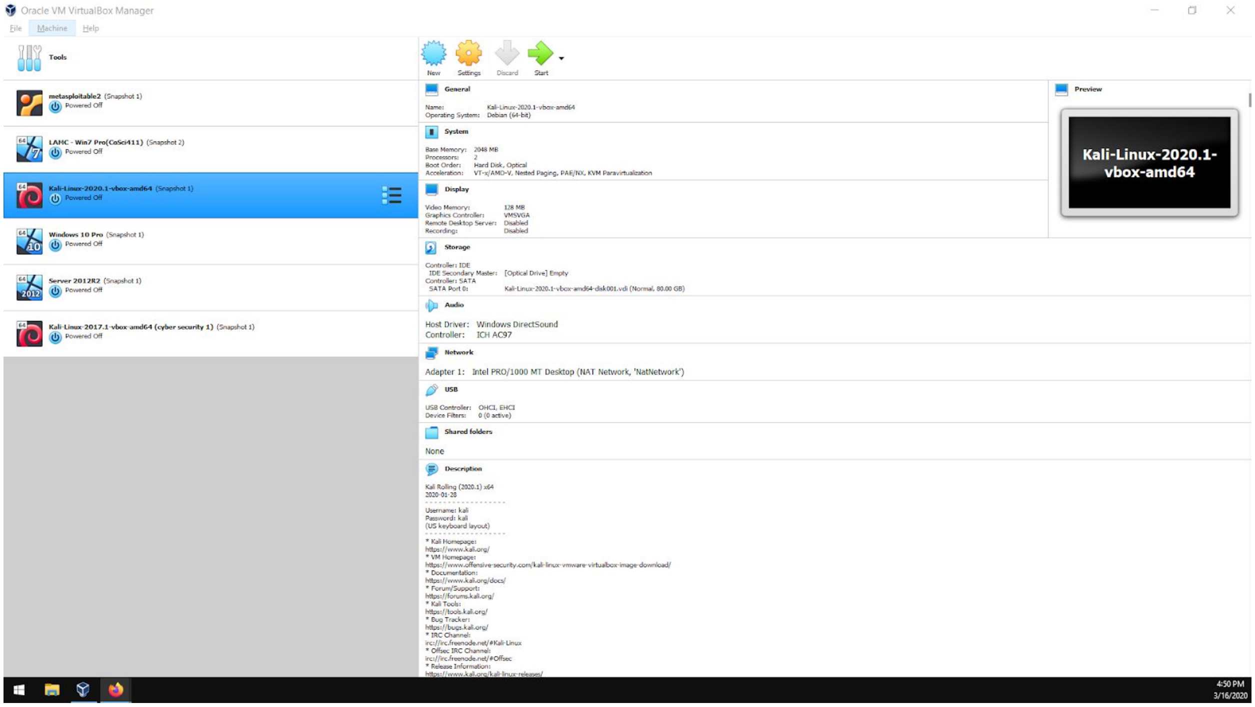
Cyber Report - Build your LAN

1. Each assignment has a goal. What is the assignment and how will you find the solution?
The goal of this

> The goal of this cyber report is to document the creation of a NAT network, connection of two virtual machines to the NAT network, open any firewalls that prevent ICMP connections and test each connection with a PING command. Procedure steps will be documented below each screenshot with an appropriate title at the top. Video tutorial notes will be located on the last page of this report.

2. Demonstration of the steps taken with screenshots (snipping tool) from your computer. You need to show the steps you took as you took them.

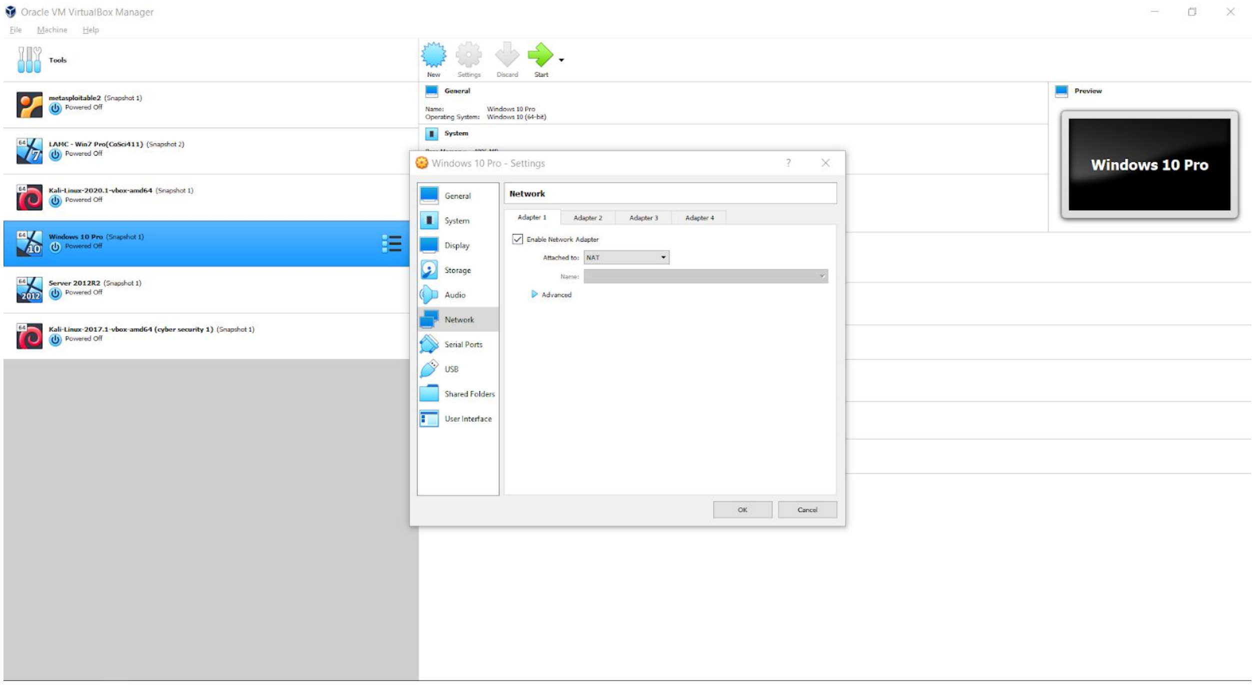
VirtualBox main menu


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
metasploitable2 (Snapshot 1)
Powered Off
LAMC - Win7 Pro(CoSci411) (Snapshot 2)
Powered Off
Kali-Linux-2020.1-vbox-amd64 (Snapshot 1)
Powered Off
Windows 10 Pro (Snapshot 1)
Powered Off
Server 2012R2 (Snapshot 1)
Powered Off
Kali-Linux-2017.1-vbox-amd64 (cyber security 1) (Snapshot 1)
Powered Off
New
Settings
Discard
Start
Preview
Kali-Linux-2020.1-vbox-amd64
4:50 PM
3/16/2020

```
General
Name:              Kali-Linux-2020.1-vbox-amd64
Operating System:  Debian (64-bit)

System
Base Memory:   2048 MB
Processors:    2
Boot Order:    Hard Disk, Optical
Acceleration:  VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

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

Storage
Controller: IDE
 IDE Secondary Master:   [Optical Drive] Empty
Controller: SATA
 SATA Port 0:            Kali-Linux-2020.1-vbox-amd64-disk001.vdi (Normal, 80.00 GB)

Audio
Host Driver:  Windows DirectSound
Controller:   ICH AC97

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

USB
USB Controller:  OHCI, EHCI
Device Filters:  0 (0 active)

Shared folders
None

Description
Kali Rolling (2020.1) x64
2020-01-28
- - - - - - - - - - - - - - - - - -
Username: kali
Password: kali
(US keyboard layout)
- - - - - - - - - - - - - - - - - -
* Kali Homepage:
https://www.kali.org/
* VM Homepage:
https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/
* Documentation:
https://www.kali.org/docs/
* Forum/Support:
https://forums.kali.org/
* Kali Tools:
https://tools.kali.org/
* Bug Tracker:
https://bugs.kali.org/
* IRC Channel:
irc://irc.freenode.net/#Kali-Linux
* Offsec IRC Channel:
irc://irc.freenode.net/#Offsec
* Release Information:
https://www.kali.org/kali-linux-releases/
```

Right-click on the image you wish to edit it’s network settings and choose Settings. Then click on Network.

