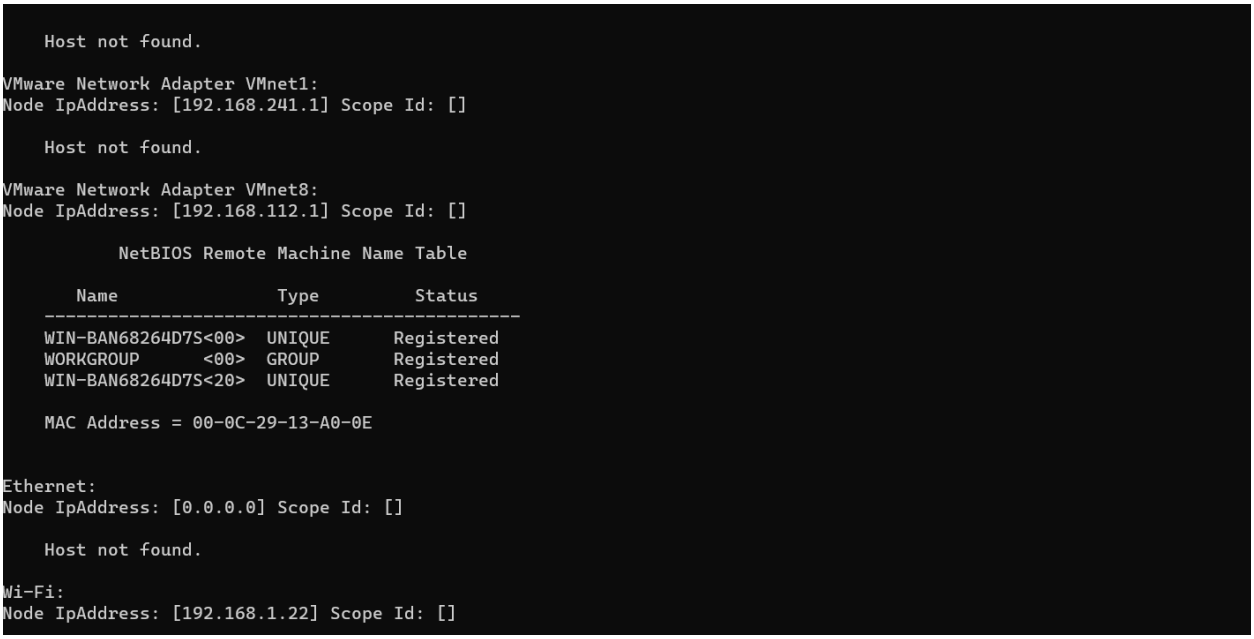
Start the Windows Server 2019 and Windows 10 virtual machines.

Open a Command Prompt window.

Type nbtstat -a <IP address of the remote machine> and press Enter.

Note: In this command, a displays the NetBIOS name table of a remote computer.

The result appears, displaying the NetBIOS name table of a remote computer (in this case, the WINDOWS10 virtual machine), as shown in the screenshot



In the same Command Prompt window, type nbtstat -e and press Enter.

Note: In this command, e lists the contents of the NetBIOS name cache of the remote computer.

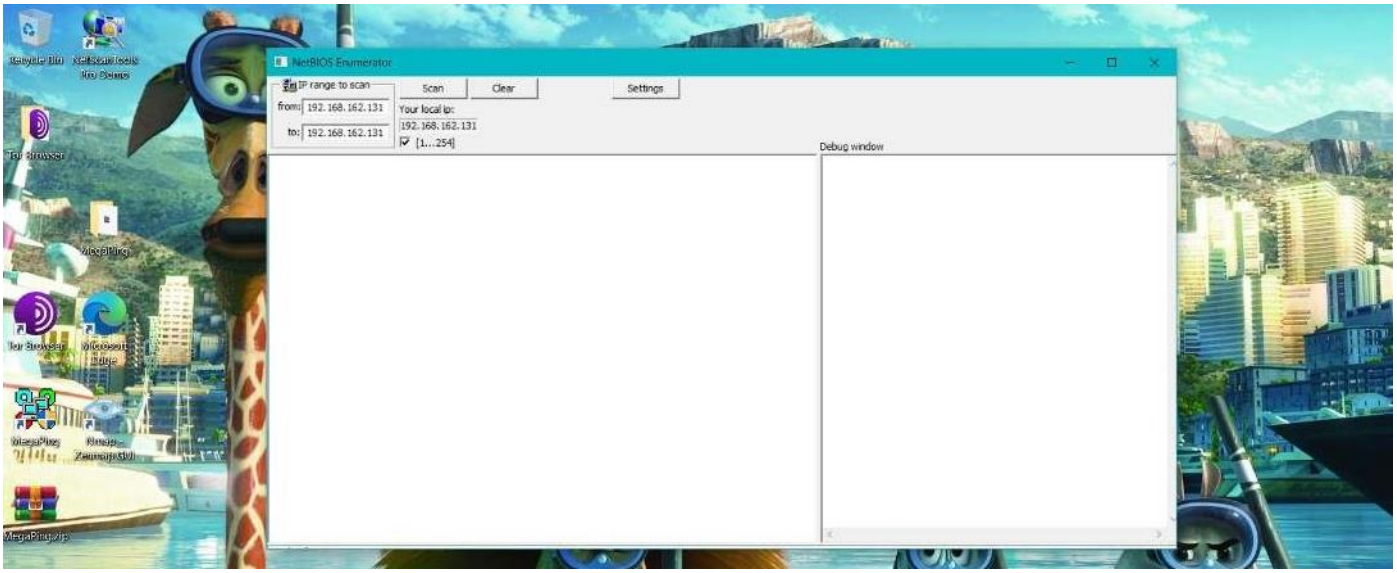
The result appears, displaying the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.

Note: It is possible to extract this information without creating a null session (an unauthenticated session).

