[INTRUSION PREVENTION]

CIS 4367.01 Computer Security, Fall 2025

Nickolas Diaz

[Xianping Wang]

Table of Contents

Contents

Abstract

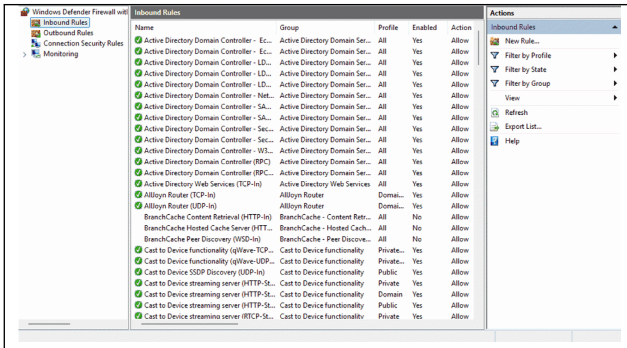
In this lab we are going to learn/interact with windows defender firewall, testing the result if we turn on/off certain features. Firewall rule like denying and allowing certain ports will allow/prevent the Parrot VM into the windows server. PowerShell commands/automations will be used to direct the flow of network traffic.

Tasks

Task 1: Configure Basic Windows Firewall Settings

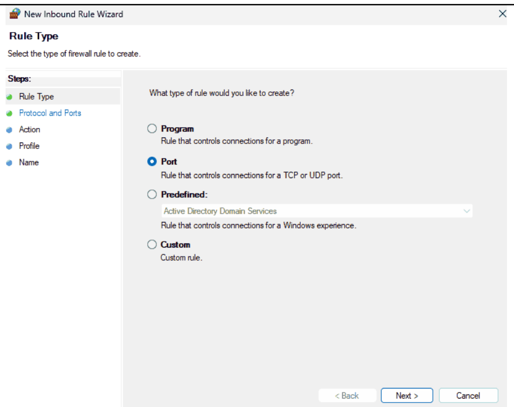
Launch Windows Defender Firewall on the Windows Server VM.
Configure Inbound Rules. Allow port 80/443, Block ICMP (Ping)

Windows Defender Firewall Menu	Create new inbound rule chose port



Inbound Rules

Name	Group	Profile	Enabled	Action
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - Net...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - SA...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - SA...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - Sec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - Sec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - W3...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller (RPC)	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller (RPC...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Web Services (TCP-In)	Active Directory Web Services	All	Yes	Allow
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes	Allow
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes	Allow
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes	Allow
Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Private	Yes	Allow



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

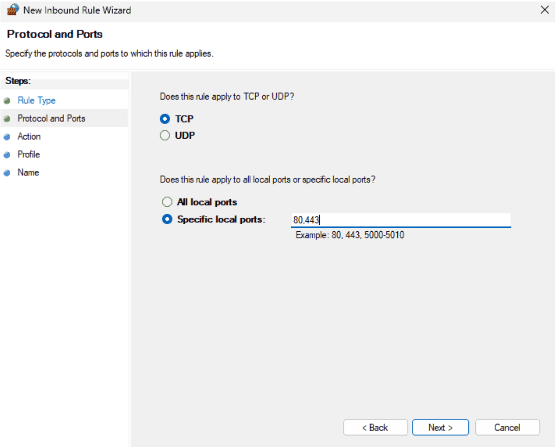
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
Active Directory Domain Services
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Chose TCP 80,443



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

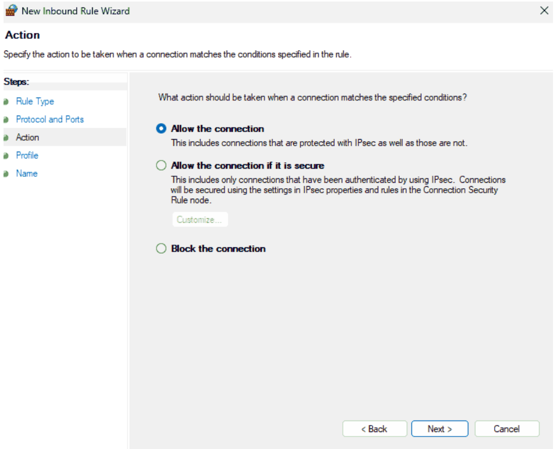
Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

Does this rule apply to all local ports or specific local ports?

