Raymond Ng

IS 3423 – Network Security

Lab 2: Access Control and Firewalls

March 9, 2023

Part A: File Sharing

For this exercise, I will use a file storage application such as OneDrive to perform permission control. To do this exercise, I executed the following steps:

Step 1 – Create a File

1. I went to OneDrive link on myUTSA page at https://my.utsa.edu/

2. Logged in with my abc123 information. You may be asked for a 2-factor authentication.

3. Clicked on the new button and created a new Word Document file.

4. Type your name in the file.

5. Using File Save As option, rename the file to RaymondNg.docx and then close the window.

Step 2 – Check File Permission

6. On the OneDrive page, I found the file I created.

7. Right clicked on the file and clicked Manage Access.

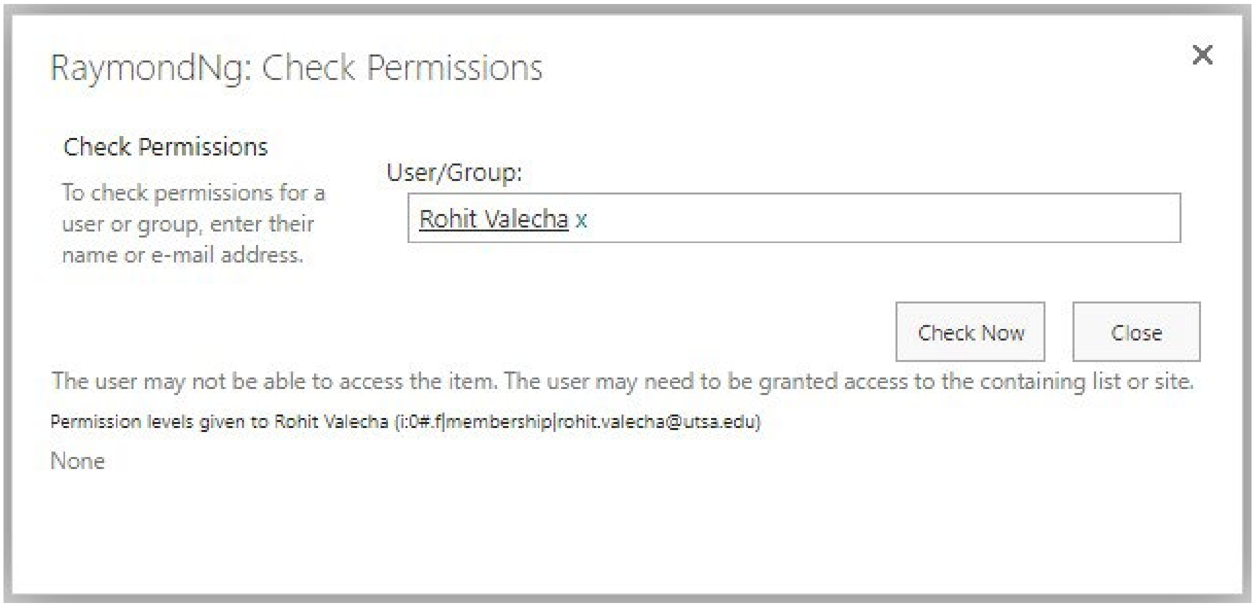
8. Clicked on the Advanced option.

9. Clicked on the Check Permissions button.

10. Type my professor's name, Rohit Valecha, and then clicked Check Now button.

11. **SNAPSHOT:** See the permission level for this user.

12. Closed the window.



RaymondNg: Check Permissions

Check Permissions

To check permissions for a user or group, enter their name or e-mail address.

User/Group: Rohit Valecha x

The user may not be able to access the item. The user may need to be granted access to the containing list or site.

Permission levels given to Rohit Valecha (i:0#.f|membership|rohit.valecha@utsa.edu)

None

Step 3 – Share the File

13. On the OneDrive page, I went back to the file I created.

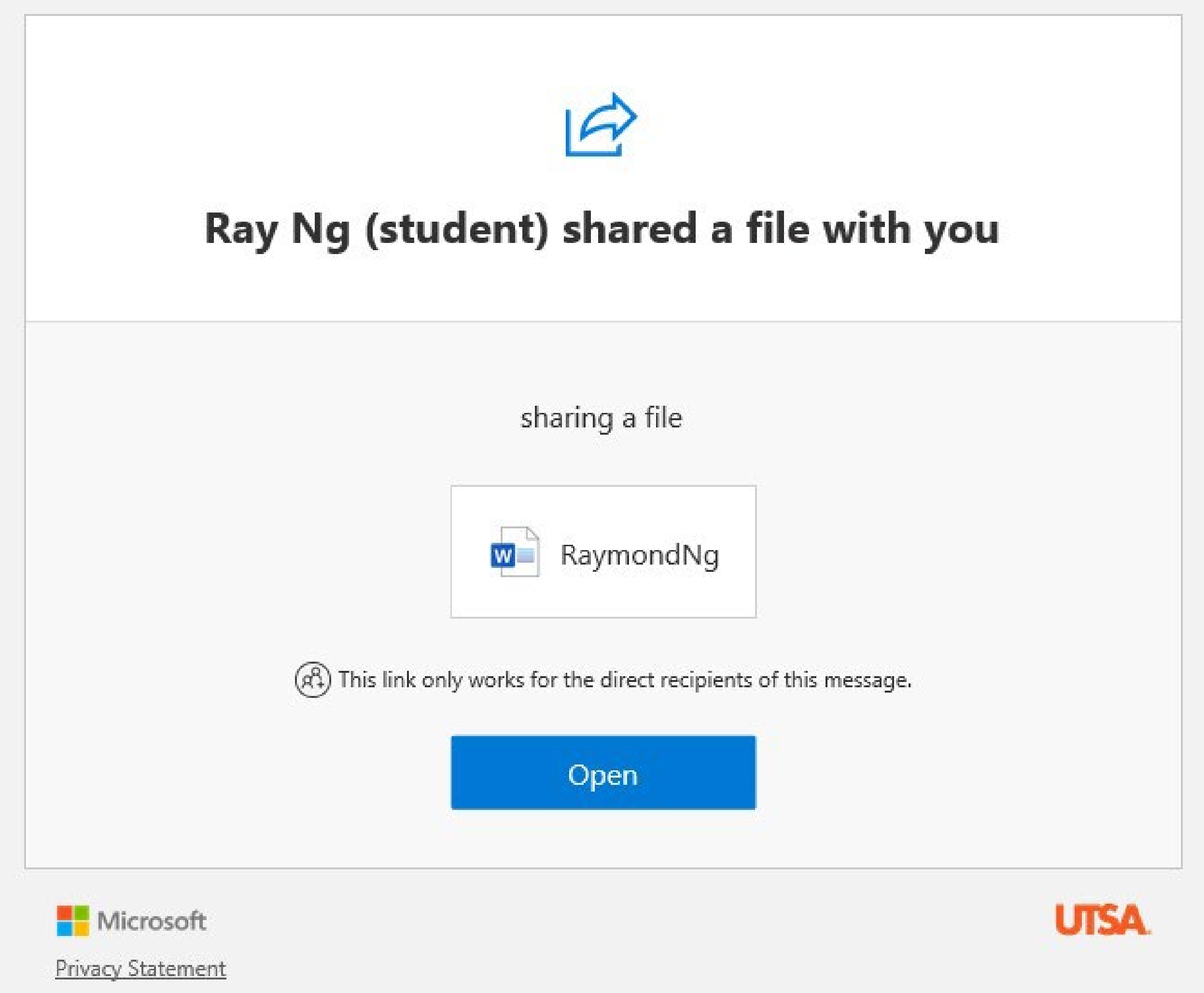
14. Right clicked on the file and click Share.

15. In the send link window, typed **my own** my.utsa.edu email address.

16. Clicked on the permission button and selected Can View option.

17. Then typed a message, *sharing a file*, and then clicked Send.

18. **SNAPSHOT:** Checked your my.utsa.edu email for the shared file. Clicked to open and viewed the file.

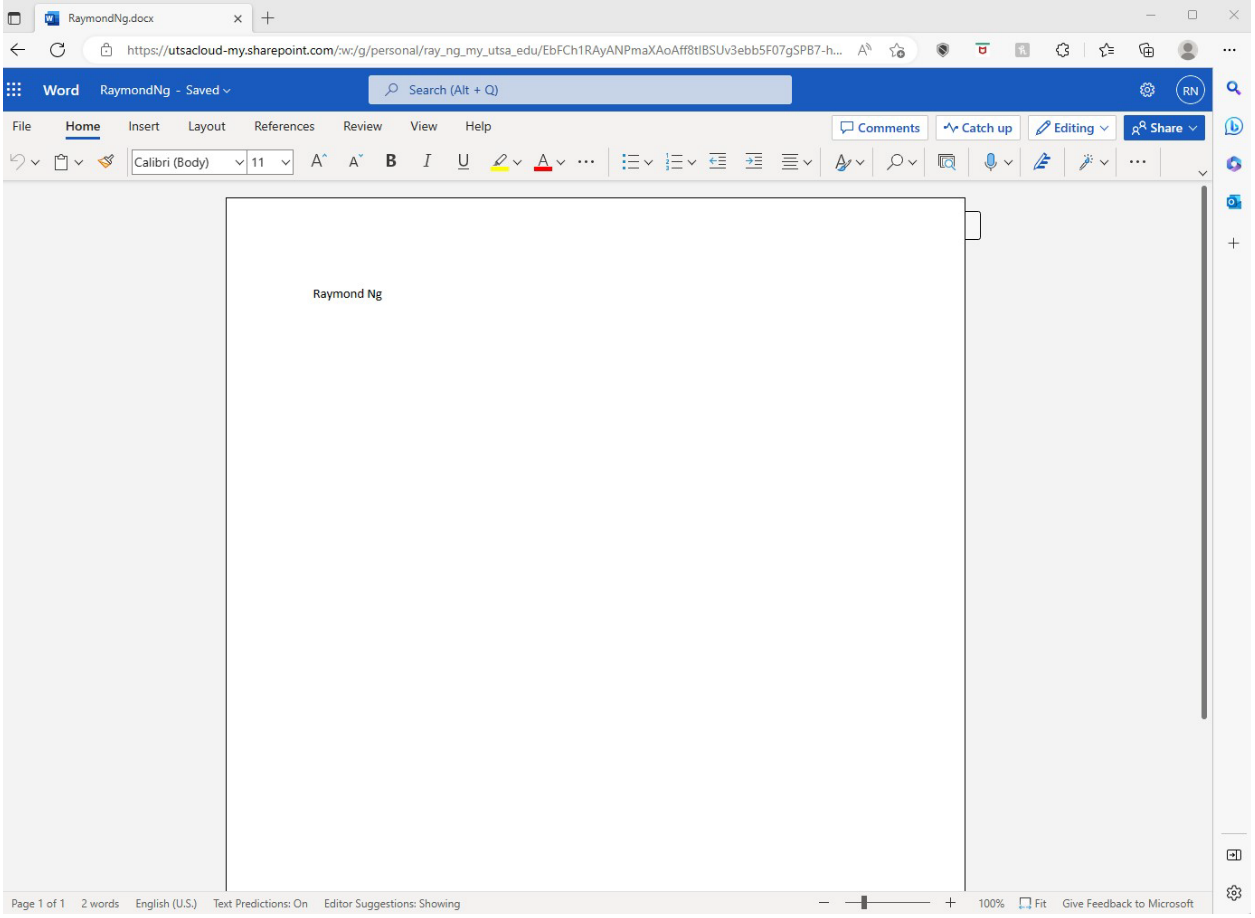


Ray Ng (student) shared a file with you

sharing a file

RaymondNg

This link only works for the direct recipients of this message.



