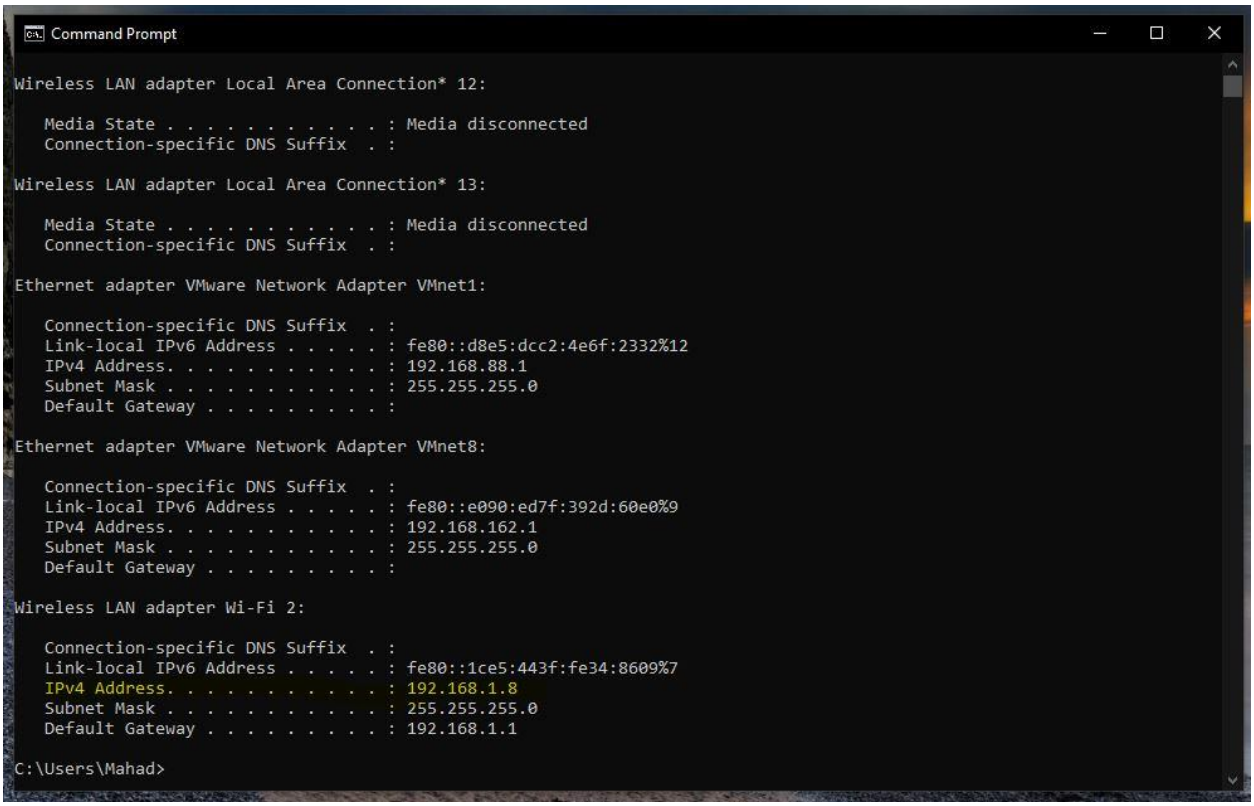
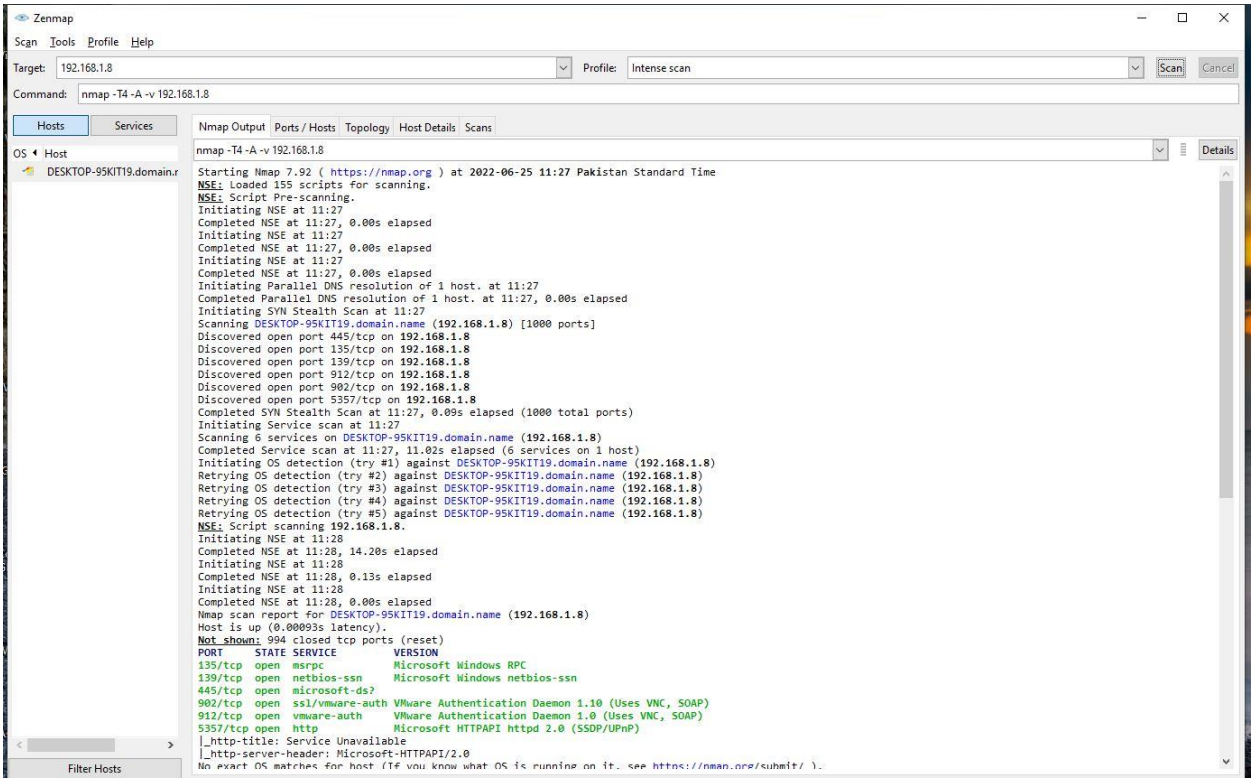
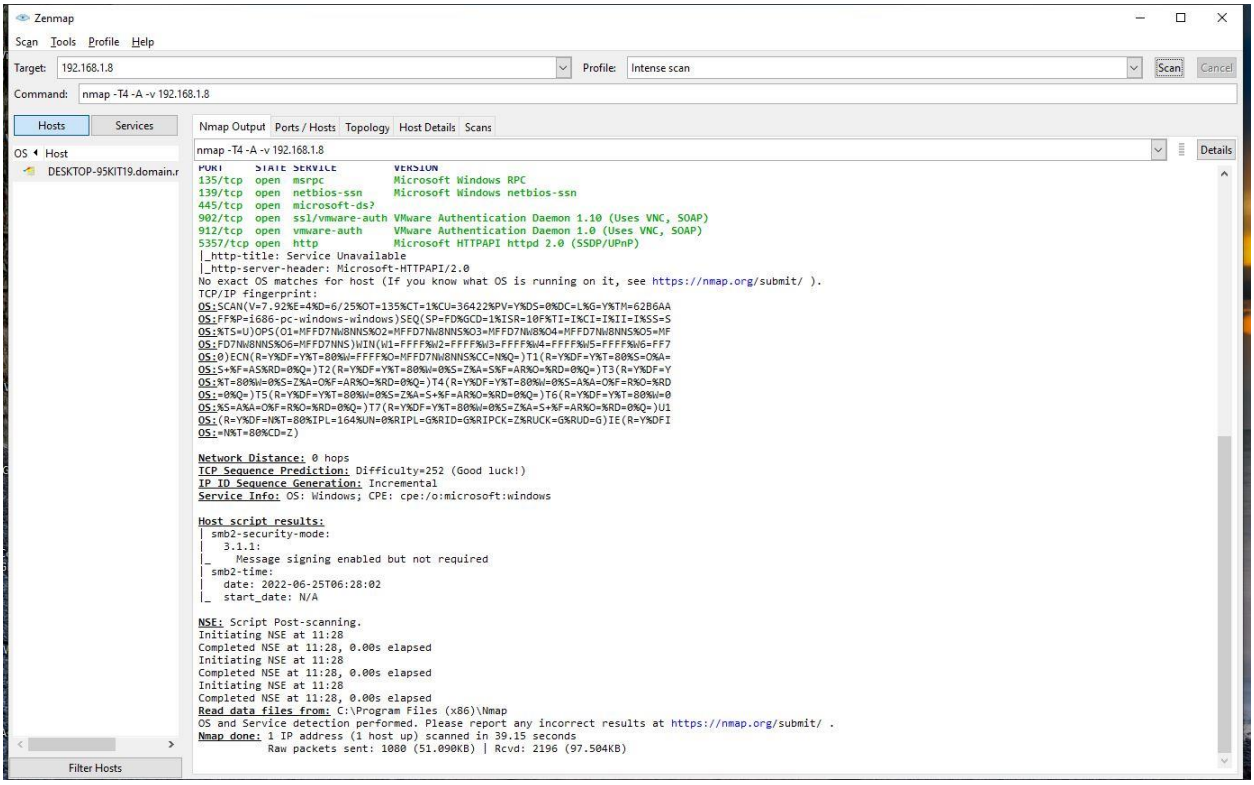
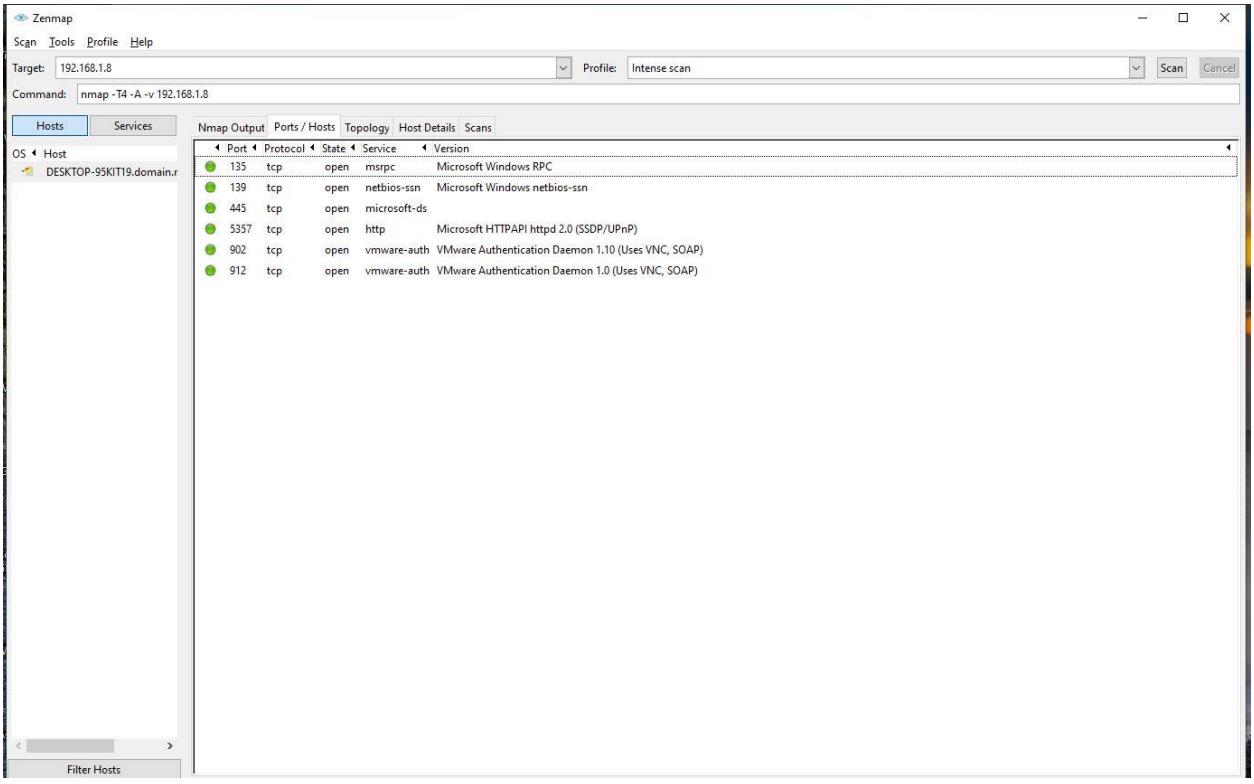
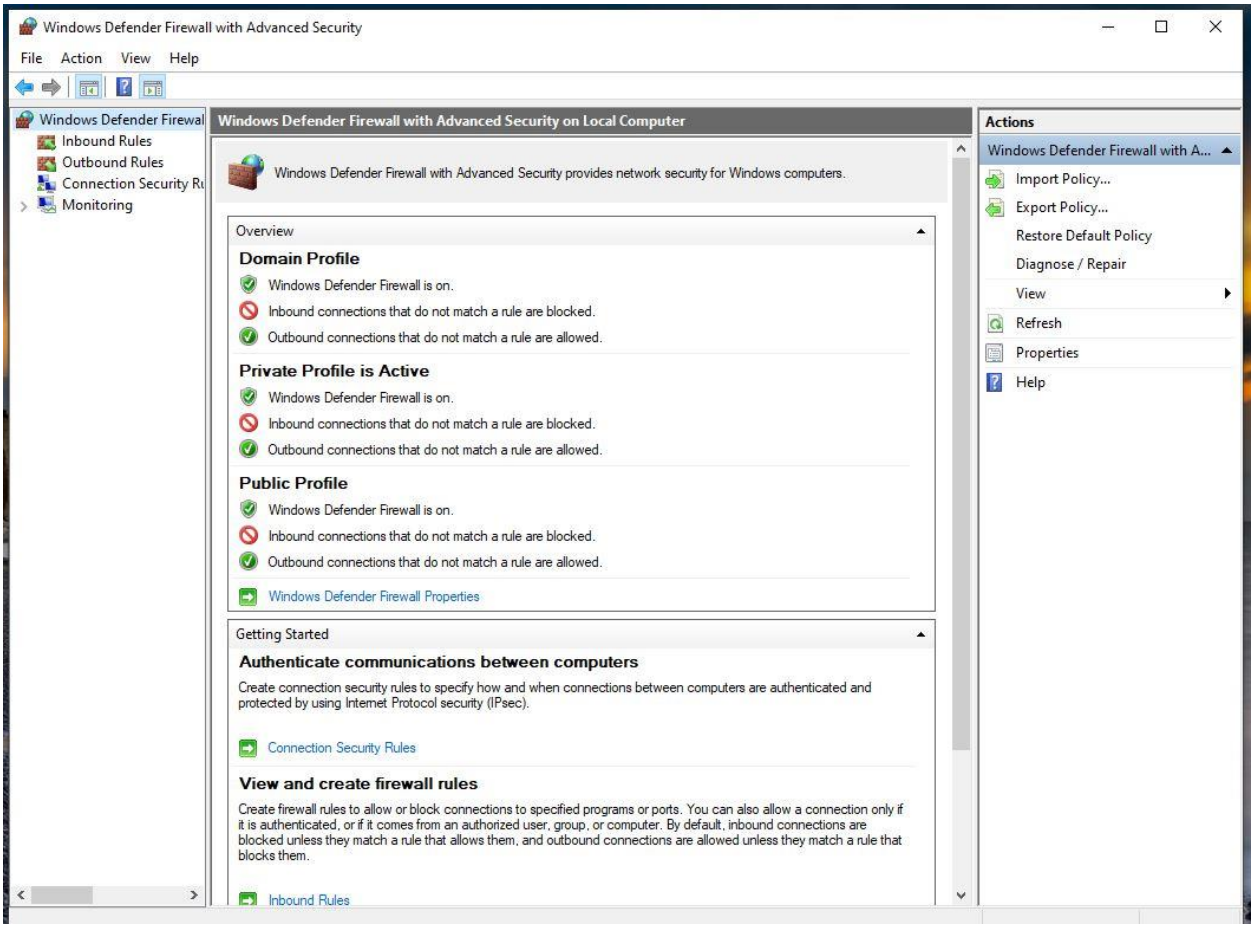
Mahad Rashid **Assignment 03** **22-11108**

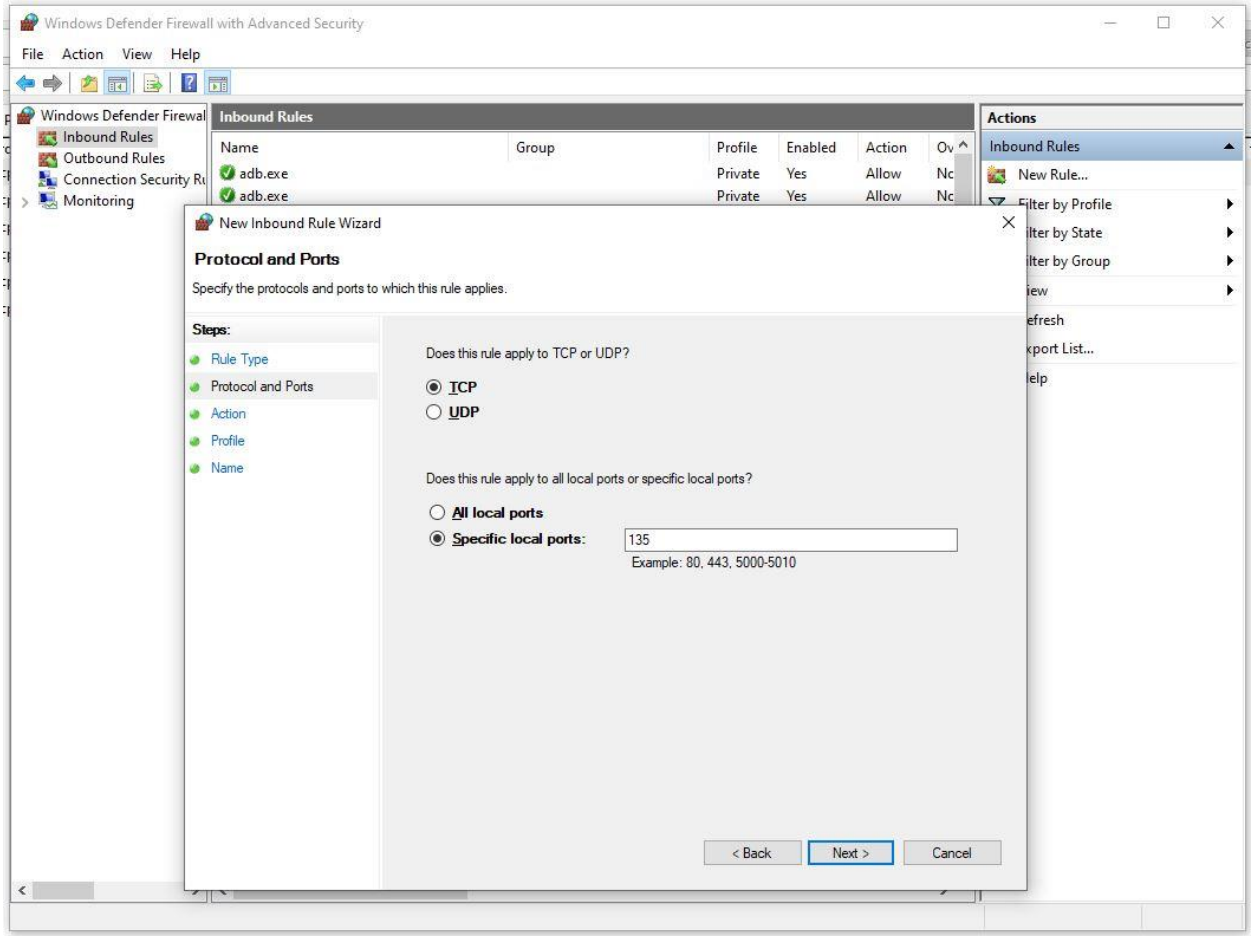