○ **All local ports**
● **Specific local ports:** 80,443
Example: 80, 443, 5000-5010

Clicked allow the connection



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

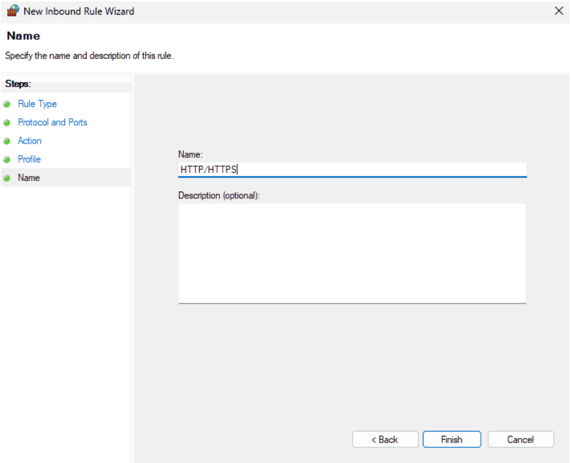
What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...

○ **Block the connection**

Named the rule HTTP/HTTPS



New Inbound Rule Wizard

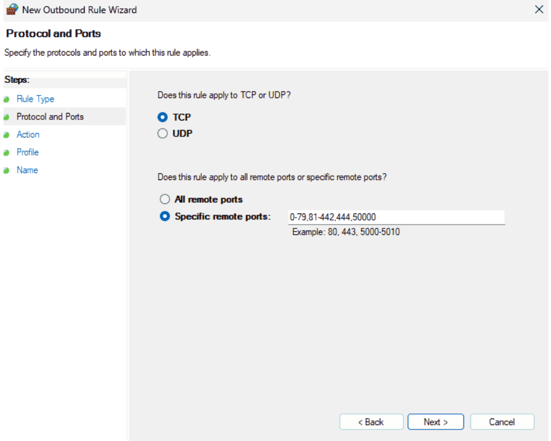
Name

Specify the name and description of this rule.

Name:
HTTP/HTTPS

Description (optional):

Created a new outbound rule where everythin is blocked except HTTP/HTTPS



New Outbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

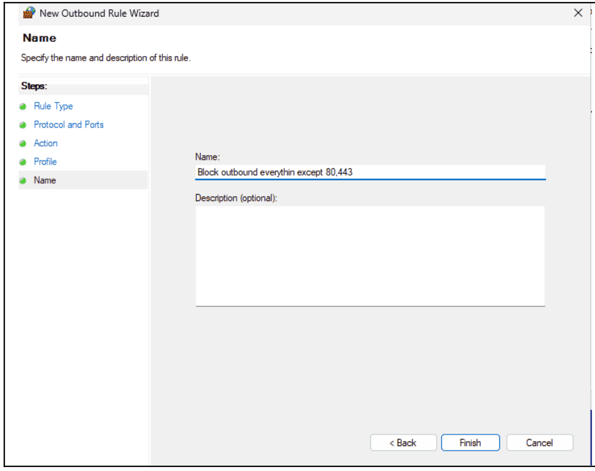
● **TCP**
○ **UDP**

Does this rule apply to all remote ports or specific remote ports?

○ **All remote ports**
● **Specific remote ports:** 0-79,81-442,444,50000
Example: 80, 443, 5000-5010

Bound out rule name

Block all UDP connections, for ping


New Outbound Rule Wizard

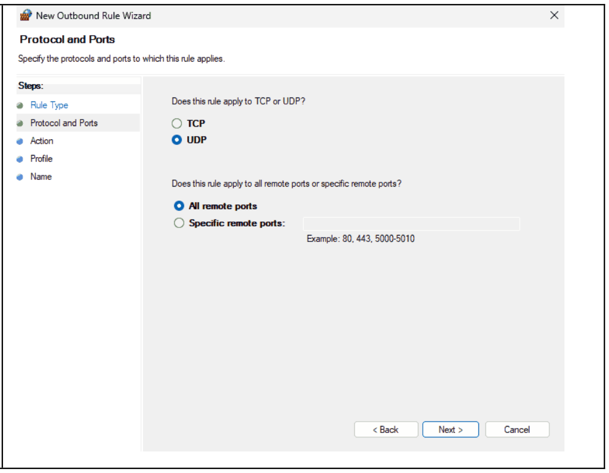
Name

Specify the name and description of this rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name: Block outbound everythin except 80,443

Description (optional):


New Outbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

○ TCP
● UDP

Does this rule apply to all remote ports or specific remote ports?