Windows 10 Pro Settings



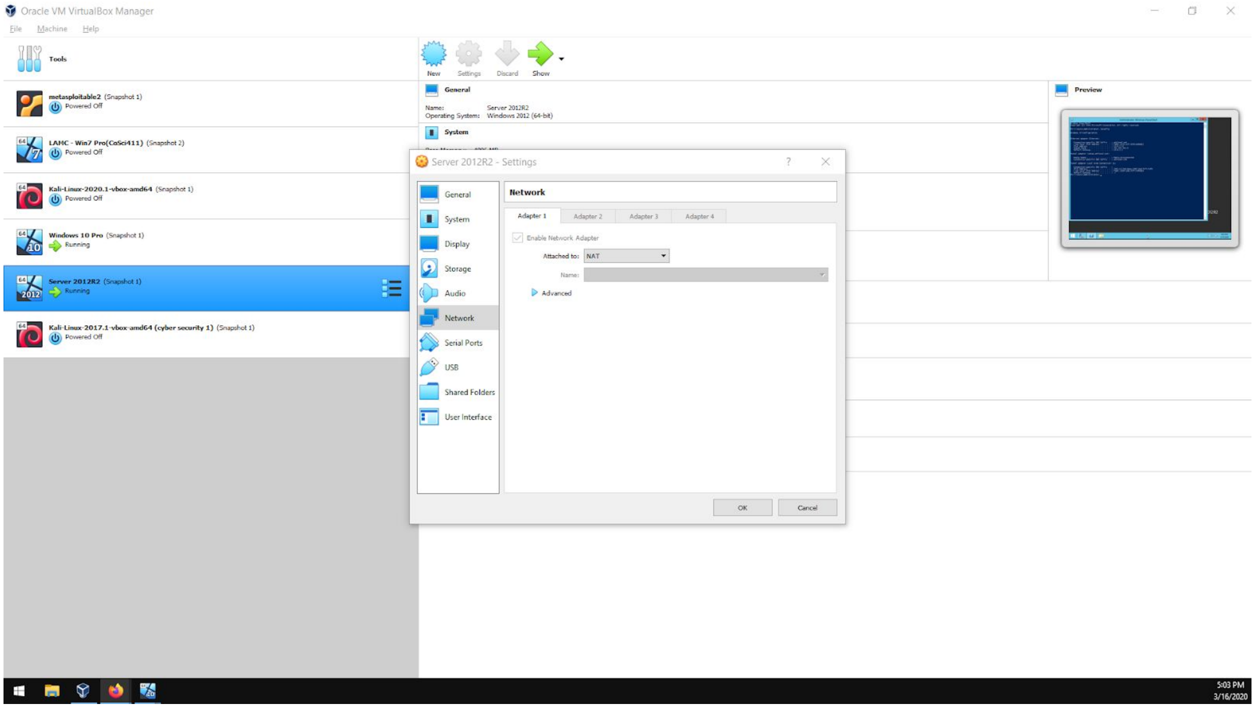
metasploitable2 (Snapshot 1) Powered Off
LAMC - Win7 Pro(CoSci411) (Snapshot 2) Powered Off
Kali-Linux-2020.1-vbox-amd64 (Snapshot 1) Powered Off
Windows 10 Pro (Snapshot 1) Powered Off
Server 2012R2 (Snapshot 1) Powered Off
Kali-Linux-2017.1-vbox-amd64 (cyber security 1) (Snapshot 1) Powered Off

General
Name: Windows 10 Pro
Operating System: Windows 10 (64-bit)

Network
☑ Enable Network Adapter
Attached to: NAT
Name:

Note that for Windows 10 Pro the Network is attached to a NAT network

Server 2012R2 Settings



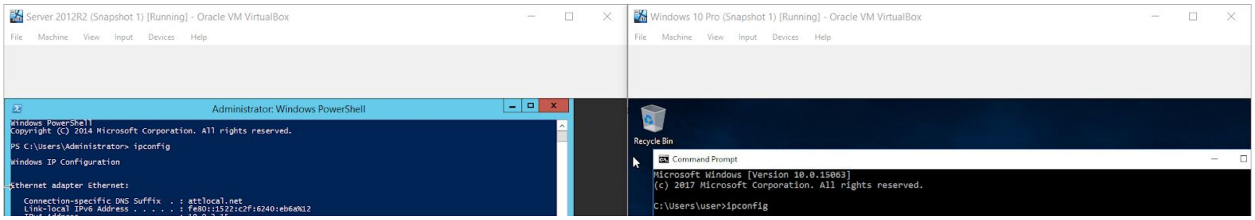
metasploitable2 (Snapshot 1) Powered Off
LAMC - Win7 Pro(CoSci411) (Snapshot 2) Powered Off
Kali-Linux-2020.1-vbox-amd64 (Snapshot 1) Powered Off
Windows 10 Pro (Snapshot 1) Running
Server 2012R2 (Snapshot 1) Running
Kali-Linux-2017.1-vbox-amd64 (cyber security 1) (Snapshot 1) Powered Off

General
Name: Server 2012R2
Operating System: Windows 2012 (64-bit)

Network
☑ Enable Network Adapter
Attached to: NAT
Name:

Note the same setting for Network “Attached to: NAT”. Both of these virtual machines should have the same IP.

Snapshot of IPCONFIG on both VM’s



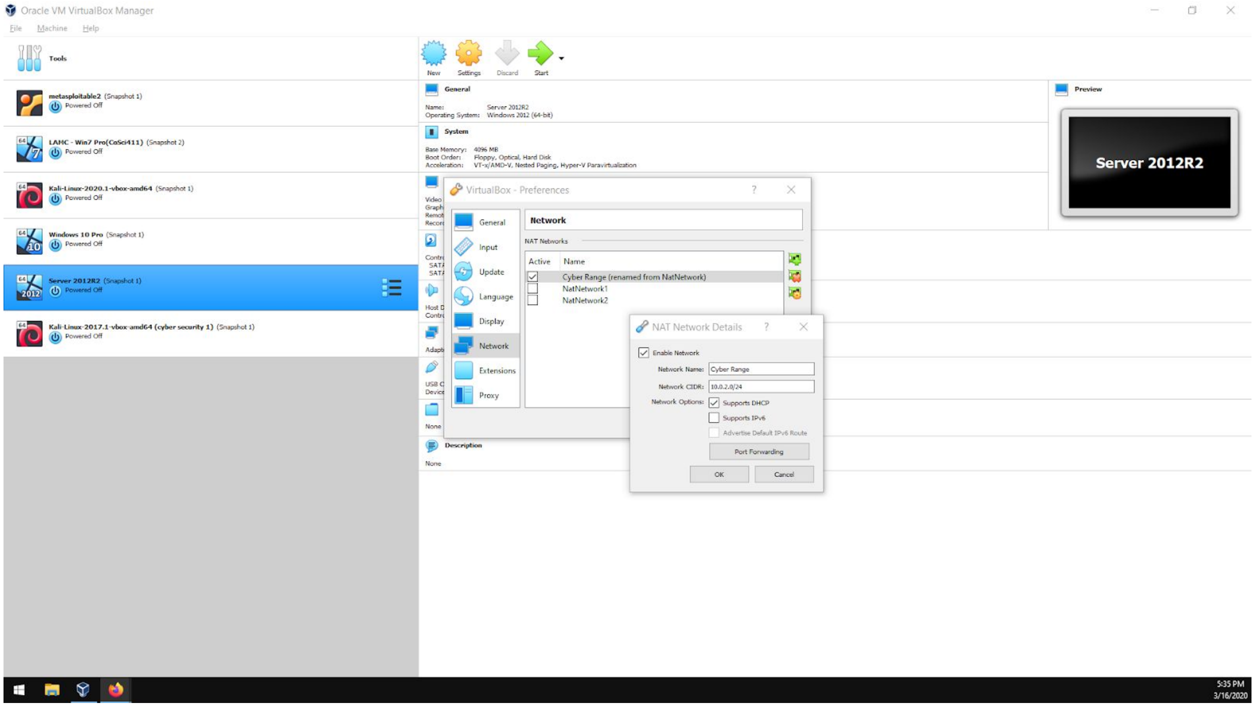
Server 2012R2 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
Windows 10 Pro (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Command Prompt

```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : attlocal.net
   Link-local IPv6 Address . . . . . : fe80::1522:c2f:6240:eb6a%12
```