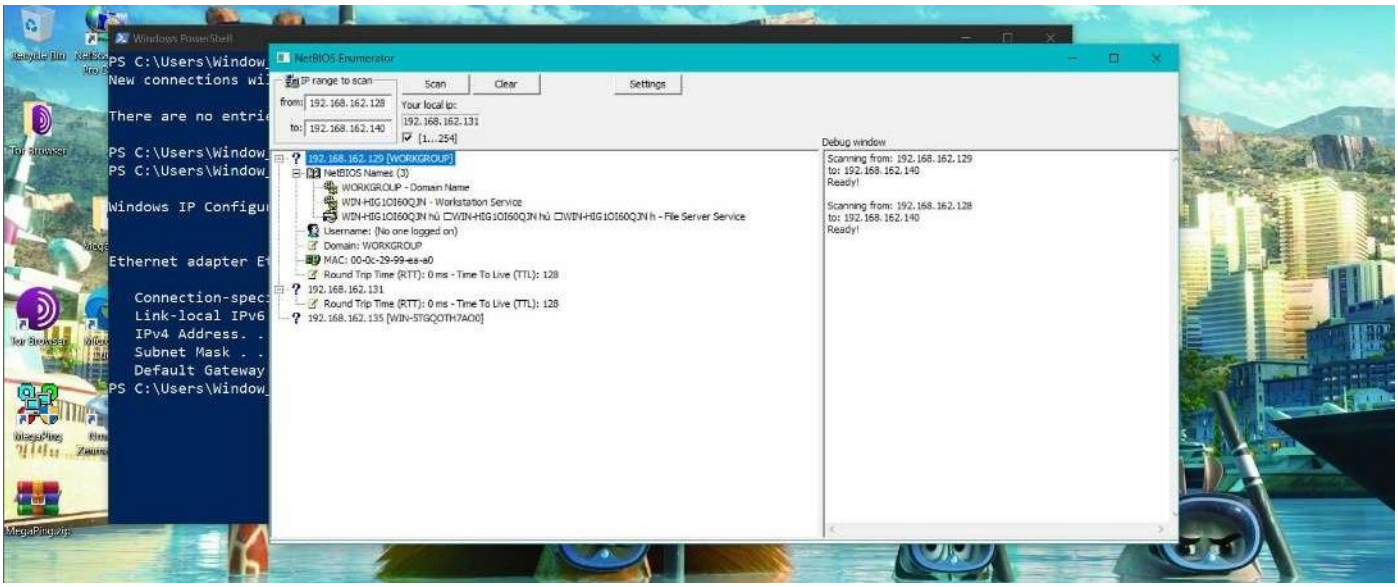
```
PS C:\Users\green> nbtstat -c

vEthernet (Default Switch):
Node IpAddress: [192.168.80.1] Scope Id: []

    No names in cache

Ethernet 2:
Node IpAddress: [192.168.56.1] Scope Id: []

    No names in cache

VMware Network Adapter VMnet1:
Node IpAddress: [192.168.241.1] Scope Id: []

    No names in cache

VMware Network Adapter VMnet8:
Node IpAddress: [192.168.112.1] Scope Id: []

                NetBIOS Remote Cache Name Table

       Name              Type       Host Address    Life [sec]
    --------------------------------------------------------
    WIN-BAN68264D7S<20>  UNIQUE          192.168.112.202     530

Ethernet:
Node IpAddress: [0.0.0.0] Scope Id: []

    No names in cache
```

Perform NetBIOS Enumeration using NetBIOS Enemerator Open

NetBIOS Enumerator:

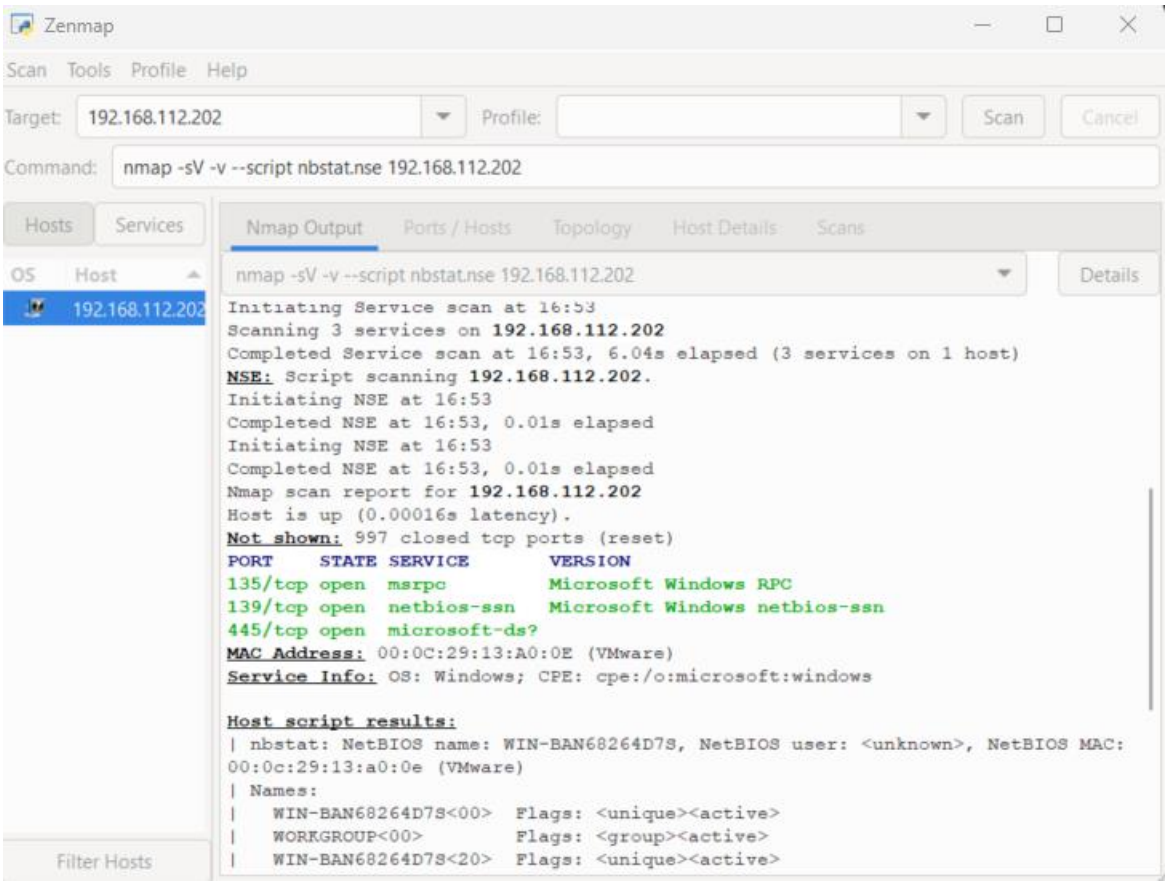


Set range IP : 192.168.162.128 -> 192.168.162.140 and scan

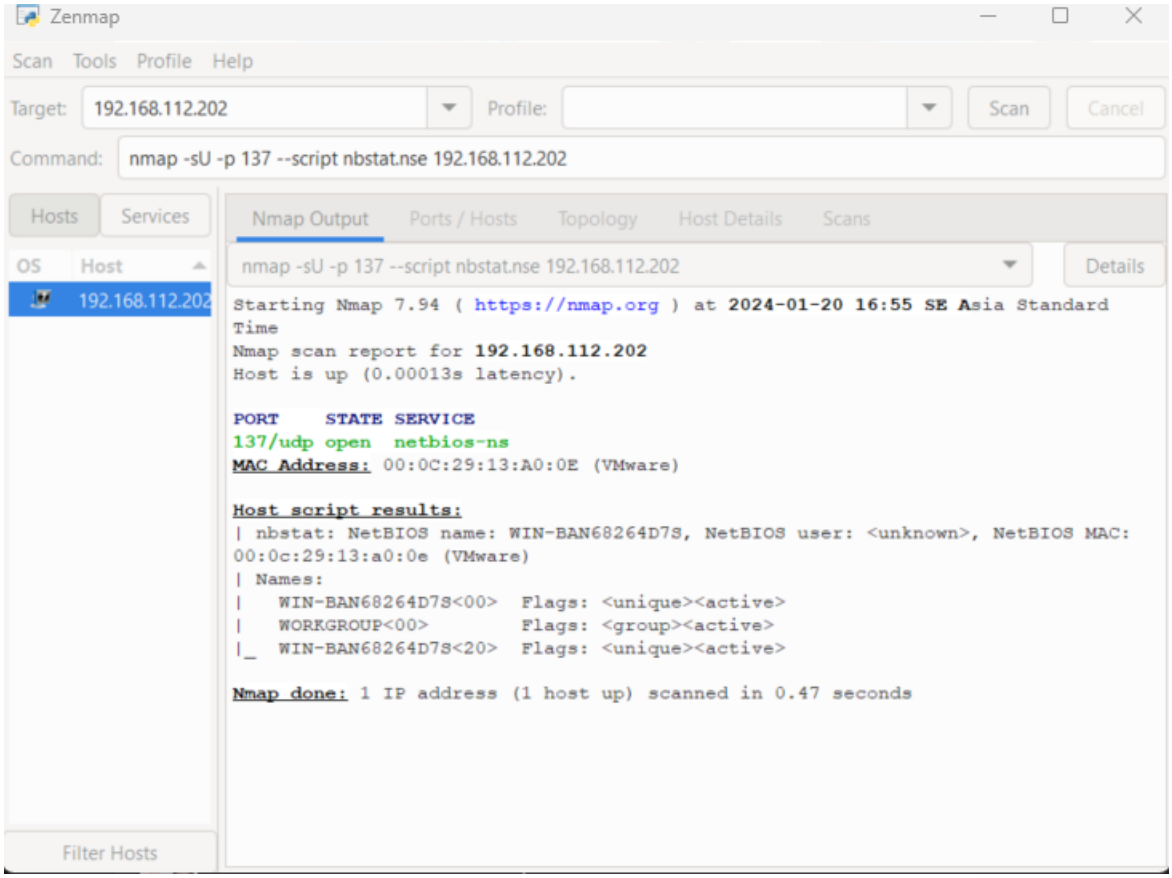


Perform NetBIOS Enumeration USING an NSE Script Open Zenmap

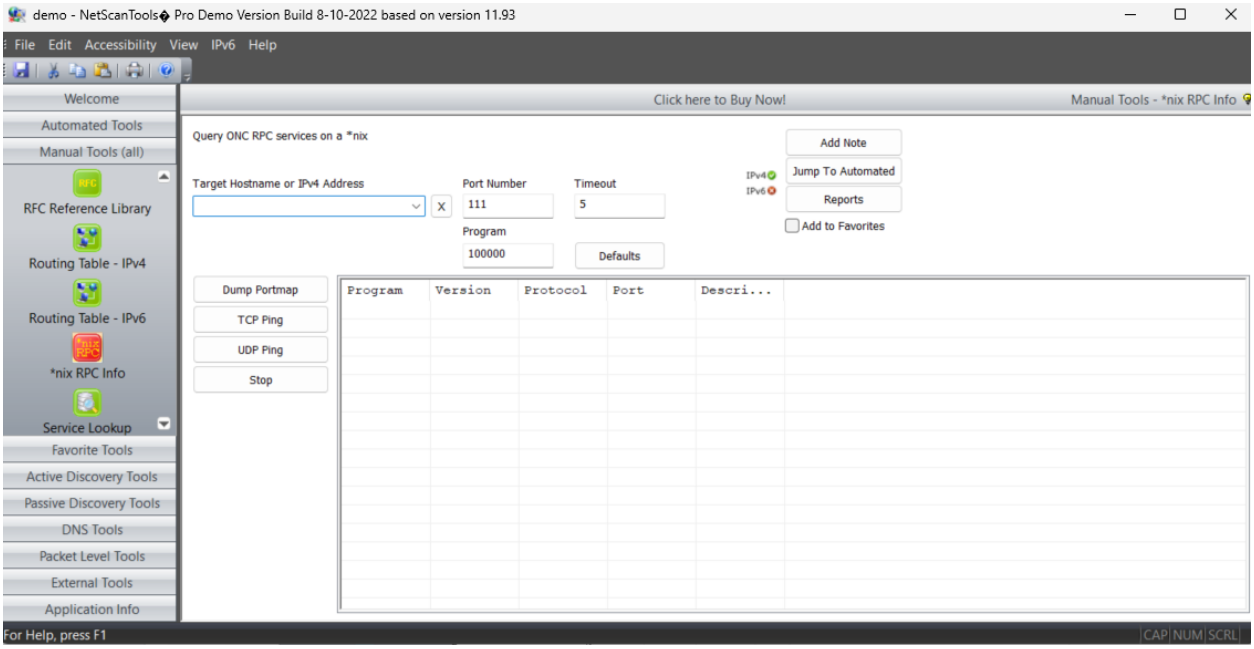
nmap -sV -v --script nbstat.nse 192.168.112.202



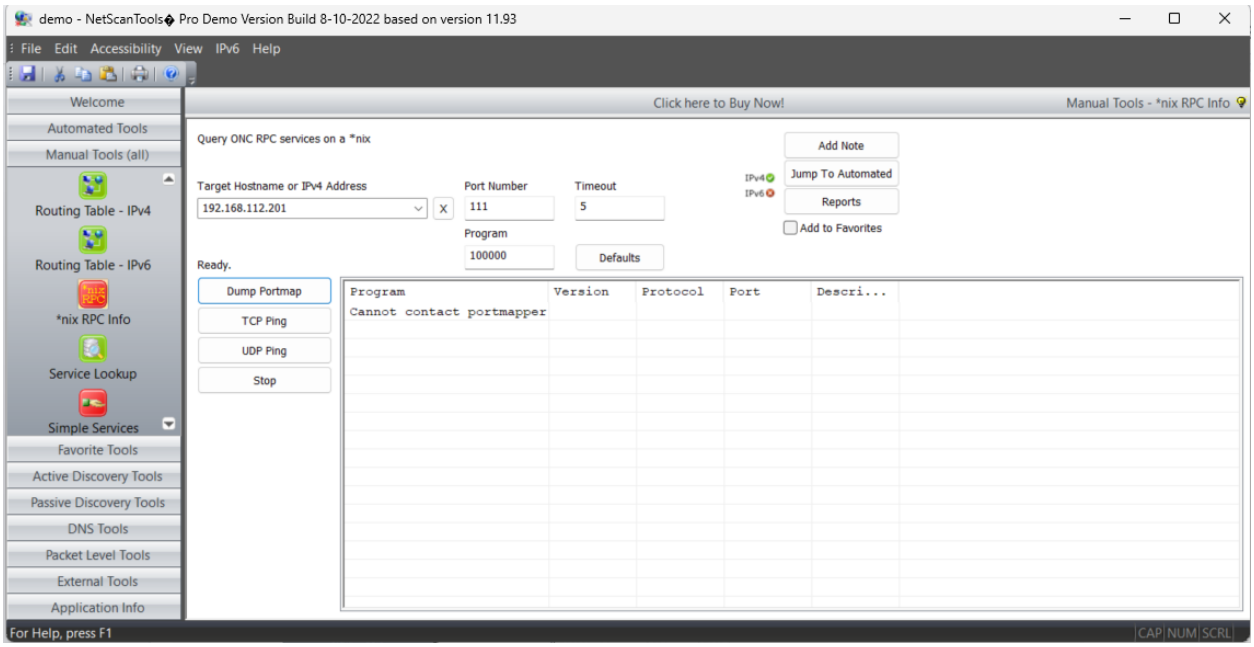
nmap -sU -p 137 --script nbstat.nse 192.168.112.202