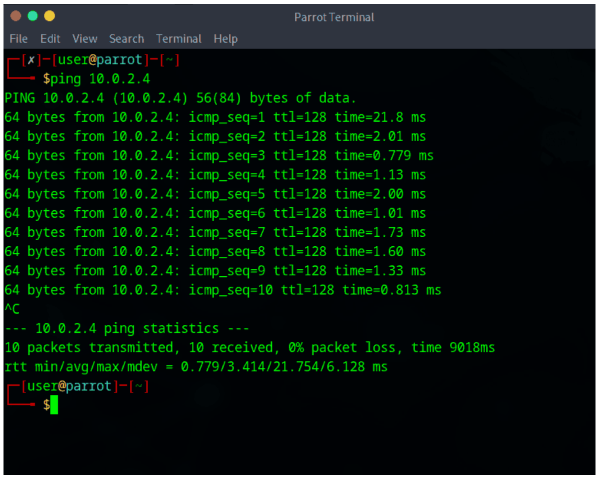
● All remote ports
○ Specific remote ports:

Example: 80, 443, 5000-5010

Task 2: Test Windows Firewall Settings Using Parrot Linux

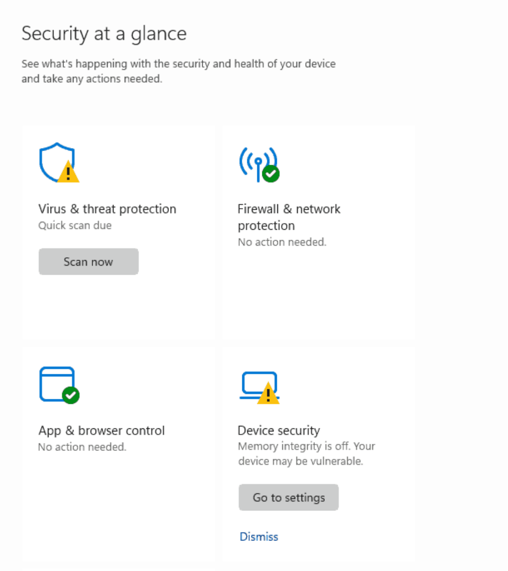
Test Inbound Rule
Ping windows Server
Nmap scanning
Curl web service

Ping worked even though UDP and TCP are blocked



```
┌─[✗]─[user@parrot]─[~]
└──╼ $ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=128 time=21.8 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=128 time=2.01 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=128 time=0.779 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=128 time=1.13 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=128 time=2.00 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=128 time=1.01 ms
64 bytes from 10.0.2.4: icmp_seq=7 ttl=128 time=1.73 ms
64 bytes from 10.0.2.4: icmp_seq=8 ttl=128 time=1.60 ms
64 bytes from 10.0.2.4: icmp_seq=9 ttl=128 time=1.33 ms
64 bytes from 10.0.2.4: icmp_seq=10 ttl=128 time=0.813 ms
^C
--- 10.0.2.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9018ms
rtt min/avg/max/mdev = 0.779/3.414/21.754/6.128 ms
┌─[user@parrot]─[~]
└──╼ $
```

Made sure that the firewall is on


Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
Quick scan due

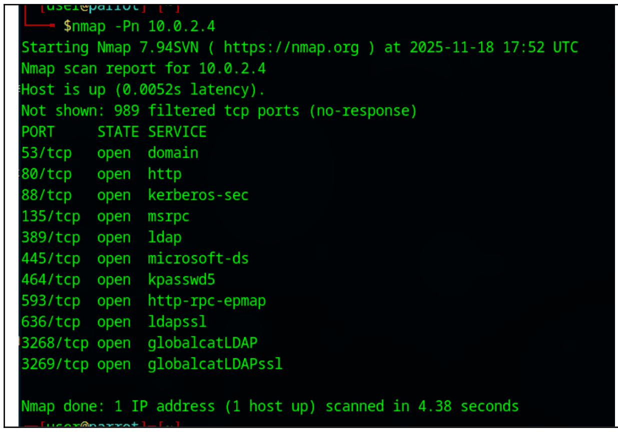
Firewall & network protection
No action needed.

