FORMAN CHRISTIAN COLLEGE

(A CHARTERED UNIVERSITY)

COMP 421

Information Security

Assignment 3

Submitted By: Komal Amjad Butt

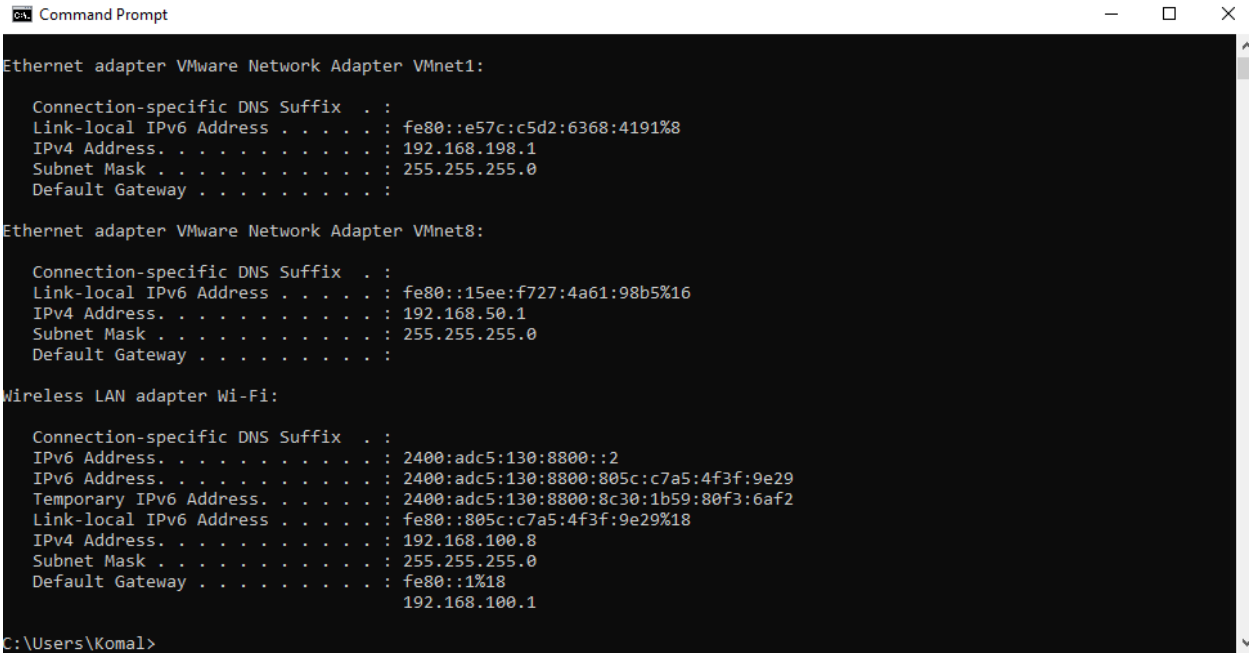
