizard, click Next.
- 23. The installation of the Windows 11 operating system begins. The machine restarts once the installation has completed.


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

Is this the right keyboard layout or input method?
If you also use another keyboard layout, you can add that next. US Canadian Multilingual Standard English (India)
Irish NZ Aotearoa
Scattish Gaalis

- 26. Skip the second keyboard option.
- 27. In the next wizard, select **Continue with limited setup**.
- 28. In the Who's going to use this device? wizard, enter Analyst 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.

	Who's going to use this device? You'll use this name to sign in to your device.
	Enter your name
0	

	Create a super memorable password
	Make sure to pick something you'll absolutely remember.
	Enter a password
	•••••
0	Next

29. Add security questions in the next wizards.

30. In the Privacy settings wizard, disable all the options and click Accept.



Certified Threat Intelligence Analyst Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

- 31. After Windows initializes, if an app window appears, close it.
- 32. Right-click on the Start icon and select System option from the list.





33. The Settings window appears, click Rename this PC button in the right pane.

34. The Rename your PC pop-up window appears; type Windows11 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: DESKTOP-AOP9LM5	
Windows11	
	Next Cancel

- 35. After the renaming process, click **Restart now** to apply the changes.
- 36. After the virtual machine restarts, log in to the virtual machine with the credentials **Analyst** and **Pa\$\$w0rd**. Open the **Network and Internet Settings** and select the **Advanced network** settings.

\leftarrow Settings	- ×
Analyst Local Account	Network & internet
Find a setting ${\cal P}$	
System	Properties Data usage Public network < 1 MB, last 30 days
8 Bluetooth & devices	Ethernet
🗣 Network & internet	Authentication, IP and DNS settings, metered network
/ Personalization	VPN Add. connect. manage >
Apps	
Accounts	Proxy Proxy server for Wi-Fi and Ethernet connections
Time & language	
🐵 Gaming	Dial-up > Set up a dial-up internet connection >
X Accessibility	
Privacy & security	View all network adapters, network reset
Windows Update	

37. In the Advanced network settings window, select More network adapter options.

← Settings	Inalyst ocal Account	••• > Network	Advanced network setting	IS
Find a setti	ng p	먗	Ethernet Unidentified network Microsoft Disable Hyper-V Network Adapter	~
 Bluete 	ooth & devices	More set	tings	
 Netw Perso 	ork & internet	Data u	isage	>
🖹 Apps	unts	Hardw	are and connection properties	>
TimeGami	& language	Netwo Reset a	r k reset II network adapters to factory settings	>
X Acces	sibility	Related s	ettings	
Privac Wind	zy & security	More r	network adapter options	Ø

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

Network Connections				-		×
$\leftarrow \rightarrow$ \checkmark \uparrow \blacksquare \checkmark Network	and Intern > Network Connections	> ~ C	Search Network	Connect	tions	P
Organize Disable this network de	vice Diagnose this connection	Rename this connection	»	82 🔻		3
Ethernet Unidentified network Microsoft Hyper-V Network A	 Disable Status Diagnose Bridge Connections Create Shortcut Delete Rename Properties 					

39. The Ethernet Properties window appears. Scroll down the list, select Internet Protocol Version 4 (TCP/IPv4), and click on Properties.

Ethernet Properties	×
Networking	
Connect using:	
Microsoft Hyper-V Network Adapter	
<u>C</u> onfigure)
This connection uses the following items:	
 File and Printer Sharing for Microsoft Networks QoS Packet Scheduler Internet Protocol Version 4 (TCP/IPv4) Microsoft Network Adapter Multiplexor Protocol Microsoft LLDP Protocol Driver Internet Protocol Version 6 (TCP/IPv6) 	
Install Uninstall Properties	ןנ
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.	
OK Cancel	

- 40. Select the Use the following IP address radio button. Assign 10.10.1.11 as the IP address, 255.255.255.0 as the Subnet mask, and 10.10.1.1 as the Default gateway.
- 41. Assign **8.8.8.8** as the **Preferred DNS server** address and click **OK**.

Internet Protocol Version 4 (TCP/IPv4) Properties		
General		
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.		
Obtain an IP address automatically		
O Use the following IP address:		
IP address: 10 . 10 . 1 . 11		
Subnet mask: 255 . 255 . 255 . 0		
<u>D</u> efault gateway: 10 . 10 . 1 . 1		
Obtain DNS server address automatically		
O Use the following DNS server addresses:		
Preferred DNS server: 8 . 8 . 8 . 8		
Alternate DNS server:		
Validate settings upon exit Ad <u>v</u> anced		
OK Cancel		

- 42. Close the Ethernet Properties window; then, close all open windows.
- 43. Right-click the **Windows** button in the lower-left corner of the screen and click **Settings**.
- 44. In the Settings window, click Update & Security.
- 45. Click **Check for updates** from the right-hand pane.

← Settings	– 🗆 X
命 Home	Windows Update *Some settings are managed by your organization (View policies)
Update & Security	No updates available We'll continue to check daily for newer updates.
⊖ Windows Update	Check for updates
些 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
🖁 For developers	See update history See updates installed on your device

- 46. Check for and install the latest updates.
- 47. After installing all the updates, restart the machine.
- 48. Turn off the virtual machine. In the **Devices** section of the **Windows 11** tab, click **CD\DVD** (SATA).



Certified Threat Intelligence Analyst Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

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

Virtual Machine Settings		×
Hardware Options		
Device Memory Processors Hard Disk (SCSI) CD/DVD (SATA) Network Adapter Sound Card Printer Display	Summary 2 GB 2 80 GB Auto detect NAT Present Auto detect Present Auto detect	Device status Connected Connect at power on Connection Use physical drive: Use ISO image file: Uvindows 11\S\ Browse Advanced
		OK Cancel Help

[Back to Configuration Task Outline]

CT#8: Create a Partition in the Windows 11 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 results.

D Create and format hard disk partitions	
All Apps Documents Settings More ~	
Best match	
Create and format hard disk partitions Control panel	Create and format hard disk partitions Control panel
	🕜 Open

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

Note: While creating the Windows 11 virtual machine, we allocated a disk space of 80 GB. Here, we will create the partitions **E**: with a disk space of 30 GB, respectively.