App & browser control
No action needed.

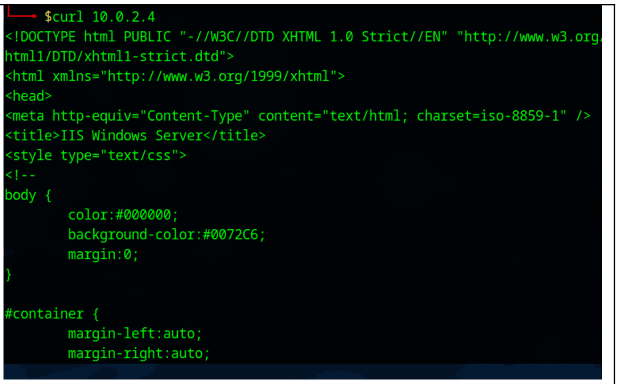
Device security
Memory integrity is off. Your device may be vulnerable.

NMAP sees all ports dispite all those ports are blocked

Curl workes as expected allow HTTP/HTTPS fire



```
└──╼ $nmap -Pn 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-18 17:52 UTC
Nmap scan report for 10.0.2.4
Host is up (0.0052s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl

Nmap done: 1 IP address (1 host up) scanned in 4.38 seconds
```



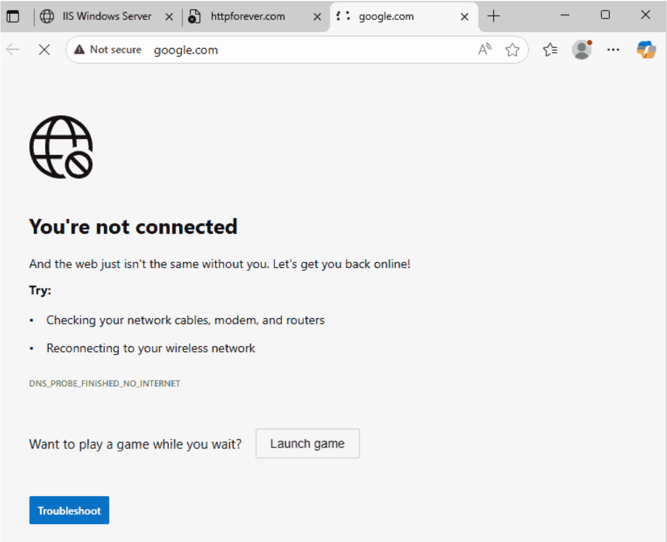
```
└──╼ $curl 10.0.2.4
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
        color:#000000;
        background-color:#0072C6;
        margin:0;
}

#container {
        margin-left:auto;
        margin-right:auto;
```

Test the Outbound Rule

Test external websites using HTTP

Test external websites using HTTPS

Websites like HTTP/HTTPS do not work all are blocked



You're not connected

And the web just isn't the same without you. Let's get you back online!

Try:

- Checking your network cables, modem, and routers
- Reconnecting to your wireless network

DNS_PROBE_FINISHED_NO_INTERNET

Want to play a game while you wait?

Task 3: Monitor Firewall Activity on Windows Server

Enable Firewall Logging

Commands PowerShell:

Enable Logging for Blocked Packets	Set-NetFirewallProfile -Profile Domain -LogBlocked True
Enable Logging for Allowed Connections	Set-NetFirewallProfile -Profile Domain -LogAllowed True

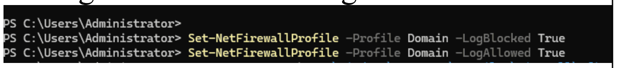
Review Firewall Logs

Commands PowerShell:

PowerShell to view logs in real time	Get-Content -Path "C:\Windows\System32\LogFiles\Firewall\pfirewall.log" -Wait