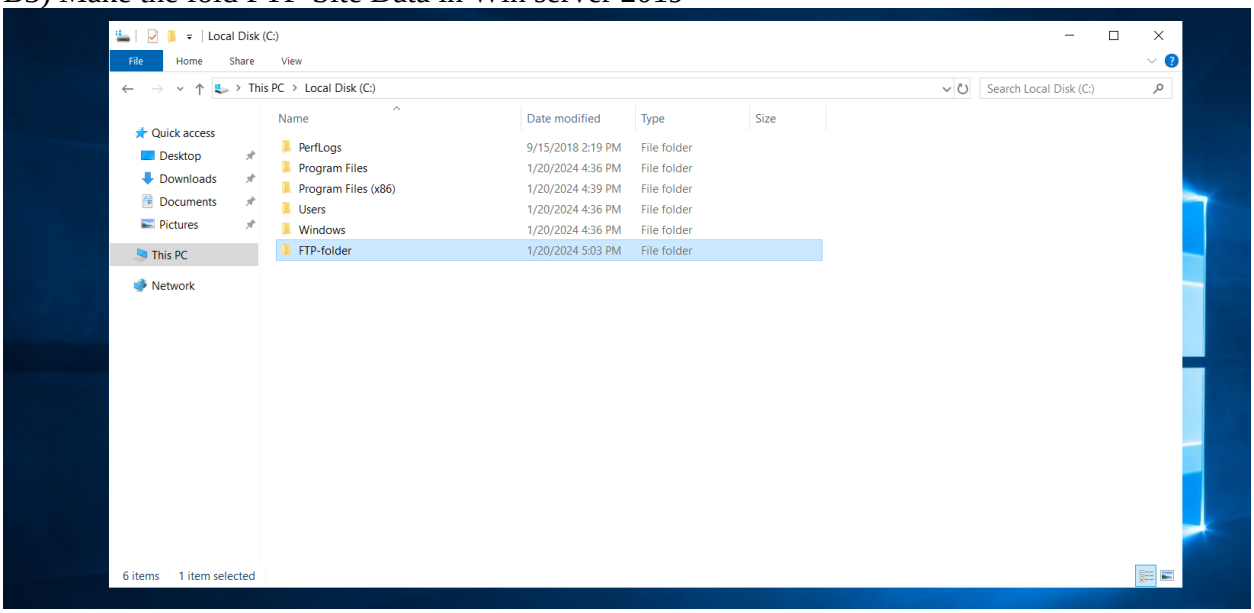
Open NetScanTools pro and select nic RPC info



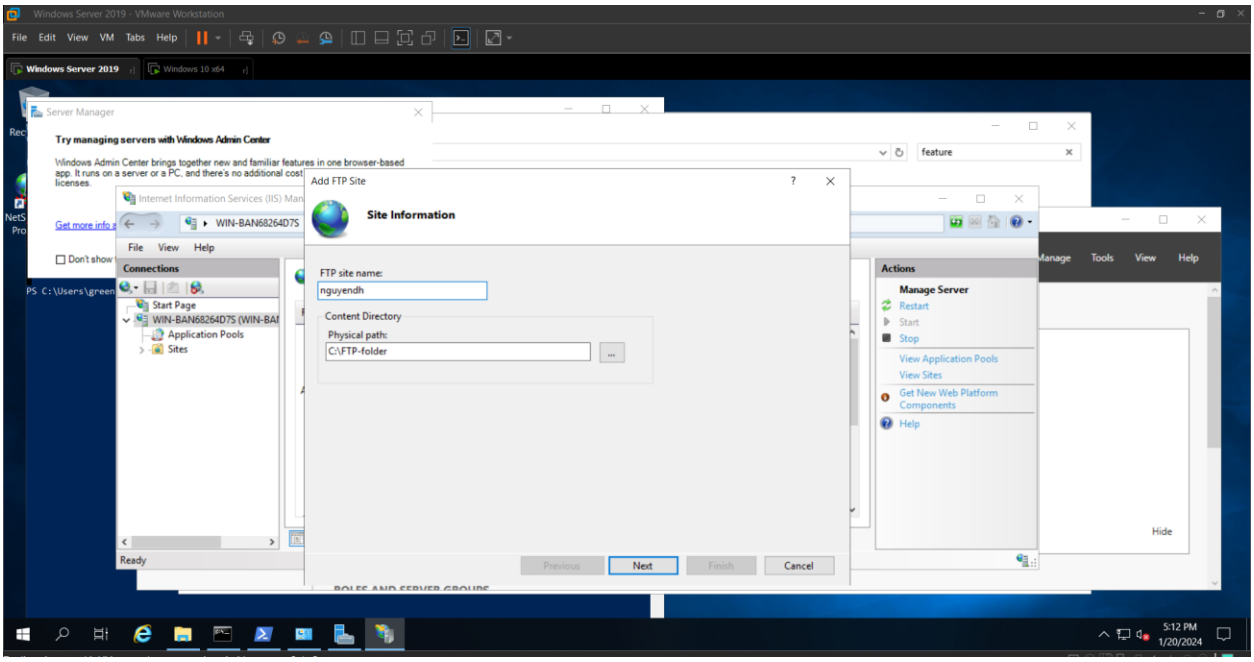
B2)Target: 192.168.112.202 dump portmap



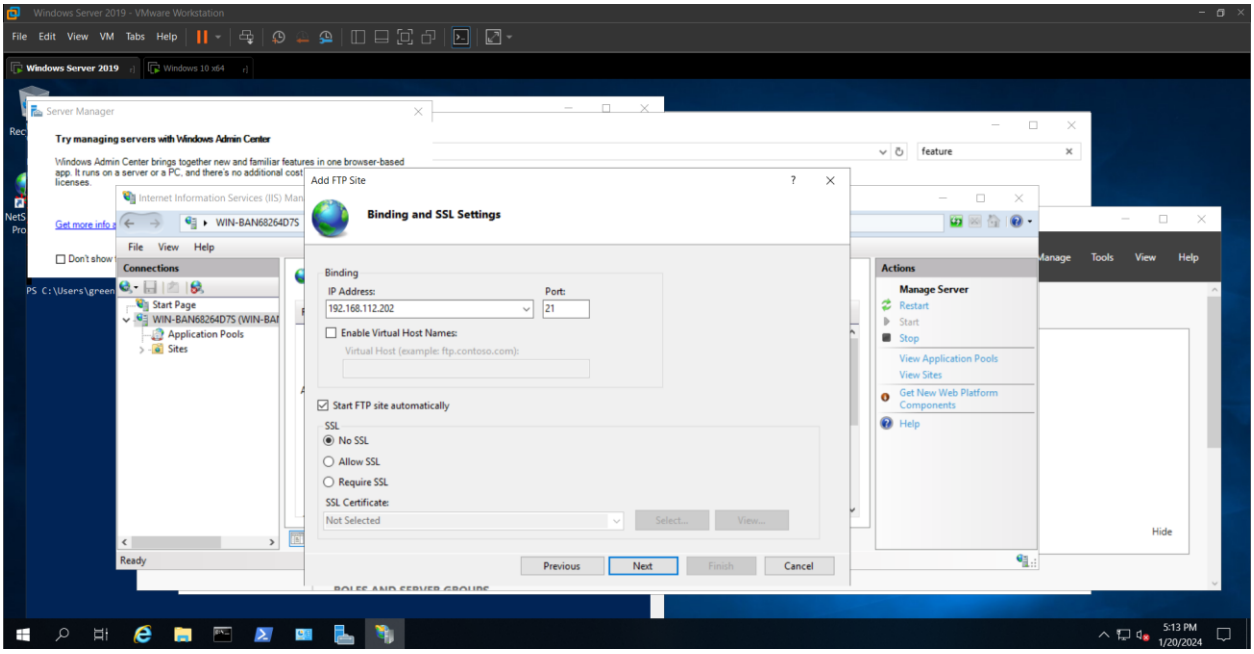
B3) Make the fold FTP-Site Data in Win server 2019