Roll Number: 22-10134

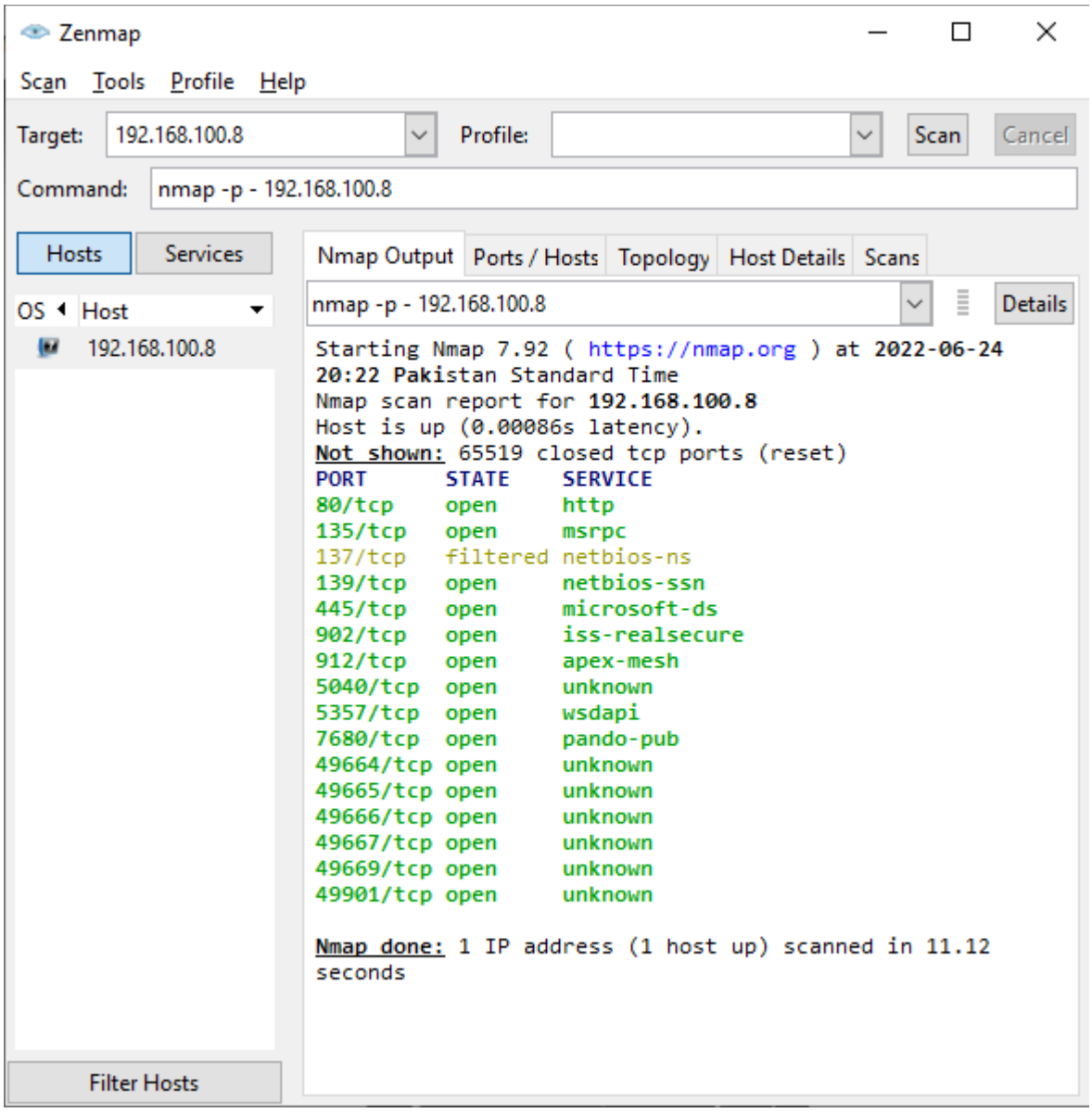
Section: B

Following steps are to be followed to perform the task:

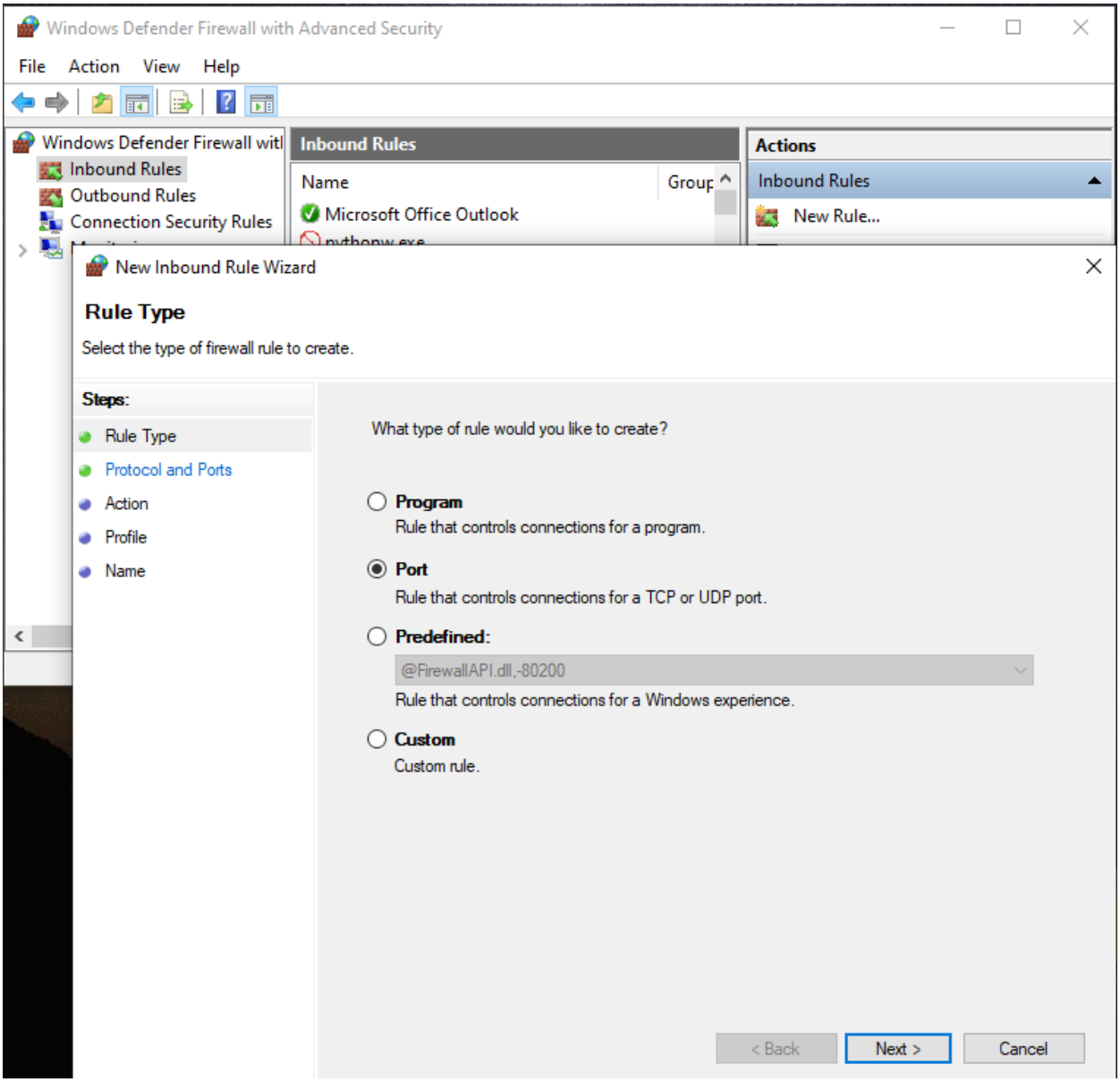
1. Install the “zenmap” tool.
2. Run zenmap.
3. Find the open ports in window machine.
4. Temporarily block a port which you think is a liability to the system’s protection.
5. This blocking is done by a rule which is defined by us in firewall section of Windows.

By entering the IP Address in Zenmap we will get the open ports:

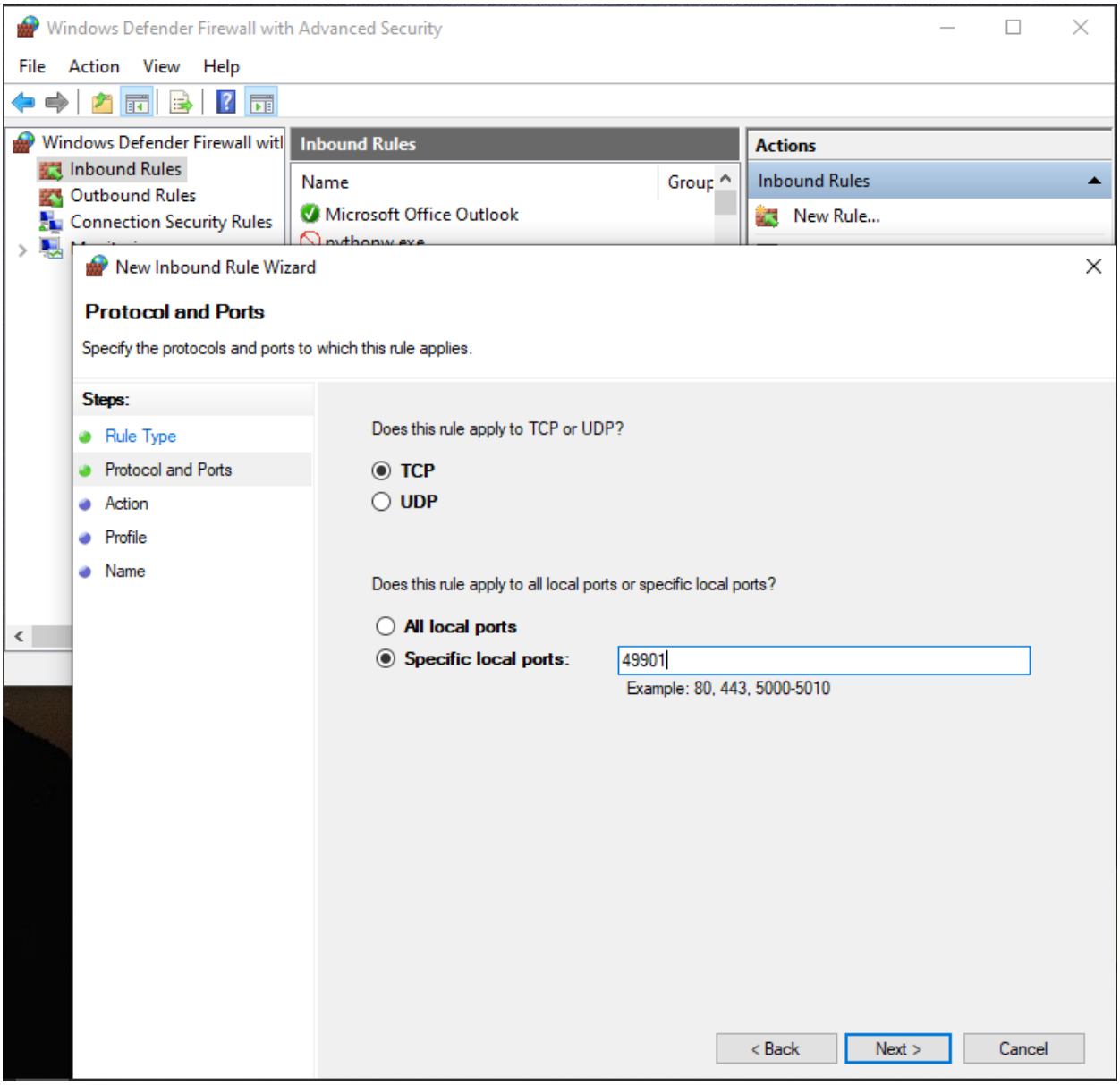



Zenmap
Scan Tools Profile Help
Target: 192.168.100.8
Profile:
Scan
Cancel
Command: nmap -p - 192.168.100.8
Hosts
Services
OS Host
192.168.100.8
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p - 192.168.100.8
Details
Starting Nmap 7.92 (https://nmap.org) at 2022-06-24 20:22 Pakistan Standard Time
Nmap scan report for 192.168.100.8
Host is up (0.00086s latency).
Not shown: 65519 closed tcp ports (reset)
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
137/tcp filtered netbios-ns
139/tcp open netbios-ssn
445/tcp open microsoft-ds
902/tcp open iss-realsecure
912/tcp open apex-mesh
5040/tcp open unknown
5357/tcp open wsdapi
7680/tcp open pando-pub
49664/tcp open unknown
49665/tcp open unknown
49666/tcp open unknown
49667/tcp open unknown
49669/tcp open unknown
49901/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 11.12 seconds