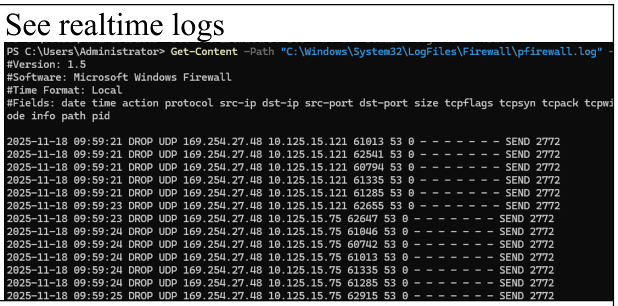
Monitor in Real-Time

Setting realtime monitoring



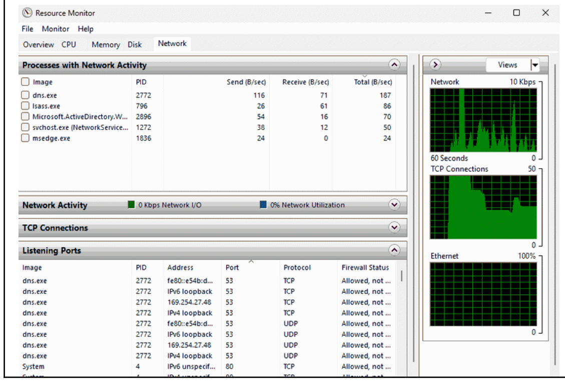
```
PS C:\Users\Administrator>
PS C:\Users\Administrator> Set-NetFirewallProfile -Profile Domain -LogBlocked True
PS C:\Users\Administrator> Set-NetFirewallProfile -Profile Domain -LogAllowed True
```

See realtime logs



```
PS C:\Users\Administrator> Get-Content -Path "C:\Windows\System32\LogFiles\Firewall\pfirewall.log" -
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwi
ode info path pid

2025-11-18 09:59:21 DROP UDP 169.254.27.48 10.125.15.121 61013 53 0 - - - - - - - - SEND 2772
2025-11-18 09:59:21 DROP UDP 169.254.27.48 10.125.15.121 62541 53 0 - - - - - - - - SEND 2772
2025-11-18 09:59:21 DROP UDP 169.254.27.48 10.125.15.121 60794 53 0 - - - - - - - - SEND 2772
2025-11-18 09:59:21 DROP UDP 169.254.27.48 10.125.15.121 61335 53 0 - - - - - - - - SEND 2772
2025-11-18 09:59:21 DROP UDP 169.254.27.48 10.125.15.121 61285 53 0 - - - - - - - - SEND 2772
2025-11-18 09:59:23 DROP UDP 169.254.27.48 10.125.15.121 62655 53 0 - - - - - - - - SEND 2772
2025-11-18 09:59:23 DROP UDP 169.254.27.48 10.125.15.75 62647 53 0 - - - - - - - - SEND 2772
2025-11-18 09:59:24 DROP UDP 169.254.27.48 10.125.15.75 61046 53 0 - - - - - - - - SEND 2772
2025-11-18 09:59:24 DROP UDP 169.254.27.48 10.125.15.75 60742 53 0 - - - - - - - - SEND 2772
2025-11-18 09:59:24 DROP UDP 169.254.27.48 10.125.15.75 61013 53 0 - - - - - - - - SEND 2772
2025-11-18 09:59:24 DROP UDP 169.254.27.48 10.125.15.75 61335 53 0 - - - - - - - - SEND 2772
2025-11-18 09:59:24 DROP UDP 169.254.27.48 10.125.15.75 61285 53 0 - - - - - - - - SEND 2772
2025-11-18 09:59:25 DROP UDP 169.254.27.48 10.125.15.75 62915 53 0 - - - - - - - - SEND 2772
```

Reasource monitor to see network connections



Processes with Network Activity

Image	PID	Send (B/sec)	Receive (B/sec)	Total (B/sec)
□ dns.exe	2772	116	71	187
□ lsass.exe	796	26	61	86
□ Microsoft.ActiveDirectory.W...	2896	54	16	70
□ svchost.exe (NetworkService...	1272	38	12	50
□ msedge.exe	1836	24	0	24

Network Activity 🟩 0 Kbps Network I/O 🟦 0% Network Utilization

TCP Connections

Listening Ports

Image	PID	Address	Port	Protocol	Firewall Status
dns.exe	2772	fe80::e54b:d...	53	TCP	Allowed, not ...
dns.exe	2772	IPv6 loopback	53	TCP	Allowed, not ...
dns.exe	2772	169.254.27.48	53	TCP	Allowed, not ...
dns.exe	2772	IPv4 loopback	53	TCP	Allowed, not ...
dns.exe	2772	fe80::e54b:d...	53	UDP	Allowed, not ...
dns.exe	2772	IPv6 loopback	53	UDP	Allowed, not ...
dns.exe	2772	169.254.27.48	53	UDP	Allowed, not ...
dns.exe	2772	IPv4 loopback	53	UDP	Allowed, not ...
System	4	IPv6 unspecif...	80	TCP	Allowed, not ...