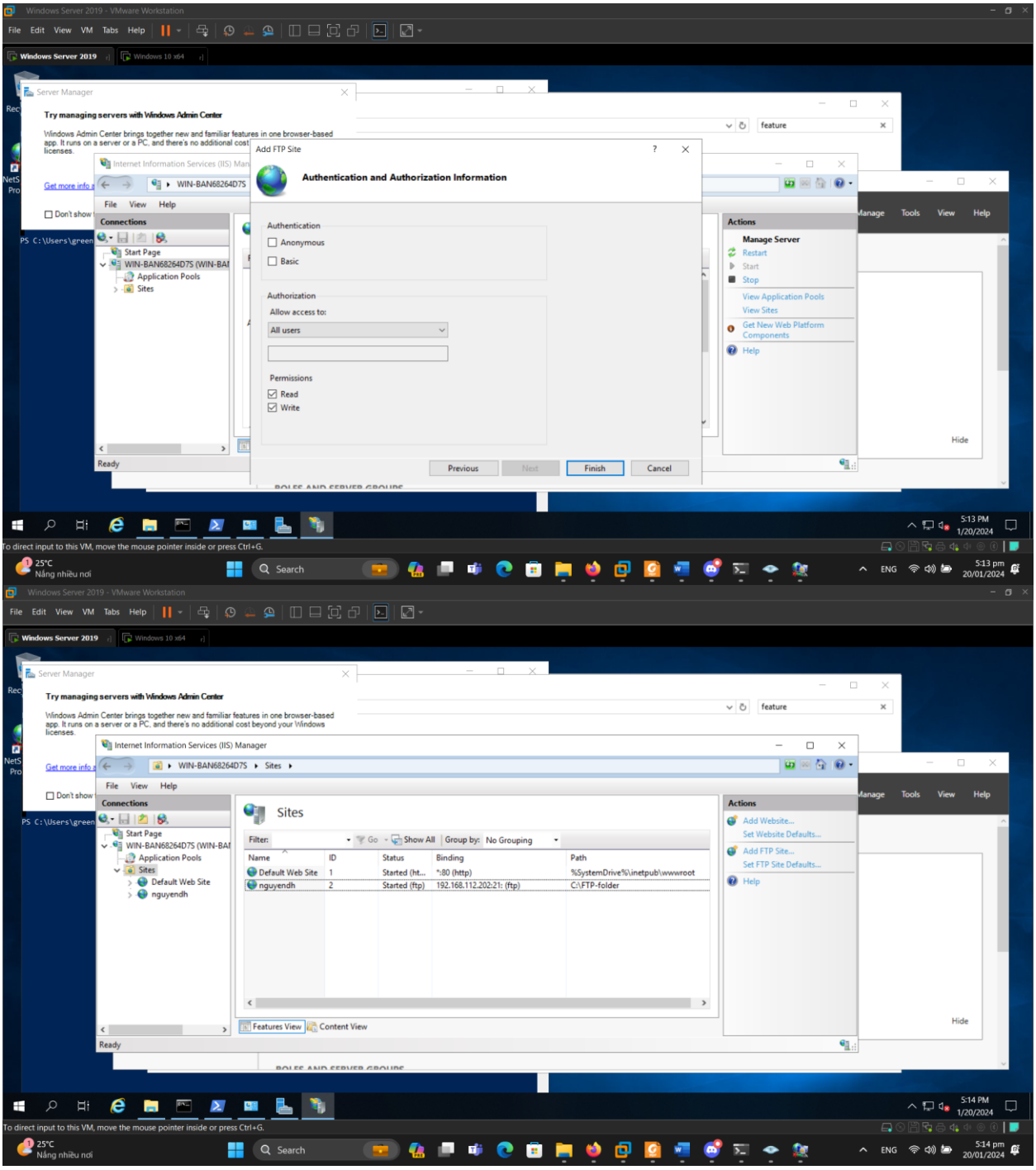


B4) Add FTP site.. in win server 2019

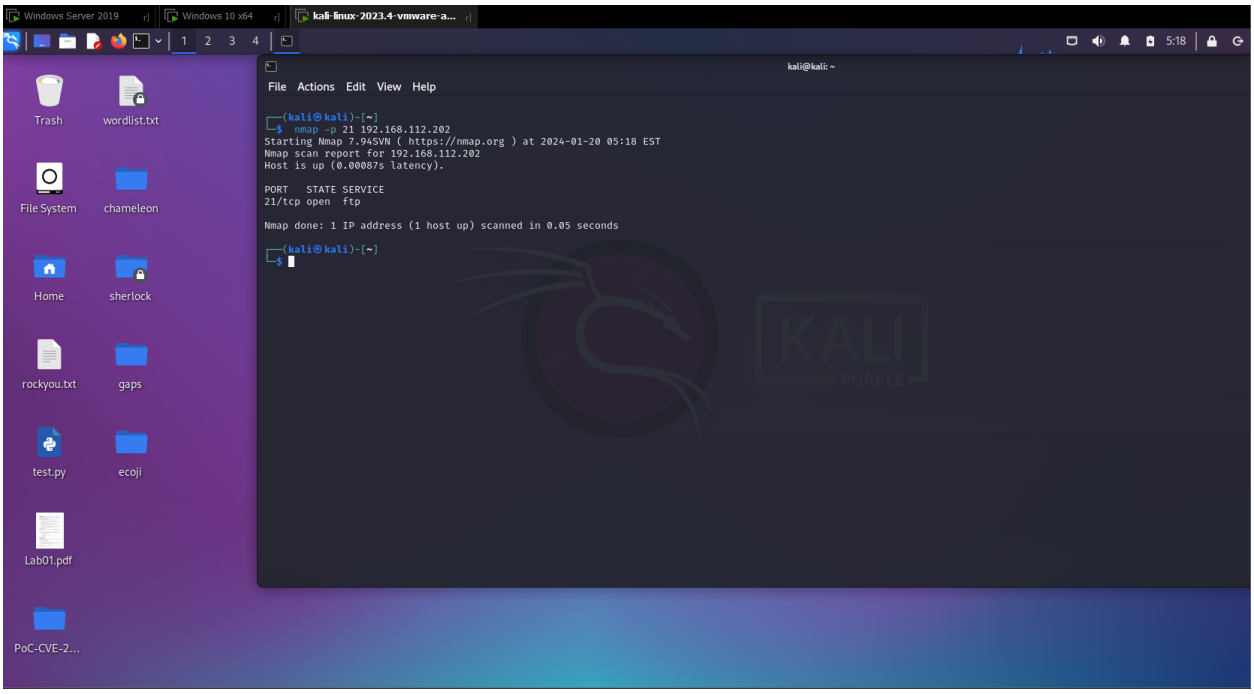


B5) Add IP address and select no ssll . Allow access