🖶 Disk Managen	nent						-		×
File Action Vi	ew Help								_
🗢 🔿 🔃 🙎	F 🖉 📂 🔀	1 🔎 🖅							_
Volume	Layout	Туре	File System	Status	Capacity	Free Spa	% Free		_
(C:)	Simple	Basic	NTFS	Healthy (B	79.35 GB	60.90 GB	77 %		
- (Disk 0 partition	3) Simple	Basic		Healthy (R	613 MB	613 MB	100 %		
CPBA_X64FRE_E	N Simple	Basic	UDF	Healthy (P	5.10 GB	0 MB	0 %		
- System Reserve	d Simple	Basic	NTFS	Healthy (S	50 MB	19 MB	38 %		
- Disk 0									-11
Basic 80.00 GB	System Reserved	(C:) //	NITES			612 MP			
Online	Healthy (System, A	Healthy (Boot. Page File.	Crash Dump, P	rimary Partition)	Healthy	(Recovery Part	ition)	
			///////////////////////////////////////	///////////////////////////////////////	///////////////////////////////////////		(
	1								
CD-ROM 0									
DVD	CPBA_X64FRE_EN	-US_DV9 ([):)						
5.10 GB	5.10 GB UDF								
Online	Healthy (Primary F	artition)							
Unallocated	Primary partition								_

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

📅 Disk Manageme	ent				-		×
File Action Vie	w Help						_
🗢 🔿 📰 📝	🖬 🔎 🖻 🔒	<u>,</u>					
Volume	Layout	Туре	File System	Status	Canacity Erec Sna 9/ Erec		
(C:)	Simple	Basic	NTFS	Healthy	Open		
- (Disk 0 partition 3	3) Simple	Basic		Healthy	Explore		_
CPBA_X64FRE_EN	I Simple	Basic	UDF	Healthy	Made Dautitian an Antice		_
 System Reserved 	Simple	Basic	NIFS	Healthy	Mark Partition as Active		
					Change Drive Letter and Paths		_
					Format		_
					Extend Volume		_
					Shrink Volume		_
					Add Mirror		_
					Delete Volume		_
					Properties		-
- Disk 0 Basic	Sustam Reserved	1 (C)//		/////	Help		-1
80.00 GB Online	50 MB NTFS Healthy (System, 1	79.35 GB Healthy (NTFS Boot, Page File,	Crash Dump, F	rimary Partition) 613 MB Healthy (Recovery	Partition)	

4. A Shrink C: window appears, showing the 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:	81254
Size of available shrink space in MB:	62313
Enter the amount of space to shrink in MB:	30000
Total size after shrink in MB:	51254
You cannot shrink a volume beyond the point where any See the "defrag" event in the Application log for detailed operation when it has completed.	unmovable files are located. Information about the
See "Shrink a basic volume" in Disk Management help f	or more information
	Shrink Cancel

- 5. The **Disk Management** window will display the newly created unallocated disk partition in the middle pane.
- 6. Select the **Unallocated** drive from the middle pane, right-click the selected drive, and click **New Simple Volume...**.

📅 Disk Managen	nent		_			-		×
File Action V	iew Help							
♦ ♦	🖬 🗩 🗹	¥2						
Volume	Layout	Type File System S	itatus	Capacity	Free Spa	% Free		
- (C:)	Simple	Basic NTFS H	Healthy (B	50.05 GB	31.61 GB	63 %		
- (Disk 0 partition	n 3) Simple	Basic H	Healthy (R	613 MB	613 MB	100 %		
PBA_X64FRE_	EN Simple	Basic UDF H	Healthy (P	5.10 GB	0 MB	0 %		
- System Reserve	d Simple	Basic NTFS H	Healthy (S	50 MB	19 MB	38 %		
Disk 0 Basic 80.00 GB Online	System Re: 50 MB NTFS Healthy (Sy	(C:) 50.05 GB NTFS Healthy (Boot, Page File, Crash Du	29.30 mp, Unallo	GB ccated	New New New New	Simple Volum Spanned Volu Striped Volum Mirrored Volu	e me ne	- 1
DVD 5.10 GB Online	CPBA_X64FRI 5.10 GB UDF Healthy (Prim	E_EN-US_DV9 (D:) ary Partition)			New	RAID-5 Volum	ie	_
	<u> </u>				Help			-

- 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	en the maximum and minimum sizes.
Maximum disk space in MB:	29999
Minimum disk space in MB:	8
<u>S</u> imple volume size in MB:	<u>29999</u> →
	< <u>B</u> ack <u>N</u> ext > Cancel

9. In the Assign Drive Letter or Path wizard, the letter E 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:	E 🗸
○ Mount in the following empty NTFS folder:	
	Browse
O Do not assign a drive letter or drive path	
	< Back Next > Cancel

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

New Simple Volume Wizard	×
Format Partition To store data on this partition, you m	nust format it first.
Choose whether you want to format	this volume, and if so, what settings you want to use.
O Do not format this volume	
Format this volume with the format the source of the so	allowing settings:
<u>F</u> ile system:	NTFS ~
Allocation unit size:	Default ~
<u>V</u> olume label:	New Volume
Perform a quick format	
<u>Enable file and folder co</u>	ompression
	< <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 Management							_		×
File Action View	Help								
🖙 🔿 🛛 🖬 🚺	🗩 🛃 🛙	E							
Volume	Layout	Туре	File System	Status	Capacity	Free Spa	% Free		
- (C:)	Simple	Basic	NTFS	Healthy (B	50.05 GB	31.61 GB	63 %		
- (Disk 0 partition 3)	Simple	Basic		Healthy (R	613 MB	613 MB	100 %		
📟 New Volume (E:)	Simple	Basic	NTFS	Healthy (L	29.30 GB	29.23 GB	100 %		
- System Reserved	Simple	Basic	NTFS	Healthy (S	50 MB	19 MB	38 %		
Disk 0 Basic Sy: 80.00 GB Online He	stem Re: MB NTFS 5 althy (Sy: H	(C:) 0.05 GB NTFS Healthy (Boot, P	¹ age File, Crash [Dump, Healt	Volume (E:) GB NTFS hy (Logical Drive)		613 MB Healthy (Re	ecovery	Pa

13. Close all windows and restart the **Windows 11** virtual machine.

[Back to Configuration Task Outline]

CT#9: Install Parrot Security Virtual Machine in

VMware

- 1. The next step is to set up the **Parrot Security** 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, leave the settings as their default (Typical) and click Next.
- 4. In the **Guest Operating System Installation** wizard, choose the **Installer disc image file** (iso): radio button. Click **Browse** to provide the ISO path of the Parrot Security ISO file.

Note: Here, we have used the **Parrot Security** (**MATE**) .iso file **Parrot-security-5.0_amd64.iso** to create the **Parrot Security** virtual machine. Navigate to the location where you have extracted the **CTIAv2 ISO.zip** file and then to **CTIAv2 ISO\Parrot Security** to locate the **Parrot Security** ISO file.

However, you can download the latest ISO file from https://www.parrotsec.org/download/.