Task 4: Troubleshoot Firewall-Related Issues

Simulate blacked RDP Connection

Enable Windows Remote Desktop

Block RDP Traffic

Attempt to connect via RDP from Parrot Linux, then unblock the service

Linux Command to use RDP	sudo apt install rdesktop rdesktop 10.0.2.4

Troubleshoot HTTP/HTTPS Service Unavailability

Block HTTP/HTTPS Traffic 80 443

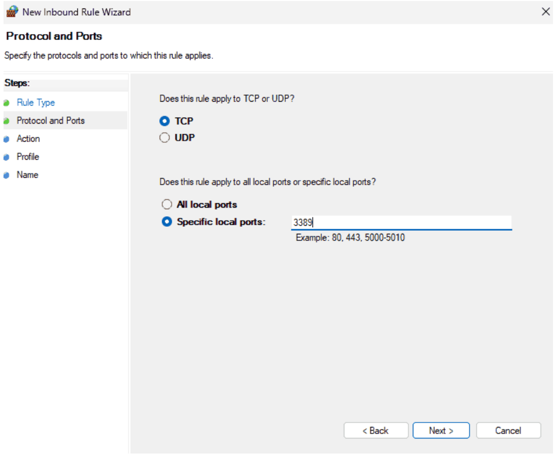
Try accessing the web service from Parrot Linux

Block C&C (Command & Control)
Block all outbound except HTTP/HTTPS, try a trojan
Disable the blocking all outbound rule, try trojan again
Enable the blocking of all outbound rule, deleting the trojan
Resolve ICMP Block

Disable the ICMP blocking rule temporary test with ping

Powershell rule to block ping	New-NetFirewallRule -DisplayName \"Block ICMP Ping\" -Direction Inbound -Protocol ICMPv4 -IcmpType 8 -Action Block

Block RDP



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

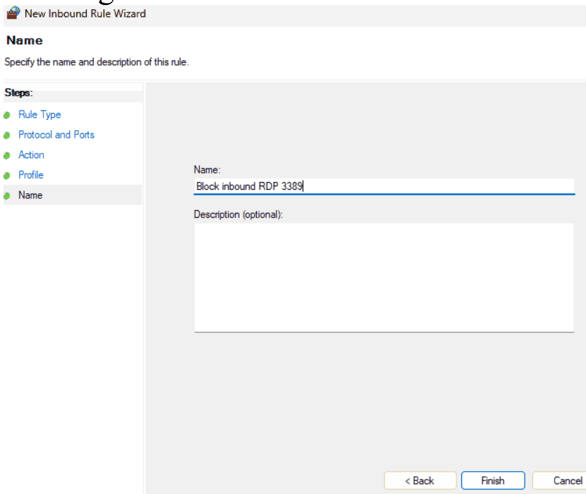
● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 3389

Example: 80, 443, 5000-5010

Creating rule name



New Inbound Rule Wizard

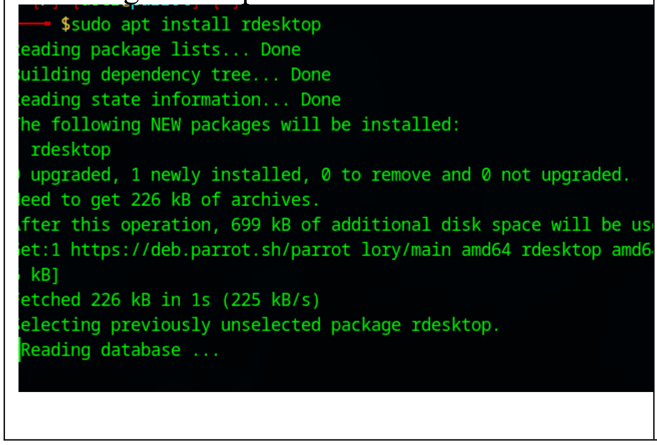
Name

Specify the name and description of this rule.