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\user>ipconfig
```

To verify that both images have the same IP, use IPCONFIG to note the IP in use. Both have the same IPv4 address of 10.0.2.15. We want each to have their own unique IP so that communication can take place.

Virtualbox main menu



metasploitable2 (Snapshot 1) Powered Off
LAMC - Win7 Pro(CoSci411) (Snapshot 2) Powered Off
Kali-Linux-2020.1-vbox-amd64 (Snapshot 1) Powered Off
Windows 10 Pro (Snapshot 1) Powered Off
Server 2012R2 (Snapshot 1) Powered Off
Kali-Linux-2017.1-vbox-amd64 (cyber security 1) (Snapshot 1) Powered Off

General
Name: Server 2012R2
Operating System: Windows 2012 (64-bit)

System
Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Description
None

VirtualBox - Preferences

Network

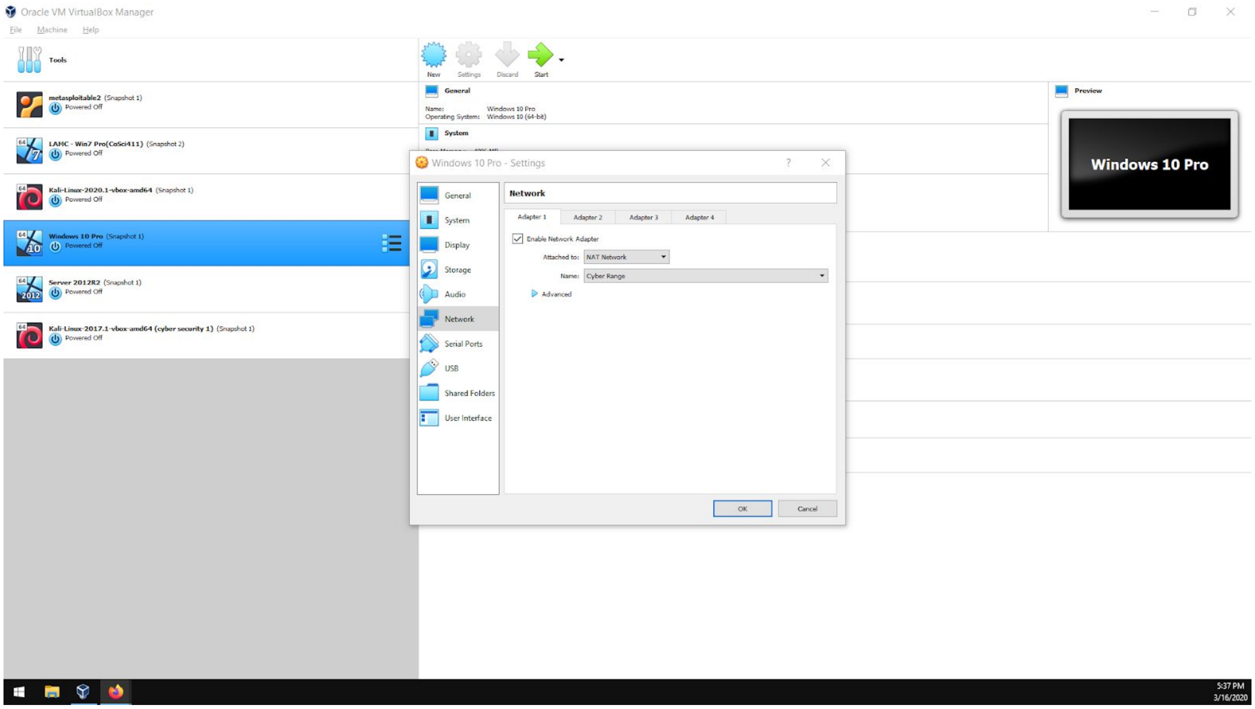
NAT Networks

Active	Name
☑	Cyber Range (renamed from NatNetwork)
□	NatNetwork1
□	NatNetwork2

NAT Network Details

☑ Enable Network
Network Name: Cyber Range
Network CIDR: 10.0.2.0/24
Network Options: ☑ Supports DHCP
□ Supports IPv6
□ Advertise Default IPv6 Route

Next we'll create a NAT Network called "Cyber Range" from the virtualbox main menu.
Windows 10 Pro Settings


Oracle VM VirtualBox Manager
File Machine Help
Tools
New Settings Discard Start
metasploitable2 (Snapshot 1) Powered Off
LAMC - Win7 Pro(CoSci411) (Snapshot 2) Powered Off
Kali-Linux-2020.1-vbox-amd64 (Snapshot 1) Powered Off
Windows 10 Pro (Snapshot 1) Powered Off
Server 2012R2 (Snapshot 1) Powered Off
Kali-Linux-2017.1-vbox-amd64 (cyber security 1) (Snapshot 1) Powered Off
General
System
Preview
Windows 10 Pro
Windows 10 Pro - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Adapter 1 Adapter 2 Adapter 3 Adapter 4
Advanced
OK Cancel
5:37 PM
3/16/2020

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

Network

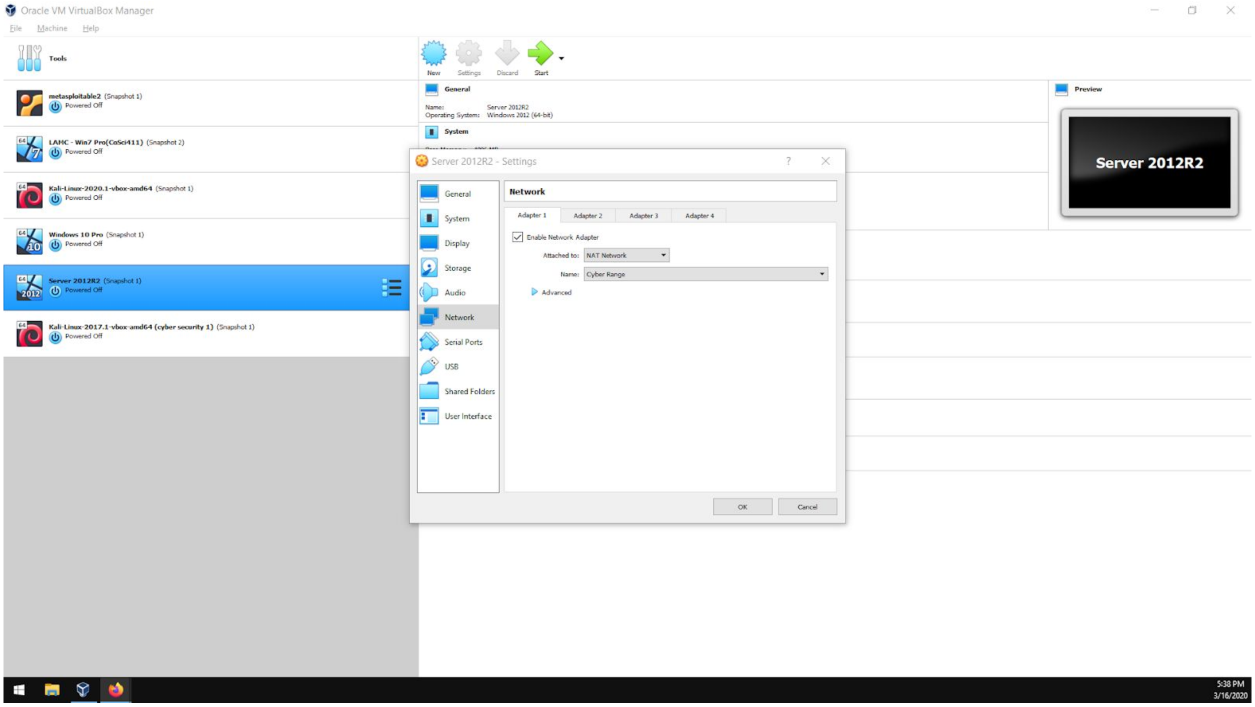
☑ Enable Network Adapter

Attached to: NAT Network

Name: Cyber Range

To accomplish unique IP's for each system we must change how the virtual adapter handles our connection to the virtual host. Right-click on each virtual machine requiring the change and choose Settings → Network → then change "Attached to: NAT" to be "Attached to: NAT Network" and select Cyber Range.

Server 2012R2 Settings



Name: Server 2012R2
Operating System: Windows 2012 (64-bit)

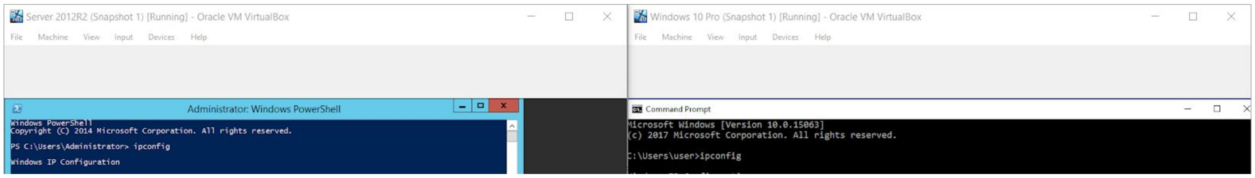
☑ Enable Network Adapter

Attached to: NAT Network

Name: Cyber Range

Setting NAT Network and Cyber Range

Snapshot of both Images with IPCONFIG results

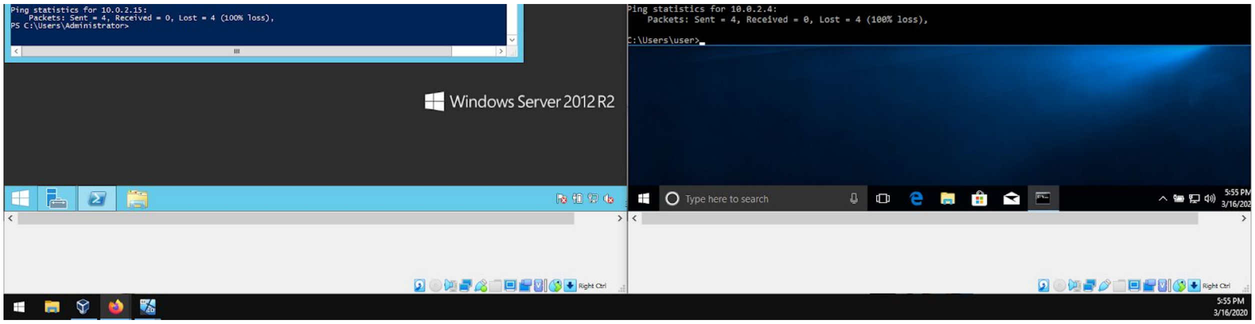

Server 2012R2 (Snapshot 1) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Administrator: Windows PowerShell
Windows 10 Pro (Snapshot 1) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Command Prompt

