Cyber lab configuration

as target machines **Win10 and** Win11

Attacking system **Kali Linux**

-Windows installation media can be found on the school network P:\Students (\\file1\programs) or online

In this lab, security updates are not applied to the Win10 machine to ensure that there is as much "attack surface" as possible.
- ***NOTE!*** *Under normal circumstances, it is advisable to get all possible security updates for the operating system and installed programs and to ensure that the virus definition databases are up to date.*

It is a good idea to disable Defender from your Win10 workstation using Local Group Policy and prevent Windows from scanning for security updates.

Win10 update and Defender blocker with Group Policy.

Gpedit.mscComputer Configuration > Administrative Templates > Windows Components > Windows Updates > Configure Automatic Updates > Disabled

Computer Configuration > Administrative Templates > Windows Components > Windows Defender > Turn off Windows Defender > Enabled

tai

Defender esto rekisterieditorilla

RegeditHKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender

-On the right-side, right-click on the empty area, click New, click DWORD (32-bit) value and then name it as DisableAntiSpyware.

-Double-click on DisableAntiSpyware and change its value data to 1 to disable Windows Defender.

-Restore the value data to “0” to enable Defender again.

Quick'n Easy FTP Server 3.2 Lite is installed on a Win10 machine (can also be installed on a Win11 machine)- can be found.zip package (ftpserver3lite.zip) in

this itsLearning course and in the school's network distribution of Z:\VAIPE\LUKU\Kyber20-ohjelmia (\\file2\common\permanent)

Win10 and Win11 machines are installed with an older Firefox browser

- can be found on the school network under Z:\VAIPE\LUKU\Kyber20-ohjelmia (\\file2\common\permanent)Win10 and Win11 machines are installed Xampp

- can be found on the school's network under Z:\VAIPE\LUKU\Kyber20-ohjelmia (\\file2\common\permanent)

- after installation, you should configure Apache and MySQL to start automatically (FileZilla can also be started on a Win11 machine if Quick'n Easy FTP Server is not installed)

Attack machine Kali Linux.
- Latest version online

Summary of operating systems, programs, and installation file locations to install:

Win 10
- Xampp (Z:\VAIPE\CHAPTER\Kyber20-ohjelmia (\\file2\common\permanent)

- Quick’n Easy FTP Server (Z:\VAIPE\LUKU\Kyber20-ohjelmia (\\file2\common\permanent)

- Older Firefox browser (Z:\VAIPE\CHAPTER\Kyber20-ohjelmia (\\file2\common\permanent)

Win 11

- Xampp (Z:\VAIPE\CHAPTER\Kyber20-ohjelmia (\\file2\common\permanent)

- Older Firefox browser (Z:\VAIPE\CHAPTER\Kyber20-ohjelmia (\\file2\common\permanent)

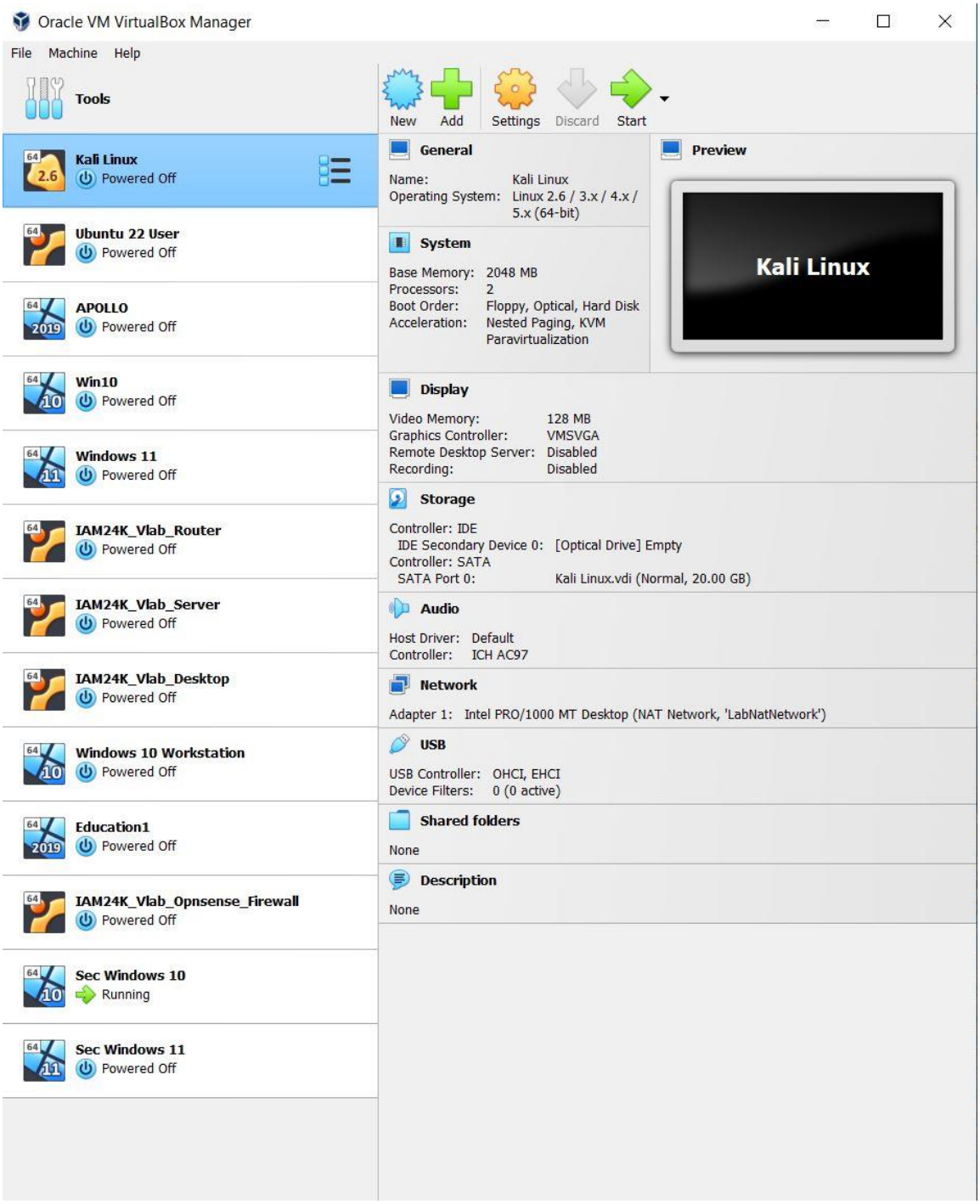
Kali Linux from the web.

