FORMAN CHRISTIAN COLLEGE
(A CHARTERED UNIVERSITY)

Course Title:

COMP 421 – Information Security

Section: A

Instructor:

Dr Saad Bin Saleem

Instrument:

Assignment 3

Student name & roll number:

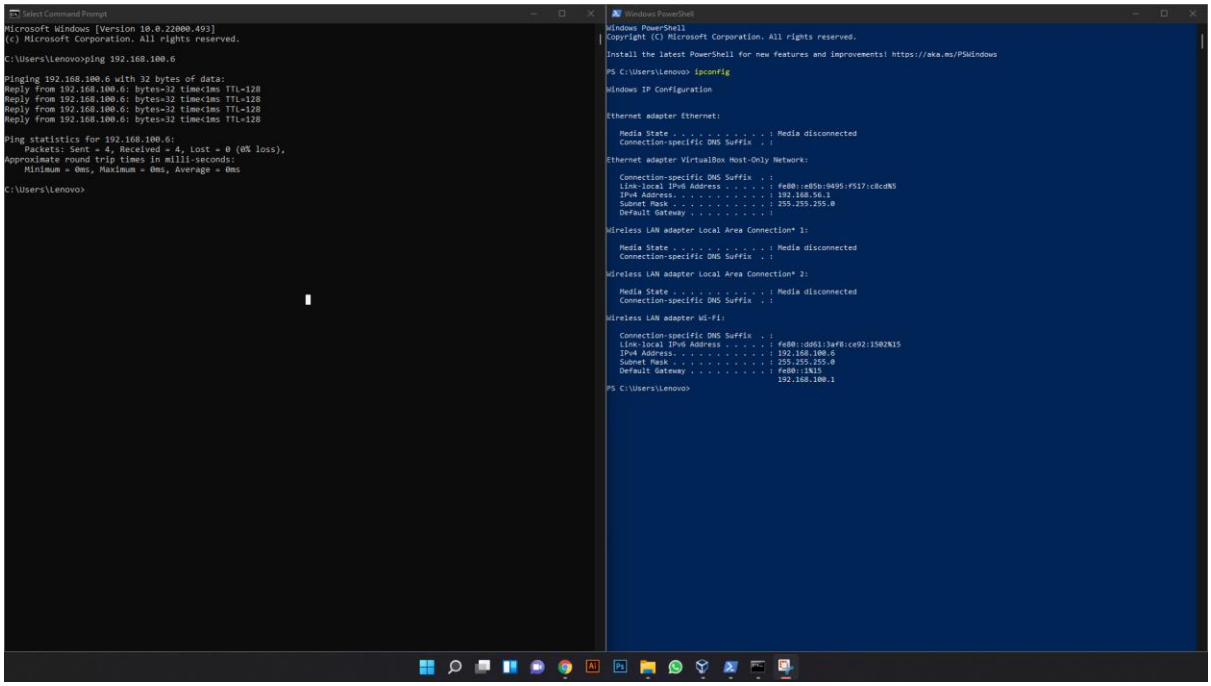
Sundas Javaid 19-10685

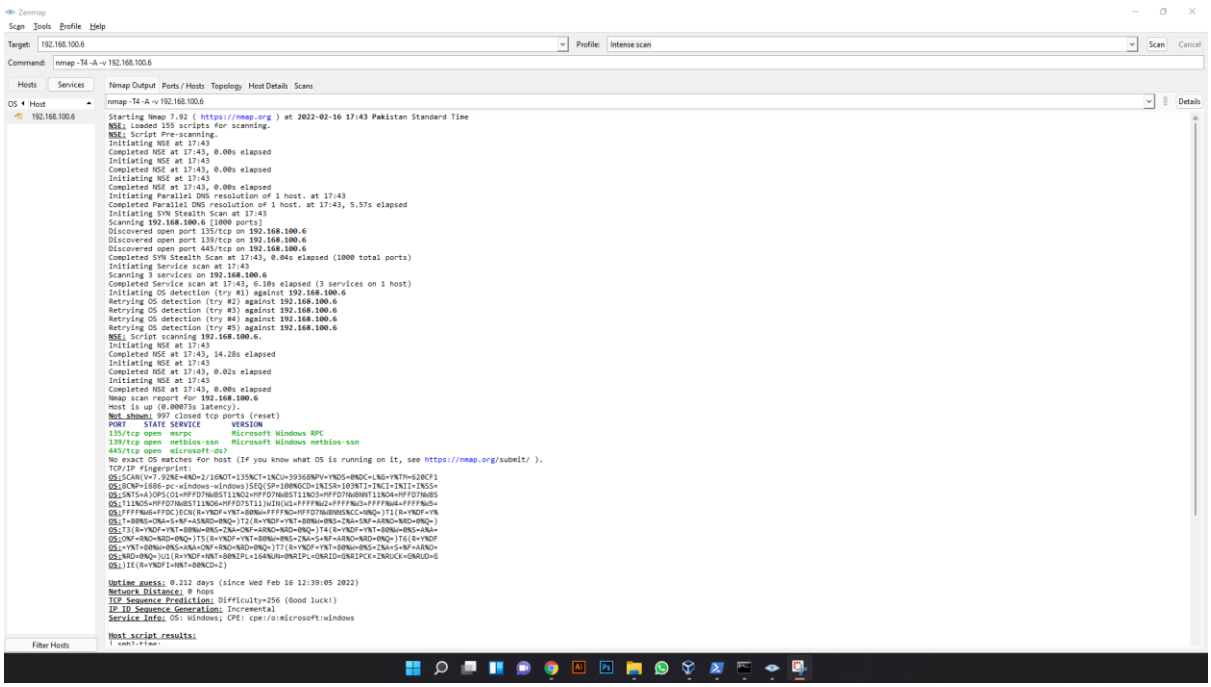
Semester: SP 22’