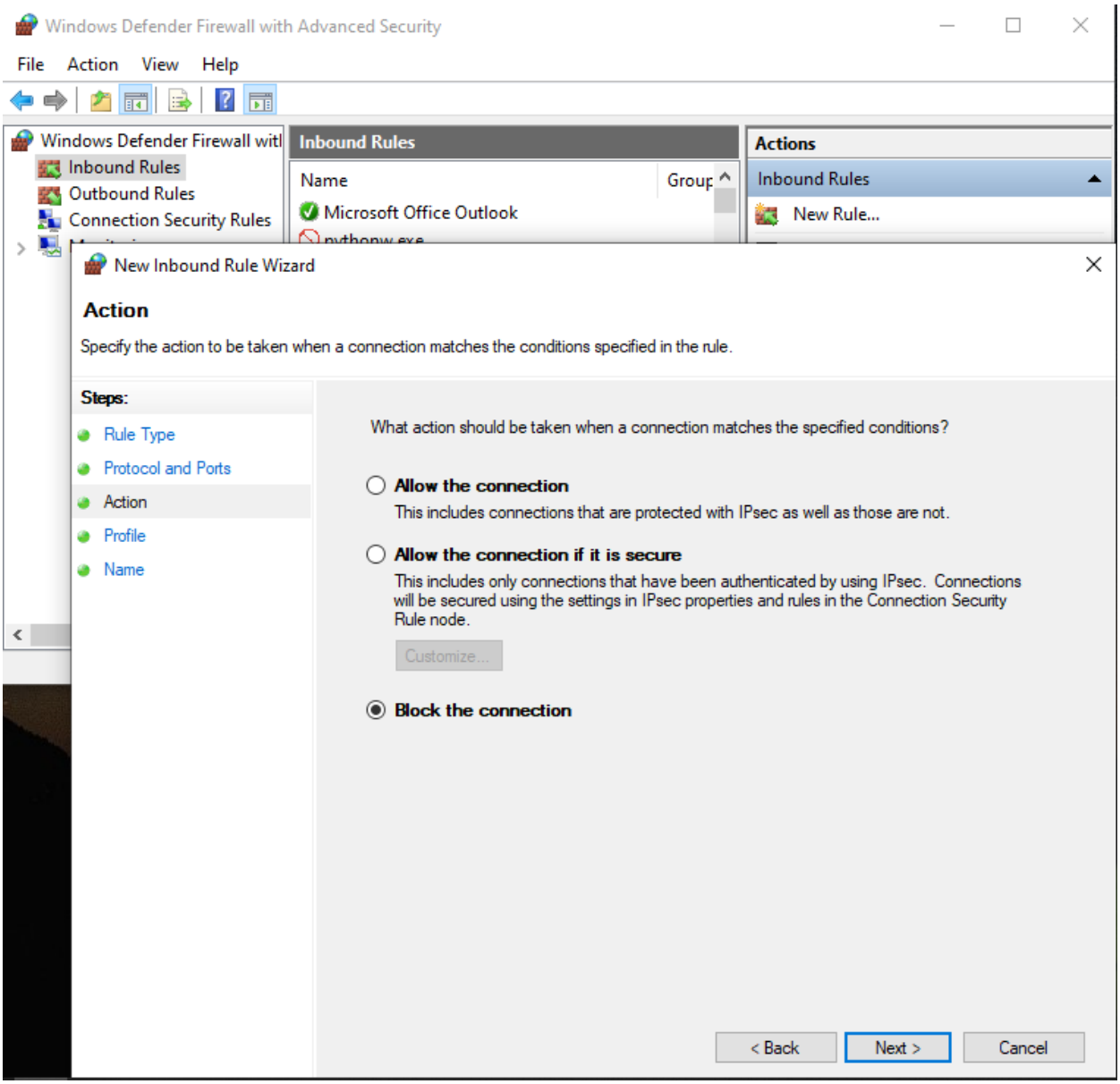
Opening firewall and making a new rule:

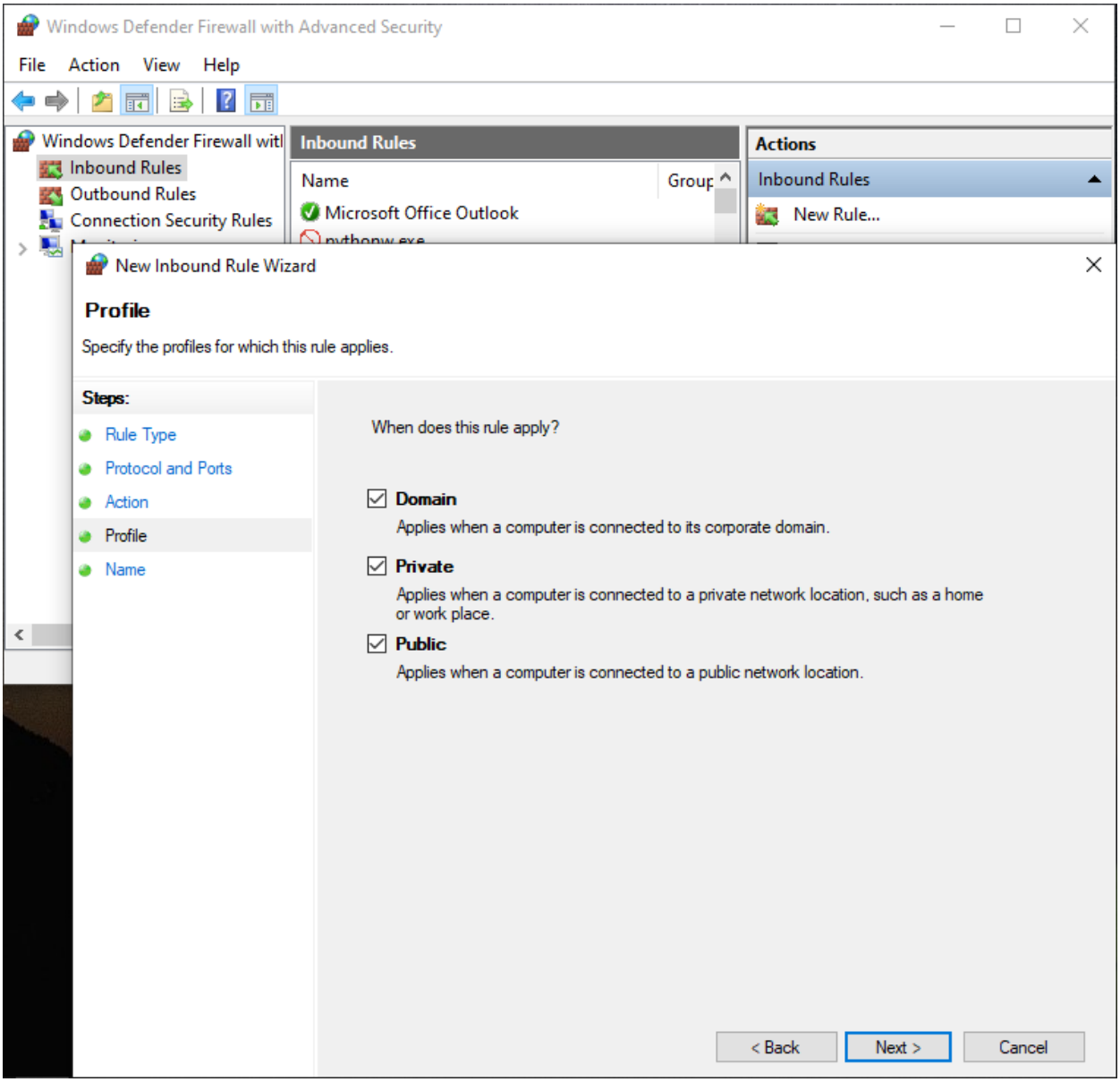


Using port number 49901:

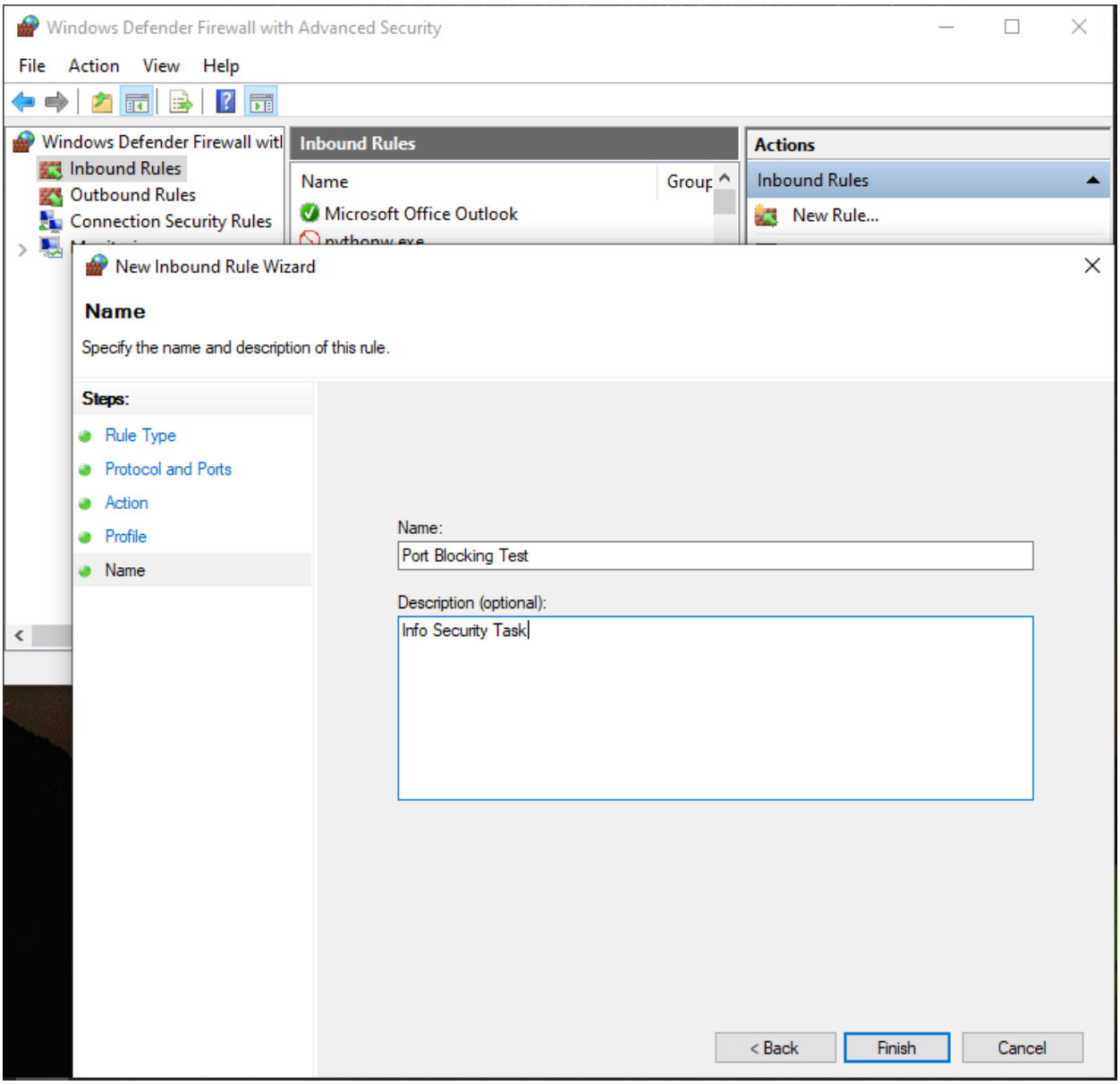


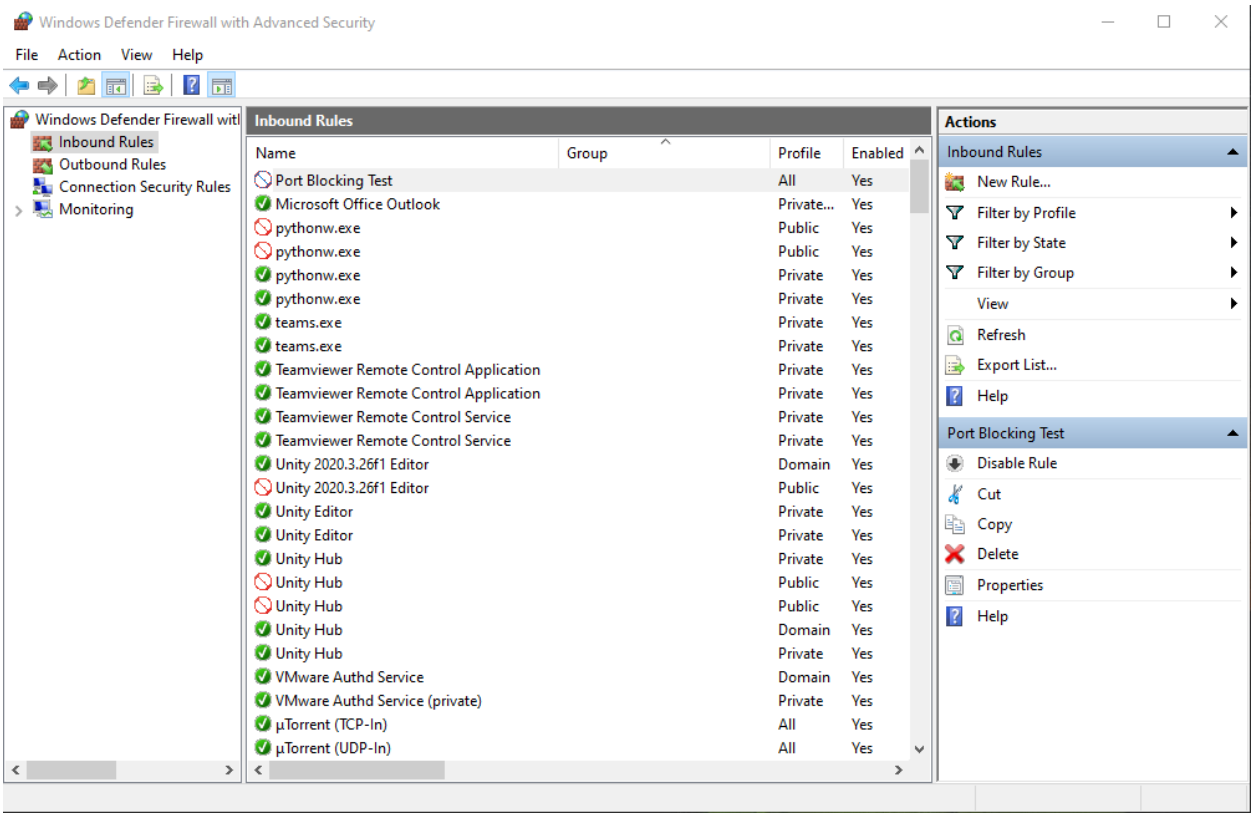
Blocking this connection:




Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Inbound Rules
Name
Group
Microsoft Office Outlook
Actions
Inbound Rules
New Rule...
New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
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.
< Back
Next >
Cancel

Probook is the new rule and it is blocked:




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
Port Blocking Test All Yes
Microsoft Office Outlook Private... Yes
pythonw.exe Public Yes
pythonw.exe Public Yes
pythonw.exe Private Yes
pythonw.exe Private Yes
teams.exe Private Yes
teams.exe Private Yes
Teamviewer Remote Control Application Private Yes
Teamviewer Remote Control Application Private Yes
Teamviewer Remote Control Service Private Yes
Teamviewer Remote Control Service Private Yes
Unity 2020.3.26f1 Editor Domain Yes
Unity 2020.3.26f1 Editor Public Yes
Unity Editor Private Yes
Unity Editor Private Yes
Unity Hub Private Yes
Unity Hub Public Yes
Unity Hub Public Yes
Unity Hub Domain Yes
Unity Hub Private Yes
VMware Authd Service Domain Yes
VMware Authd Service (private) Private Yes
µTorrent (TCP-In) All Yes
µTorrent (UDP-In) All Yes
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Port Blocking Test
Disable Rule
Cut
Copy
Delete
Properties
Help