Network:

Finally, change the network settings of the machines so that they are on the same network and they ping each other.- On Win10 and Win11 machines, remember to enable ping (Inpound Rules – File and Printer Sharing (Echo Request – ICMPv4-In) Enable

One way to configure the network is as follows:
- In VirtualBox, configure NatNetwork (e.g. 10.114.48.0/24) or use an existing one- Assign Win10 and Win11 and Kali machines fixed IP addresses from this space (e.g. 10.114.48.10, 10.114.48.11 and 10.114.48.30) * You can check the required dhcp and dns settings on the machines once they have received the IP address automatically.

Installing Operating Systems: Kali Linux and Windows 10



Oracle VM VirtualBox Manager

File Machine Help

Tools

New Add Settings Discard Show

- Kali Linux — Powered Off
- Ubuntu 22 User — Powered Off
- APOLLO — Powered Off
- Win10 — Powered Off
- Windows 11 — Powered Off
- IAM24K_Vlab_Router — Powered Off
- IAM24K_Vlab_Server — Powered Off
- IAM24K_Vlab_Desktop — Powered Off
- Windows 10 Workstation — Powered Off
- Education1 — Powered Off
- IAM24K_Vlab_Opnsense_Firewall — Powered Off
- Sec Windows 10 — Running
- Sec Windows 11 — Powered Off

General

Name: Sec Windows 10
Operating System: Windows 10 (64-bit)

System

Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Preview

Storage

Controller: SATA
SATA Port 0: Sec Windows 10.vdi (Normal, 50.00 GB)
SATA Port 1: [Optical Drive] Windows10_.21H2.iso (4.98 GB)

Audio

Host Driver: Default
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'LabNatNetwork')

USB

USB Controller: xHCI
Device Filters: 0 (0 active)