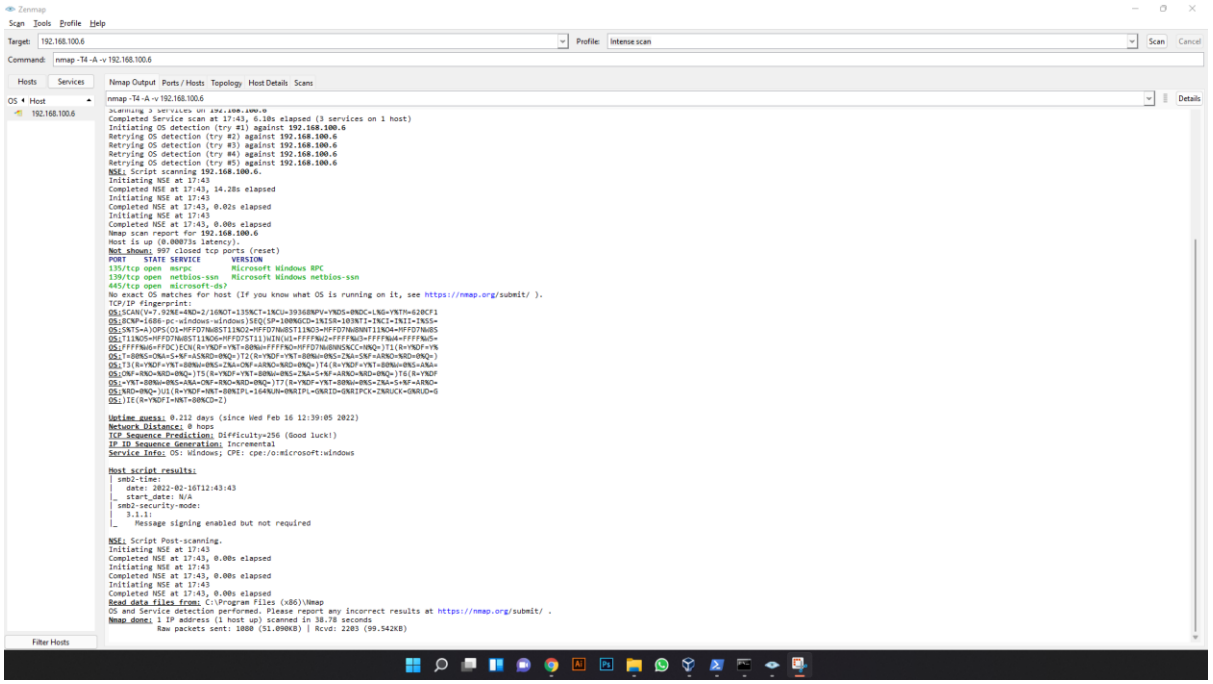
Submission date:

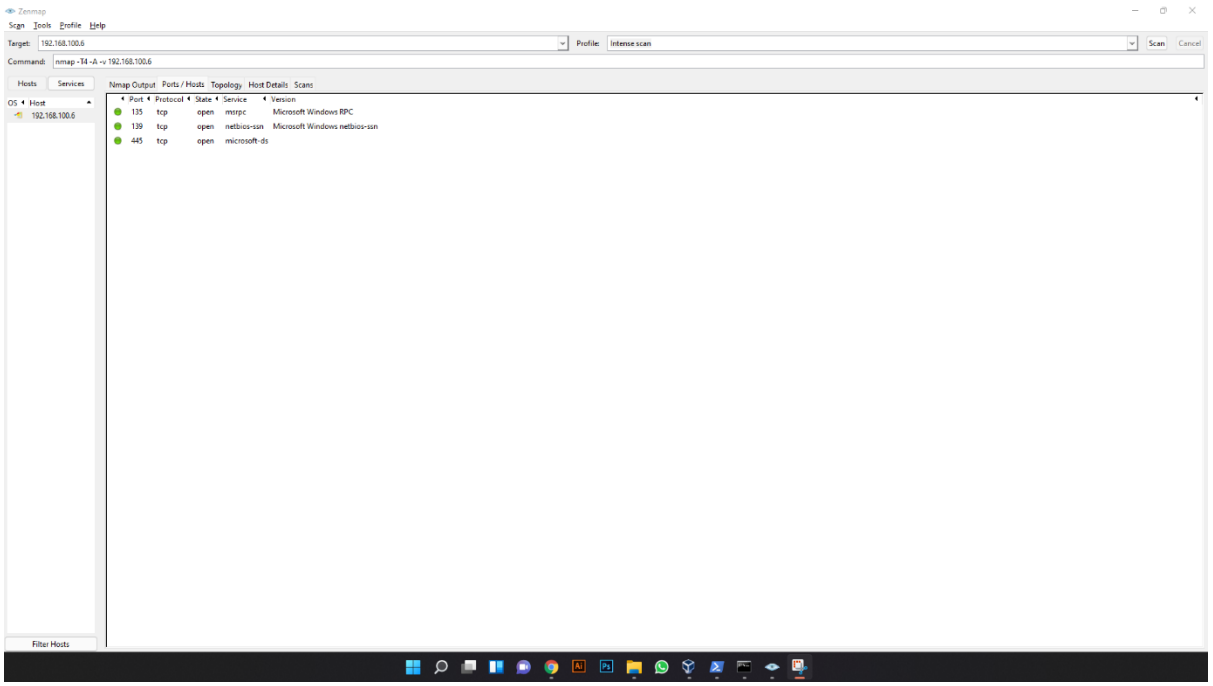
June 23rd, 2022

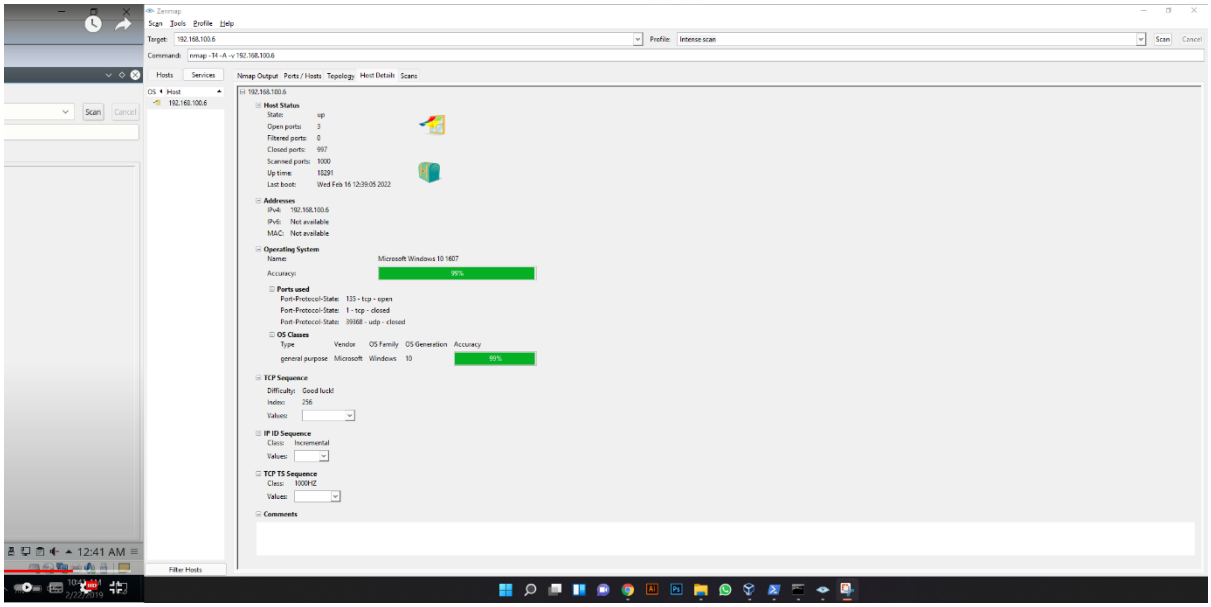
Task 1: Identifying open ports by running Zenmap.