```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig

Windows IP Configuration
```

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\user>ipconfig
```

To verify we have unique IP addresses on each machine we have to boot up each machine again and use IPCONFIG at a command prompt or powershell (Server 2012R2). Note that Server 2012R2 has an IPv4 of 10.0.2.4 and Windows 10 Pro has an IPv4 of 10.0.2.15. Next we will test the connection between the virtual machines using PING.

PING results

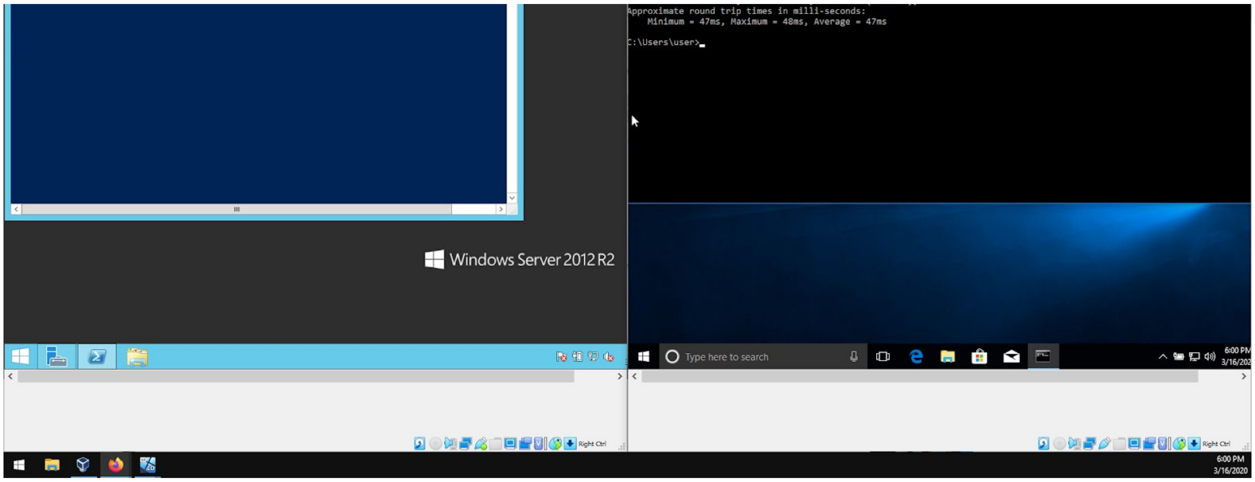


```
Ping statistics for 10.0.2.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Administrator>
```

```
Ping statistics for 10.0.2.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user>
```

Both virtual machines have timed out of the ping request. So we test each independent machine by pinging google.

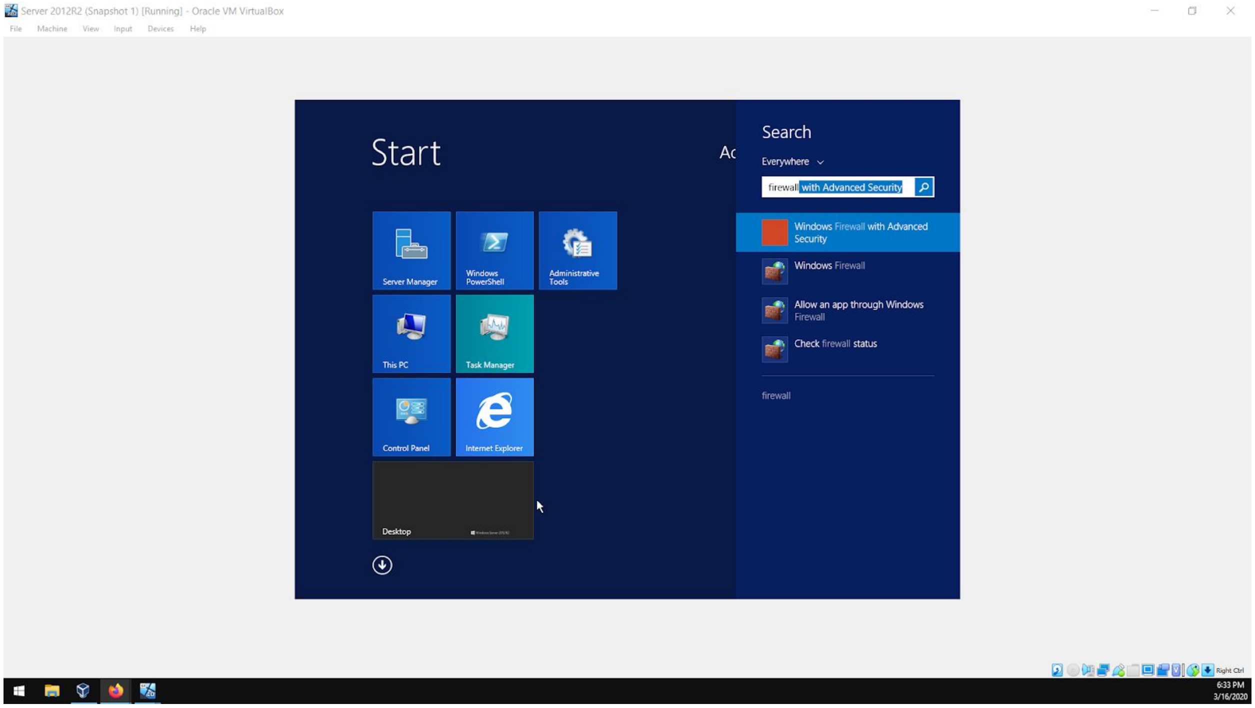
PING command investigation



```
Approximate round trip times in milli-seconds:
    Minimum = 47ms, Maximum = 48ms, Average = 47ms

C:\Users\user>
```

We can see that each PING command was successful. So each of our virtual machines can complete a PING but not to the machine we want so far. Since both computers are behind a firewall we investigate whether that’s the cause of not delivering an ICMP message.