Raymond Ng

Part B: Window Firewall

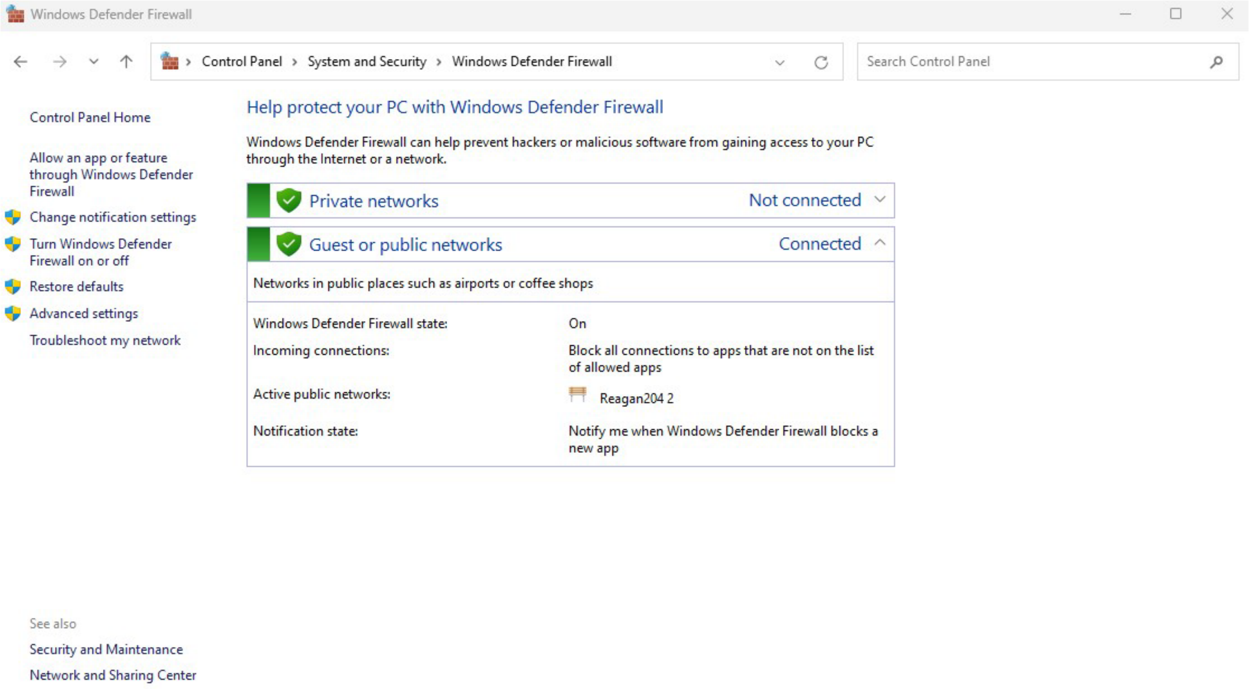
In this exercise, I viewed the settings on the Windows firewall and then added a rule to block an IP Address. To do this exercise, I executed the following steps:

Step 1 – Firewall Status

1. Navigated to the Windows Defender Firewall:

2. Clicked Start > Control Panel > System and Security > Windows Firewall.

3. **SNAPSHOT:** The Firewall indicator showed the status of the firewall for any available network (domain, private or public).


Windows Defender Firewall
Control Panel > System and Security > Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

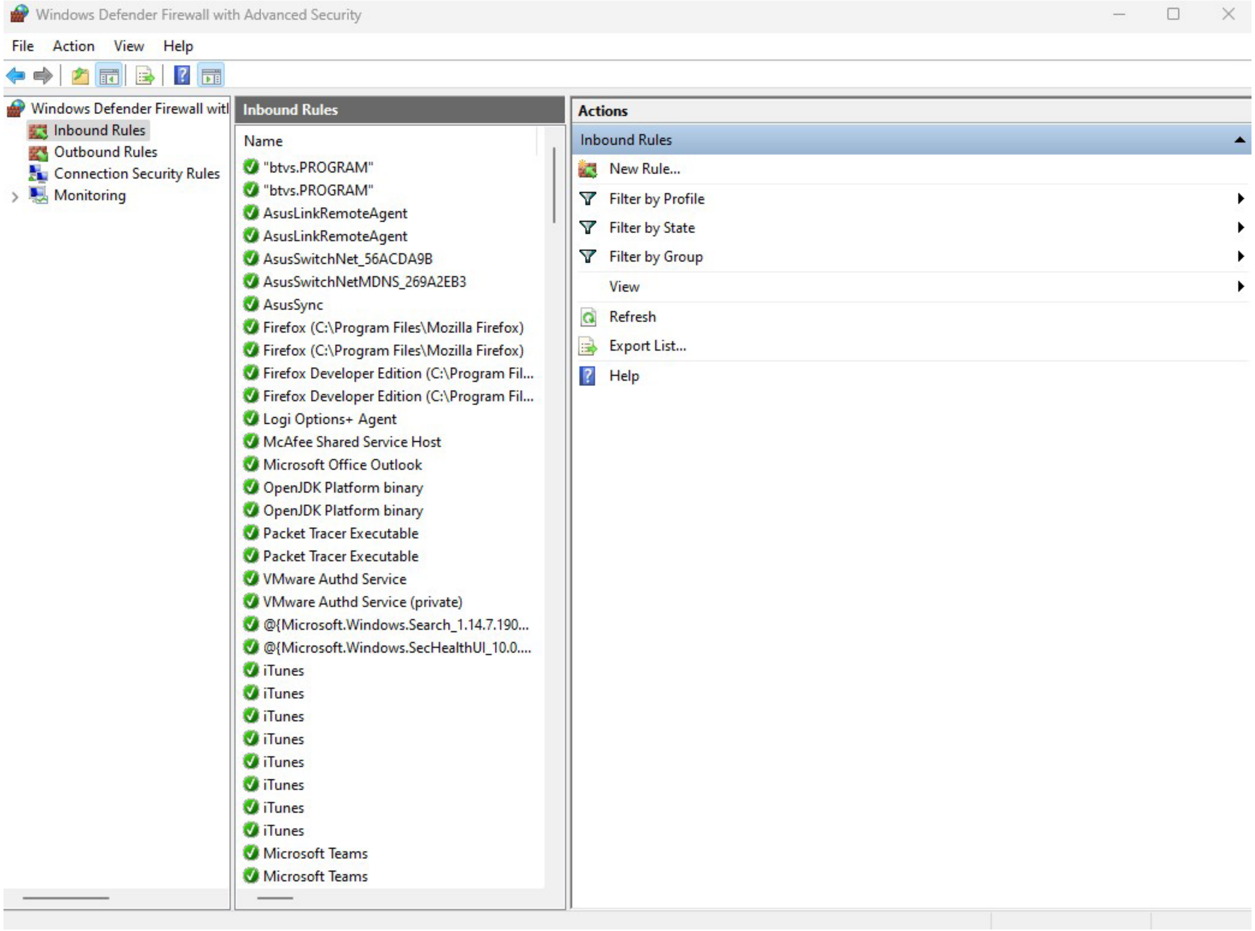
Active public networks: Reagan204 2

Notification state: Notify me when Windows Defender Firewall blocks a new app

Step 2 – Inbound Rules

4. Clicked on Advanced Settings > Inbound Rules.

5. **SNAPSHOT:** Observed Inbound rules.