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

5. Then, select the Parrot Security ISO file and click **Open** to provide the ISO path. Finally, click **Next**.

New Virtual Machine Wizard	×
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:	
O Installer disc:	
No drives available	
◉ Installer disc image file (iso):	
VParrot-secur V Browse	
🗊 Debian 5 64-bit detected.	
○ I will install the operating system later.	
The virtual machine will be created with a blank hard disk.	
Help < Back Next > Cancel	

6. The Select a Guest Operating System wizard appears. Choose the Linux radio button under the Guest operating system field and select Debian 10.x 64-bit in the Version drop-down box. Then, click Next.

New Virtual Machine Wizard X
Select a Guest Operating System Which operating system will be installed on this virtual machine?
Guest operating system
O Microsoft <u>W</u> indows ● Linux
O VMware ES <u>X</u> O <u>O</u> ther
Version
Debian 10.x 64-bit 🗸
Help < <u>B</u> ack <u>Next</u> Cancel

7. The Name the Virtual Machine wizard appears. Type Parrot Security in the Virtual machine name field and click the Browse button to store the virtual hard disk. Then, click Next.

New Virtual Machine Wizard	×
Name the Virtual Machine What name would you like to use for this virtual machine?	
<u>V</u> irtual machine name:	
Parrot Security	
Location:	
C:\ Parrot Security	Browse
The default location can be changed at Edit > Preferences.	
< <u>B</u> ack <u>N</u> ext >	Cancel

Certified Threat Intelligence Analyst Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

8. The Specify Disk Capacity wizard appears; type 35.0 GB in the Maximum disk size (GB) field and choose the Store virtual disk as a single file radio button. Then, 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): 35.0 Recommended size for Debian 10.x 64-bit: 20 GB
 Store virtual disk as a single file Split virtual disk into multiple files Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help < <u>B</u> ack <u>N</u> ext > Cancel

9. Click the Customize Hardware... button in the Ready to Create Virtual Machine wizard.

ew Virtual Machine	Wizard	
Ready to Create Click Finish to c 10.x 64-bit.	Virtual Machine reate the virtual machine. Then you can install Debian	
The virtual machine w	ill be created with the following settings:	
Name:	Parrot Security	
Location:	VParrot Security	
Version:	Workstation 15.x	
Operating System:	Debian 10.x 64-bit	
Hard Disk:	35 GB	
Memory:	2048 MB	
Network Adapter:	NAT	
Other Devices:	CD/DVD, USB Controller, Printer, Sound Card	
<u>C</u> ustomize Hardwa	are	
	< Back Finish Cano	P

10. The Hardware window appears; ensure that Memory is assigned as 2 GB or 2048 MB and click Close.



11. Click Finish in the Ready to Create Virtual Machine wizard.

New	New Virtual Machine Wizard				
Re	cady to Create Click Finish to c 10.x 64-bit.	Virtual Machine reate the virtual machine. Then you can install Debian			
The	virtual machine w	ill be created with the following settings:			
Na	ime:	Parrot Security	~		
Lo	cation:	Parrot Security			
Ve	rsion:	Workstation 15.x			
Op	perating System:	Debian 10.x 64-bit			
Ha	ard Disk:	35 GB			
Me	emory:	2048 MB			
Ne	etwork Adapter:	NAT			
Ot	her Devices:	CD/DVD, USB Controller, Printer, Sound Card	×		
<u>(</u>	Qustomize Hardwa	are			
		< <u>B</u> ack Finish Cano	el		

12. In the Parrot Security tab, click the Power on this virtual machine link.





13. The Parrot security – 5.0 amd64 boot menu appears; select Install and press Enter.

14. The Parrot Security desktop appears. Double-click the **Install Parrot** shortcut to initialize the installation process.



Lab Setup Guide Page 56

Certified Threat Intelligence Analyst Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

15. A Parrot OS Installer window appears. In the Welcome wizard, leave default selected language as American English, and click Next.



- 16. In the Location wizard, leave default settings and click Next.
- 17. In the Keyboard wizard, leave default settings and click Next.
- 18. In the Partitions wizard, select the Erase disk checkbox and click Next.

Note: If the Encrypt system checkbox is selected, then unselect it.

• • •	Parrot Security Installer (as superuser)
	BIOS Select storage device: Virtual Disk - 80.0 GiB (/dev/sda) 🔹 ③ 7
	Erase disk This will delete all data currently present on the selected storage device.
Welcome	Mo Swap
Location	ito sitah
Keyboard	Manual partitioning You can create or resize partitions yourself.
Partitions	
Users	
Summary	Encrypt system
Install	
Finich	Current:
FILISI	Unpartitioned space or unknown partition table 80.0 GiB
	After:
	Parrot 80.0 GiB Btrfs
	Boot loader location: Master Boot Record of Virtual Disk (/dev/sda) 🔻
	Back Next Cancel

19. In the Users wizard, enter analyst in the What is your Name? field. In the What is the name of this computer? field, enter parrot.



20. In the Choose a password to keep your account safe section, enter toor in both the Password and Repeat Password fields. Click Next.

	Parrot Security Installer (as superuser)
	What is your name? analyst What name do you want to use to log in?
Welcome	analyst
Location	What is the name of this computer?
Keyboard	parrot 📀
Partitions	Choose a password to keep your account safe.
Users	Log in automatically without asking for the password.
Summary	
Install	
Finish	
	Back Next Cancel

21. The Summary wizard appears. Check the settings and click Install.

	Parrot Security Installer (as superuser)			
	This is an overview of what will happen once you start the install procedure.			
Welcome	Set timezone to America/New_York. The system language will be set to American English (United States). The numbers and dates locale will be set to American English (United States).			
Location	Keyboard			
Partitions	Set keyboard model to Generic 105-key PC (intl.). Set keyboard layout to English (US)/Default.			
Users	Partitions			
Summary	Erase disk /dev/sda (Virtual Disk) and install Parrot 5.0. Current:			_
Install	Unpartitioned space or unknown partition table 80.0 GiB			
Finish	After:			
	80.0 GiB Btrfs			
	Create new MSDOS partition table on /dev/sda (Virtual Disk). Create new 81916MiB partition on /dev/sda (Virtual Disk) with file system btrfs . Flag 81916MiB btrfs partition as boot . Install Parrot OS on new btrfs system partition. Install boot loader on /dev/sda .			
		<u>B</u> ack	Install	<u>C</u> ancel

22. In the Continue with installation? dialog box, click Install Now.



23. The installation process begins. Observe the status in the installation bar, as shown in the screenshot below.



- 24. System installation will take some time.
- 25. After the completion of the installation process, an **All done** message appears. Ensure that the **Restart now** check box is selected and click **Done**.





26. After the reboot, the **analyst** username is selected by default on the login screen. Enter **toor** in the **Password** field and press **Enter** to log in to the machine.

27. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.