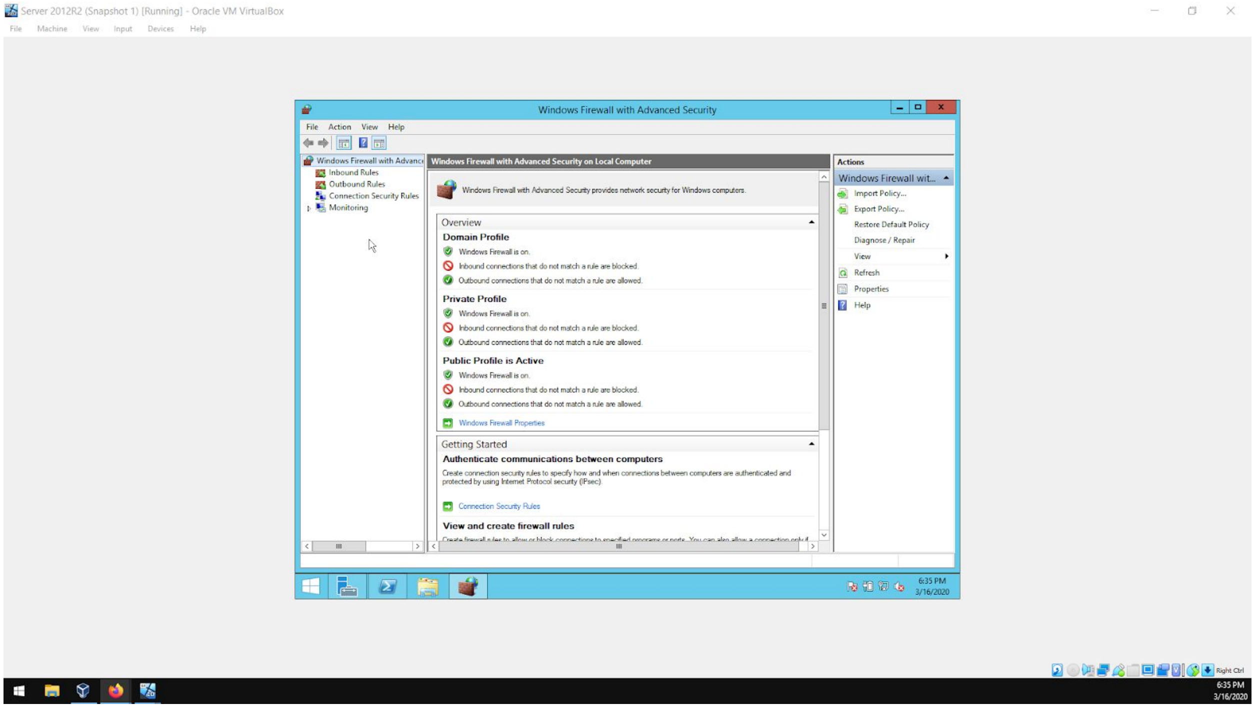
Server 2012R2 Search



firewall with Advanced Security

Searching for firewall displays the option we want

Windows Firewall with Advanced Security Server 2012R2


Server 2012R2 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Actions
Windows Firewall wit...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help
Overview
Windows Firewall Properties
Getting Started
Connection Security Rules
6:35 PM
3/16/2020

Windows Firewall with Advanced Security provides network security for Windows computers.

Domain Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

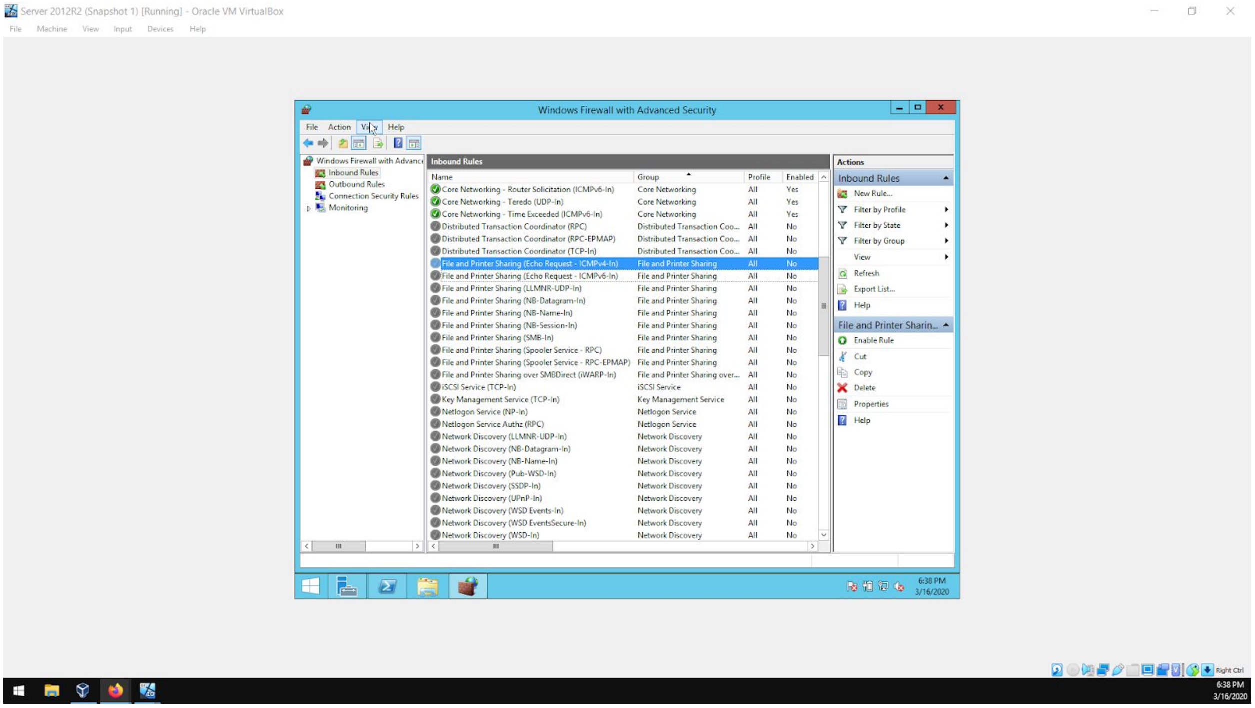
Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

View and create firewall rules

Navigate to Inbound Rules then on the right side select File and Printer Sharing (Echo Request - ICMPv4-In).

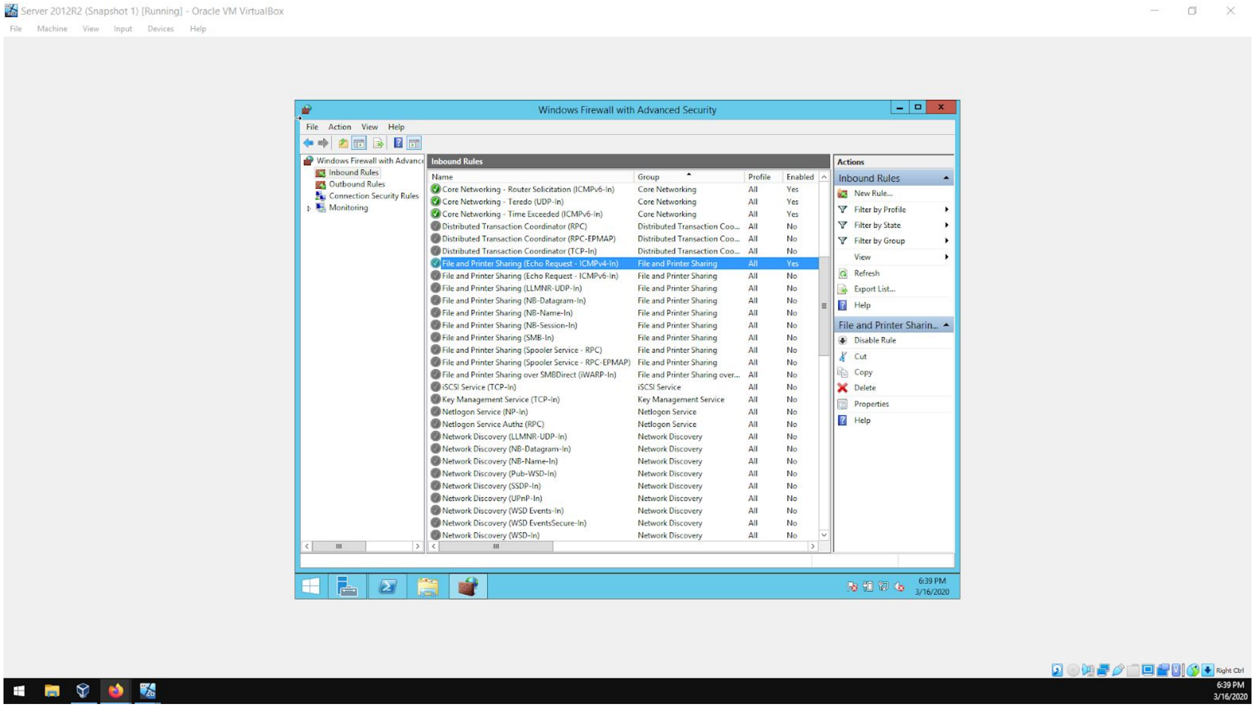
Inbound Rules Windows Firewall with Advanced Security Server 2012R2



Name	Group	Profile	Enabled
Core Networking - Router Solicitation (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	All	Yes
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	All	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	All	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	All	No
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	All	No
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	All	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	All	No
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	No
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	All	No
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	All	No
File and Printer Sharing over SMBDirect (iWARP-In)	File and Printer Sharing over...	All	No
iSCSI Service (TCP-In)	iSCSI Service	All	No
Key Management Service (TCP-In)	Key Management Service	All	No
Netlogon Service (NP-In)	Netlogon Service	All	No
Netlogon Service Authz (RPC)	Netlogon Service	All	No
Network Discovery (LLMNR-UDP-In)	Network Discovery	All	No
Network Discovery (NB-Datagram-In)	Network Discovery	All	No
Network Discovery (NB-Name-In)	Network Discovery	All	No
Network Discovery (Pub-WSD-In)	Network Discovery	All	No
Network Discovery (SSDP-In)	Network Discovery	All	No
Network Discovery (UPnP-In)	Network Discovery	All	No
Network Discovery (WSD Events-In)	Network Discovery	All	No
Network Discovery (WSD EventsSecure-In)	Network Discovery	All	No
Network Discovery (WSD-In)	Network Discovery	All	No

Note that Enabled is set to No. We right-click on that to enable.