Inbound Rules

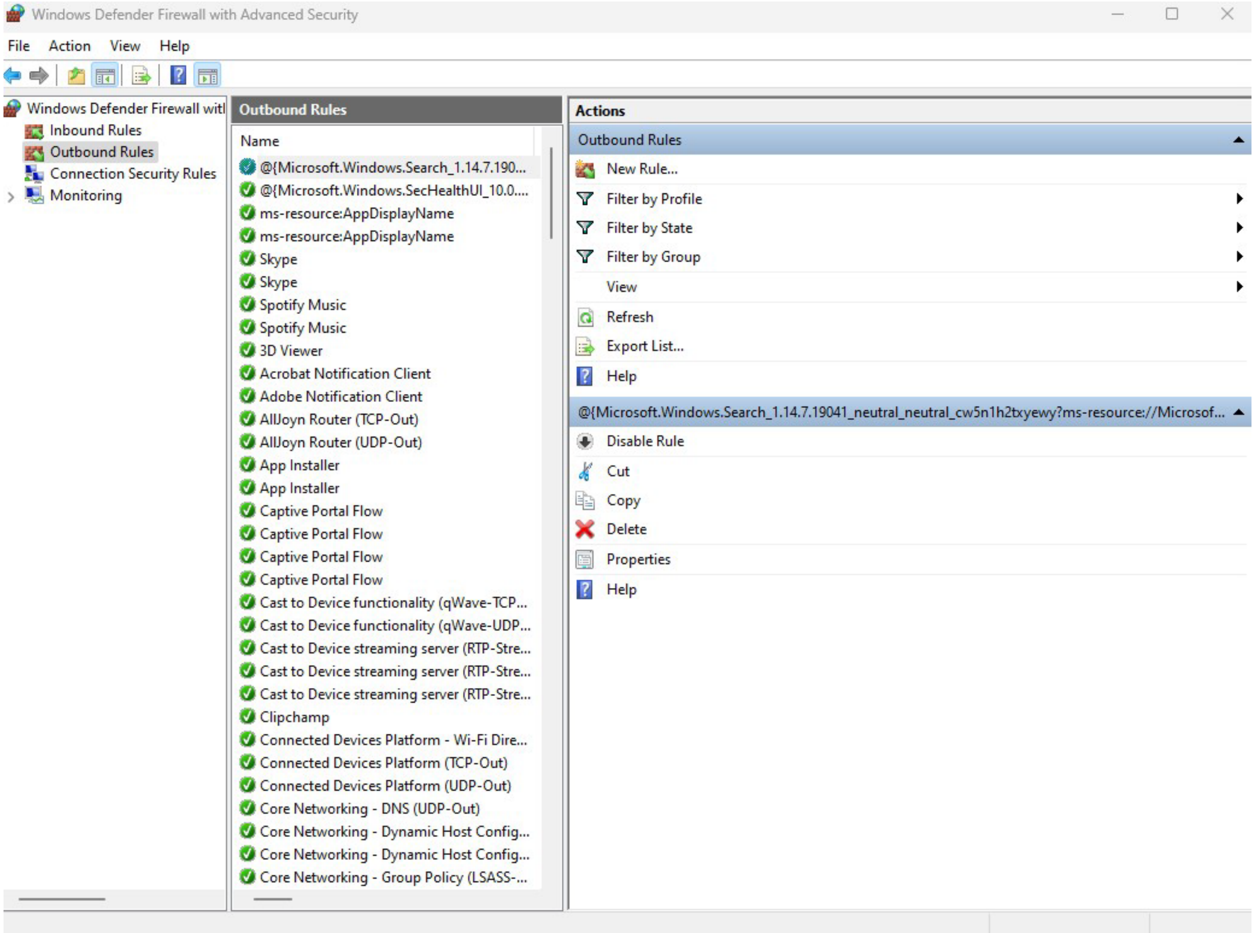
Name

- "btvs.PROGRAM"
- "btvs.PROGRAM"
- AsusLinkRemoteAgent
- AsusLinkRemoteAgent
- AsusSwitchNet_56ACDA9B
- AsusSwitchNetMDNS_269A2EB3
- AsusSync
- Firefox (C:\Program Files\Mozilla Firefox)
- Firefox (C:\Program Files\Mozilla Firefox)
- Firefox Developer Edition (C:\Program Fil...
- Firefox Developer Edition (C:\Program Fil...
- Logi Options+ Agent
- McAfee Shared Service Host
- Microsoft Office Outlook
- OpenJDK Platform binary
- OpenJDK Platform binary
- Packet Tracer Executable
- Packet Tracer Executable
- VMware Authd Service
- VMware Authd Service (private)
- @{Microsoft.Windows.Search_1.14.7.190...
- @{Microsoft.Windows.SecHealthUI_10.0....
- iTunes
- iTunes
- iTunes
- iTunes
- iTunes
- iTunes
- iTunes
- iTunes
- Microsoft Teams
- Microsoft Teams

Step 3 – Outbound Rules

6. Clicked on Advanced Settings > Outbound Rules.

7. **SNAPSHOT**: Observed the Outbound rules.

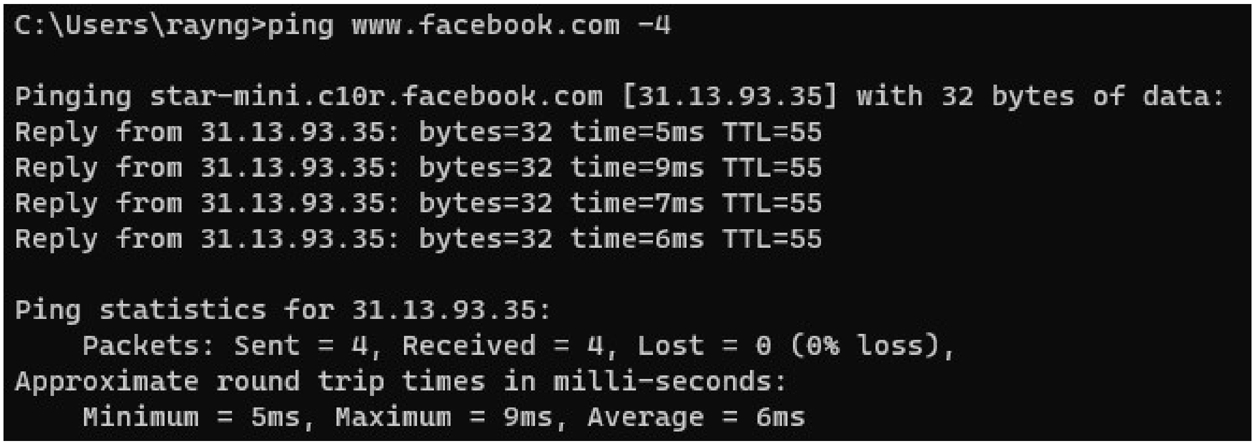


@{Microsoft.Windows.Search_1.14.7.190...
@{Microsoft.Windows.SecHealthUI_10.0....
ms-resource:AppDisplayName
ms-resource:AppDisplayName
Skype
Skype
Spotify Music
Spotify Music
3D Viewer
Acrobat Notification Client
Adobe Notification Client
AllJoyn Router (TCP-Out)
AllJoyn Router (UDP-Out)
App Installer
App Installer
Captive Portal Flow
Captive Portal Flow
Captive Portal Flow
Captive Portal Flow
Cast to Device functionality (qWave-TCP...
Cast to Device functionality (qWave-UDP...
Cast to Device streaming server (RTP-Stre...
Cast to Device streaming server (RTP-Stre...
Cast to Device streaming server (RTP-Stre...
Clipchamp
Connected Devices Platform - Wi-Fi Dire...
Connected Devices Platform (TCP-Out)
Connected Devices Platform (UDP-Out)
Core Networking - DNS (UDP-Out)
Core Networking - Dynamic Host Config...
Core Networking - Dynamic Host Config...
Core Networking - Group Policy (LSASS-...

Step 4 – Blocking Outbound IP Address through Firewall ACLs

8. Open Command Prompt.

9. Pinged www.facebook.com. Using command `ping www.facebook.com -4` to output IPv4.



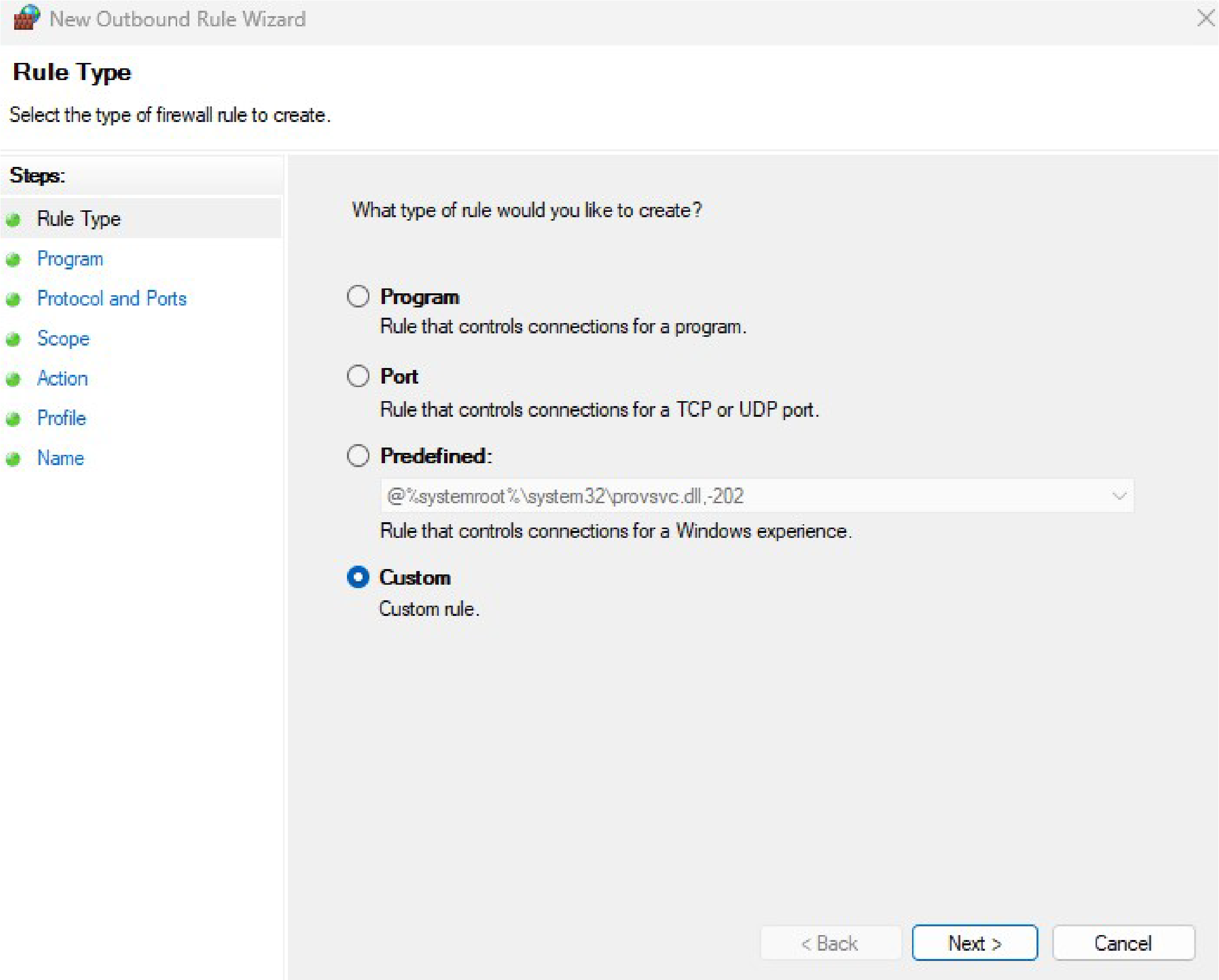
```
C:\Users\rayng>ping www.facebook.com -4

Pinging star-mini.c10r.facebook.com [31.13.93.35] with 32 bytes of data:
Reply from 31.13.93.35: bytes=32 time=5ms TTL=55
Reply from 31.13.93.35: bytes=32 time=9ms TTL=55
Reply from 31.13.93.35: bytes=32 time=7ms TTL=55
Reply from 31.13.93.35: bytes=32 time=6ms TTL=55

Ping statistics for 31.13.93.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 9ms, Average = 6ms
```

10. Went to my Firewall window.

11. Clicked on advanced settings.

12. Selected the Outbound Rules category in the left pane and clicked the Create Rule link in the right pane.

13. Under Rule Type, selected Custom > Click Next.



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

What type of rule would you like to create?