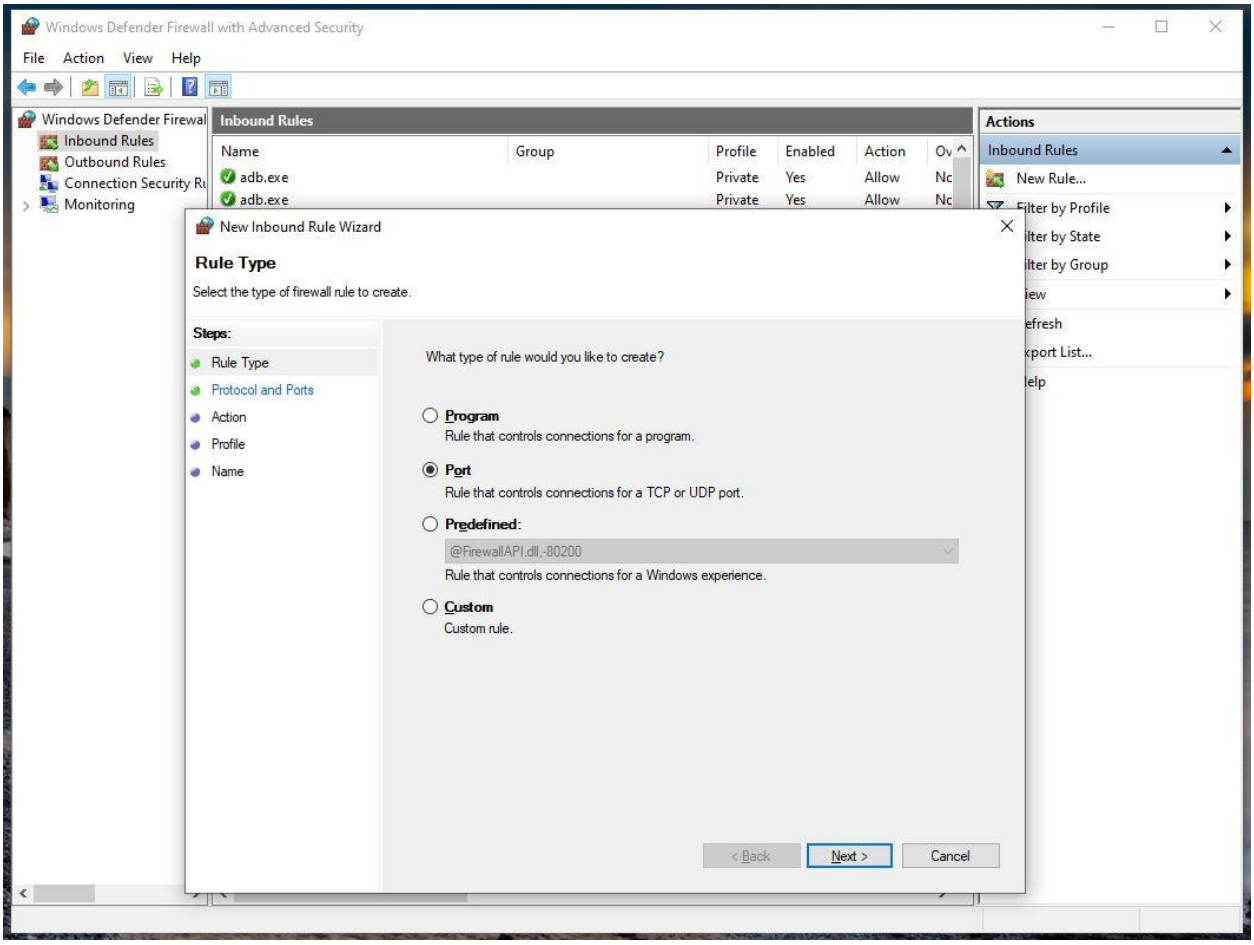


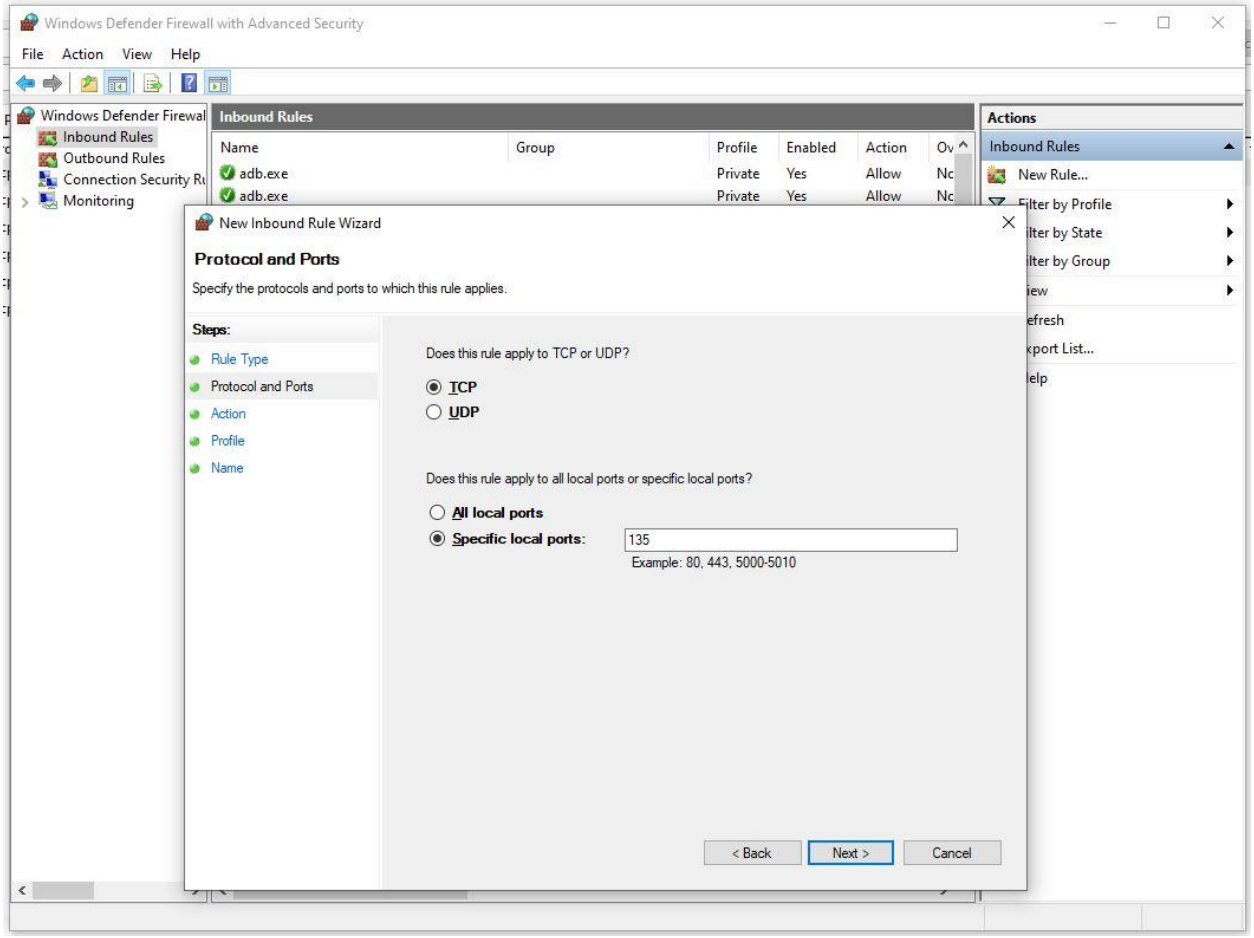

Zenmap
Scan Tools Profile Help
Target: 192.168.1.8
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 192.168.1.8
Hosts Services
OS Host
DESKTOP-95KIT19.domain.r
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 192.168.1.8
Details
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds?
902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp open vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
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=6/25%OT=135%CT=1%CU=36422%PV=Y%DS=0%DC=L%G=Y%TM=62B6AA
OS:FF%P=i686-pc-windows-windows)SEQ(SP=FD%GCD=1%ISR=10F%TI=I%CI=I%II=I%SS=S
OS:%TS=U)OPS(O1=MFFD7NW8NNS%O2=MFFD7NW8NNS%O3=MFFD7NW8%O4=MFFD7NW8NNS%O5=MF
OS:FD7NW8NNS%O6=MFFD7NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF7
OS:0)ECN(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=
OS: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=)T3(R=Y%DF=Y
OS:%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=O%F=R%O=%RD
OS:=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=Y%T=80%W=0
OS:%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=%RD=0%Q=)U1
OS:(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI
OS:=N%T=80%CD=Z)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=252 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-security-mode:
| 3.1.1:
|_ Message signing enabled but not required
| smb2-time:
| date: 2022-06-25T06:28:02
|_ start_date: N/A
NSE: Script Post-scanning.