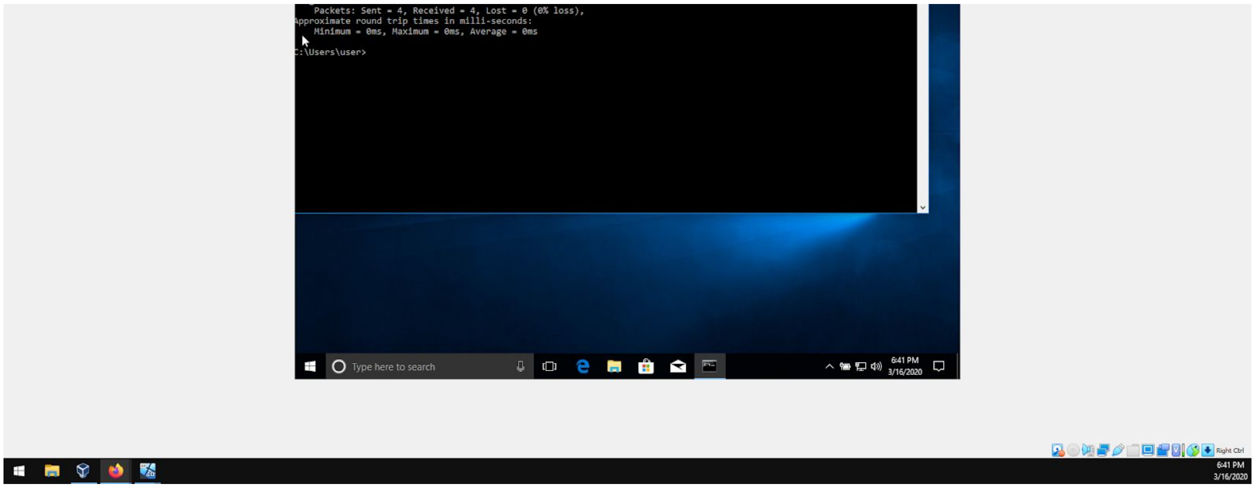
Inbound Rules Windows Firewall with Advanced Security Server 2012R2



Name	Group	Profile	Enabled
Core Networking - Router Solicitation (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	All	Yes
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	All	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	All	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	All	No
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	All	Yes
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	All	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	All	No
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	No
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	All	No
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	All	No
File and Printer Sharing over SMBDirect (iWARP-In)	File and Printer Sharing over...	All	No
iSCSI Service (TCP-In)	iSCSI Service	All	No
Key Management Service (TCP-In)	Key Management Service	All	No
Netlogon Service (NP-In)	Netlogon Service	All	No
Netlogon Service Authz (RPC)	Netlogon Service	All	No
Network Discovery (LLMNR-UDP-In)	Network Discovery	All	No
Network Discovery (NB-Datagram-In)	Network Discovery	All	No
Network Discovery (NB-Name-In)	Network Discovery	All	No
Network Discovery (Pub-WSD-In)	Network Discovery	All	No
Network Discovery (SSDP-In)	Network Discovery	All	No
Network Discovery (UPnP-In)	Network Discovery	All	No
Network Discovery (WSD Events-In)	Network Discovery	All	No
Network Discovery (WSD EventsSecure-In)	Network Discovery	All	No
Network Discovery (WSD-In)	Network Discovery	All	No

We have enabled the Echo Request option and will now verify our Windows 10 Pro computer receives a response.

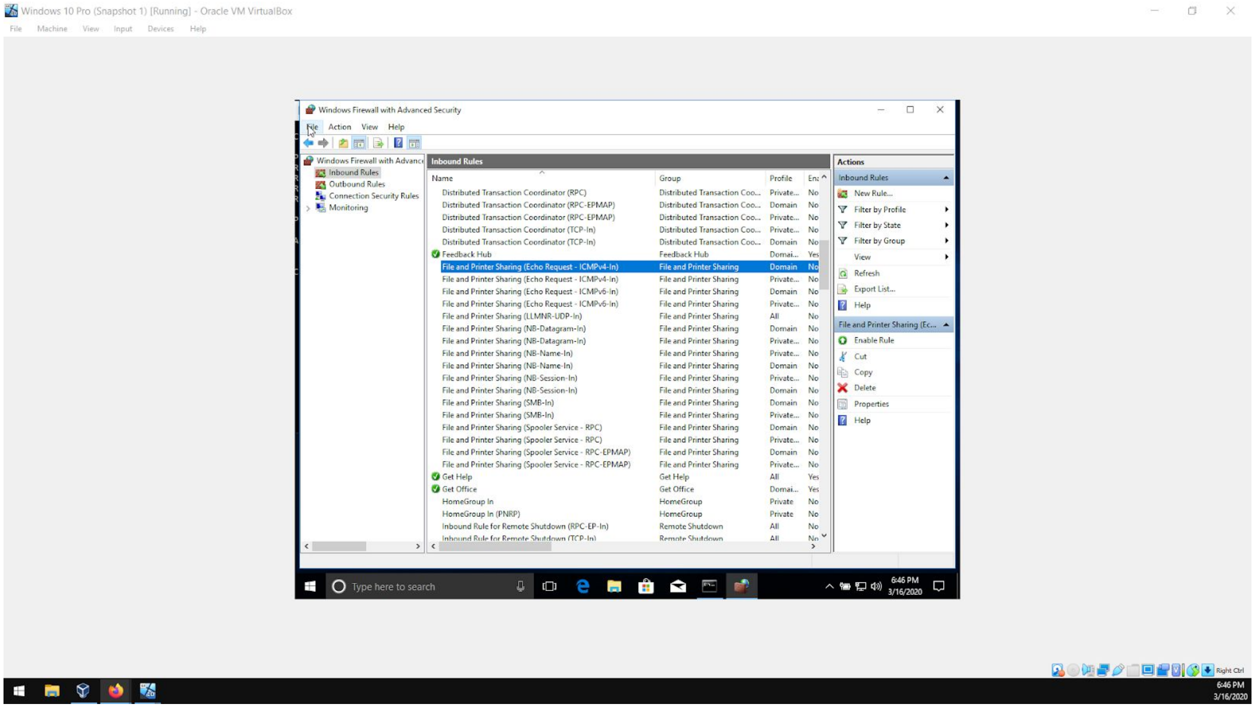
PING command Windows 10 Pro



```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\user>
```

Success! Now we check windows for the same firewall solution.