to: all users with permissions: read and write

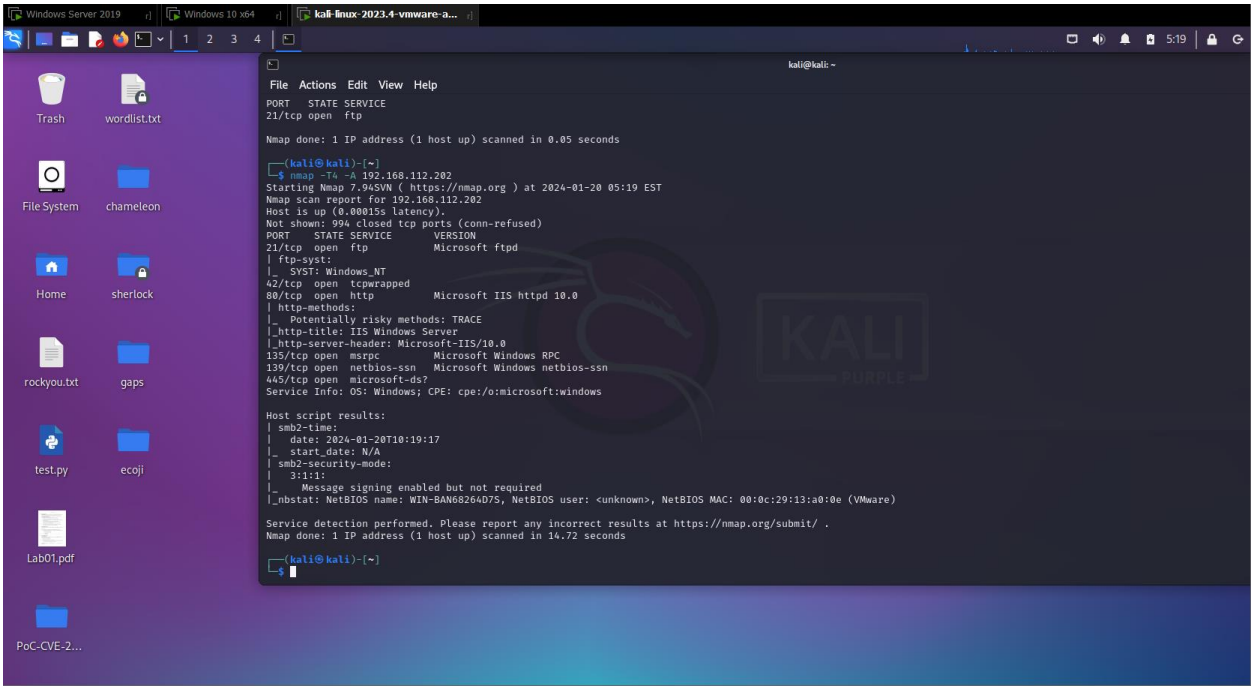




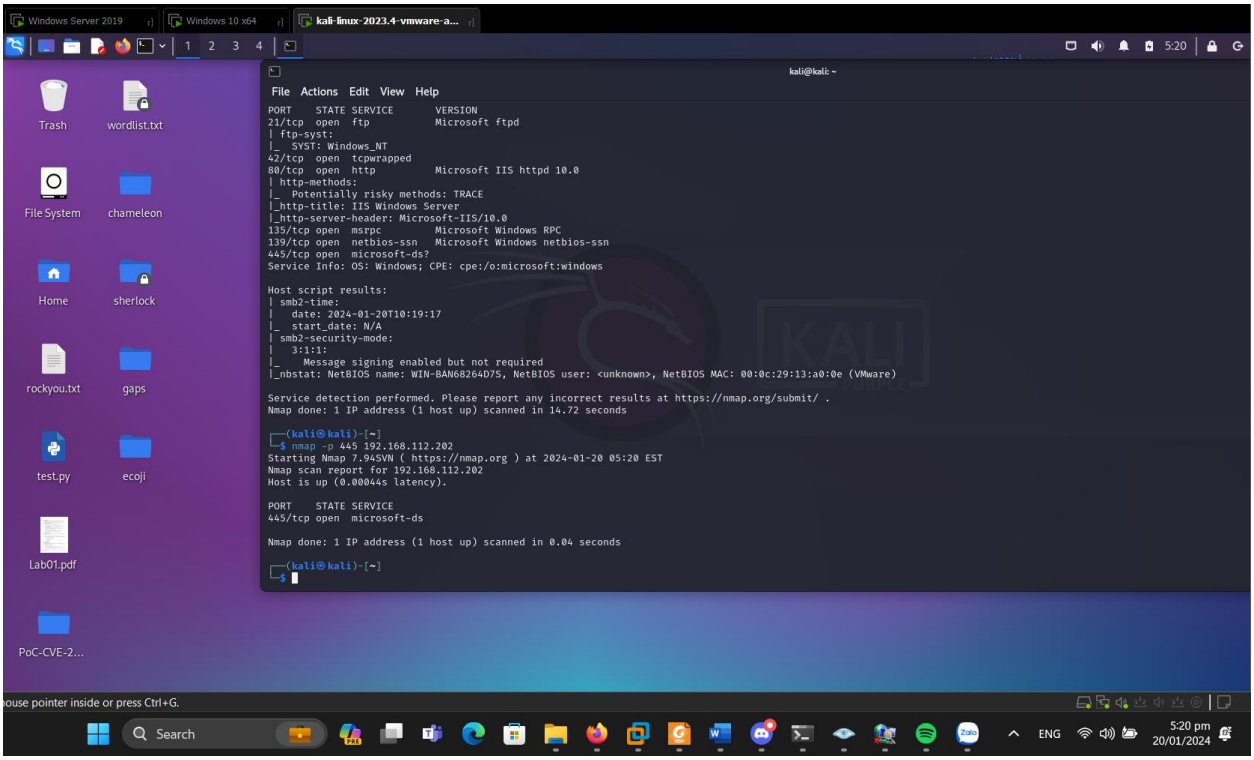
B6) Type: nmap -p 21 192.168.112.202 in kali