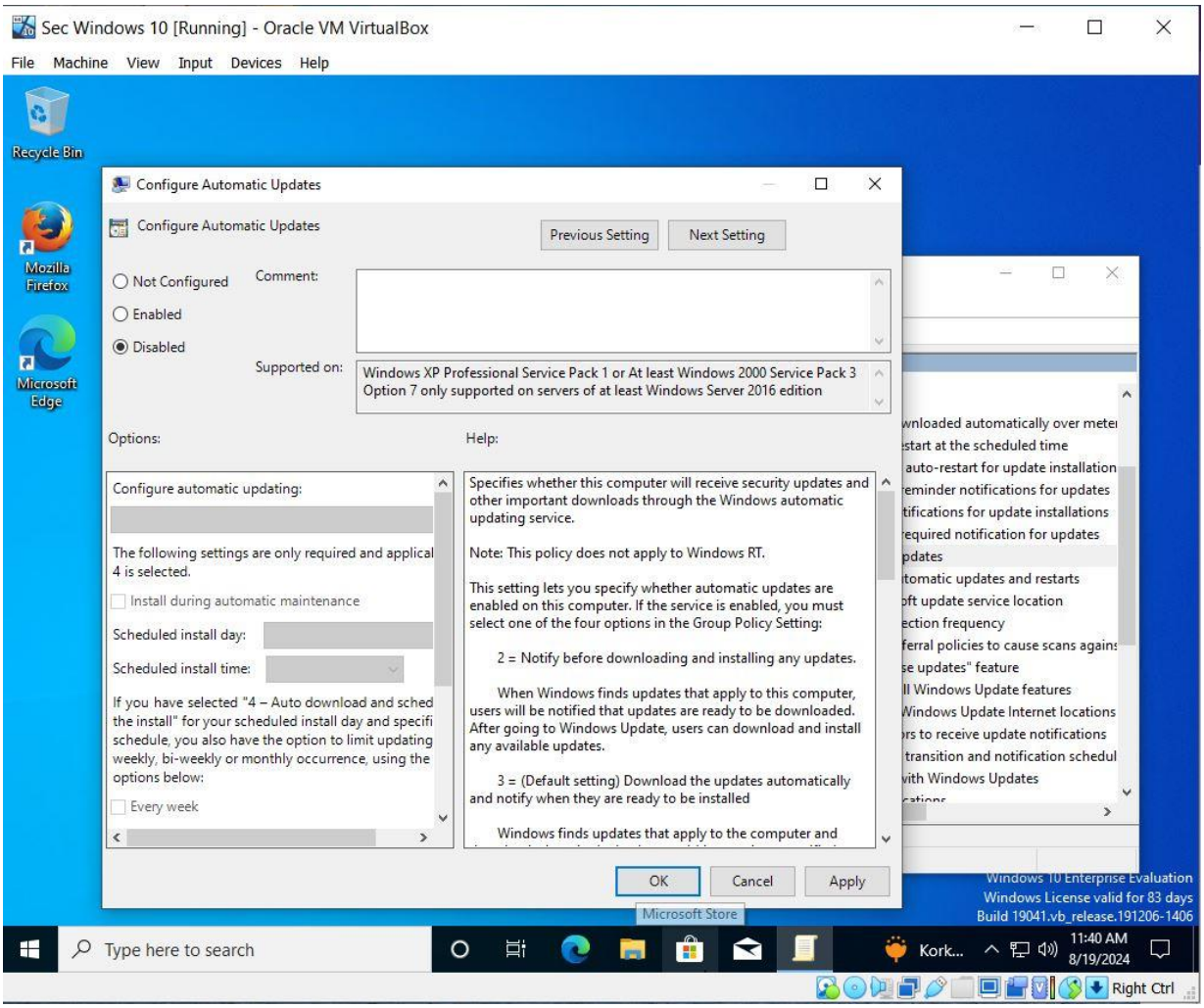
Shared folders

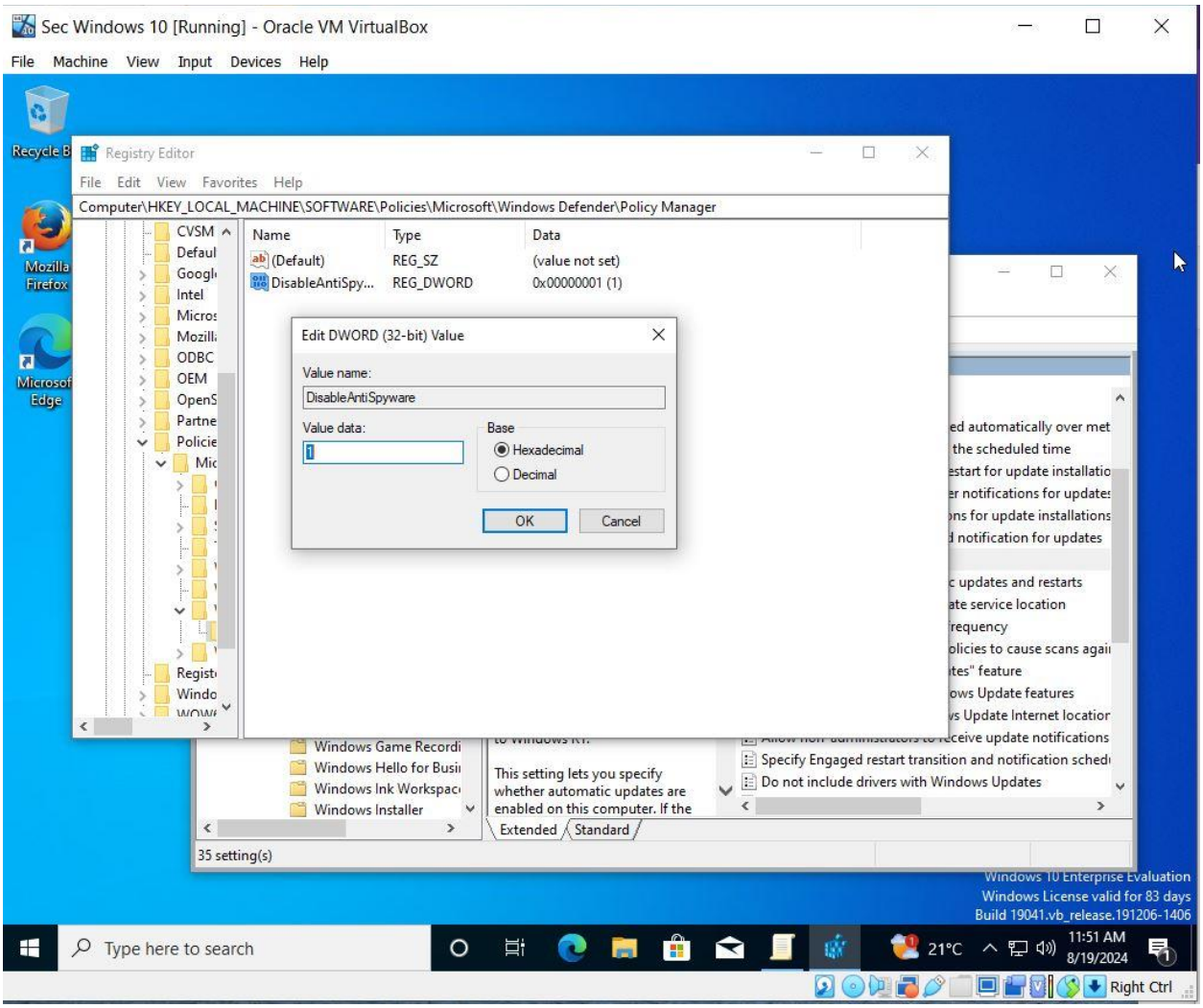
None

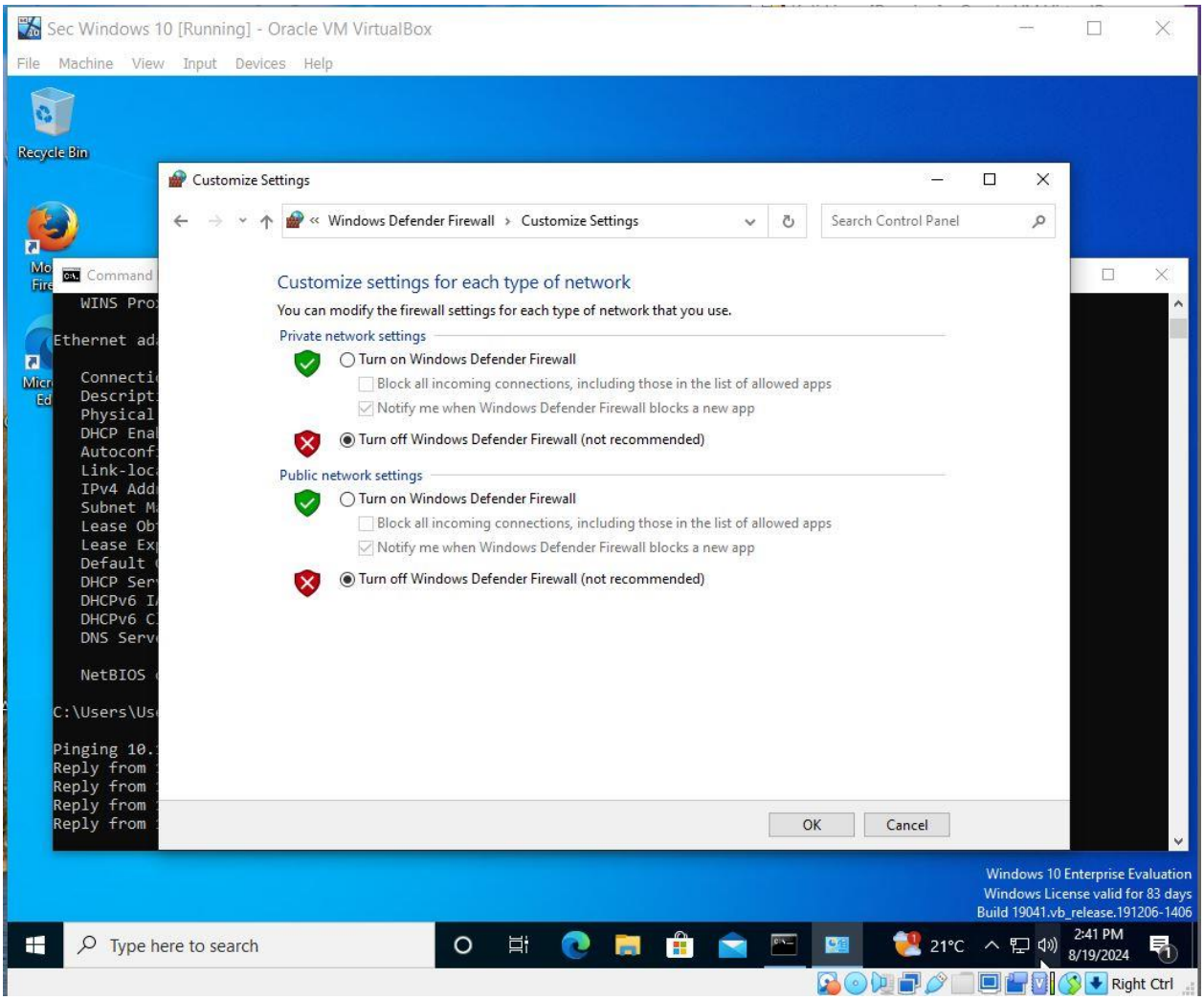
Description

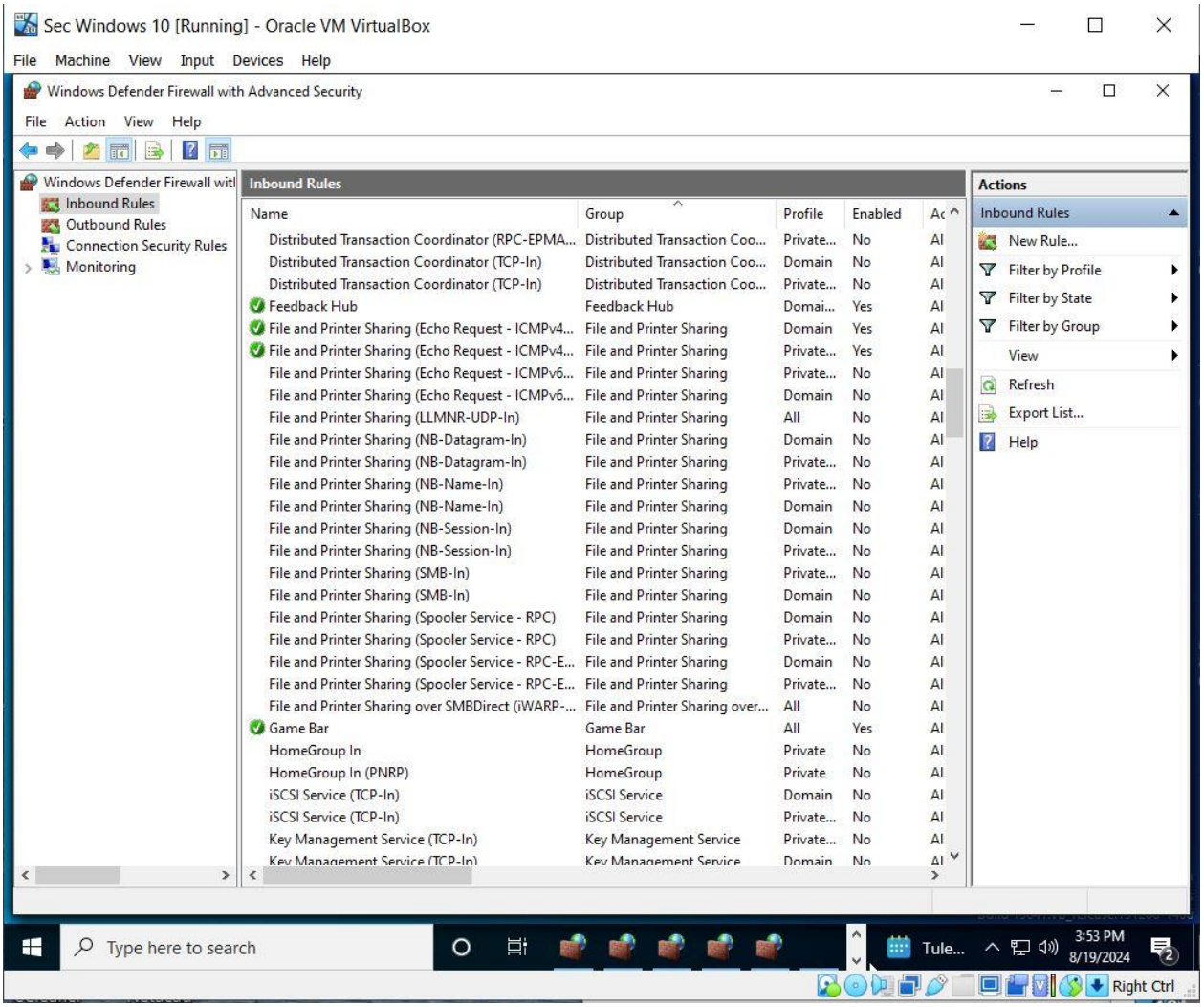
None

Disabling Security Update, Defender and Enabling Ping

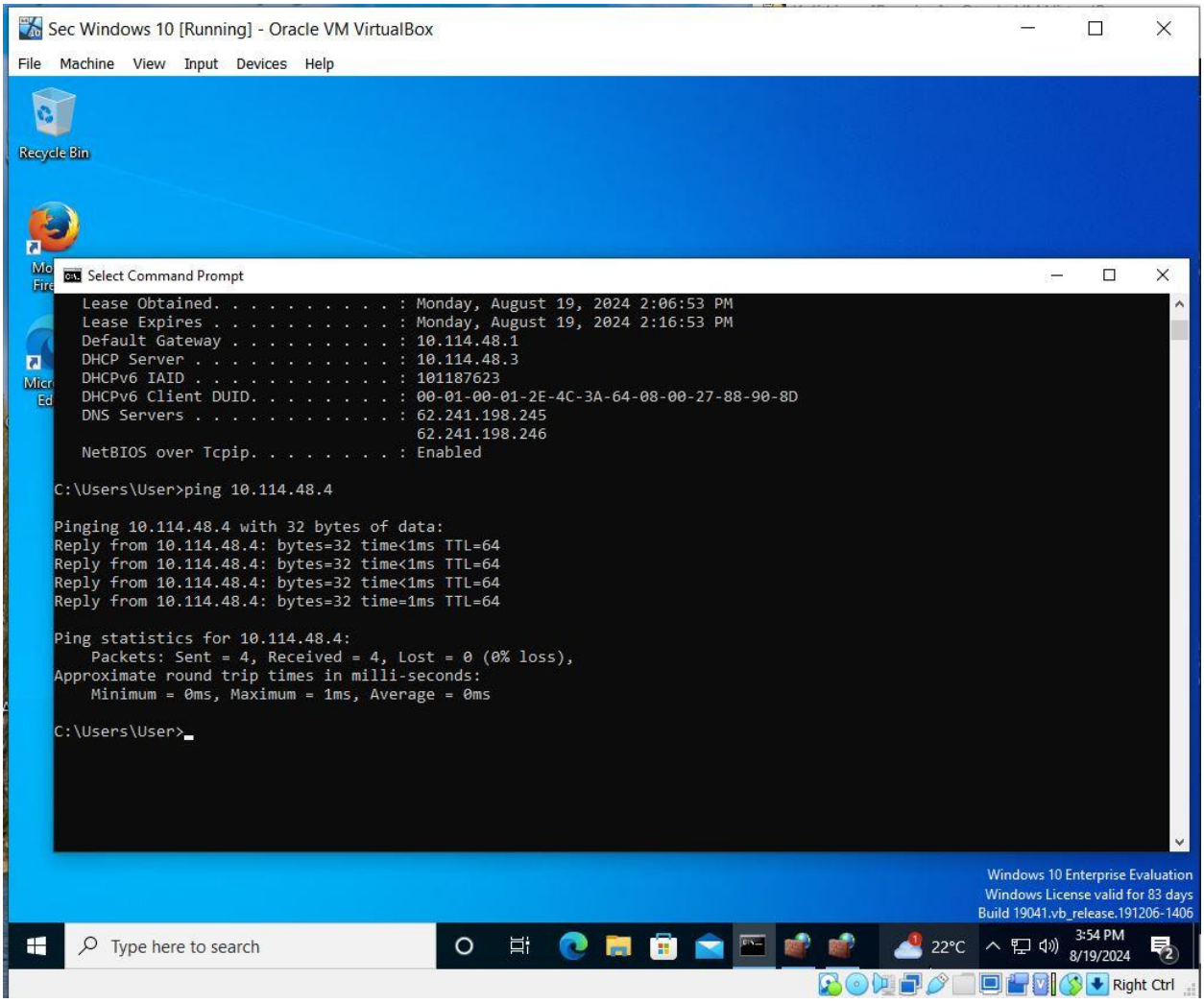


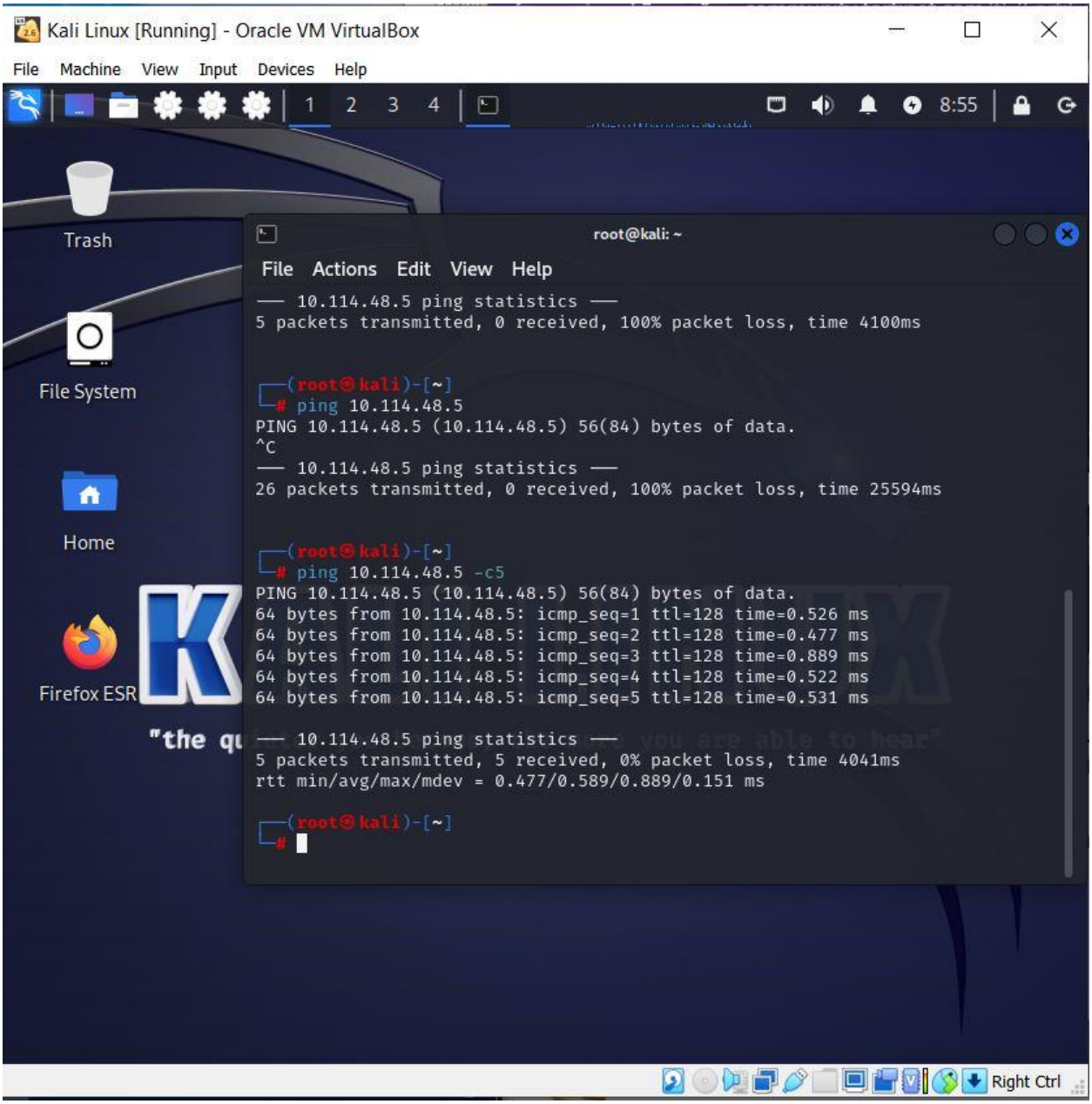

Sec Windows 10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Policy Manager
Name Type Data
(Default) REG_SZ (value not set)
DisableAntiSpy... REG_DWORD 0x00000001 (1)
Edit DWORD (32-bit) Value
Value name:
DisableAntiSpyware
Value data:
1
Base
Hexadecimal
Decimal
OK
Cancel
Windows Game Recordi
Windows Hello for Busi
Windows Ink Workspac
Windows Installer
This setting lets you specify whether automatic updates are enabled on this computer. If the
Specify Engaged restart transition and notification sched
Do not include drivers with Windows Updates
Extended Standard
35 setting(s)
Windows 10 Enterprise Evaluation
Windows License valid for 83 days
Build 19041.vb_release.191206-1406
Type here to search
21°C
11:51 AM
8/19/2024
Right Ctrl


Sec Windows 10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Customize Settings
Windows Defender Firewall › Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network that you use.
Private network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
Public network settings
Turn on Windows Defender Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Defender Firewall blocks a new app
Turn off Windows Defender Firewall (not recommended)
OK
Cancel
Command
Windows 10 Enterprise Evaluation
Windows License valid for 83 days
Build 19041.vb_release.191206-1406
Type here to search
21°C
2:41 PM
8/19/2024
Right Ctrl