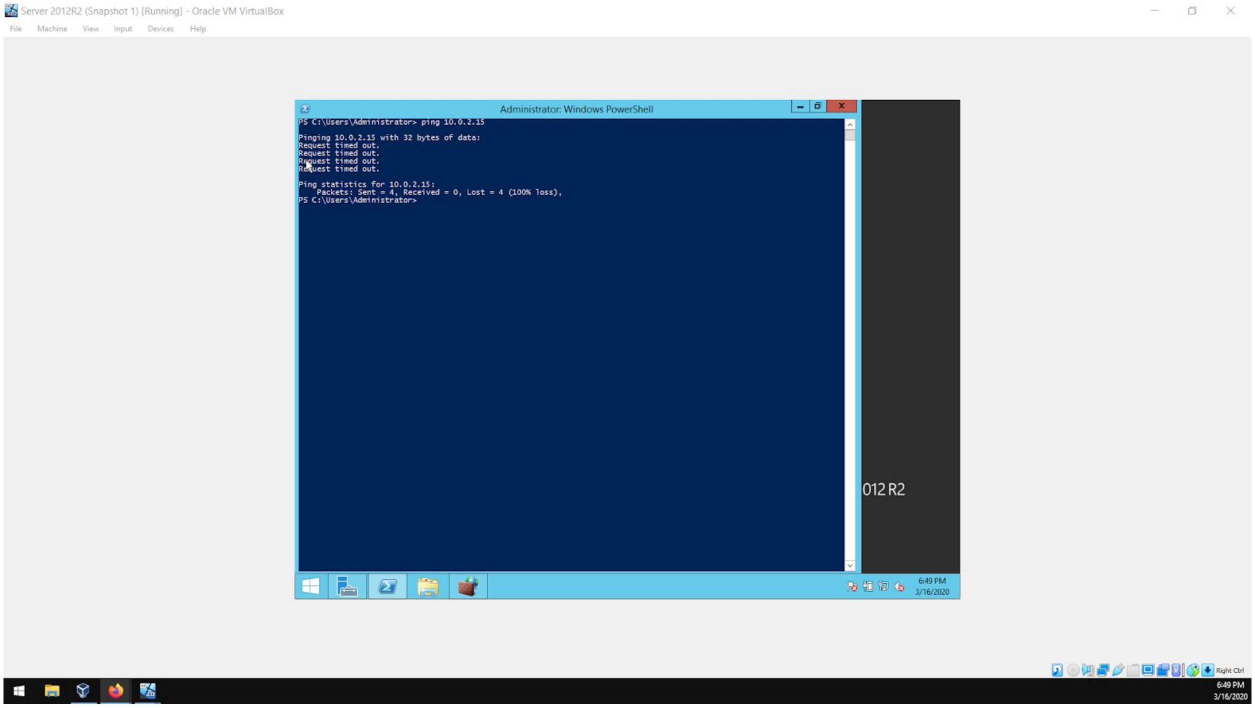
Inbound Rules Windows Firewall with Advanced Security Windows 10 Pro



Name	Group	Profile	Ena
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Domain	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Domain	No
✓ Feedback Hub	Feedback Hub	Domai...	Yes
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private...	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	Private...	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	Private...	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-EPMAP)	File and Printer Sharing	Domain	No
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	Private...	No
✓ Get Help	Get Help	All	Yes
✓ Get Office	Get Office	Domai...	Yes
HomeGroup In	HomeGroup	Private	No
HomeGroup In (PNRP)	HomeGroup	Private	No
Inbound Rule for Remote Shutdown (RPC-EP-In)	Remote Shutdown	All	No
Inbound Rule for Remote Shutdown (TCP-In)	Remote Shutdown	All	No

Here there is an option for a Profile set to Domain and Private but not for all as seen in Server 2012R2. Neither are enabled, so a Profile Domain Echo Request will be enabled then verified.

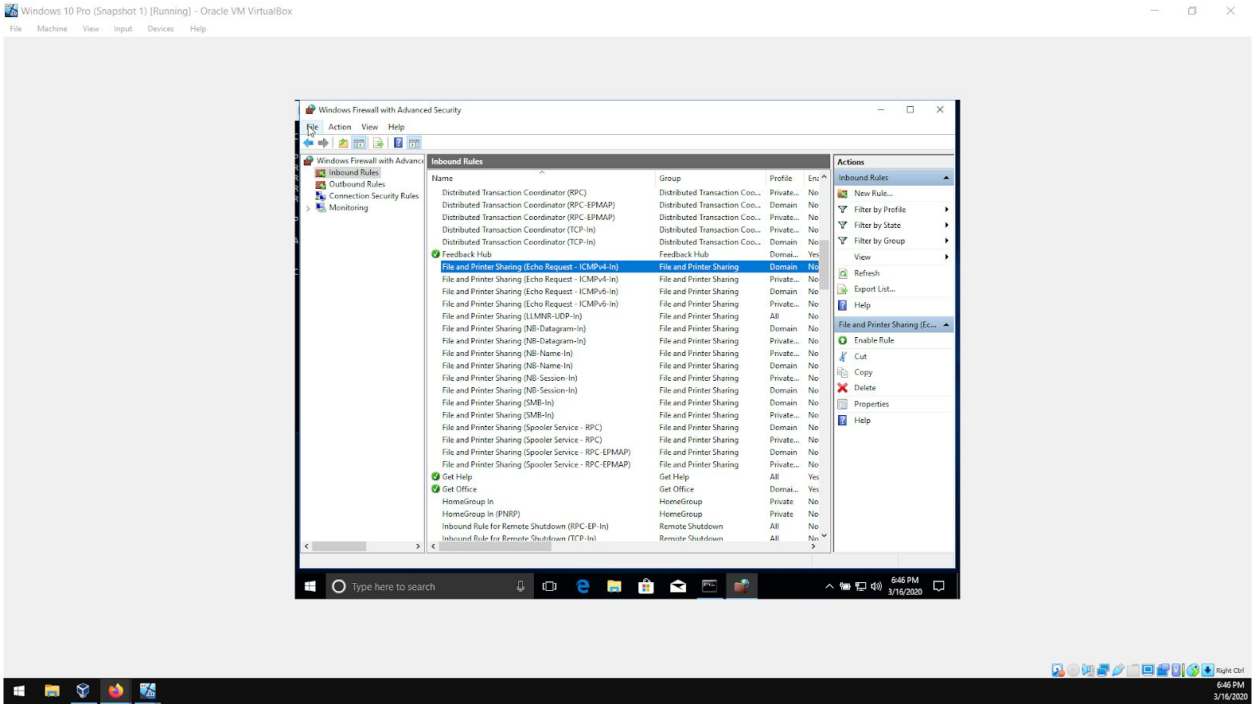
PING command Server 2012R2


Server 2012R2 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
012 R2
6:49 PM
3/16/2020
Right Ctrl

```
PS C:\Users\Administrator> ping 10.0.2.15

Pinging 10.0.2.15 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.2.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Administrator>
```

The requests have timed out for the PING command. The previous step will be undone.

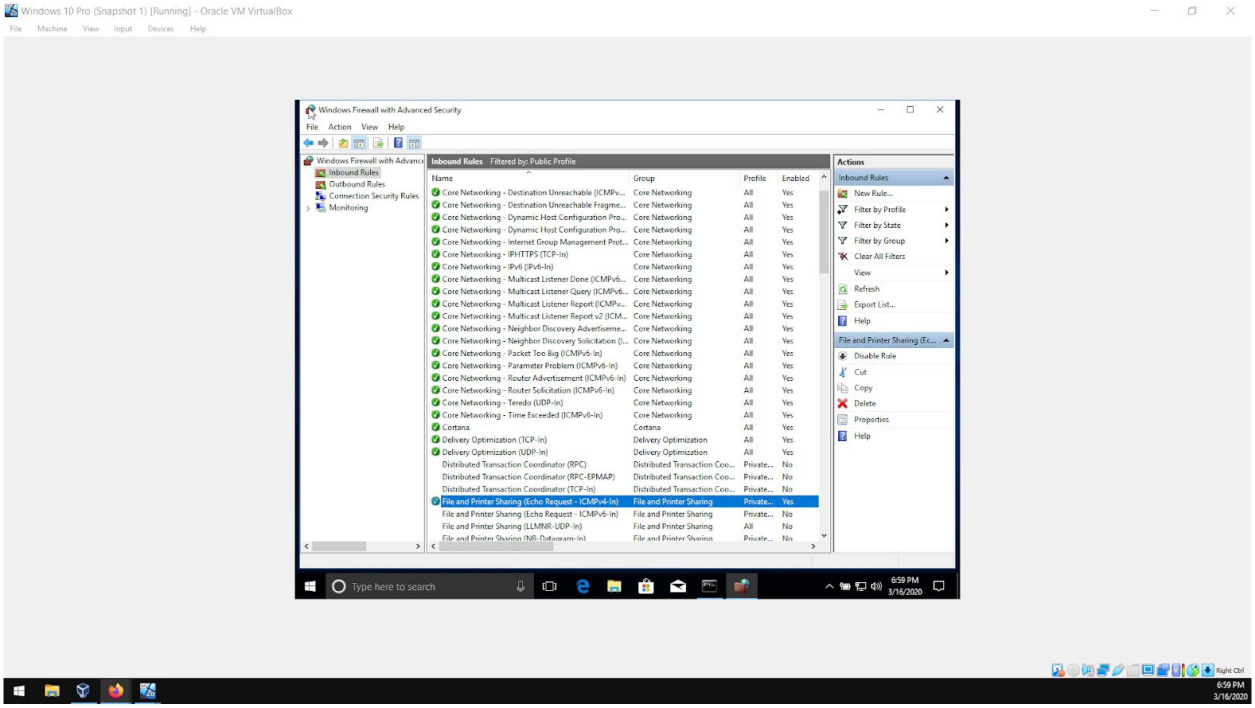
Inbound Rules Windows Firewall with Advanced Security Windows 10 Pro



Name	Group	Profile	Ena
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Domain	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Domain	No
✓ Feedback Hub	Feedback Hub	Domai...	Yes
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private...	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	Private...	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	Private...	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-EPMAP)	File and Printer Sharing	Domain	No
File and Printer Sharing (Spooler Service - RPC-EPMAP)	File and Printer Sharing	Private...	No
✓ Get Help	Get Help	All	Yes
✓ Get Office	Get Office	Domai...	Yes
HomeGroup In	HomeGroup	Private	No
HomeGroup In (PNRP)	HomeGroup	Private	No
Inbound Rule for Remote Shutdown (RPC-EP-In)	Remote Shutdown	All	No
Inbound Rule for Remote Shutdown (TCP-In)	Remote Shutdown	All	No

Now that Domain Profile has been set to No, the Private Profile will be enabled.