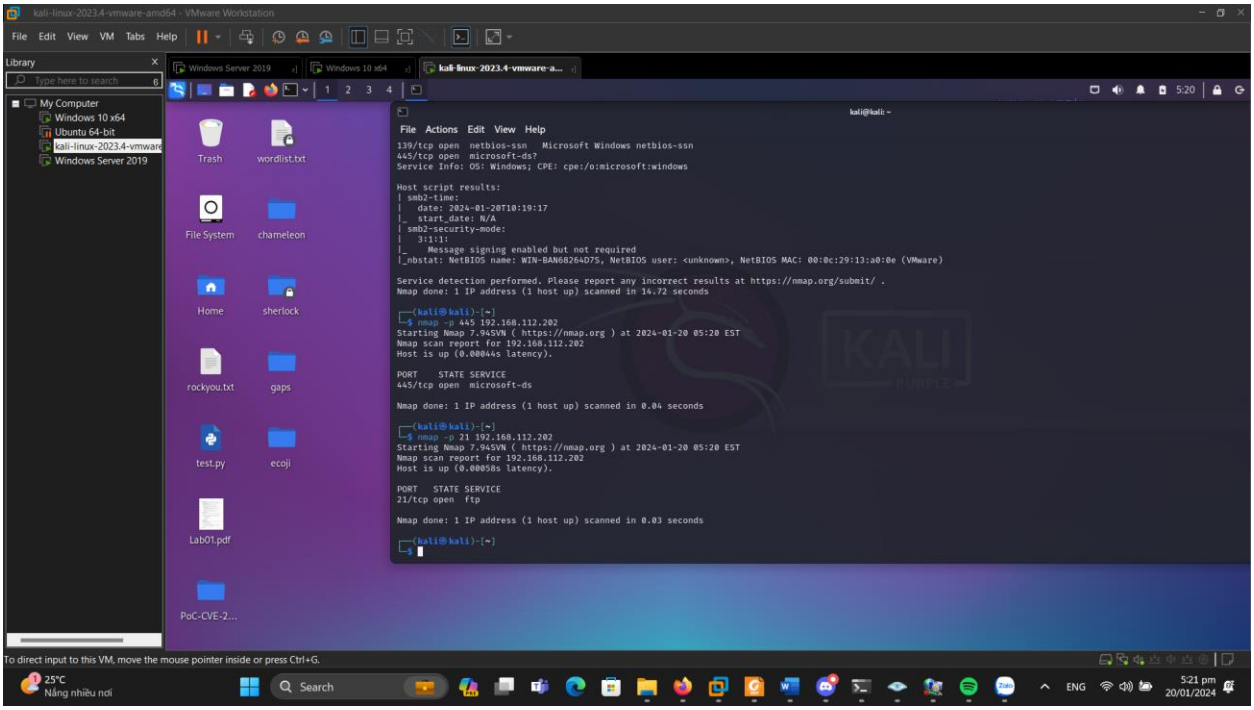
B7) nmap -T4 -A 192.168.112.202 (ACK flag is set)



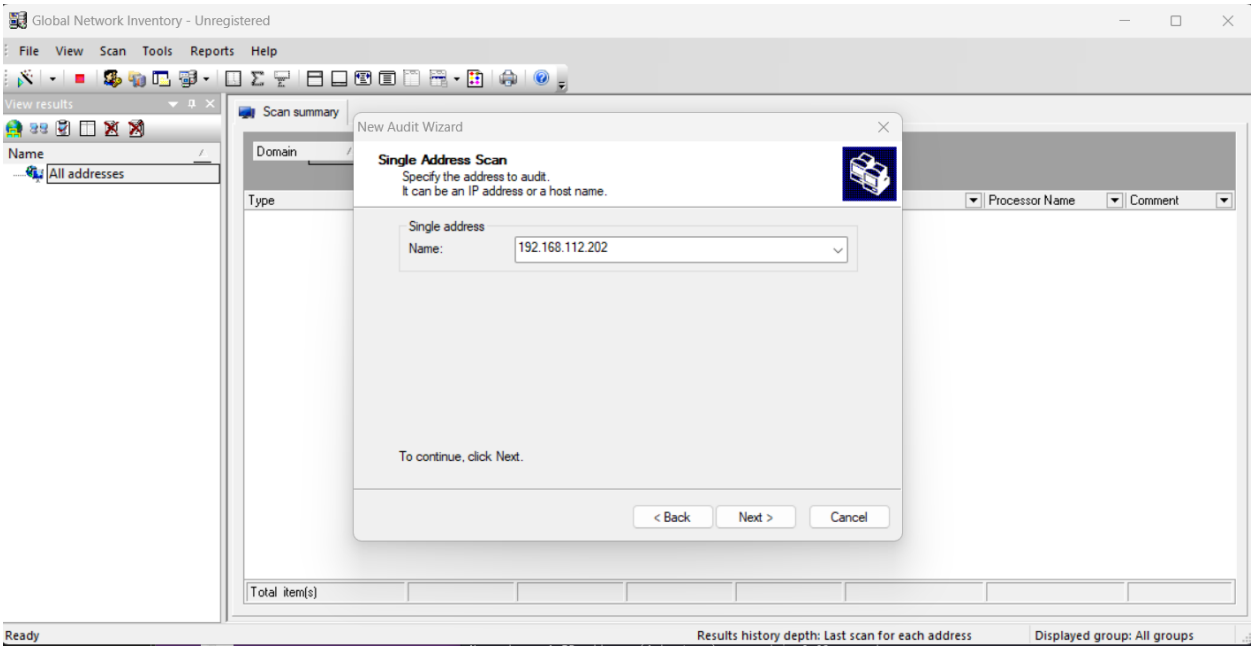
B8) nmap -p 445 -A 10.10.10.19 (port 445: smb)



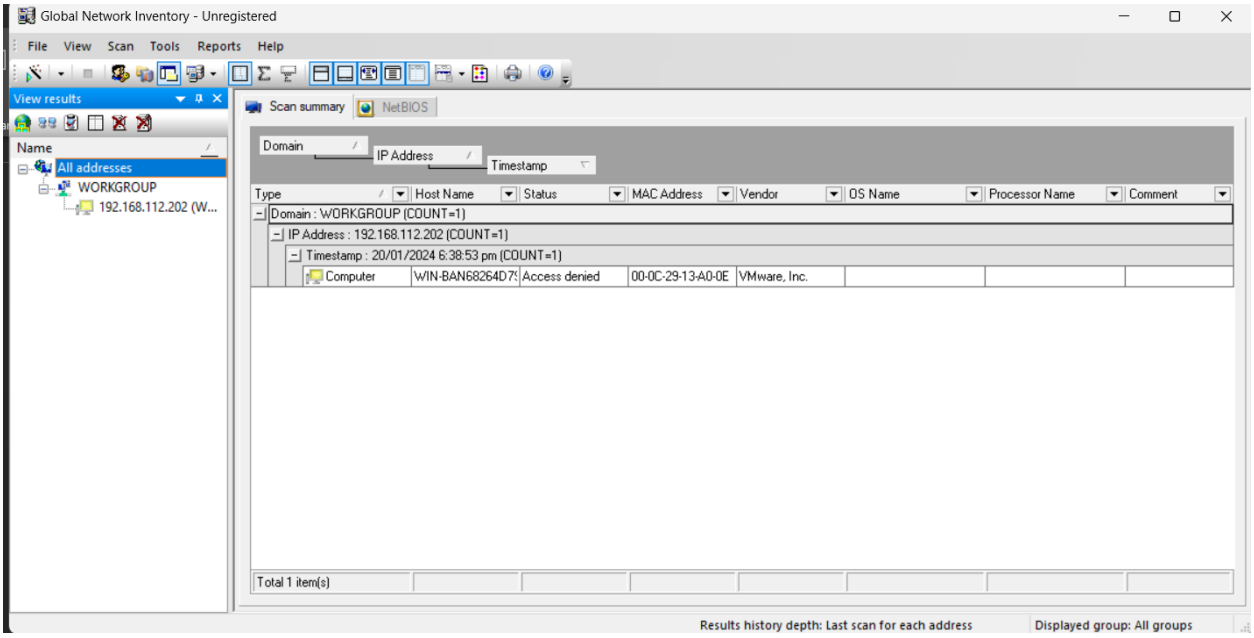
nmap -p 21 -A 10.10.10.19 (FTP)