28. Now, verify the configured network adapter setting of the virtual machine. In the **Parrot Terminal** window, type **ifconfig** and press **Enter** to check the network adapter—here, it is **eth0** (this might differ in your lab environment). Close the Terminal window after noting the adapter.

🔴 🔵 🕐 Parrot Terminal	
File Edit View Search Terminal Help	
<pre>[analyst@parrot]-[~]</pre>	
eth0: flags=4163 <up,broadcast,running,multicast> mtu</up,broadcast,running,multicast>	1500
inet 10.10.1.2 netmask 255.255.255.0 broadca inet6 fe80::82f0:ae2f:de83:cedf prefixlen 64 ether 02:15:5d:11:da:36 txqueuelen 1000 (Eth RX packets 11 bytes 1926 (1.8 KiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 26 bytes 2518 (2.4 KiB) TX errors 0 dropped 0 overruns 0 carrier 0	ast 10.10.1.255 scopeid 0x20 <link/> mernet) collisions 0
<pre>lo: flags=73<up,l00pback,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 4 bytes 240 (240.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 4 bytes 240 (240.0 B) TX errors 0 dropped 0 overruns 0 carrier 0</host></up,l00pback,running></pre>	collisions 0

29. Since this adapter IP address has been assigned through DHCP, we must now configure the network adapter to static. To do so, navigate to **Menu** in the bottom-left corner of the **Desktop** and click **Control Center**.



Certified Threat Intelligence Analyst Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

30. The Control Center window appears; click Advanced Network Configuration under the Internet and Network section.



31. A Network Connections window appears. Select Wired connection 1 and click the Settings icon.



Lab Setup Guide Page 62

32. In the Editing Wired connection 1 window, navigate to the IPv4 Settings tab. Select the Manual option from the Method drop-down box. In the Addresses section, click the Add button and add 10.10.1.12, 255.255.255.0, and 10.10.1.2 as the Address, Netmask, and Gateway. Type 8.8.8.8 in the DNS servers field and click Save.

Editing Wired connection 1							
Connection	name	Wired con	nection 1			1	
	Ethern	et 802.1)	(Security	DCB	Proxy	IPv4 Settings	IPv6 Settings
Method	Manua	ι 2					~
Addresse	5						3
Addres	s	Ne	etmask		Gatev	vay	Add
10.10.1	.12	24			10.10.	1.1	Delete
			4				
DNS	servers	8.8.8.8	5			Ĩ	
Search	domains						
DHCP	client ID						
Requ	ire IPv4	addressing	for this cor	nnection	to compl	ete	
							Routes
						Cancel	✓ Save

- 33. Close all windows and **reboot** the virtual machine to enable the setting.
- 34. Once the machine has restarted, log in to the machine and open a Terminal window.

35. Type ifconfig and press Enter to verify the configured IP address. Then, type ping www.eccouncil.org to check Internet connectivity.

••	Parrot Terminal	
File	it View Search Terminal Help	
	lyst@parrot]-[~] lfconfig	
eth0	lags=4163 <up,broadcast,running,multicast> mtu 1500</up,broadcast,running,multicast>	
lome	<pre>inet 10.10.1.12 netmask 255.255.255.0 broadcast 10.10.1.255 inet6 fe80::82f0:ae2f:de83:cedf prefixlen 64 scopeid 0x20<link/> ether 02:15:5d:11:da:36 txqueuelen 1000 (Ethernet) RX packets 3 bytes 126 (126.0 B)</pre>	
	RX errors 0 dropped 0 overruns 0 frame 0	
cense	TX packets 29 bytes 2142 (2.0 K1B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0	
lo: '	ags=73 <up,l00pback,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 4 bytes 240 (240.0 B) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 4 bytes 240 (240.0 B) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0</host></up,l00pback,running>	
	<pre>Lyst@parrot]-[~] ping www.eccouncil.org</pre>	
PING	w.eccouncil.org (104.18.8.180) 56(84) bytes of data.	
64 by 64 by	es from 104.18.8.180 (104.18.8.180): icmp_seq=1 ttl=58 time=2.38 ms es from 104.18.8.180 (104.18.8.180): icmp_seq=2 ttl=58 time=2.41 ms	
64 b	es from 104.18.8.180 (104.18.8.180): icmp seq=3 ttl=58 time=2.31 ms	

[Back to Configuration Task Outline]

CT#10: Turn Off Windows Defender Firewall on the Windows 11 Virtual Machine

1. Turn on the Windows 11 virtual machine, press any key, and log in with the credentials Analyst 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.



 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.



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.

Windows Defe	nder Firewall with Adv	anced S	Security on Loc	al Com 🗙
Domain Profile	Private Profile Public	Profile	IPsec Settings	
Specify beha domain. State	avior for when a compute	er is conr	nected to its corp	orate
E	irewall state:	Off		\sim
	Inbound connections:		Block (default)	\sim
	Outbound connections	8:	Allow (default)	\sim
	Protected network cor	nections	s: Cu <u>s</u> to	mize
Settings	pecify settings that cont befender Firewall behavio	rol Windo or.	ows <u>C</u> usto	mize
Logging S tr	pecify logging settings fo oubleshooting.	or	C <u>u</u> sto	mize
	ОК		Cancel	Apply

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

lask wanager	
Settings	
File Explorer	
Search	
Run	
Shut down or sign out >	
Desktop	

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	rus		-		×
Turn off Microsoft Defender Antivi	rus	Previous Setting	<u>N</u> ext Setting		
Not <u>C</u> onfigured Comment:					
O Disabled Supported on:	At least Windows Vista				•
Options:	Help:				•
	This poli If you does not potentia If you will run n If you internall another Microso Antiviru: potentia Enabli unsuppo policy se	cy setting turns off Micr enable this policy setting trun, and will not scan c lly unwanted software. disable this policy settin regardless of any other ir do not configure this pol y manage Microsoft Def- antivirus program, Wind ft Defender Antivirus. Ot s will scan your compute lly unwanted software. ng or disabling this polic orted behavior. It is recor etting unconfigured.	psoft Defender Antivi , Microsoft Defender omputers for malwar g, Microsoft Defende Istalled antivirus proc licy setting, Windows ender Antivirus. If you ows automatically di herwise, Microsoft De rs for malware and o	rus. r Antiviru e or othe duct. s will u install isables efender ther ected or eave this	s r is
		ОК	Cancel	Арр	ly