Initiating NSE at 11:28
Completed NSE at 11:28, 0.00s elapsed
Initiating NSE at 11:28
Completed NSE at 11:28, 0.00s elapsed
Initiating NSE at 11:28
Completed NSE at 11:28, 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 39.15 seconds
Raw packets sent: 1080 (51.090KB) | Rcvd: 2196 (97.504KB)
Filter Hosts

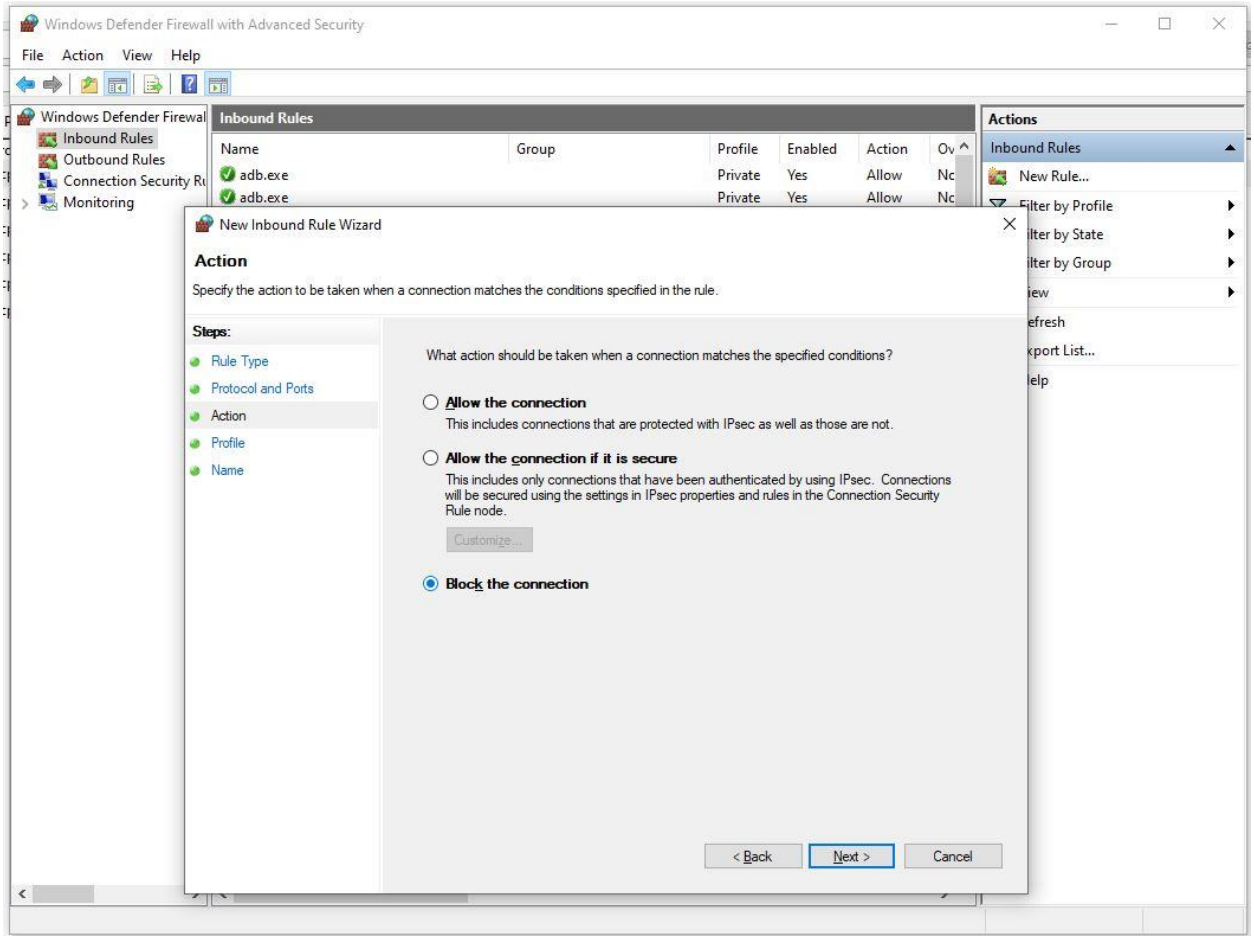

Zenmap
Scan Tools Profile Help
Target: 192.168.1.8
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 192.168.1.8
Hosts Services
OS Host
DESKTOP-95KIT19.domain.r
Nmap Output Ports / Hosts Topology Host Details Scans
Port Protocol State Service Version
135 tcp open msrpc Microsoft Windows RPC
139 tcp open netbios-ssn Microsoft Windows netbios-ssn
445 tcp open microsoft-ds
5357 tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
902 tcp open vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912 tcp open vmware-auth VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
Filter Hosts

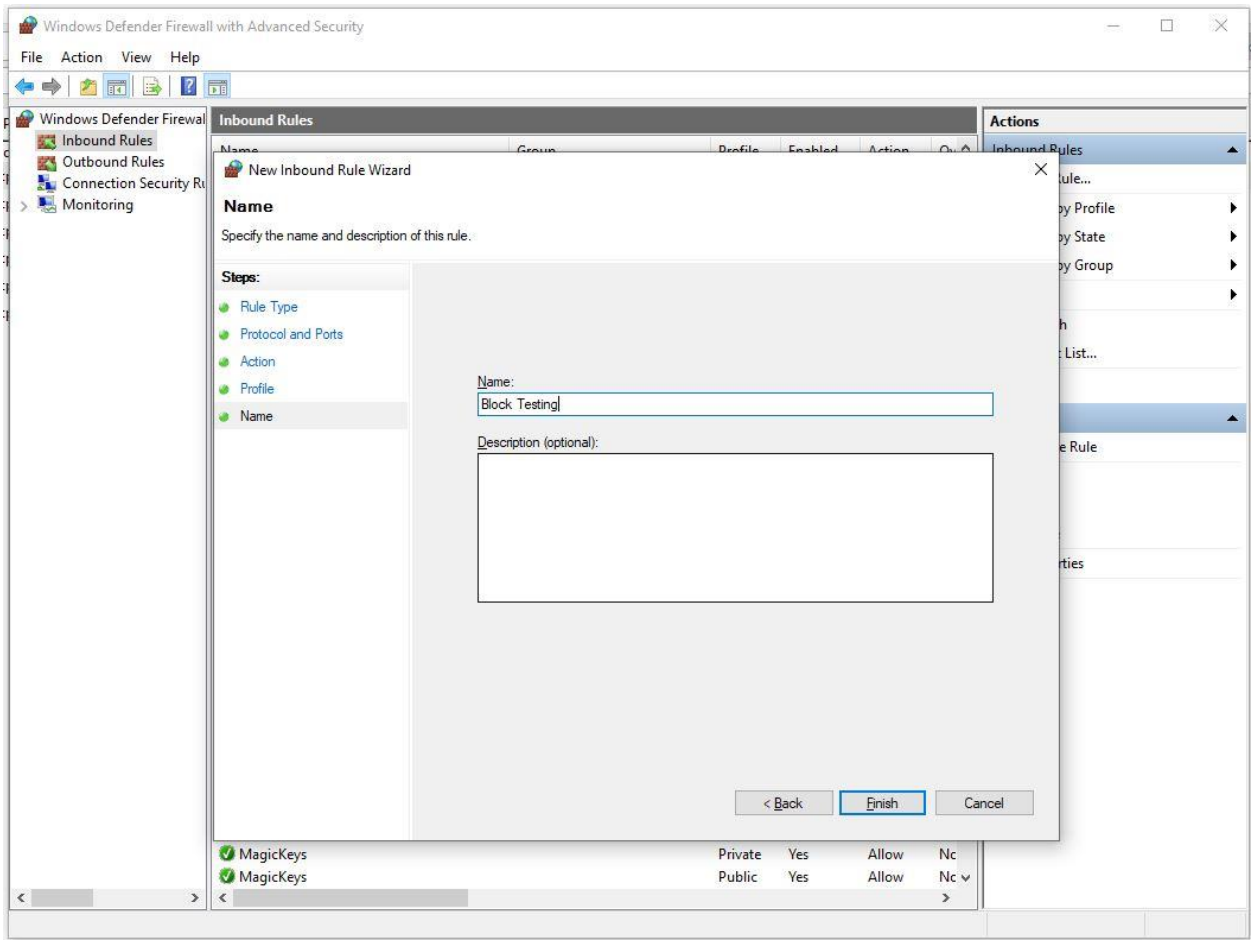

Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall
Inbound Rules
Outbound Rules
Connection Security Ru
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Windows Defender Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Defender 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 is Active
Windows Defender 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
Windows Defender Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Defender Firewall Properties
Getting Started
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).
Connection Security Rules
View and create firewall rules
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.
Inbound Rules
Actions
Windows Defender Firewall with A...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled Action
adb.exe Private Yes Allow
adb.exe Private Yes Allow
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
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:
135
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled Action
adb.exe Private Yes Allow
adb.exe Private Yes Allow
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Protocol and Ports
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:
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled Action
adb.exe Private Yes Allow
adb.exe Private Yes Allow
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
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:
135
Example: 80, 443, 5000-5010
< Back
Next >
Cancel


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name Group Profile Enabled Action
adb.exe Private Yes Allow
adb.exe Private Yes Allow
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
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


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewal
Inbound Rules
Outbound Rules
Connection Security Ru
Monitoring
Inbound Rules
Actions
New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Protocol and Ports
Action
Profile
Name
Name:
Block Testing
Description (optional):
< Back
Finish
Cancel
MagicKeys Private Yes Allow
MagicKeys Public Yes Allow