Inbound Rules Windows Firewall with Advanced Security Windows 10 Pro

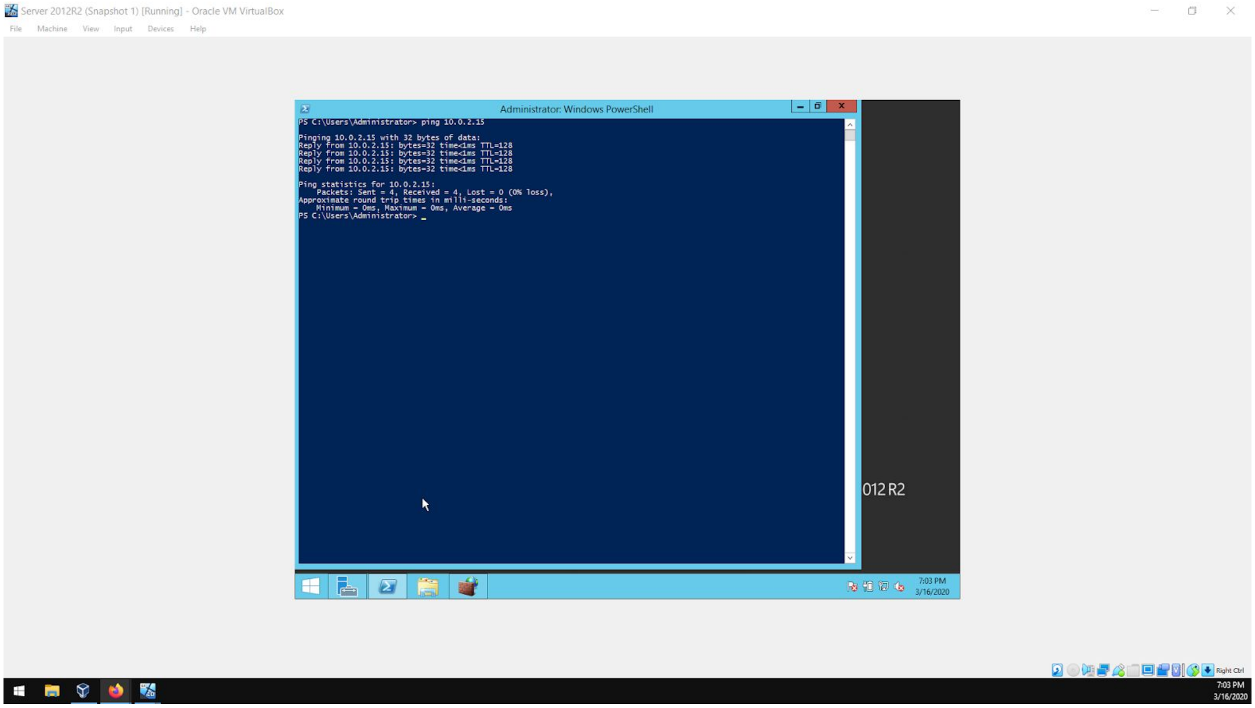


Inbound Rules Filtered by: Public Profile

Name	Group	Profile	Enabled
Core Networking - Destination Unreachable (ICMPv...	Core Networking	All	Yes
Core Networking - Destination Unreachable Fragme...	Core Networking	All	Yes
Core Networking - Dynamic Host Configuration Pro...	Core Networking	All	Yes
Core Networking - Dynamic Host Configuration Pro...	Core Networking	All	Yes
Core Networking - Internet Group Management Prot...	Core Networking	All	Yes
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Done (ICMPv6...	Core Networking	All	Yes
Core Networking - Multicast Listener Query (ICMPv6...	Core Networking	All	Yes
Core Networking - Multicast Listener Report (ICMPv...	Core Networking	All	Yes
Core Networking - Multicast Listener Report v2 (ICM...	Core Networking	All	Yes
Core Networking - Neighbor Discovery Advertiseme...	Core Networking	All	Yes
Core Networking - Neighbor Discovery Solicitation (I...	Core Networking	All	Yes
Core Networking - Packet Too Big (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Parameter Problem (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Router Advertisement (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Router Solicitation (ICMPv6-In)	Core Networking	All	Yes
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes
Core Networking - Time Exceeded (ICMPv6-In)	Core Networking	All	Yes
Cortana	Cortana	All	Yes
Delivery Optimization (TCP-In)	Delivery Optimization	All	Yes
Delivery Optimization (UDP-In)	Delivery Optimization	All	Yes
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Private...	No
File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private...	Yes
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private...	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	Private...	No

Private Profile set to Yes

PING command Server 2012R2


Server 2012R2 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell
012 R2
7:03 PM
3/16/2020

```
PS C:\Users\Administrator> ping 10.0.2.15

Pinging 10.0.2.15 with 32 bytes of data:
Reply from 10.0.2.15: bytes=32 time<1ms TTL=128
Reply from 10.0.2.15: bytes=32 time<1ms TTL=128
Reply from 10.0.2.15: bytes=32 time<1ms TTL=128
Reply from 10.0.2.15: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.2.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Administrator> _
```

Success! The ping was successful and we now have the computers communicating.

3. Surprises. Things rarely go as planned. Include this in your report. If things aren't working, documenting the problem can help you to find the solution.

The surprise came in choosing the correct profile to enable a firewall The Profile column in Windows Firewall dictates who will see the changes take place. According to Microsoft,

> “The domain profile applies to networks where the host system can authenticate to a domain controller. The private profile is a user-assigned profile and is used to designate private or home networks. Lastly, the default profile is the public profile, which is used to designate public networks such as Wi-Fi hotspots at coffee shops, airports, and other locations.”[1]

Which is good news, knowing this may help with firewall settings when the domain controller is set up in the next module. Knowing that Private refers to a private network (the 10 prefix in the IPv4 address) makes sense given that this is a private network.

5. Summary. Did it work as expected? Did you need more research?

This cyber report documents a successful attempt at four goals: the creation of a NAT network, connection of two virtual machines to a NAT network, correct firewall settings and a PING test for each connection. Research was conducted to clarify terminology of a Windows Firewall Domain and Private Profiles. From the documentation, a future setting for a domain controller was noted in the procedure. For future reference, many default settings may return an unexpected result given the security focus Server 2012R2 has with the user. Default parameters should be checked when appropriate.

6. Video lecture notes

Network Topology

In a non virtual machine set up: computers in a room connected to a switch, which is then connected to a router that’s connected to the internet.
Each computer has its own IP connected to the switch, but in the virtual case, there is only one real physical adapter (and associated IP) and then the remaining IP’s coming from a virtual adapter located on the virtual host.
Each VM gets its own IP and connection as NAT to the virtual host.

NAT default

NAT networks are located under file -> preferences -> network. Here click on the plus icon to make a new NAT Network, “Cyber Range”. All Vbox’s will be in a single NAT network. Default NAT setting will make each machine independent. Verify this with IPCONFIG from the command prompt. Note the identical IP’s for each VM

[1] https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ics/windows-firewall-profiles

NAT networking details

IP prefix that starts with 10 denotes a private address. DHCP will configure IP addresses on the network automatically. The domain controller will require a manually configured DHCP but for now it’s left at automatic. From file -> preferences -> network -> adapter 1 tab: change “Attached to:” NAT Network and choose the name of the network created. Verify with IPCONFIG and note the IP’s are different.

Verify connection

A packet goes to the computer we are looking for, bounces off and returns the ECHO reply. Thus the computer is reachable. A firewall may block ICMP messages to be delivered. From Windows Firewall with Advanced Security Inbound roles -> file and print sharing, is this enabled? Proceed with the PING test. At this point the domain controller can be added and joined via each workstation.