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			- o ×		
<u>File Action View H</u> elp					
Maintenance Scheduler Maps MDM Messaging Microsoft account Microsoft Defender Antivirus Microsoft Defender Application Microsoft Defender Exploit Gua Microsoft Bdge Microsoft User Experience Virtu Microsoft User Experience Virtu Microsoft User Experience Virtu Microsoft User Experience Virtu Online Assistance ODBE Portable Operating System Presentation Settings Push To Install Remote Desktop Services Search Search	Microsoft Defender Antivirus Allow antimalware service to remain running always Edit policy setting 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 antispware security intelligence is disabled. It is recommended that this setting remain disabled. If you enable this setting, the antivirus and antispyware security intelligence is disabled.	Setting Remediation Reporting Scan Security Intelligence Updates Threats 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 netwo Define proxy server for connecting to the network Randomize scheduled task times Configure scheduled task times randomization window Allow antimalware service to remain running always Define the directory path to copy support log files	State Not configured Enabled Not configured Not configured		
Shutdown Options	If you disable or do not	·	-		

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

Allow antimalware service to re	nain running always —	
Allow antimalware service to re	nain running always <u>P</u> revious Setting <u>N</u> ext Setting	
O Not <u>Configured</u> Comment:		
Enabled Disabled		v
Supported o	¹¹ At least Windows Server 2012, Windows 8 or Windows RT	A
Options:	Help:	
	This policy setting allows you to configure whether or n antimalware service remains running when antivirus an antispyware security intelligence is disabled. It is recom that this setting remain disabled. If you enable this setting, the antimalware service wil remain running even if both antivirus and antispyware intelligence is disabled. If you disable or do not configure this setting, the an service will be stopped when both antivirus and antispy security intelligence is disabled. If the computer is resta service will be started if it is set to Automatic startup. A service has started, there will be a check to see if antivir antispyware security intelligence is enabled. If at least o enabled, the service will remain running. If both are dis service will be stopped.	not the id imended II always security timalware yware arted, the fter the rus and one is iabled, the
	OK Cancel	Apply
- 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	— D X
Turn off routine remediation	Previous Setting <u>N</u> ext Setting
Not <u>C</u> onfigured Comment:	*
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



Cocal Group Policy Editor × <u>File Action View H</u>elp • 🔿 🙍 🖬 🔒 🚺 🗊 💙 Maintenance Scheduler Microsoft Defender Antivirus 📔 Maps Setting **Real-time Protection** State MDM 📔 Client Interface Messaging Device Control Microsoft account Exclusions > 📔 Microsoft Defender Antivirus Microsoft Defender Application MAPS > 🧾 Microsoft Defender Exploit Guar 🗂 Microsoft Defender Exploit Guard Microsoft Edge MpEngine Microsoft Secondary Authentica Network Inspection System > 🧾 Microsoft User Experience Virtui Quarantine NetMeeting Real-tin 📋 OneDrive Remediation Online Assistance Reporting COBE Scan Portable Operating System 🧮 Security Intelligence Updates Presentation Settings 🚞 Threats 📔 Push To Install 🗄 Allow antimalware service to startup with normal priority Not configure > 🧾 Remote Desktop Services Turn off Microsoft Defender Antivirus Enabled RSS Feeds 🗄 Configure local administrator merge behavior for lists Not configure Search E Turn off routine remediation Enabled Security Center Shutdown Options Extended Standard /

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.

】 Local Group Policy Editor File <u>A</u> ction <u>V</u> iew <u>H</u> elp		-	o x
Image: Second Science Scheduler Image: Science Science Scheduler Image: Science Scien	Real-time Protection Turn off real-time protection Edit policy setting Requirements: At least Windows Vista Description: 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	Setting Setting Turn off real-time protection Turn on behavior monitoring Scan all downloaded files and attachments Monitor file and program activity on your computer Turn on raw volume write notifications Turn on process scanning whenever real-time protection is Turn on script scanning Define the maximum size of downloaded files and attachme Configure local setting override for turn on behavior monito Configure local setting override for monitoring file and prog Configure local setting override to turn on real-time protecti Configure local setting override for monitoring for incomin Configure local setting override for monitoring for incomin Configure local setting override for monitoring file and prog Configure local setting override for monitoring file and prog Configure local setting override for monitoring file and prog Configure local setting override for monitoring file and prog Configure local setting override for monitoring file and prog Configure local setting override for monitoring file and prog Configure local setting override for monitoring for incomin Configure local setting override for monitoring for incomin	State Not configured Not configured
Microsoft Edge	Evidend (Standard)		

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



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

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

- × 4 Settings **Privacy & security** Analyst Local Account Security ρ Find a setting Windows Security O > Antivirus, browser, firewall, and network protection for your device System Bluetooth & devices Find my device > Å Track your device if you think you've lost it Network & internet Personalization For developers 78 > These settings are intended for development use only Apps Windows permissions Accounts Time & language General 3 ß > Advertising ID, local content, app launches, settings suggestions, productivity tools 63 Gaming × Accessibility Speech 2) Online speech recognition for dictation and other voice-based > interactions 0 Privacy & security 0 Windows Update Inking & typing personalization
- 25. In the Settings window, click Privacy & security from the left-hand pane.

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.

← Settings	- D X
Analyst Local Account	··· > Windows Security
Find a setting	A health of your device.
	Open Windows Security
System	
8 Bluetooth & devices	Protection areas
 Network & internet 	Virus & threat protection No actions needed.
🥖 Personalization	Q Account protection
Apps	No actions needed.
Accounts	Firewall & network protection Actions needed.
Time & language	App & browser control
🔨 Gaming	No actions needed.
X Accessibility	Bevice security No actions needed.
Privacy & security	Device performance & health

Certified Threat Intelligence Analyst Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

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

Wind	dows Security
1	No current threats.
	Last scan: Not available
=	Quick scan
ŵ	Scan options
0	Allowed threats
8	Protection history
((ŋ))	
0	🍫 Virus & threat protection settings
	No action needed.
	Manage 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.



Windows S	Windows Security		×
\leftarrow			
=	Automatic sample submission		
â	Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.		
0	Automatic sample submission is off. Your device may be Dismiss vulnerable.		
8	• Off		- 1
((م))			
	Submit a sample manually		
	Tompor Protection		
~	Prevents others from tampering with important security features.		
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	A Tamper protection is off. Your device may be vulnerable. Dismiss		
J	• Off		
	Learn more		
	Controlled folder access requires turning on Real-time protection.		
¢	Controlled folder access		

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



Certified Threat Intelligence Analyst Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

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

Windov	vs Security	-	×
+ ≡ 3	App & browser control App protection and online security.		
0	Reputation-based protection		
00 (m) 00 00 00 00 00 00 00 00 00 00 00 00 00	These settings protect your device from malicious or potentially unwanted apps, files, and websites. The settings to block potentially unwanted apps are turned off. Your device may be vulnerable. Turn on Reputation-based protection settings		
÷	Dismiss Isolated browsing Microsoft Defender Application Guard opens Microsoft Edge in an isolated browsing environment to better protect your device and data from malware.		
¢	Install Microsoft Defender Application Guard		

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.