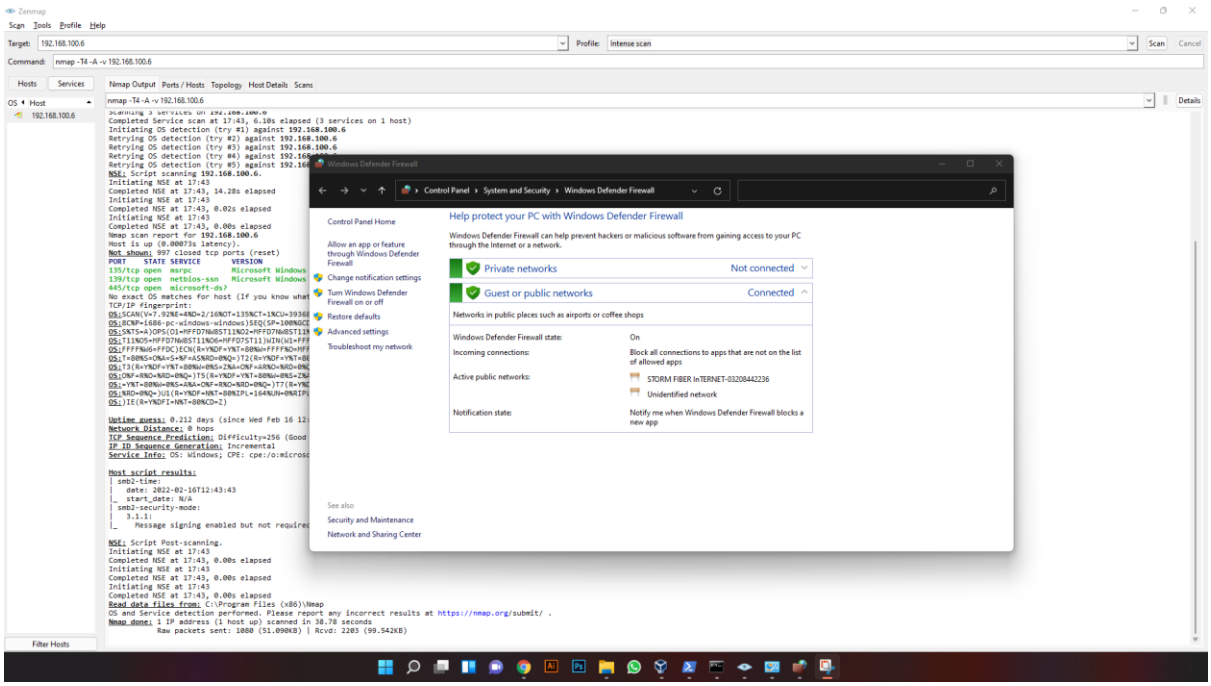


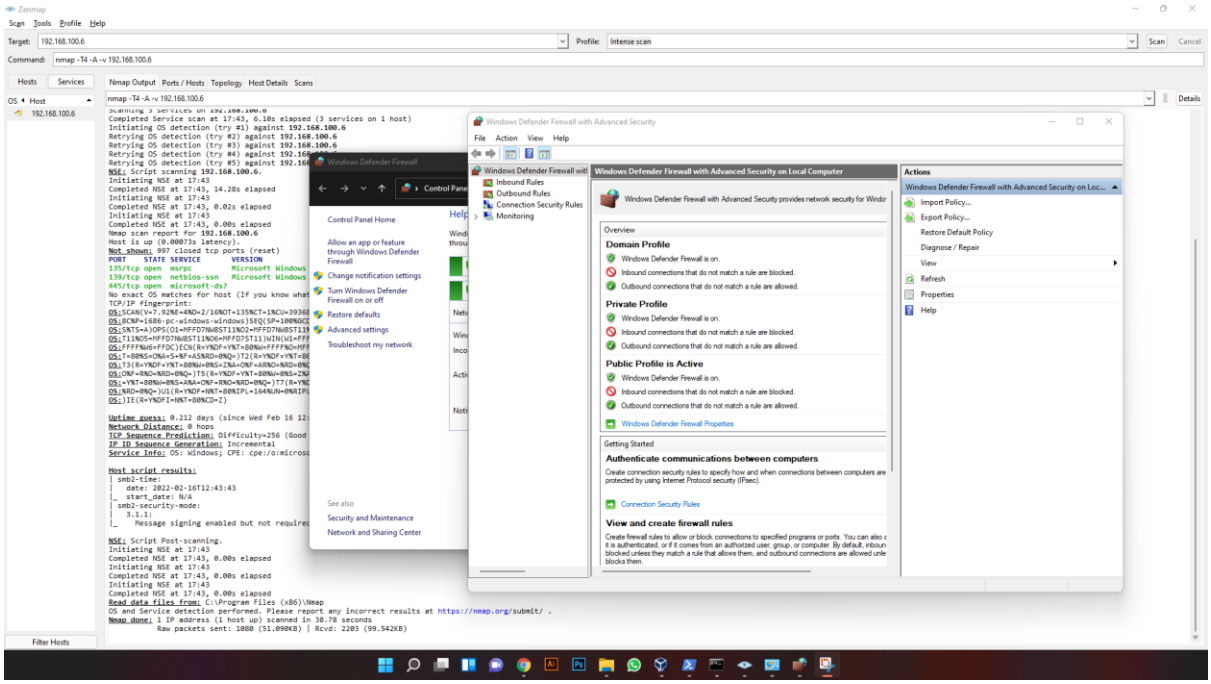

Zenmap
Scan Tools Profile Help
Target: 192.168.100.6
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 192.168.100.6
Hosts Services
OS Host
192.168.100.6
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 192.168.100.6
Details
Completed Service scan at 17:43, 6.10s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.100.6
Retrying OS detection (try #2) against 192.168.100.6
Retrying OS detection (try #3) against 192.168.100.6
Retrying OS detection (try #4) against 192.168.100.6
Retrying OS detection (try #5) against 192.168.100.6
NSE: Script scanning 192.168.100.6.
Initiating NSE at 17:43
Completed NSE at 17:43, 14.28s elapsed
Initiating NSE at 17:43
Completed NSE at 17:43, 0.02s elapsed
Initiating NSE at 17:43
Completed NSE at 17:43, 0.00s elapsed
Nmap scan report for 192.168.100.6
Host is up (0.00073s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=2/16%OT=135%CT=1%CU=39368%PV=Y%DS=0%DC=L%G=Y%TM=620CF1
OS:BCNP=i686-pc-windows-windows)SEQ(SP=100%GCD=1%ISR=103%TI=I%CI=I%II=I%SS=
OS:S%TS=A)OPS(O1=MFFD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8S
OS:T11%O5=MFFD7NW8ST11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=
OS:FFFF%W6=FFDC)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%
OS:T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
OS:T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=
OS:O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF
OS:=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G
OS:)IE(R=Y%DFI=N%T=80%CD=Z)
Uptime guess: 0.212 days (since Wed Feb 16 12:39:05 2022)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-time:
| date: 2022-02-16T12:43:43
|_ start_date: N/A
| smb2-security-mode:
| 3.1.1:
|_ Message signing enabled but not required
NSE: Script Post-scanning.
Initiating NSE at 17:43
Completed NSE at 17:43, 0.00s elapsed
Initiating NSE at 17:43
Completed NSE at 17:43, 0.00s elapsed
Initiating NSE at 17:43
Completed NSE at 17:43, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.78 seconds
Raw packets sent: 1080 (51.090KB) | Rcvd: 2203 (99.542KB)
Filter Hosts