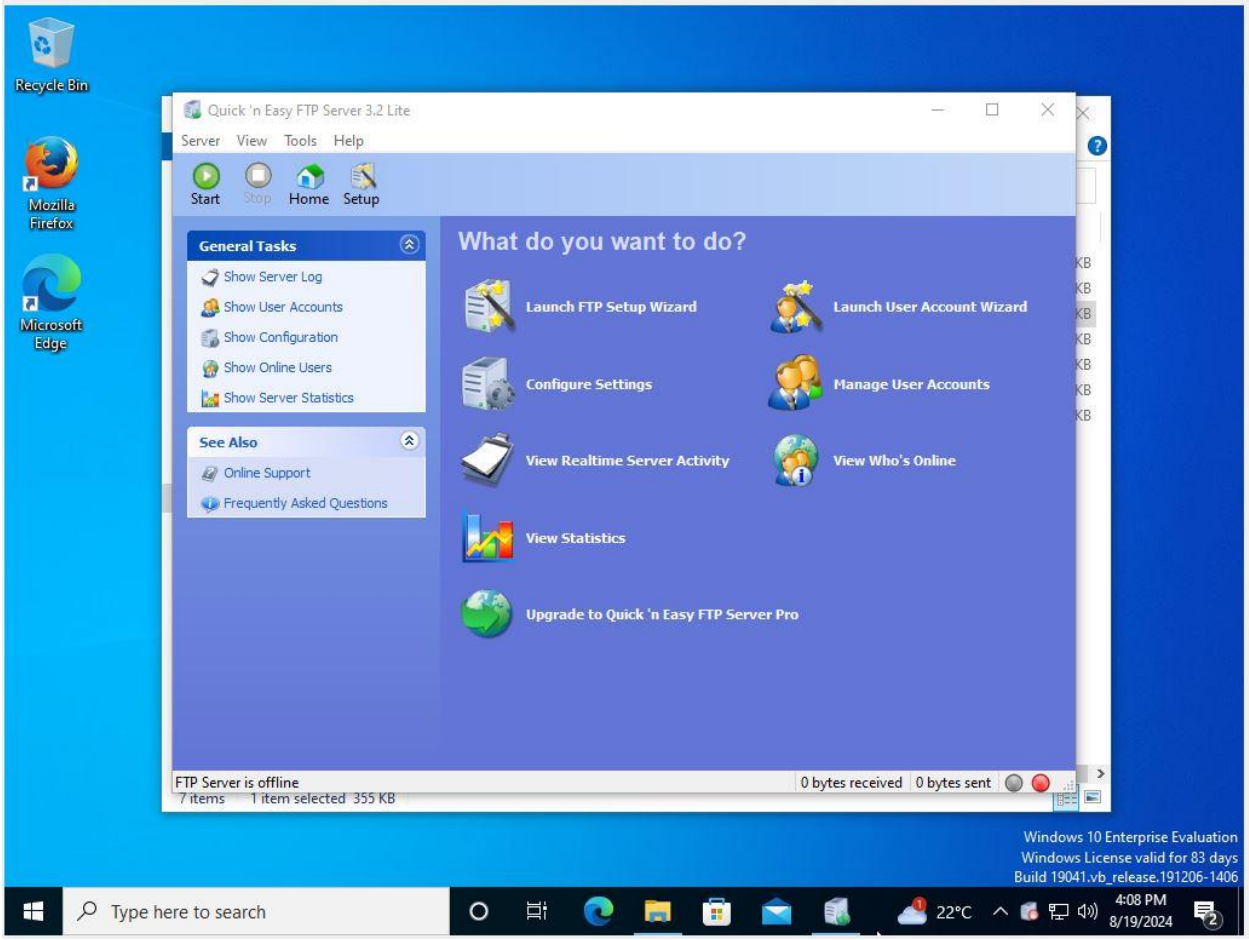

Sec Windows 10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Distributed Transaction Coordinator (RPC-EPMA... Distributed Transaction Coo... Private... No
Distributed Transaction Coordinator (TCP-In) Distributed Transaction Coo... Domain No
Distributed Transaction Coordinator (TCP-In) Distributed Transaction Coo... Private... No
Feedback Hub Feedback Hub Domai... Yes
File and Printer Sharing (Echo Request - ICMPv4... File and Printer Sharing Domain Yes
File and Printer Sharing (Echo Request - ICMPv4... File and Printer Sharing Private... Yes
File and Printer Sharing (Echo Request - ICMPv6... File and Printer Sharing Private... No
File and Printer Sharing (Echo Request - ICMPv6... File and Printer Sharing Domain No
File and Printer Sharing (LLMNR-UDP-In) File and Printer Sharing All No
File and Printer Sharing (NB-Datagram-In) File and Printer Sharing Domain No
File and Printer Sharing (NB-Datagram-In) File and Printer Sharing Private... No
File and Printer Sharing (NB-Name-In) File and Printer Sharing Private... No
File and Printer Sharing (NB-Name-In) File and Printer Sharing Domain No
File and Printer Sharing (NB-Session-In) File and Printer Sharing Domain No
File and Printer Sharing (NB-Session-In) File and Printer Sharing Private... No
File and Printer Sharing (SMB-In) File and Printer Sharing Private... No
File and Printer Sharing (SMB-In) File and Printer Sharing Domain No
File and Printer Sharing (Spooler Service - RPC) File and Printer Sharing Domain No
File and Printer Sharing (Spooler Service - RPC) File and Printer Sharing Private... No
File and Printer Sharing (Spooler Service - RPC-E... File and Printer Sharing Domain No
File and Printer Sharing (Spooler Service - RPC-E... File and Printer Sharing Private... No
File and Printer Sharing over SMBDirect (iWARP-... File and Printer Sharing over... All No
Game Bar Game Bar All Yes
HomeGroup In HomeGroup Private No
HomeGroup In (PNRP) HomeGroup Private No
iSCSI Service (TCP-In) iSCSI Service Domain No
iSCSI Service (TCP-In) iSCSI Service Private... No
Key Management Service (TCP-In) Key Management Service Private... No
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Type here to search
Tule...
3:53 PM
8/19/2024
Right Ctrl