#### **CT#11: Configure Windows Components on the Windows 11 Virtual Machine**

- 1. Log in to the Windows 11 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 Manage end user experience.
- 5. Under Manage end user experience, double-click **Configure Automatic Updates** in the right-hand pane, as shown in the screenshot below.

J Local Group Policy Editor	- • ×
File Action View Help	
⊨ ⇒   22 📷   📴 🗊   🍸	
<ul> <li>Windows Logon Options</li> <li>Windows Media Digital Rights</li> <li>Windows Media Player</li> <li>Windows Mobility Center</li> <li>Windows Robility Center</li> <li>Windows Reliability Analysis</li> <li>Windows Remote Managemer</li> <li>Windows Security</li> <li>Windows Security</li> <li>Windows Security</li> <li>Windows Update</li> <li>Legacy Policies</li> <li>Manage end user experient</li> <li>Manage updates offered fr</li> <li>Manage updates offered</li></ul>	Setting Setting Setting Specify active hours range for auto-restarts Allow updates to be downloaded automatically over me Always automatically restart at the scheduled time Configure Automatic Updates Specify deadlines for automatic updates and restarts Remove access to "Pause updates" feature Remove access to use all Windows Update features Update Power Policy for Cart Restarts Display options for update notifications

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

			- 0	×
Configure Automatic Updates		<u>P</u> revious Setting	Next Setting	
Not <u>C</u> onfigured Comment: <u>E</u> nabled <u>Disabled</u> Supported on:	Windows XP Profession Option 7 only supporte	nal Service Pack 1 or At least d on servers of at least Win	t Windows 2000 Service Pa dows Server 2016 edition	ack 3 ^
options:	neip:			
The following settings are only required 4 is selected. Install during automatic maintenanc Scheduled install day: Scheduled install time: If you have selected "4 – Auto downlo the install" for your scheduled install da	and applical Note: e This s e e 2 ad and sched sy and specifi	This policy does not apply etting lets you specify whet ed on this computer. If the one of the four options in t = Notify before downloadi When Windows finds update will be notified that update going to Windows Update,	ugn the windows automa to Windows RT. her automatic updates ar service is enabled, you mi the Group Policy Setting: ng and installing any upd es that apply to this comp s are ready to be downloa users can download and i	e ust ates. uter, ded. install

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

- Local Group Policy Editor Eile Action View Help 🗢 🔿 🙋 📆 🗟 🖬 🍞 📋 Digital Locker 📋 Real-time Protection 📔 Edge Ul Turn on behavior monitoring Setting State 📔 Event Forwarding Turn off real-time protection Enabled > 📔 Event Log Service Edit policy setting Turn 📋 Event Logging Requirements: At least Windows Server 2012, Windows 8 or Windows RT Scan all downloaded files and attachments Not configured Event Viewer > 🧾 File Explorer E Monitor file and program activity on your computer Not configured File History E Turn on raw volume write notifications Not configured Find My Device 🗄 Turn on process scanning whenever real-time protection is ... Not configured Description: 📔 Handwriting 📰 Turn on script scanning This policy setting allows you to configure behavior monitoring. Not configured HomeGroup Define the maximum size of downloaded files and attachme... Not configured > 📔 Internet Explorer Configure local setting override for turn on behavior monito... Not configured If you enable or do not configure Internet Information Services Configure local setting override for scanning all downloade... Not configured this setting, behavior monitoring will be enabled. > 🚞 Location and Sensors 🖹 Configure local setting override for monitoring file and prog... Not configured Maintenance Scheduler E Configure local setting override to turn on real-time protecti... Not configured Maps If you disable this setting, behavior monitoring will be disabled. E Configure local setting override for monitoring for incomin... Not configured MDM E Configure monitoring for incoming and outgoing file and p... Not configured Messaging Microsoft account Client Interface Exclusions MAPS > 🛗 Microsoft Defender Exploit Guard MpEngine Network Inspection System Quarantine Real-time Protection Remediation Reporting Scan Security Intelligence Updates Threats
- 8. Double-click the **Turn on behavior monitoring** setting to configure its settings.

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

💭 Turn on behavior monitoring	– 🗆 X
Turn on behavior monitoring	Previous Setting Next Setting
Not <u>Configured</u> Comment: <u>Enabled</u> <u>Disabled</u> Supported on:	At least Windows Server 2012, Windows 8 or Windows RT
Options:	Help: This policy setting allows you to configure behavior monitoring. If you enable or do not configure this setting, behavior monitoring will be enabled. If you disable this setting, behavior monitoring will be disabled.
	OK Cancel Apply

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



11. 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	nments	– 🗆 X
Scan all downloaded files and attac	nments <u>Previous Setting</u>	Next Setting
○ Not <u>Configured</u> Comment: ○ Enabled		^
Disabled     Supported on:	At least Windows Server 2012, Windows 8 or Wi	indows RT
		~
Options:	Help:	
	In spong setting allows you downloaded files and attachn lf you enable or do not con downloaded files and attachn lf you disable this setting, s and attachments will be disab	figure this setting, scanning for all rents will be enabled. canning for all downloaded files iled.
		OK Cancel <u>A</u> pply

[Back to Configuration Task Outline]

#### **CT#12: Install WinRAR on the Windows 11 Virtual** Machine

- 1. Log in to the Windows 11 virtual machine with the credentials Analyst 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#13: Install MS Office on the Windows 11 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#14: Download CTIA Tools on the Windows 11** Virtual Machine

- 1. Log in to the Windows 11 virtual machine with the credentials Analyst and Pa\$\$w0rd.
- 2. Create a folder on drive **E:** named **CTIA-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.

Lab Setup Guide Page 86

- 4. Click the module names in the right-hand pane (except CTIAv2 ISO.zip) and download all the **CTIA Tools** files to the **E:\CTIA-Tools** folder.
- 5. Right-click the .zip files in the **E:\CTIA-Tools** folder and select the **Extract Here** option.

[Back to Configuration Task Outline]

#### **CT#15: Adding .NET Framework in the Windows 11** Virtual Machine

- 1. Log in to the Windows 11 virtual machine using the credentials Analyst and Pa\$\$w0rd.
- 2. Navigate to the E:\CTIA-Tools\CTIA Lab Prerequisites\.NET Framework folder.
- 3. Alternatively, you may download the latest version of **.NET Framework** from the official website.
- 4. Double-click on the dotNetFx35setup.exe setup file to begin the installation. If a User Account Control pop-up window appears, click Yes.
- 5. The .NET Framework setup window appears; click Install.
- 6. Complete the installation by choosing the default options throughout.
- 7. Close the window.