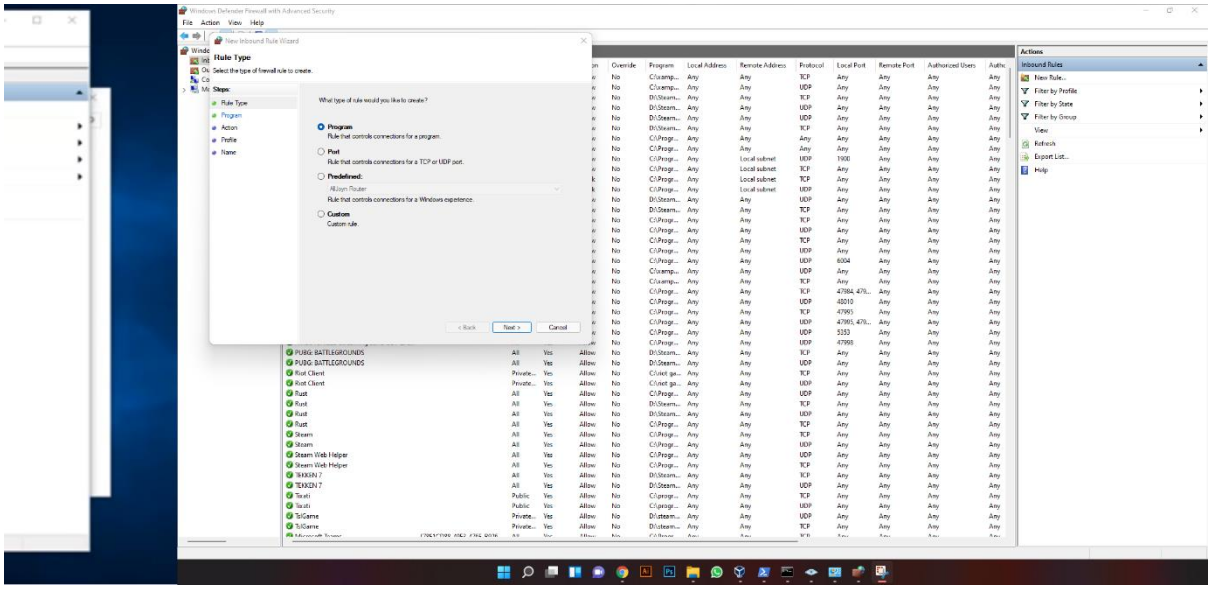

Zenmap
Scan Tools Profile Help
Target: 192.168.100.6
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 192.168.100.6
Hosts Services
OS Host
192.168.100.6
Nmap Output Ports / Hosts Topology Host Details Scans
Port Protocol State Service Version
135 tcp open msrpc Microsoft Windows RPC
139 tcp open netbios-ssn Microsoft Windows netbios-ssn
445 tcp open microsoft-ds
Filter Hosts