Name: Block inbound RDP 3389

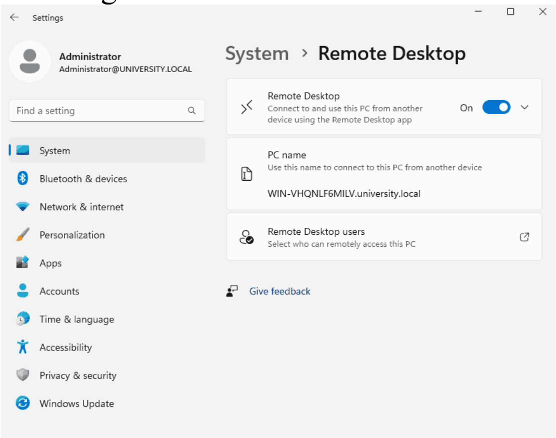
Description (optional):

Installing rdesktop



```
──▪ $sudo apt install rdesktop
eading package lists... Done
uilding dependency tree... Done
eading state information... Done
he following NEW packages will be installed:
 rdesktop
 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
eed to get 226 kB of archives.
fter this operation, 699 kB of additional disk space will be us
et:1 https://deb.parrot.sh/parrot lory/main amd64 rdesktop amd6
 kB]
etched 226 kB in 1s (225 kB/s)
electing previously unselected package rdesktop.
Reading database ...
```

Enabling RDP on the Windows Server



Settings

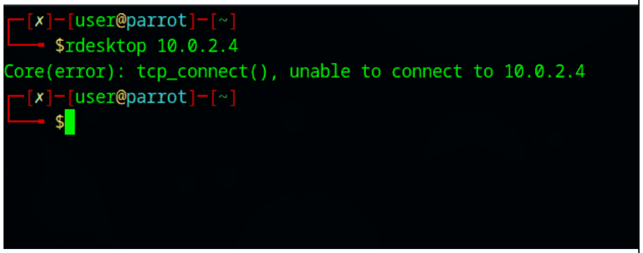
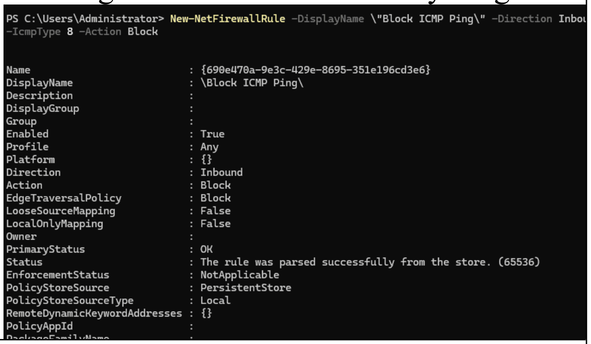
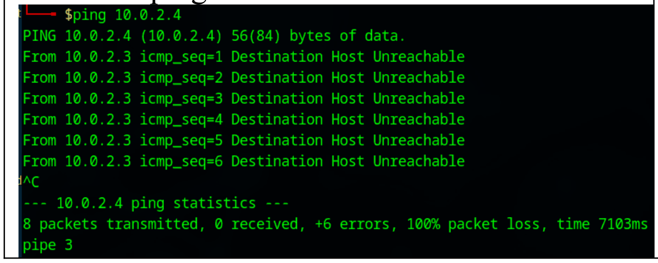
Administrator
Administrator@UNIVERSITY.LOCAL

System › Remote Desktop

Remote Desktop
Connect to and use this PC from another device using the Remote Desktop app
On

PC name
Use this name to connect to this PC from another device
WIN-VHQNLF6MILV.university.local

Remote Desktop users
Select who can remotely access this PC

Parrot Linux could not connect 	Creating new firewall rule to deny Ping 
It worked ping is disabled 	

```
┌─[✗]─[user@parrot]─[~]
└──╼ $rdesktop 10.0.2.4
Core(error): tcp_connect(), unable to connect to 10.0.2.4
┌─[✗]─[user@parrot]─[~]
└──╼ $
```

```
PS C:\Users\Administrator> New-NetFirewallRule -DisplayName \"Block ICMP Ping\" -Direction Inbou
-IcmpType 8 -Action Block


Name                          : {690e470a-9e3c-429e-8695-351e196cd3e6}
DisplayName                   : \Block ICMP Ping\
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Block
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
PackageFamilyName             :
```

```
└──╼ $ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
From 10.0.2.3 icmp_seq=1 Destination Host Unreachable
From 10.0.2.3 icmp_seq=2 Destination Host Unreachable
From 10.0.2.3 icmp_seq=3 Destination Host Unreachable
From 10.0.2.3 icmp_seq=4 Destination Host Unreachable
From 10.0.2.3 icmp_seq=5 Destination Host Unreachable
From 10.0.2.3 icmp_seq=6 Destination Host Unreachable
^C
--- 10.0.2.4 ping statistics ---
8 packets transmitted, 0 received, +6 errors, 100% packet loss, time 7103ms
pipe 3
```