[Back to Configuration Task Outline]

#### **CT#16: Install Java Runtime Environment and Java Development Kit in the Windows 11 Virtual Machine**

- 1. In the Windows 11 virtual machine, navigate to E:\CTIA-Tools\CTIA Lab Prerequisites.
- 2. Open the Java Runtime Environment folder.
- 3. Double-click the **jre-8u391-windows-x64.exe** file and follow the **wizard-driven** installation steps to install Java Runtime Environment.
- 4. Similarly, navigate to E:\CTIA-Tools\CTIA Lab Prerequisites\Java Development Kit folder.
- 5. Double-click the **jdk-8u171-windows-i586.exe** file and follow the **wizard-driven** installation steps to install Java Development Kit.
- 6. You can also download the **latest versions** of Java Runtime Environment and Java Development Kit from the respective vendors.

[Back to Configuration Task Outline]

#### **CT#17: Share and Map CTIA-Tools Folder to Parrot** Security Virtual Machine

- 1. Log in to the Windows 11 virtual machine with the credentials Analyst and Pa\$\$w0rd.
- 2. Open Network and Sharing Center by navigating to Control Panel  $\rightarrow$  Network and Internet  $\rightarrow$  Network and Sharing Center.
- 3. In the Network and Sharing Center window, click the Change advanced sharing settings link in the left pane.



4. 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 —	0	×	
$\leftarrow \rightarrow \checkmark \uparrow$ $\blacksquare$ « Net > Advanced shari $\checkmark$ $\bigcirc$ Search Control Panel		Q	
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 ^			
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     I'urn on automatic setup of network connected devices.     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.			
<ul> <li>Turn on file and printer sharing</li> <li>Turn off file and printer sharing</li> </ul>			
Guest or Public (current profile) ————————————————————————————————————			
All Networks			
Save changes Cancel		_	

				-	
Advanced sharing s	ettings		_		×
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$	$<\!\!<$ Net $>$ Advanced shari $<\!\!>$	Search Control Panel			Q
Chang	e elemente entire en for different estuardo profiler				
Window	e snaring options for different network profiles s creates a separate network profile for each network you use.	You can choose specific (	options for		
each pro	file.				
Private -			~ ~		
Guest or	Public (current profile)		~ ^		
Net	work discovery				
	When network discovery is on, this computer can see other r visible to other network computers.	network computers and d	evices and is		
	Turn on network discovery				
File	and printer sharing				
	When file and printer sharing is on, files and printers that you be accessed by people on the network.	ı have shared from this co	omputer can		
	<ul> <li>Turn on file and printer sharing</li> <li>Turn off file and printer sharing</li> </ul>				
All Netw	orks		v		
		Save changes	Cancel		_
Advanced sharing s	ettings		_		>
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$	« Net > Advanced shari > C	Search Control Panel			,c
All Networ	ke l				
Public	folder sharing				
V	<ul> <li>Vhen Public folder sharing is on, people on the network, inclu ccess files in the Public folders.</li> </ul>	uding homegroup memb	ers, can		
	• Turn on sharing so anyone with network access can re	ad and write files in the P	ublic folders		
	<ul> <li>Turn off Public folder sharing (people logged on to thi folders)</li> </ul>	s computer can still acce	ss these		
Media	streaming				
V	Vhen media streaming is on, people and devices on the netwo ideos on this computer. This computer can also find media o	ork can access pictures, n n the network.	nusic, and		
	Choose media streaming options				
File sł	aring connections				
V	Vindows uses 128-bit encryption to help protect file sharing c upport 128-bit encryption and must use 40- or 56-bit encrypt	onnections. Some device ion.	s don't		
	• Use 128-bit encryption to help protect file sharing con	nections (recommended)	)		
	Enable file sharing for devices that use 40- or 56-bit en	cryption	_		
Passw	ord protected sharing				
V	Iden password protected sharing is on, only people who have omputer can access shared files, printers attached to this con ther people access, you must turn off password protected sh	e a user account and pass nputer, and the Public fol aring.	word on this ders. To give		
	• Turn on password protected sharing	2			
	O rain on passiona protected sharing				

- 5. Close the **Network and Sharing Center** window.
- 6. Now, open a File Explorer window, navigate to the E: drive, right-click on the CTIA-Tools folder, and navigate to Show more options → Properties from the context menu.

- New Volume (E:)				
🕀 New 🗸			🖻 🛍 🛝 Sort - 🗮 View -	
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$	-	■ > This PC > New Vo	ume (E:) >	∼ C ,⊃ Search New 1
🗸 🛧 Quick access		Name	^ Date modified	Type Size
🛄 Desktop	*	CTIA-Tools	Open	File folder
🛓 Downloads	*		Open in new window Pin to Quick access	
📔 Documents	*		WinRAR >	
🚬 Pictures	*		Open in Windows Terminal	
Ø Music			Give access to	
🔀 Videos			Restore previous versions	
> 🌰 OneDrive			Include in library > Pin to Start	
> 📮 This PC			Copy as path	
> 🚰 Network			Send to >	
			Сит Сору	
			Create shortcut Delete Rename	
			Properties	

7. Select the **Sharing** tab from the **CTIA-Tools Properties** window to modify and display the current shared folder settings.

8. Click the Share... button to access the File Sharing options.

📒 CTIA-Tools Pro	perties				×
General Sharing	Security	Previou	is Versions	Customize	
Network File and	I Folder Sk	naring			
CTIA-T Not Sh	ools ared				
Network Path: Not Shared					
Share					
Advanced Sharir	ng				
Set custom perm advanced sharin	nissions, cr ng options.	eate mul	tiple shares,	, and set other	
Advanced	d Sharing				
Password Protec	tion				
People must hav computer to acc	ve a user a ess share	account a d folders.	and passwo	rd for this	
To change this s	etting, use	e the <u>Net</u>	work and S	haring Center.	
	0	ĸ	Cance	Apj	ply

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

E Network access	×
Choose people to share with	
Type a name and then click Add, or click the arrow	v to find someone.
Everyone	✓ <u>A</u> dd
Name	Permission Level
🛃 Analyst	Owner
Per las ina trauble desvina	
i m naving trouble snanng	
	S <u>h</u> are Cancel

Lab Setup Guide Page 91

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

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

÷	📑 Network access	×
	Choose people to share with	
	Type a name and then click Add, or click the arrow to find so	meone.
		✓ <u>A</u> dd
	Name	Permission Level
	🙎 Analyst	Owner
	🤽 Everyone	Read 🔻 🗸 Read
		Read/Write
		Remove
	I'm having trouble sharing	
		Share Cancel

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

_		×
÷	3 Network access	^
	Your folder is shared.	
	You can <b><u>e-mail</u></b> someone links to these shared items, or <u>copy</u> and paste the links into another app.	
	Individual Items	•
	CTIA-Tools \\WINDOWS11\CTIA-Tools	
	Show me all the network shares on this computer.	_
		one

13. Close the CTIA-Tools Properties window.

CTIA-Tools Properties	×
General Sharing Security Previous Versions Customize	
Network File and Folder Sharing	
CTIA-Tools Shared	
Network Path: \\\WINDD\WS11\CTIA-Tools	
Share	
Advanced Sharing	
Set custom permissions, create multiple shares, and set other advanced sharing options.	
Second Sharing	
Password Protection	
People must have a user account and password for this computer to access shared folders.	
To change this setting, use the <u>Network and Sharing Center</u> .	
Close Cancel App	y

14. Close all open windows.

[Back to Configuration Task Outline]

#### **CT#18: Install Adobe Acrobat Reader DC on the** Windows 11 Virtual Machine

- 1. Log in to the Windows 11 virtual machine with the credentials Analyst and Pa\$\$w0rd.
- 2. Open a File Explorer window and navigate to the E:\CTIA-Tools\CTIA 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.
- 6. After the installation has completed, close all windows.