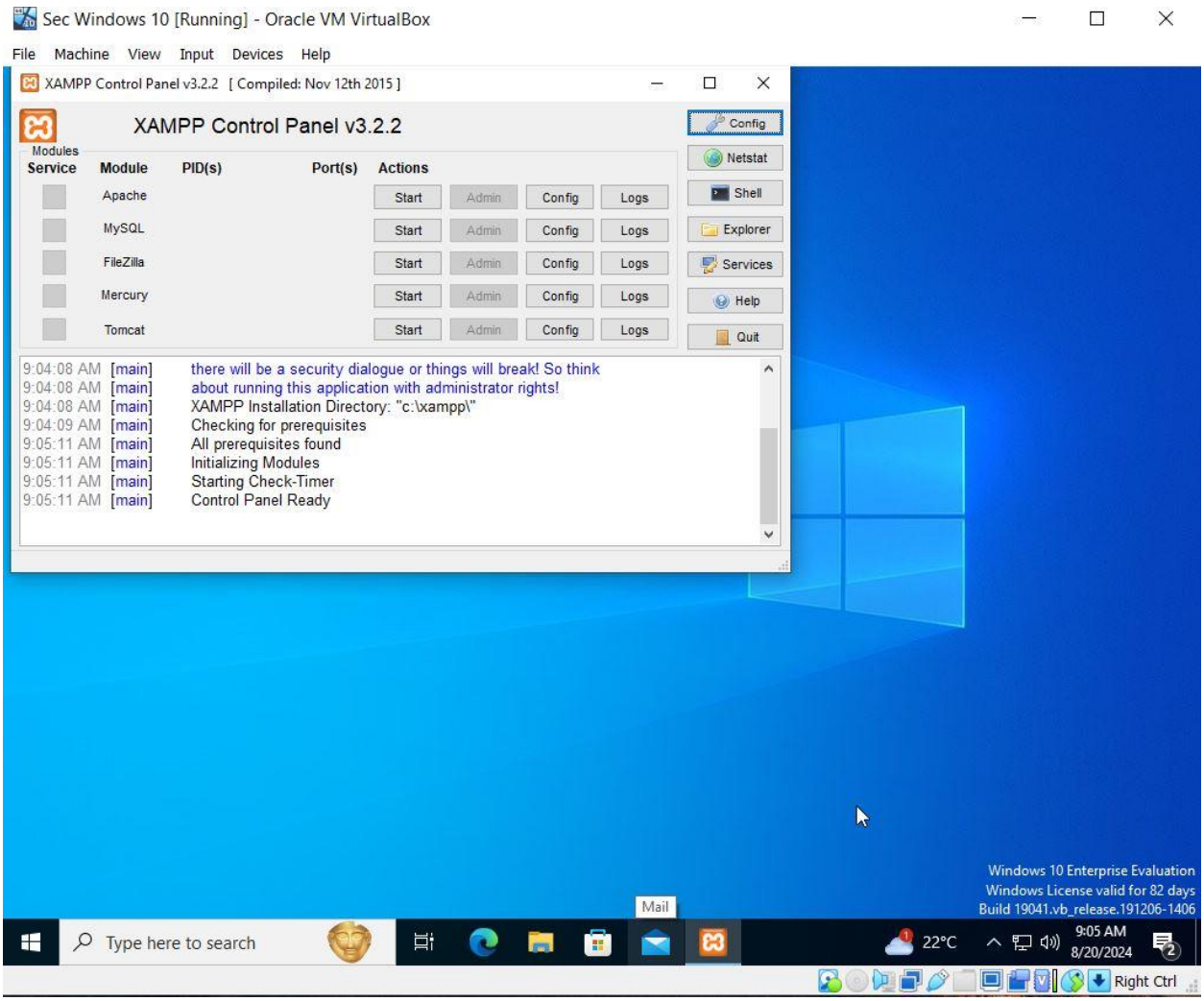
Pinging and Communicating devices




Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
8:55
Trash
File System
Home
Firefox ESR
root@kali: ~
File Actions Edit View Help
── 10.114.48.5 ping statistics ──
5 packets transmitted, 0 received, 100% packet loss, time 4100ms
┌──(root㉿kali)-[~]
└─# ping 10.114.48.5
PING 10.114.48.5 (10.114.48.5) 56(84) bytes of data.
^C
── 10.114.48.5 ping statistics ──
26 packets transmitted, 0 received, 100% packet loss, time 25594ms
┌──(root㉿kali)-[~]
└─# ping 10.114.48.5 -c5
PING 10.114.48.5 (10.114.48.5) 56(84) bytes of data.
64 bytes from 10.114.48.5: icmp_seq=1 ttl=128 time=0.526 ms
64 bytes from 10.114.48.5: icmp_seq=2 ttl=128 time=0.477 ms
64 bytes from 10.114.48.5: icmp_seq=3 ttl=128 time=0.889 ms
64 bytes from 10.114.48.5: icmp_seq=4 ttl=128 time=0.522 ms
64 bytes from 10.114.48.5: icmp_seq=5 ttl=128 time=0.531 ms
── 10.114.48.5 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4041ms
rtt min/avg/max/mdev = 0.477/0.589/0.889/0.151 ms
┌──(root㉿kali)-[~]
└─#
Right Ctrl

Installing Mozilla, FTP server and XAMPP




Sec Windows 10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
XAMPP Control Panel v3.2.2 [Compiled: Nov 12th 2015]
XAMPP Control Panel v3.2.2
Modules
Service Module PID(s) Port(s) Actions
Apache Start Admin Config Logs
MySQL Start Admin Config Logs
FileZilla Start Admin Config Logs
Mercury Start Admin Config Logs
Tomcat Start Admin Config Logs
Config
Netstat
Shell
Explorer
Services
Help
Quit
9:04:08 AM [main] there will be a security dialogue or things will break! So think
9:04:08 AM [main] about running this application with administrator rights!
9:04:08 AM [main] XAMPP Installation Directory: "c:\xampp\"
9:04:09 AM [main] Checking for prerequisites
9:05:11 AM [main] All prerequisites found
9:05:11 AM [main] Initializing Modules
9:05:11 AM [main] Starting Check-Timer
9:05:11 AM [main] Control Panel Ready
Windows 10 Enterprise Evaluation
Windows License valid for 82 days
Build 19041.vb_release.191206-1406
Mail
Type here to search
22°C
9:05 AM
8/20/2024
Right Ctrl