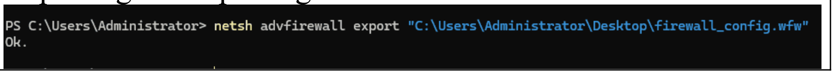
Task 5: Automate Firewall Configuration and Export Rules

Automate Rule Creation with PowerShell
Allow HTTP/HTTPS rule

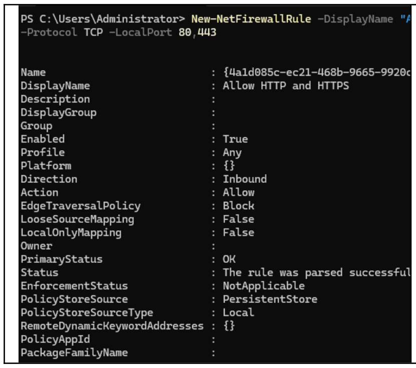
Allowing HTTP/HTTPS rule	New-NetFirewallRule -DisplayName \"Block ICMP Ping\" -Direction Inbound -Protocol ICMPv4 -IcmpType 8 -Action Block

Use PowerShell to create and apply rules
Export and Import Firewall Configurations

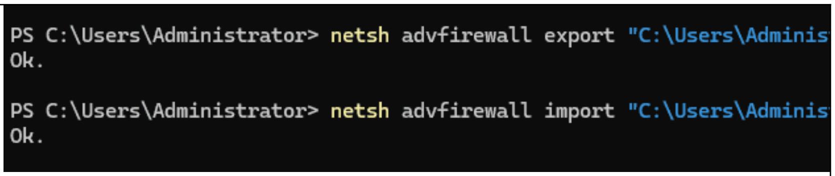
Export firewall rule	netsh advfirewall export "C:\Users\Administrator\Desktop\firewall_config.wfw"
Import firewall rule	netsh advfirewall import "C:\Users\Administrator\Desktop\firewall_config.wfw"

Create new rule to allow HTTP/HTTPS	Exporting and inporting firewall rules 

```
PS C:\Users\Administrator> netsh advfirewall export "C:\Users\Administrator\Desktop\firewall_config.wfw"
Ok.
```



```
PS C:\Users\Administrator> New-NetFirewallRule -DisplayName "A
-Protocol TCP -LocalPort 80,443


Name                             : {4a1d085c-ec21-468b-9665-9920c
DisplayName                      : Allow HTTP and HTTPS
Description                      :
DisplayGroup                     :
Group                            :
Enabled                          : True
Profile                          : Any
Platform                         : {}
Direction                        : Inbound
Action                           : Allow
EdgeTraversalPolicy              : Block
LooseSourceMapping               : False
LocalOnlyMapping                 : False
Owner                            :
PrimaryStatus                    : OK
Status                           : The rule was parsed successful
EnforcementStatus                : NotApplicable
PolicyStoreSource                : PersistentStore
PolicyStoreSourceType            : Local
RemoteDynamicKeywordAddresses    : {}
PolicyAppId                      :
PackageFamilyName                :
```



```
PS C:\Users\Administrator> netsh advfirewall export "C:\Users\Adminis
Ok.

PS C:\Users\Administrator> netsh advfirewall import "C:\Users\Adminis
Ok.
```

Conclusions

This lab explored how firewall work on windows server. It allows blocking on many different criteria, such as programs and ports. It showed how blocking/allowing certain TCP/UDP/ICMP ports, using inbound/outbound can allow/block other computers from interacting with the machine. Various services were experimented on such as HTTP/HTTPS website, PING/ICMP, Nmap ports, and RDP. Lastly, I learned how to automate much of the firewall, such as using PowerShell to create and delete rules, and be able to import and export the firewall rules.

References

https://github.com/ufidon/comsec/blob/main/labs/lab06/README.md