[Back to Configuration Task Outline]

#### **CT#19: Install Web Browsers on the Windows 11** Virtual Machine

- 1. On the Windows 11 virtual machine, navigate to the E:\CTIA-Tools\CTIA 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.

[Back to Configuration Task Outline]

#### **CT#20: Install WinPcap on the Windows 11 Virtual** Machine

- 1. In the Windows 11 virtual machine, navigate to E:\CTIA-Tools\CTIA Lab Prerequisites.
- 2. Open WinPcap folder.
- 3. Double-click the WinPcap_4_1_3.exe file and follow the wizard-driven installation steps to install WinPcap.
- 4. You can also download the latest version of WinPcap from the respective vendors.

[Back to Configuration Task Outline]

# **CT#21: Turn Off Screen Savers on the Windows 11** Virtual Machine

Note: Before performing this CT, you must activate the Windows 11 virtual machine.

1. In the **Windows 11** virtual machine, right-click on the **Desktop** and select **Personalize** to open the personalization settings.



- X Settings Personalization Analyst R Local Account Colors 6) > Accent color, transparency effects, color theme Find a setting Q ß Themes > Install, create, manage System 8 Bluetooth & devices Lock screen > C, Lock screen images, apps, animations Network & internet Personalization Touch keyboard :::: > Themes, size 1 Apps Start • Accounts  $\square$ > Recent apps and items, folders Time & language Taskbar > Gaming Taskbar behaviors, system pins X Accessibility Fonts Ą > Install, manage Privacy & security Windows Update 8
- 2. In the **Personalization** window scroll down and click **Lock screen** in the right pane.

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

← Settings	- o ×
Analyst Local Account	Personalization > Lock screen
Find a setting 0	Personalize your lock screen Windows spotlight ~
System	Lock screen status Choose an app to show detailed status on the lock screen
<ul> <li>Bluetooth &amp; devices</li> <li>Network &amp; internet</li> </ul>	Show the lock screen background On On
Personalization	
🖹 Apps	Related settings
Accounts	Screen timeout >
🌖 Time & language	
Gaming	Screen saver
★ Accessibility	L
Privacy & security	Get help
Windows Update	Give feedback

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.

💐 Screen Saver Settings		×
Screen Saver		
	Reservation - Lad asses	
	A Second Se	
	a tan anala anal	
	2 Martine 2 Martine	
	• 0	
Screen saver		
(None)	✓ Settings Preview	
Wait: 1 🛊 m	inutes 🔲 On resume, display logon screen	
Power management		
Conserve energy or r	naximize performance by adjusting display	
brightness and other	power settings.	
Change power settin	<u>95</u>	
		_
	OK Cancel Apply	/

5. Close all windows.

[Back to Configuration Task Outline]

#### **CT#22: Ping Test Among Both Virtual Machines**

1. On the Windows 11 virtual machine, open a Command Prompt window.

(b) Chat All Apps Documents	Web	Settings Folders Photos
Best match		
Command Prompt App		
Search the web		Command Prompt
𝒫 cmd - See more search results	>	74F
	>	🖸 Open
,	>	Run as administrator
,O cmd <b>b</b>	>	Open file location
,O cmd <b>er</b>	>	Pin to taskbar
,O cmd <b>cd</b>	>	
,O cmd hostname	>	
,O cmd diskpart	>	
,O cmdlet	>	

2. Before pinging the **Parrot Security** virtual machine, ensure that it is running.

3. Check for a reply from the virtual machine. Here, as an example, we are using the **Parrot Security** virtual machine with the IP address **10.10.1.12** (this IP address may be different in your lab network).



- 4. Now, switch to the **Parrot Security** virtual machine and login using credentials **analyst/toor**.
- 5. Select the **MATE Terminal** icon available at the top section of the Desktop to launch Terminal window.



Lab Setup Guide Page 98

🛑 🔵 😑 Parrot Terminal
File Edit View Search Terminal Help
[analyst@parrot]-[~] [sping 10.10.1.11]
PING 10.10.1.11 (10.10.1.11) 56(84) bytes of data.
54 bytes from 10.10.1.11: icmp_seq=1 ttl=128 time=0.729 ms
54 bytes from 10.10.1.11: icmp_seq=2 ttl=128 time=0.988 ms
54 bytes from 10.10.1.11: icmp_seq=3 ttl=128 time=0.924 ms
54 bytes from 10.10.1.11: icmp_seq=4 ttl=128 time=1.26 ms
54 bytes from 10.10.1.11: icmp_seq=5 ttl=128 time=0.658 ms
54 bytes from 10.10.1.11: icmp_seq=6 ttl=128 time=0.492 ms
54 bytes from 10.10.1.11: icmp seq=7 ttl=128 time=0.893 ms

6. In the Terminal window, type ping 10.10.1.11 to ping the Windows 11 virtual machine.

7. This shows that both the virtual machines are interconnected.

[Back to Configuration Task Outline]

#### **CT#23: Take Snapshots of Virtual Machines**

- 1. Ensure that all the virtual machines are turned off.
- 2. In the VMware Workstation window, click on Windows 11 in the left pane and then the

Take a snapshot of this virtual machine  $\binom{1+5}{1}$  icon, as shown in the screenshot.



Certified Threat Intelligence Analyst Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

3. The Windows 11 – 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 1	1 - Take Snapshot X
C Ta	king a snapshot lets you preserve the state of the virtual achine so that you can return to the same state later.
Name:	Windows 11 Snapshot 1
Description:	
	Tako Spanchot Cancol
	Take Shapshot Cancer

4. Similarly, take a snapshot of the **Parrot Security** virtual machine once all the CTs have been completed.

[Back to Configuration Task Outline]

# **End of the Document**



# **EC-COUNCI** Building A Culture Of Security

EC-Council Official Curricula