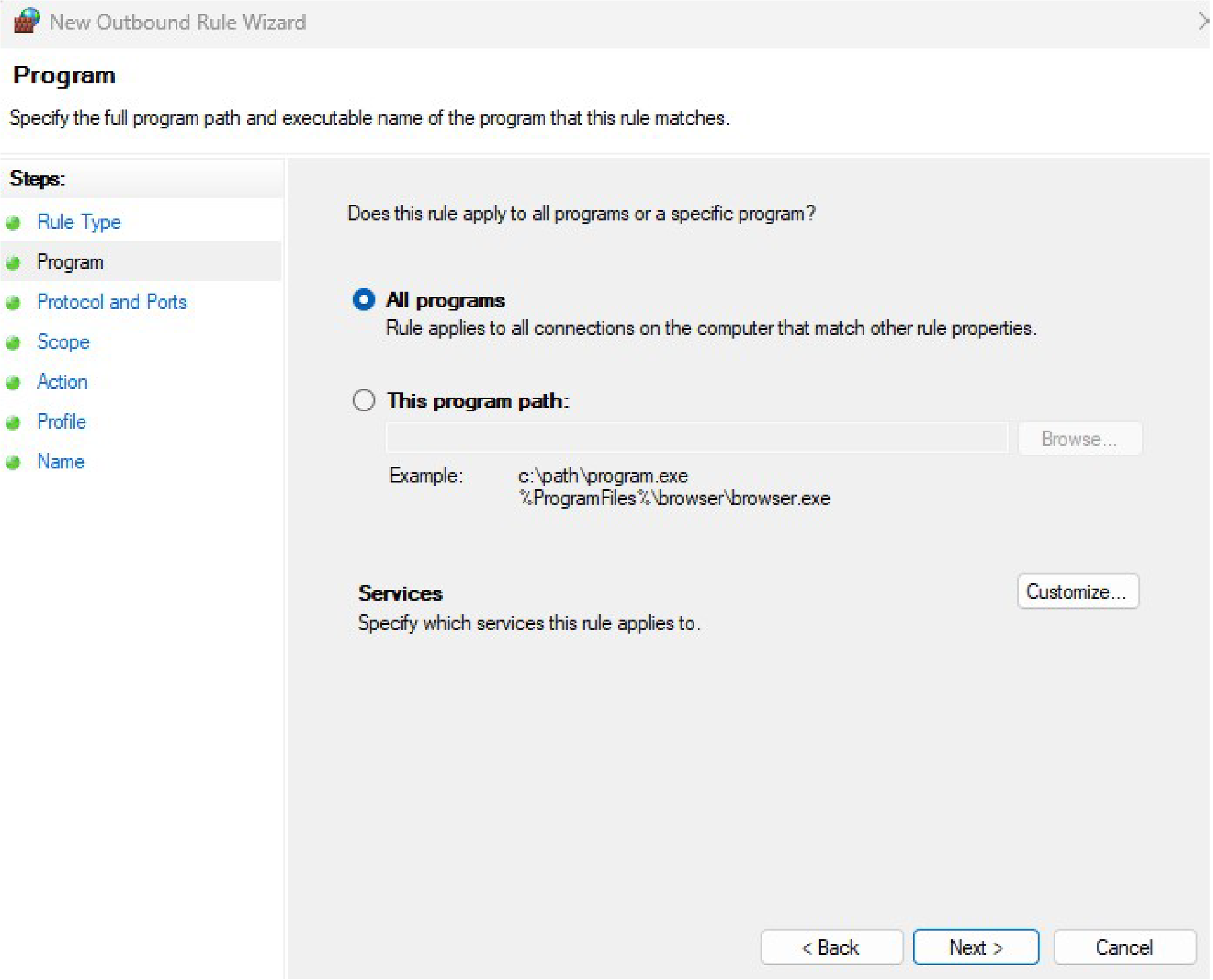
○ **Program**
Rule that controls connections for a program.

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

○ **Predefined:**
@%systemroot%\system32\provsvc.dll,-202
Rule that controls connections for a Windows experience.

● **Custom**
Custom rule.

14. Under Program, selected All Programs > Click Next.



New Outbound Rule Wizard

Program

Specify the full program path and executable name of the program that this rule matches.

Steps:

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Does this rule apply to all programs or a specific program?

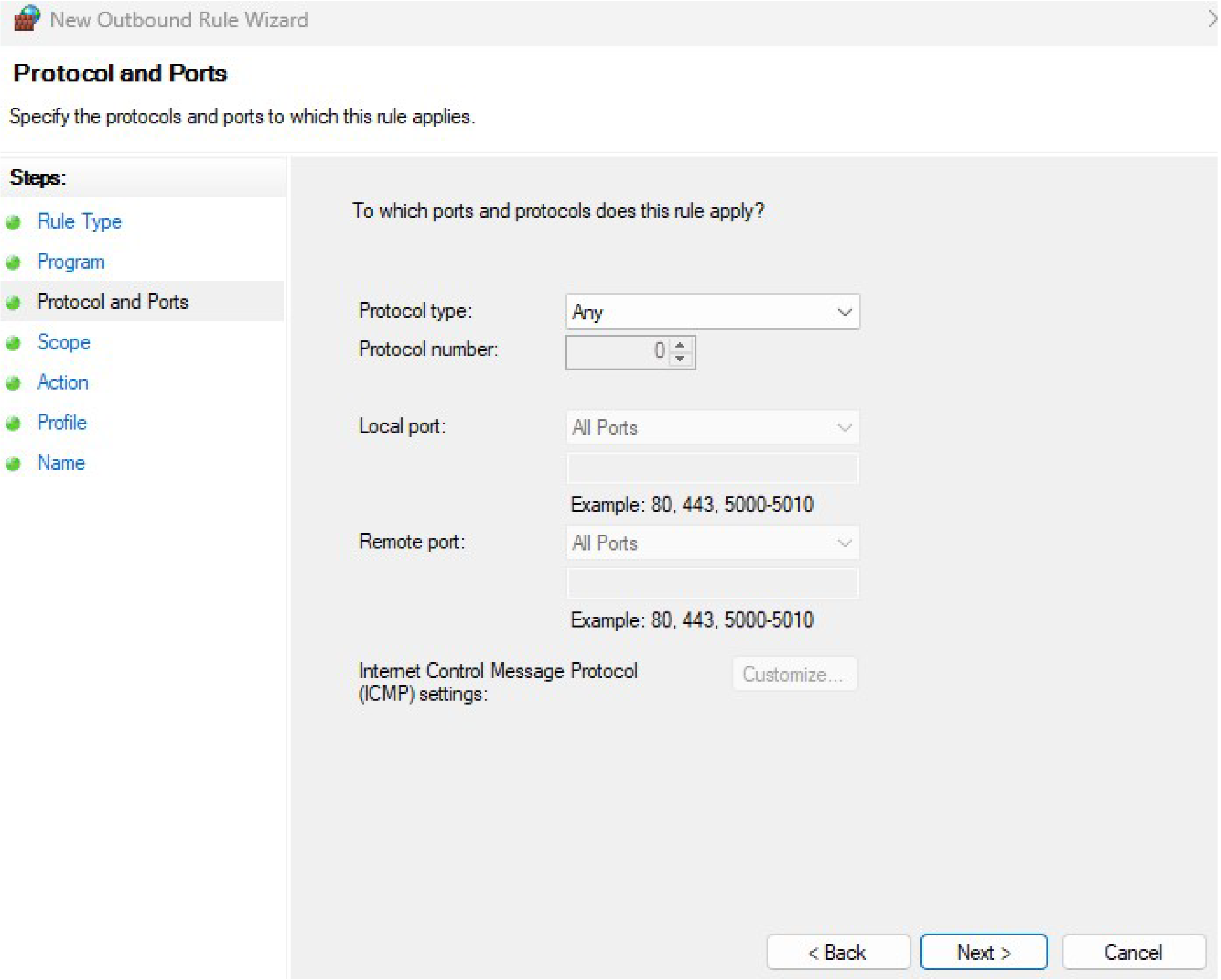
● **All programs**
Rule applies to all connections on the computer that match other rule properties.

○ **This program path:**

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Services
Specify which services this rule applies to.

15. Under Protocols and Ports, left default settings > Clicked Next.



Protocol and Ports

Specify the protocols and ports to which this rule applies.

To which ports and protocols does this rule apply?

Protocol type: Any

Protocol number: 0

Local port: All Ports

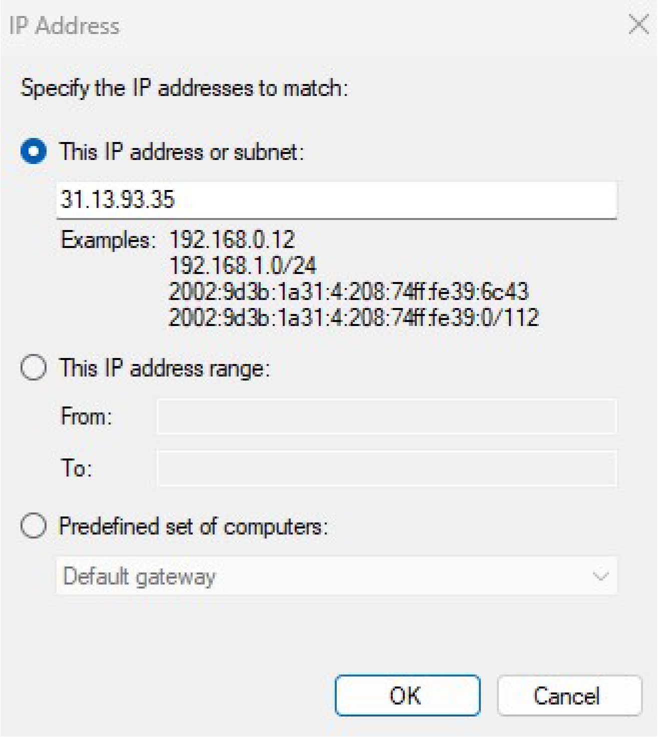
Example: 80, 443, 5000-5010

Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

16. Under Scope, selected These IP Addresses under remote IP address section > Clicked Add.



IP Address

Specify the IP addresses to match:

● This IP address or subnet:

31.13.93.35

Examples: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

○ This IP address range:

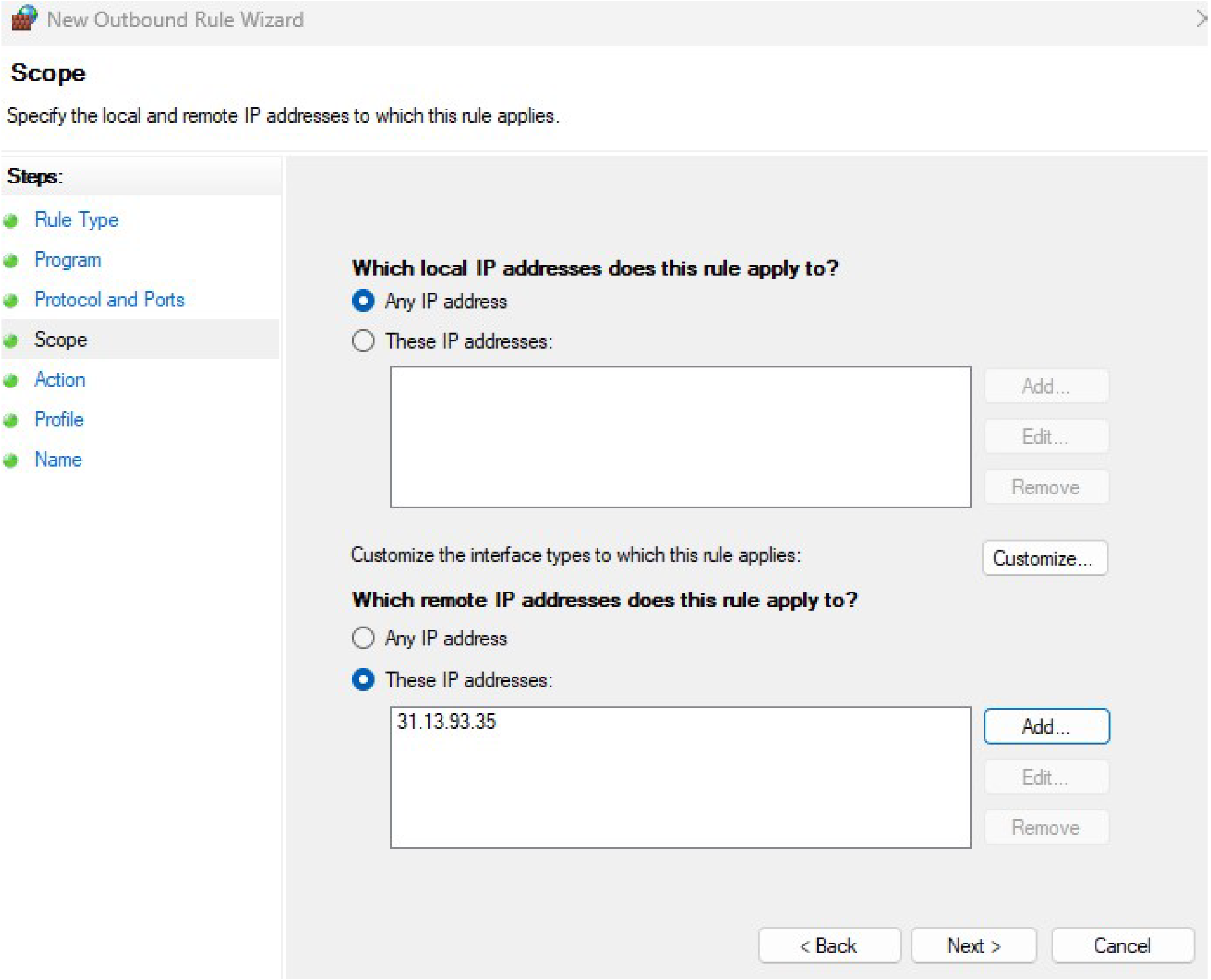
From:

To:

○ Predefined set of computers:

Default gateway

17. In the IP Address popup box, typed the IP address I got from the command prompt > Clicked OK.



Scope

Specify the local and remote IP addresses to which this rule applies.

Which local IP addresses does this rule apply to?

● Any IP address

○ These IP addresses:

Customize the interface types to which this rule applies:

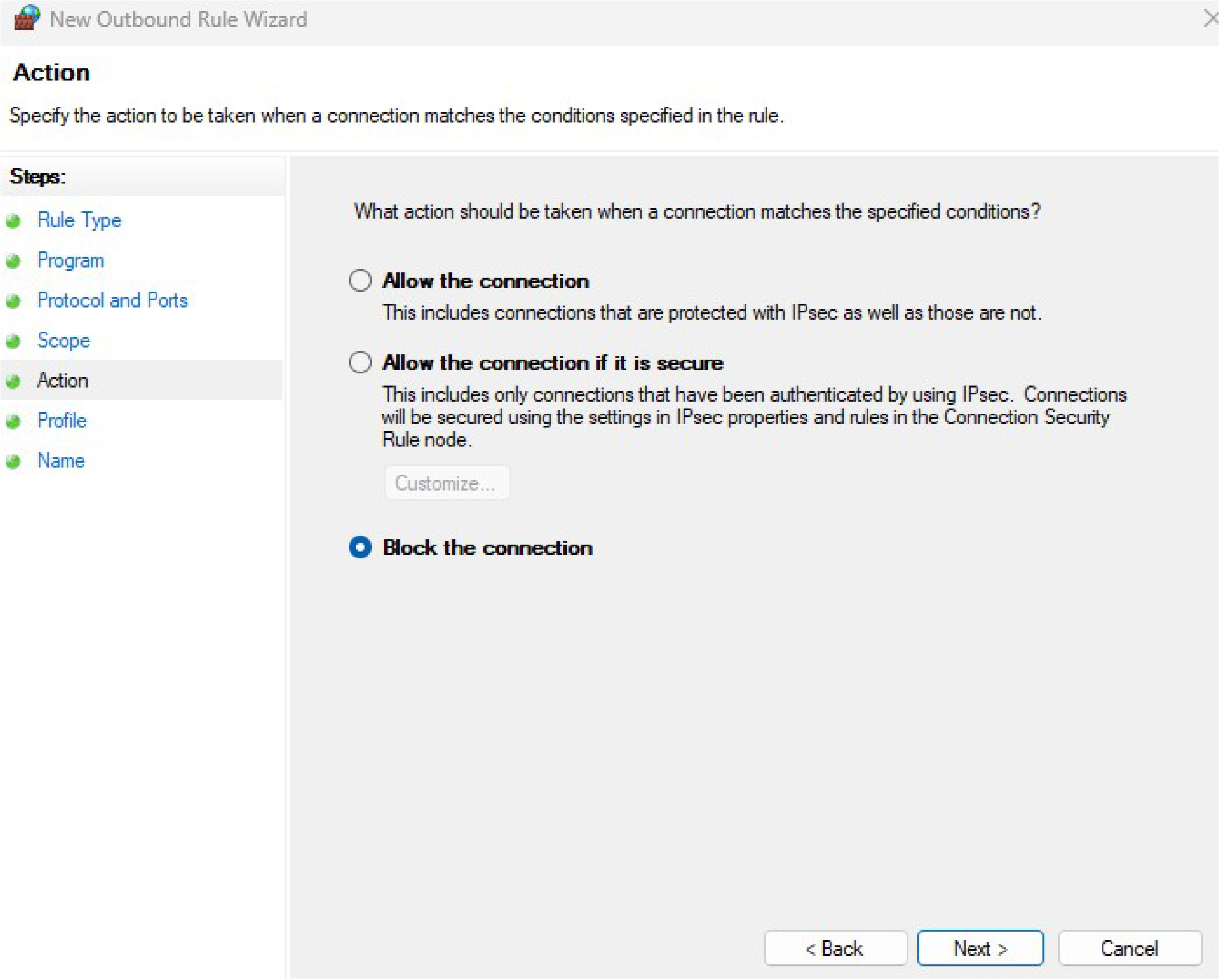
Which remote IP addresses does this rule apply to?

○ Any IP address

● These IP addresses:

31.13.93.35

18. Under Action, selected Block Connection > Clicked Next.



New Outbound Rule Wizard

Action

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

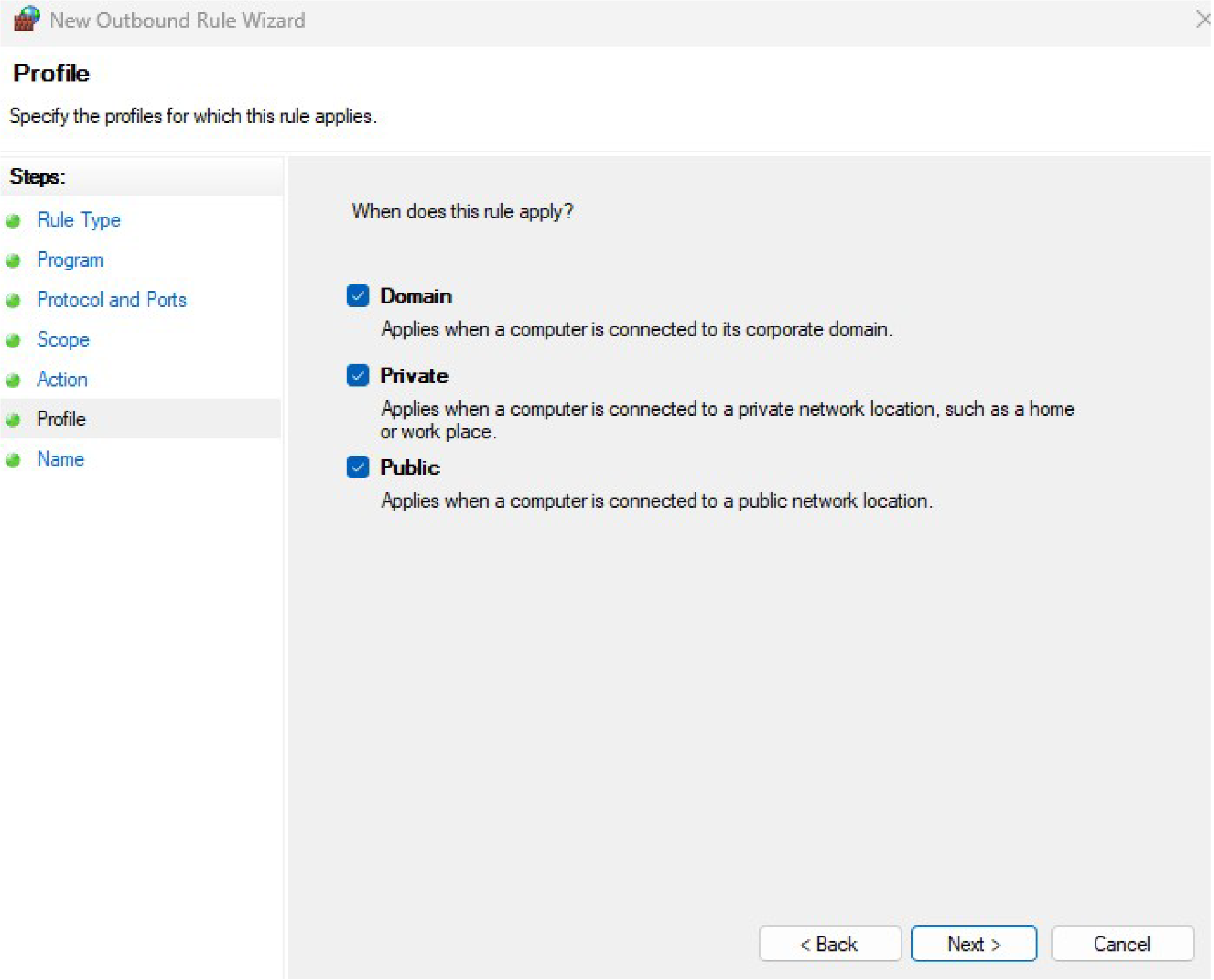
What action should be taken when a connection matches the specified conditions?