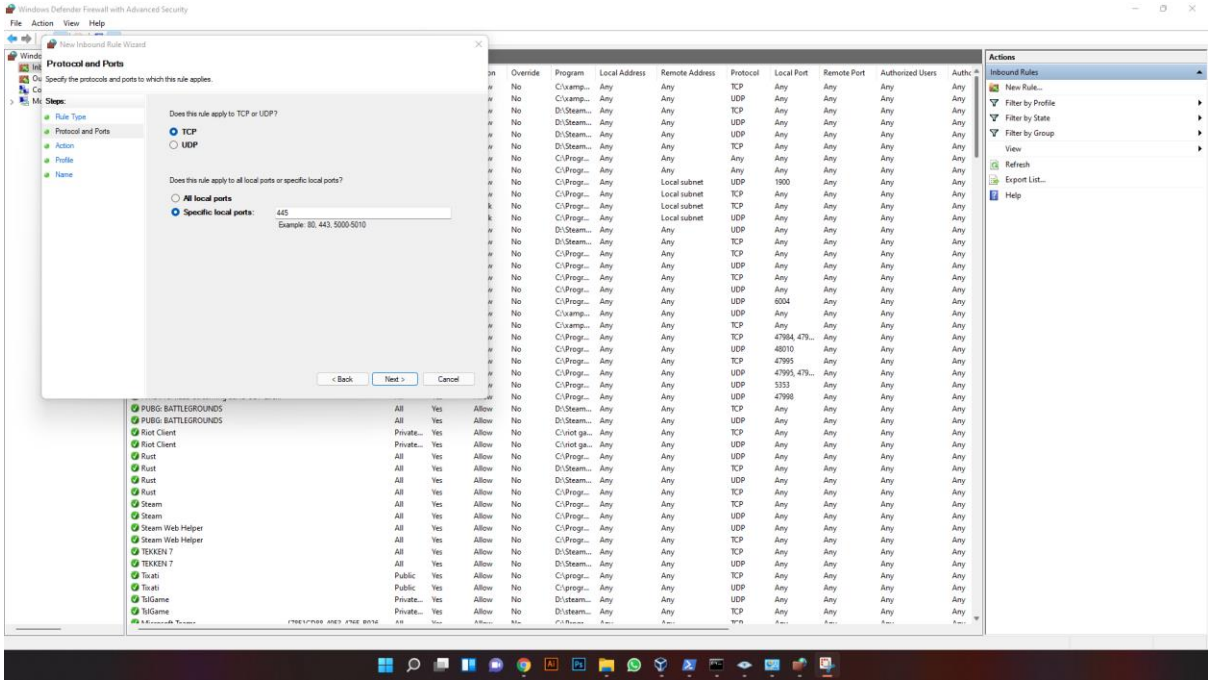


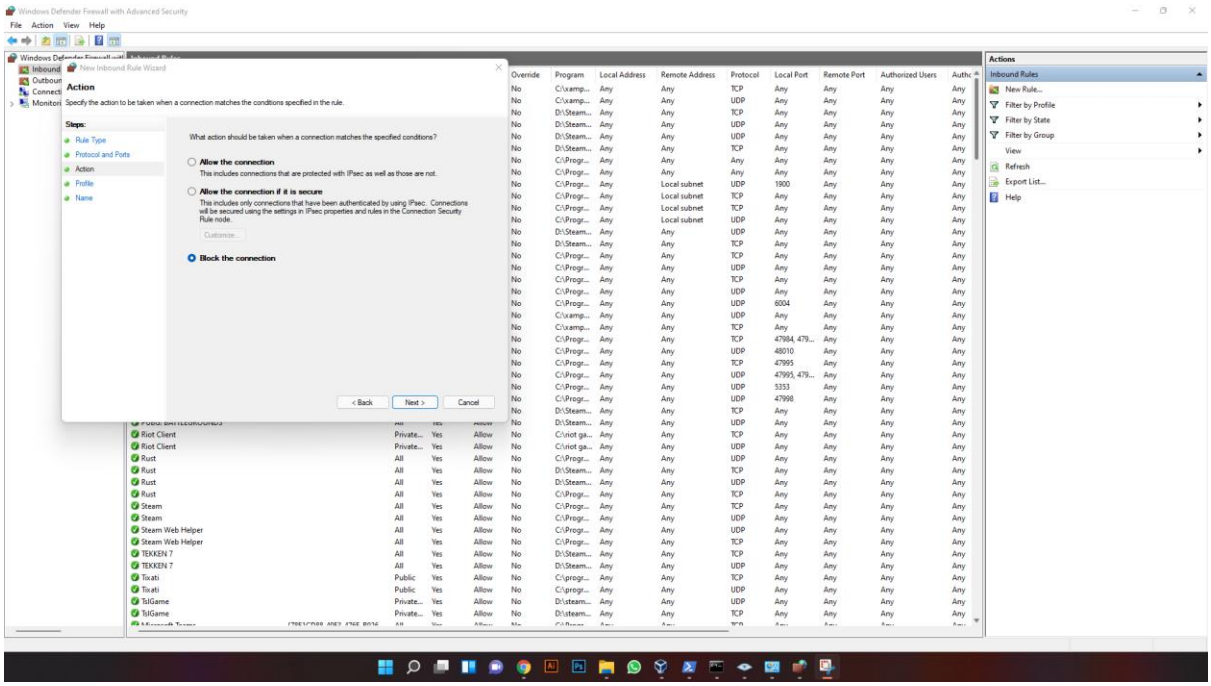
Task 2: Temporarily blocking a port with Windows Defender Firewall.