○ **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.

● **Block the connection**

19. Under Profile, left default settings > Clicked Next.



Profile

Specify the profiles for which this rule applies.

When does this rule apply?

☑ **Domain**

Applies when a computer is connected to its corporate domain.

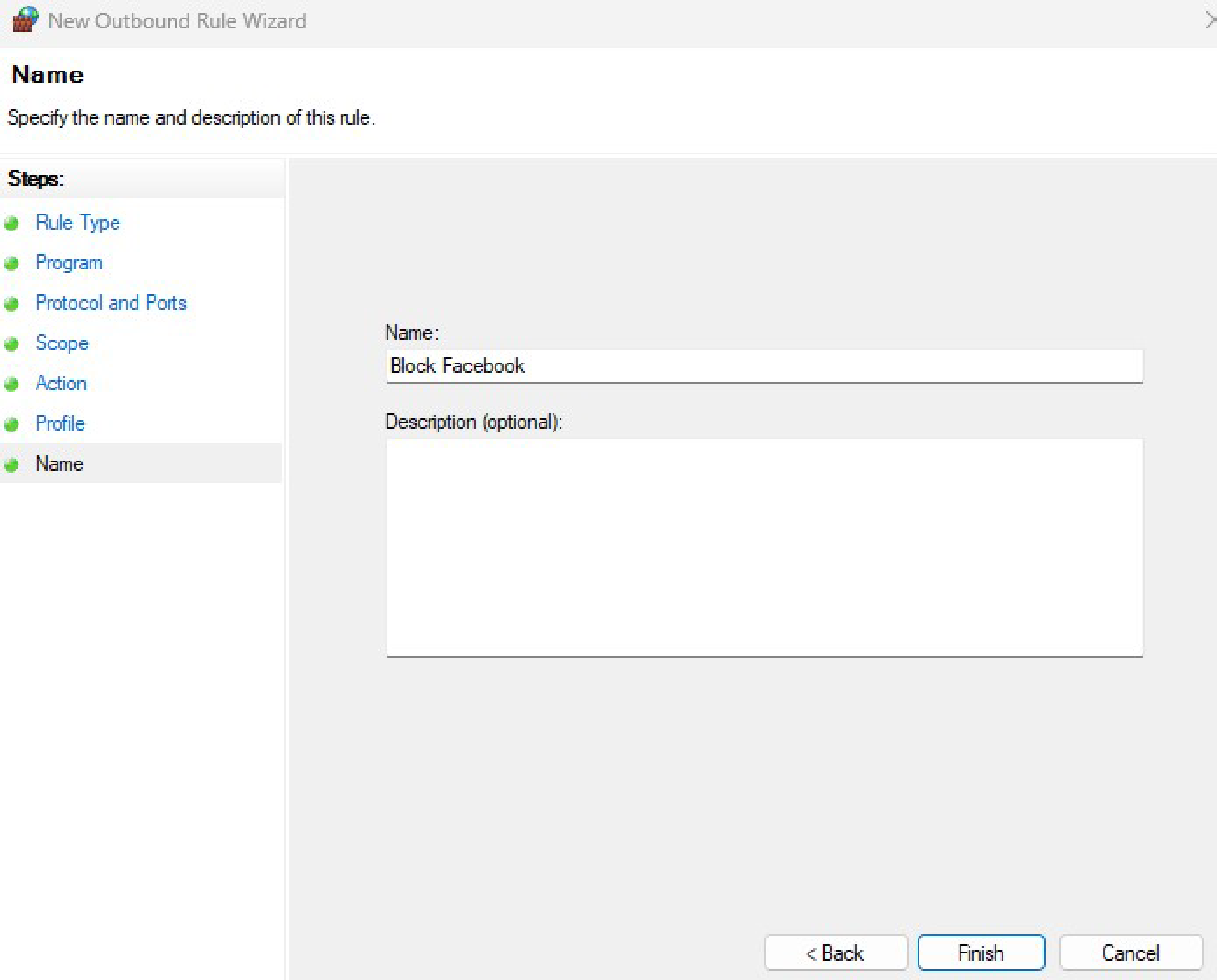
☑ **Private**

Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**

Applies when a computer is connected to a public network location.

20. Under Name, typed Block Facebook



New Outbound Rule Wizard

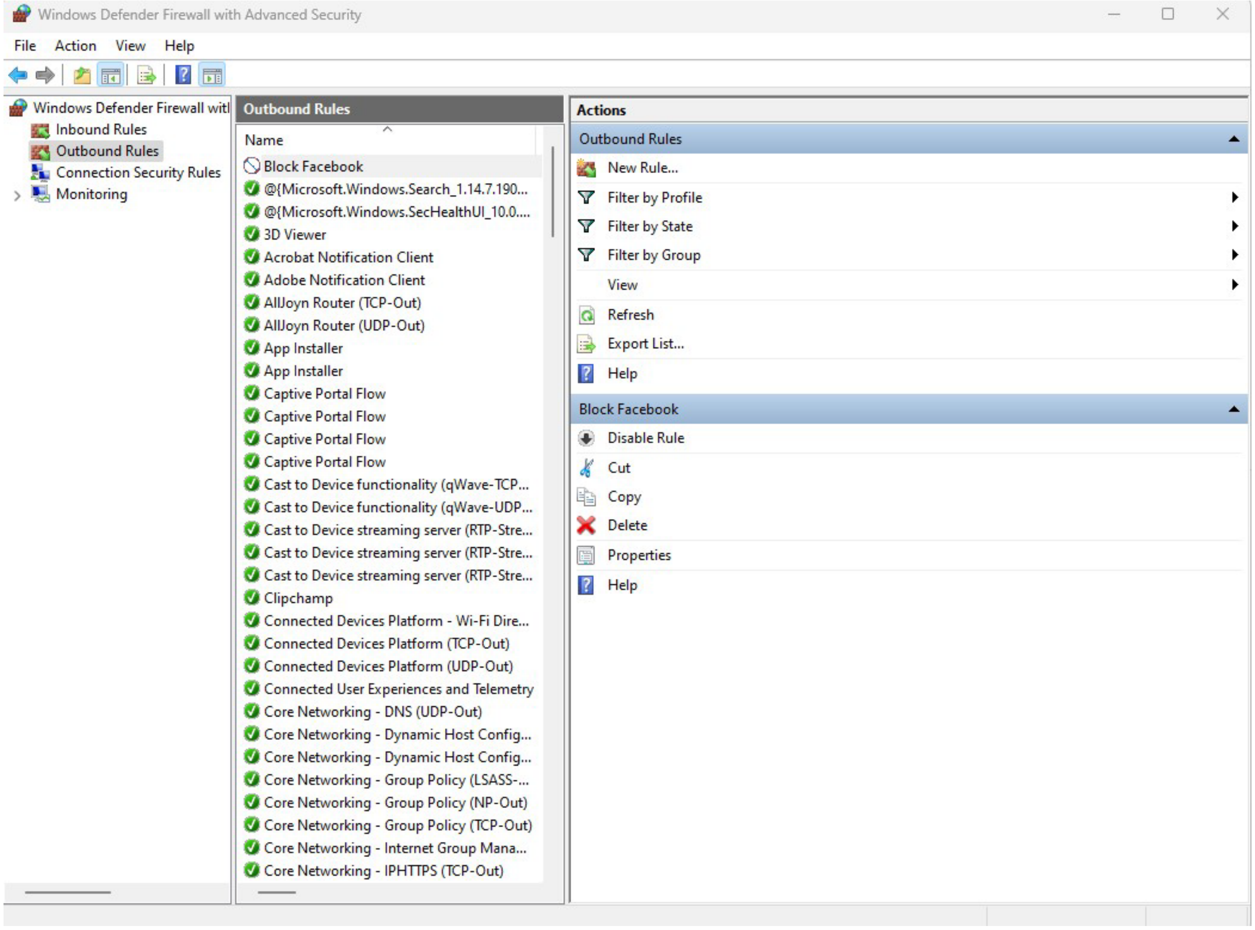
Name

Specify the name and description of this rule.

Name: Block Facebook

Description (optional):

21. **SNAPSHOT**: For each setting, and the outbound rules.



Block Facebook
@{Microsoft.Windows.Search_1.14.7.190...
@{Microsoft.Windows.SecHealthUI_10.0....
3D Viewer
Acrobat Notification Client
Adobe Notification Client
AllJoyn Router (TCP-Out)
AllJoyn Router (UDP-Out)
App Installer
App Installer
Captive Portal Flow
Captive Portal Flow
Captive Portal Flow
Captive Portal Flow
Cast to Device functionality (qWave-TCP...
Cast to Device functionality (qWave-UDP...
Cast to Device streaming server (RTP-Stre...
Cast to Device streaming server (RTP-Stre...
Cast to Device streaming server (RTP-Stre...
Clipchamp
Connected Devices Platform - Wi-Fi Dire...
Connected Devices Platform (TCP-Out)
Connected Devices Platform (UDP-Out)
Connected User Experiences and Telemetry
Core Networking - DNS (UDP-Out)
Core Networking - Dynamic Host Config...
Core Networking - Dynamic Host Config...
Core Networking - Group Policy (LSASS-...
Core Networking - Group Policy (NP-Out)
Core Networking - Group Policy (TCP-Out)
Core Networking - Internet Group Mana...
Core Networking - IPHTTPS (TCP-Out)

Part C: Virus Total (30 points)

VirusTotal is a free online service that analyzes files and URLs in order to identify potential malware. VirusTotal scans and detects various types of content, including a Windows executable program, Android, PDFs, and images.

In this exercise, I will use VirusTotal to scan a file and a URL. To do this exercise, I executed the following steps:

Step 1 – Scan a File

1. Used Microsoft Word and created a document that contained the above paragraph about VirusTotal. Saved the document as VirusTotal.docx.

2. Then, saved the document as a PDF.

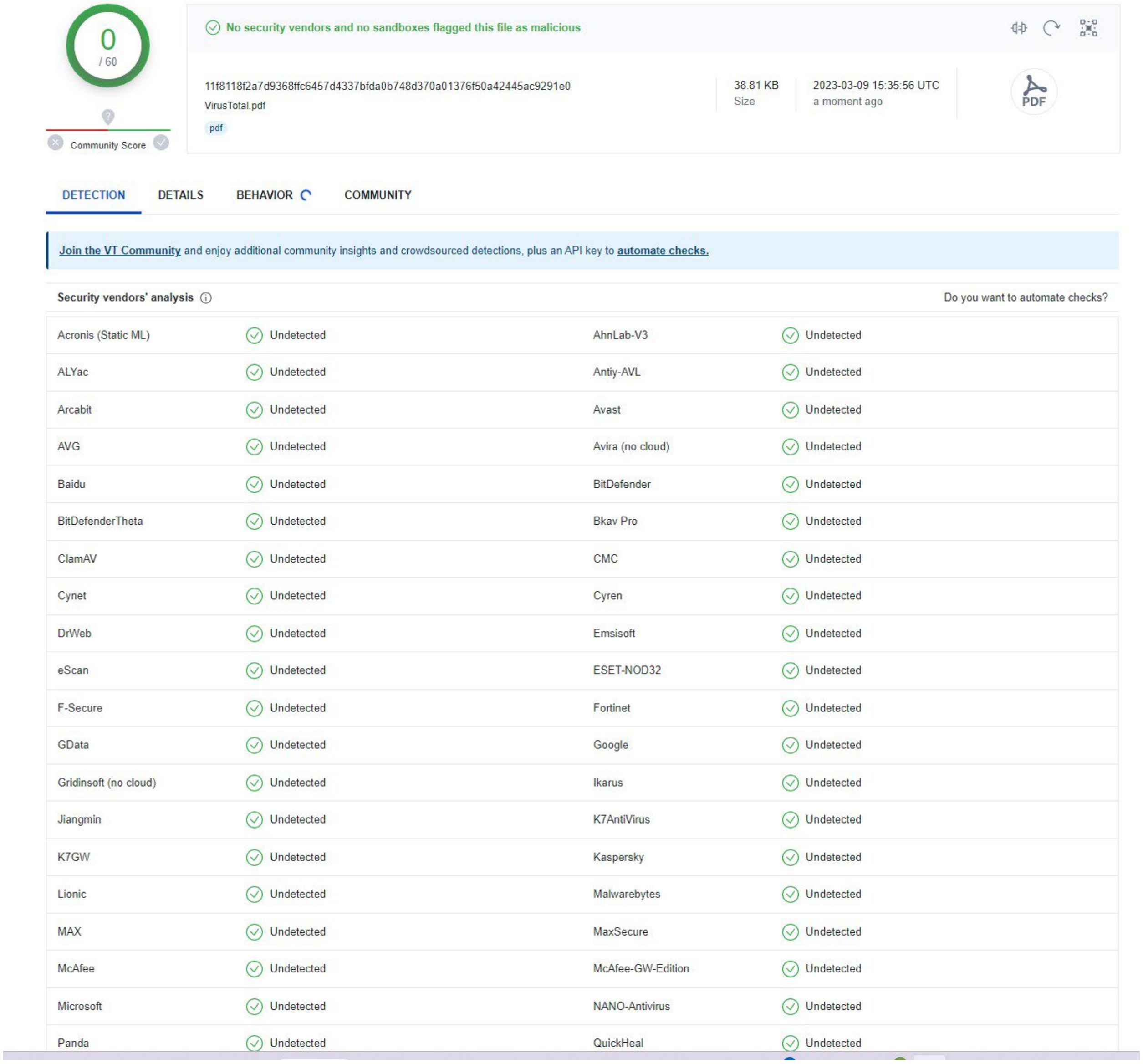
3. Went to the following URL https://www.virustotal.com/

4. Under the File tab, clicked Choose File.

5. Navigated to the location of the pdf file and clicked Open.

6. Clicked Scan / upload.

7. **SNAPSHOT:** Observed the analysis results by scrolling through the list of AV vendors that had been polled regarding the file as well as clicked the detail tab and read through the analysis.



No security vendors and no sandboxes flagged this file as malicious

11f8118f2a7d9368ffc6457d4337bfda0b748d370a01376f50a42445ac9291e0
VirusTotal.pdf
pdf

38.81 KB
Size

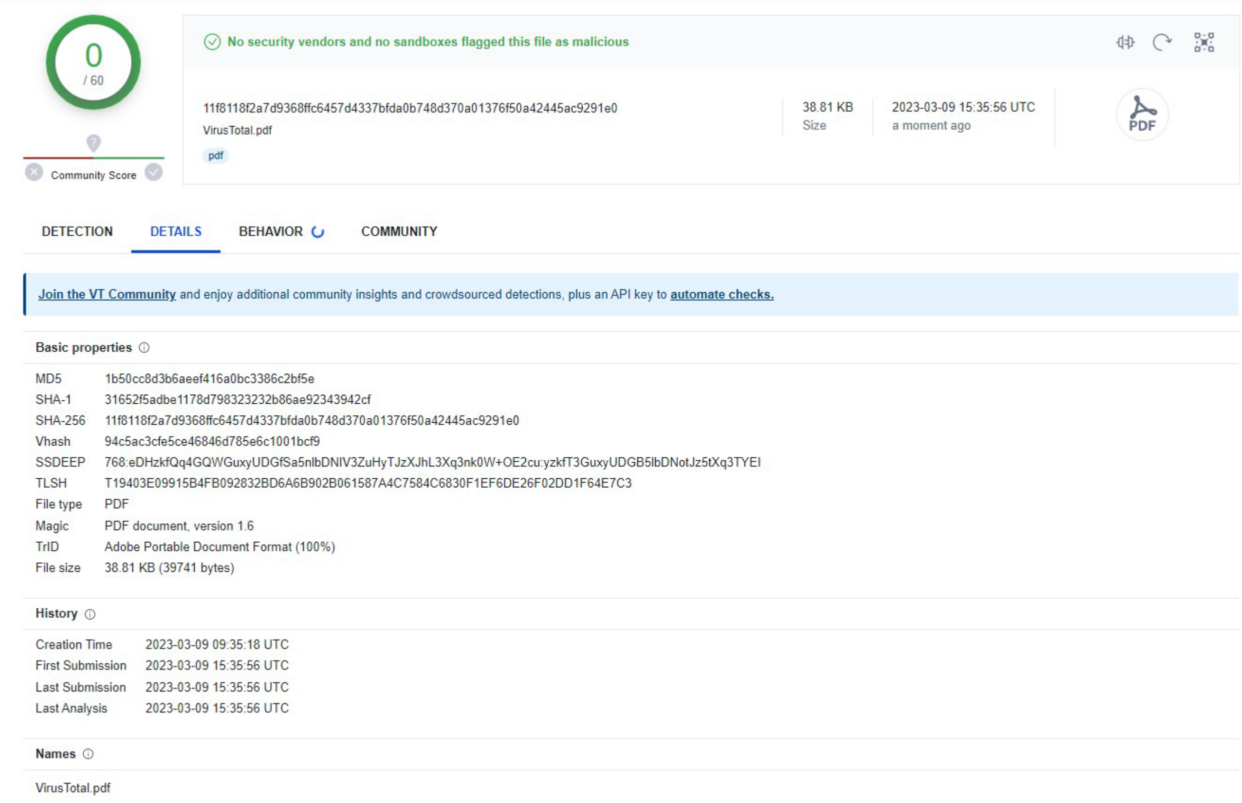
2023-03-09 15:35:56 UTC
a moment ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected
Cynet	Undetected	Cyren	Undetected
DrWeb	Undetected	Emsisoft	Undetected
eScan	Undetected	ESET-NOD32	Undetected
F-Secure	Undetected	Fortinet	Undetected
GData	Undetected	Google	Undetected
Gridinsoft (no cloud)	Undetected	Ikarus	Undetected
Jiangmin	Undetected	K7AntiVirus	Undetected
K7GW	Undetected	Kaspersky	Undetected
Lionic	Undetected	Malwarebytes	Undetected
MAX	Undetected	MaxSecure	Undetected
McAfee	Undetected	McAfee-GW-Edition	Undetected
Microsoft	Undetected	NANO-Antivirus	Undetected
Panda	Undetected	QuickHeal	Undetected



No security vendors and no sandboxes flagged this file as malicious

11f8118f2a7d9368ffc6457d4337bfda0b748d370a01376f50a42445ac9291e0
VirusTotal.pdf
pdf

38.81 KB
Size

2023-03-09 15:35:56 UTC
a moment ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	1b50cc8d3b6aeef416a0bc3386c2bf5e
SHA-1	31652f5adbe1178d798323232b86ae92343942cf
SHA-256	11f8118f2a7d9368ffc6457d4337bfda0b748d370a01376f50a42445ac9291e0
Vhash	94c5ac3cfe5ce46846d785e6c1001bcf9
SSDEEP	768:eDHzkfQq4GQWGuxyUDGfSa5nlbDNIV3ZuHyTJzXJhL3Xq3nk0W+OE2cu:yzkfT3GuxyUDGB5lbDNotJz5tXq3TYEI
TLSH	T19403E09915B4FB092832BD6A6B902B061587A4C7584C6830F1EF6DE26F02DD1F64E7C3
File type	PDF
Magic	PDF document, version 1.6
TrID	Adobe Portable Document Format (100%)
File size	38.81 KB (39741 bytes)