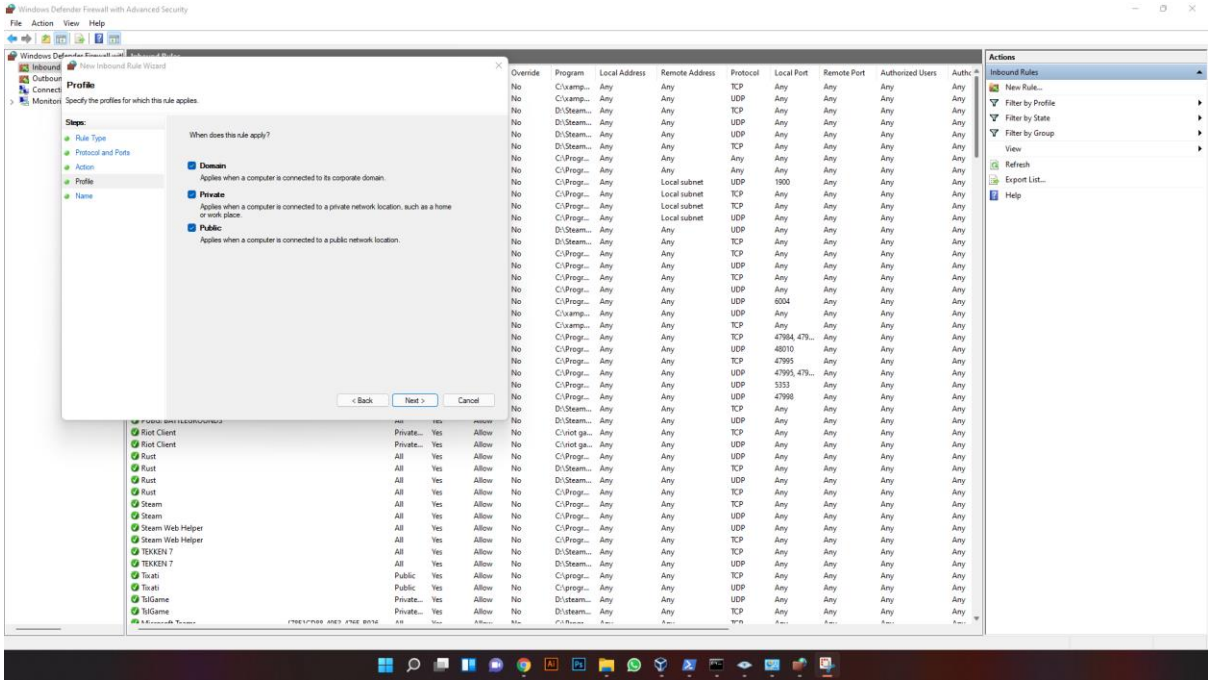


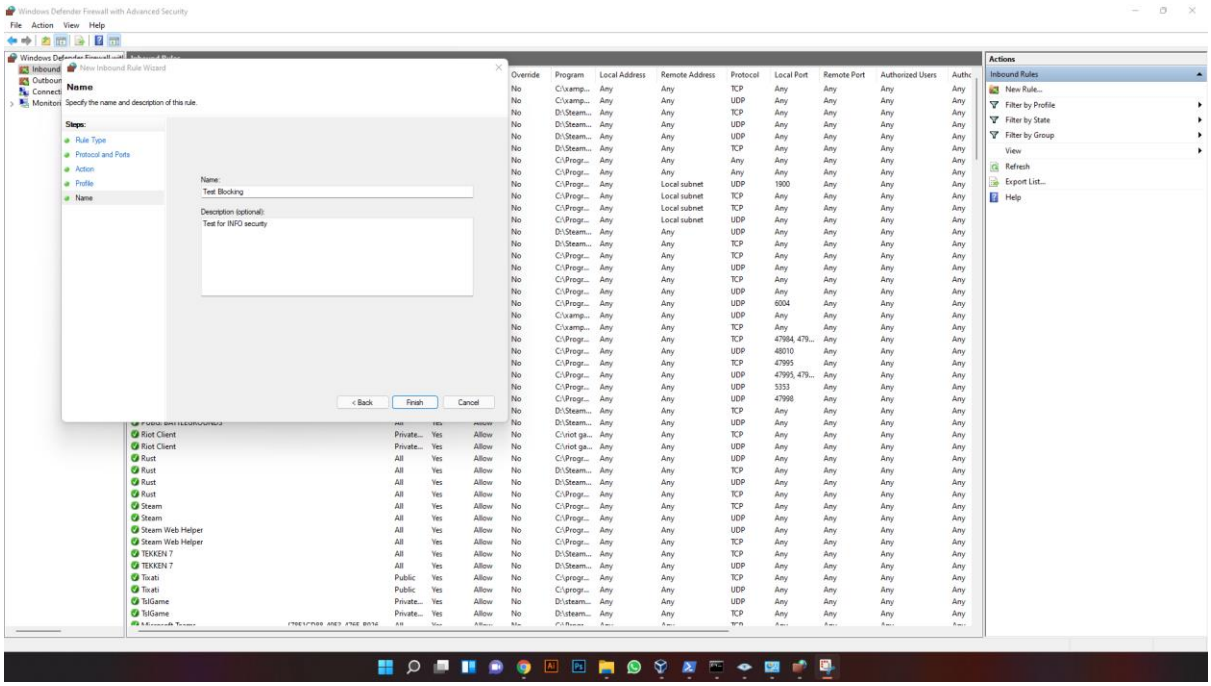

Zenmap
Scan Tools Profile Help
Target: 192.168.100.6
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.100.6
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
Windows Defender Firewall with Advanced Security
Windows Defender Firewall with Advanced Security on Local Computer
Domain Profile
Private Profile
Public Profile is Active
Authenticate communications between computers
View and create firewall rules
Actions


New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Program
Port
Predefined:
Custom
Next >
Cancel
Inbound Rules


Windows Defender Firewall with Advanced Security
File Action View Help
New Inbound 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 local ports or specific local ports?
All local ports
Specific local ports:
445
Example: 80, 443, 5000-5010
< Back
Next >
Cancel
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help


Windows Defender Firewall with Advanced Security
File Action View Help
New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
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
< Back
Next >
Cancel
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help


Windows Defender Firewall with Advanced Security
File Action View Help
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
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help


Windows Defender Firewall with Advanced Security
File Action View Help
New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Name:
Test Blocking
Description (optional):
Test for INFO security
< Back
Finish
Cancel
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help

******