History

Creation Time	2023-03-09 09:35:18 UTC
First Submission	2023-03-09 15:35:56 UTC
Last Submission	2023-03-09 15:35:56 UTC
Last Analysis	2023-03-09 15:35:56 UTC

Names

VirusTotal.pdf

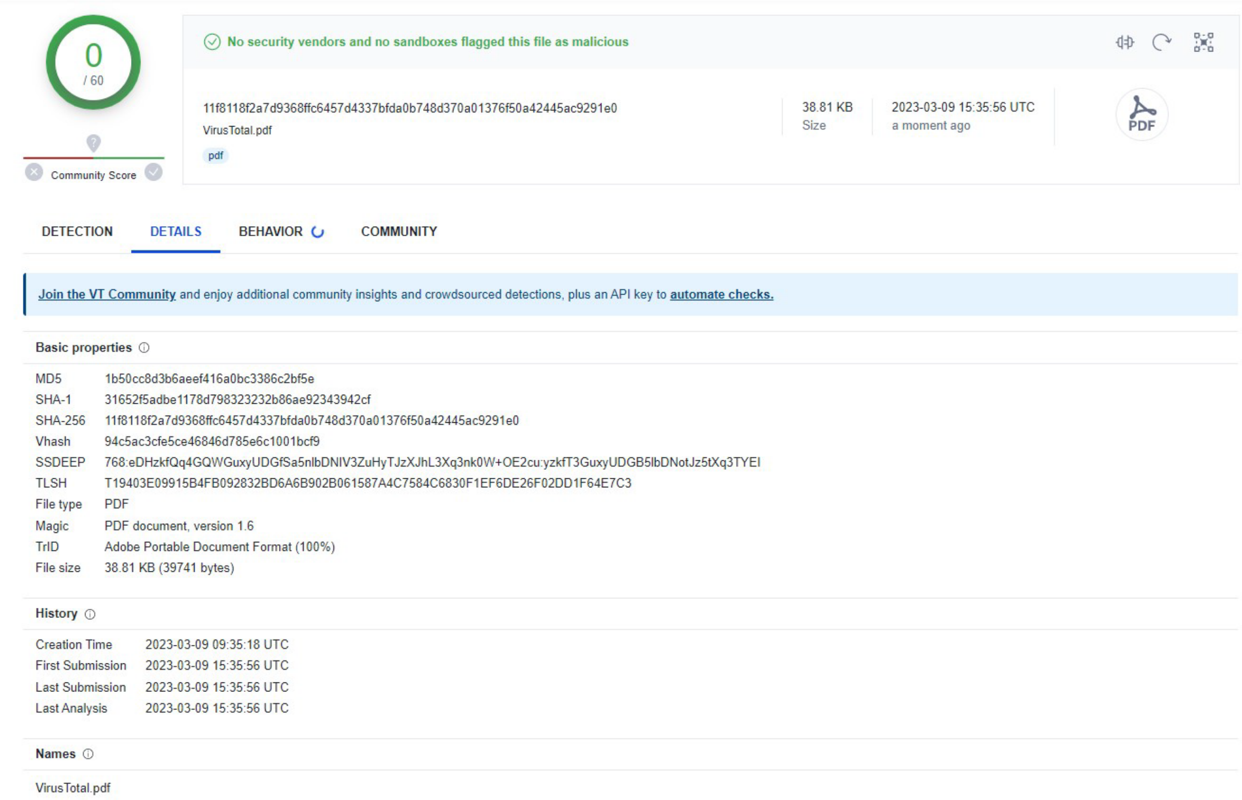
Step 2 – Scan a URL

8. Went to the following URL https://www.virustotal.com/

9. Under the URL tab, enter the URL of my school, `https://www.utsa.edu/`.

10. Clicked Scan it!

11. **SNAPSHOT:** Observed the analysis results.



No security vendors and no sandboxes flagged this file as malicious

11f8118f2a7d9368ffc6457d4337bfda0b748d370a01376f50a42445ac9291e0
VirusTotal.pdf
pdf

38.81 KB
Size

2023-03-09 15:35:56 UTC
a moment ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

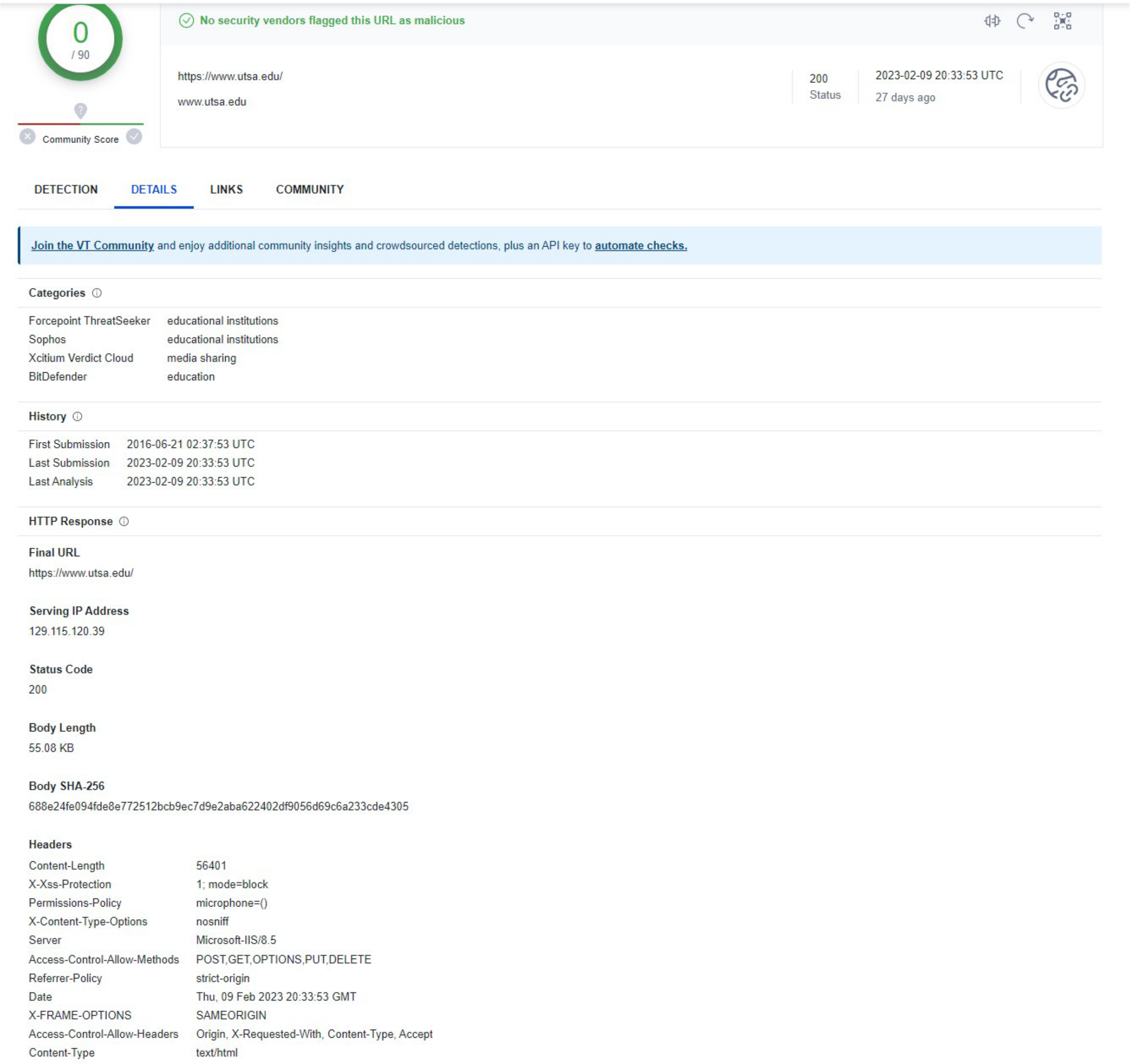
MD5	1b50cc8d3b6aeef416a0bc3386c2bf5e
SHA-1	31652f5adbe1178d798323232b86ae92343942cf
SHA-256	11f8118f2a7d9368ffc6457d4337bfda0b748d370a01376f50a42445ac9291e0
Vhash	94c5ac3cfe5ce46846d785e6c1001bcf9
SSDEEP	768:eDHzkfQq4GQWGuxyUDGfSa5nlbDNIV3ZuHyTJzXJhL3Xq3nk0W+OE2cu:yzkfT3GuxyUDGB5lbDNotJz5tXq3TYEI
TLSH	T19403E09915B4FB092832BD6A6B902B061587A4C7584C6830F1EF6DE26F02DD1F64E7C3
File type	PDF
Magic	PDF document, version 1.6
TrID	Adobe Portable Document Format (100%)
File size	38.81 KB (39741 bytes)

History

Creation Time	2023-03-09 09:35:18 UTC
First Submission	2023-03-09 15:35:56 UTC
Last Submission	2023-03-09 15:35:56 UTC
Last Analysis	2023-03-09 15:35:56 UTC

Names

VirusTotal.pdf



No security vendors flagged this URL as malicious

https://www.utsa.edu/

www.utsa.edu

200
Status

2023-02-09 20:33:53 UTC
27 days ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Categories ⓘ

Forcepoint ThreatSeeker	educational institutions
Sophos	educational institutions
Xcitium Verdict Cloud	media sharing
BitDefender	education

History ⓘ

First Submission	2016-06-21 02:37:53 UTC
Last Submission	2023-02-09 20:33:53 UTC
Last Analysis	2023-02-09 20:33:53 UTC

HTTP Response ⓘ

Final URL
https://www.utsa.edu/

Serving IP Address
129.115.120.39

Status Code
200

Body Length
55.08 KB

Body SHA-256
688e24fe094fde8e772512bcb9ec7d9e2aba622402df9056d69c6a233cde4305

Headers

Content-Length	56401
X-Xss-Protection	1; mode=block
Permissions-Policy	microphone=()
X-Content-Type-Options	nosniff
Server	Microsoft-IIS/8.5
Access-Control-Allow-Methods	POST,GET,OPTIONS,PUT,DELETE
Referrer-Policy	strict-origin
Date	Thu, 09 Feb 2023 20:33:53 GMT
X-FRAME-OPTIONS	SAMEORIGIN
Access-Control-Allow-Headers	Origin, X-Requested-With, Content-Type, Accept
Content-Type	text/html