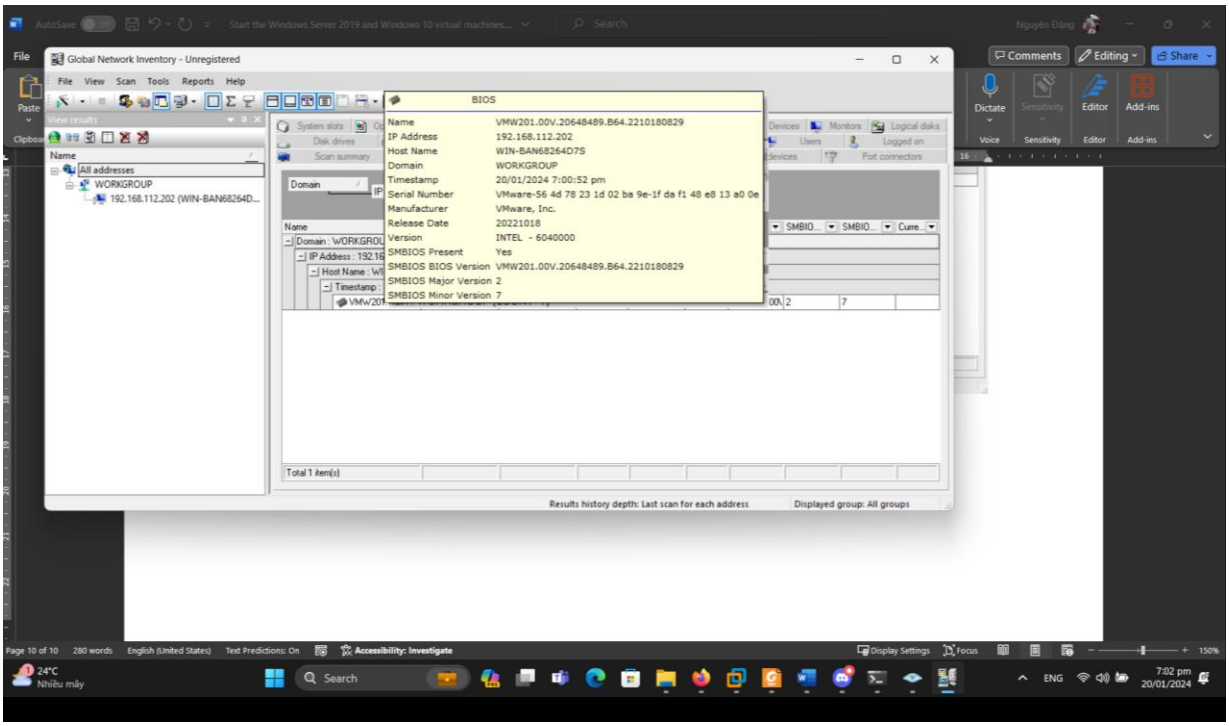
Install Global Network Inventory, choose Single address scan and enter IP address

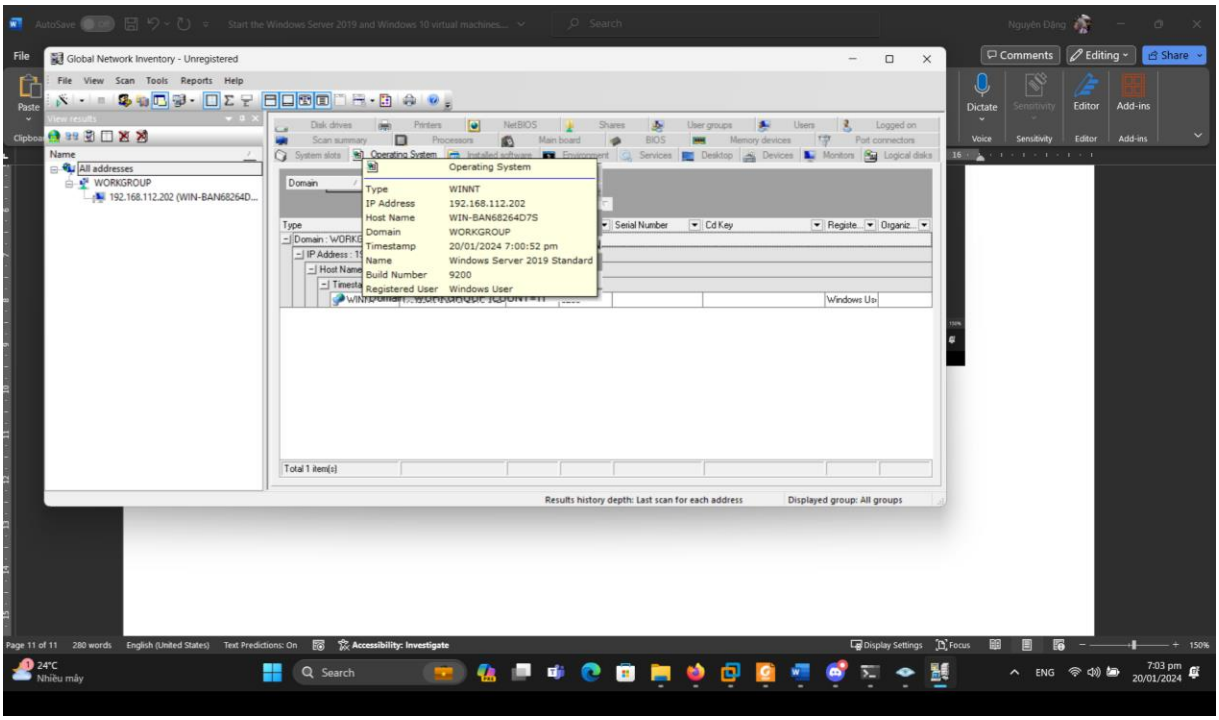


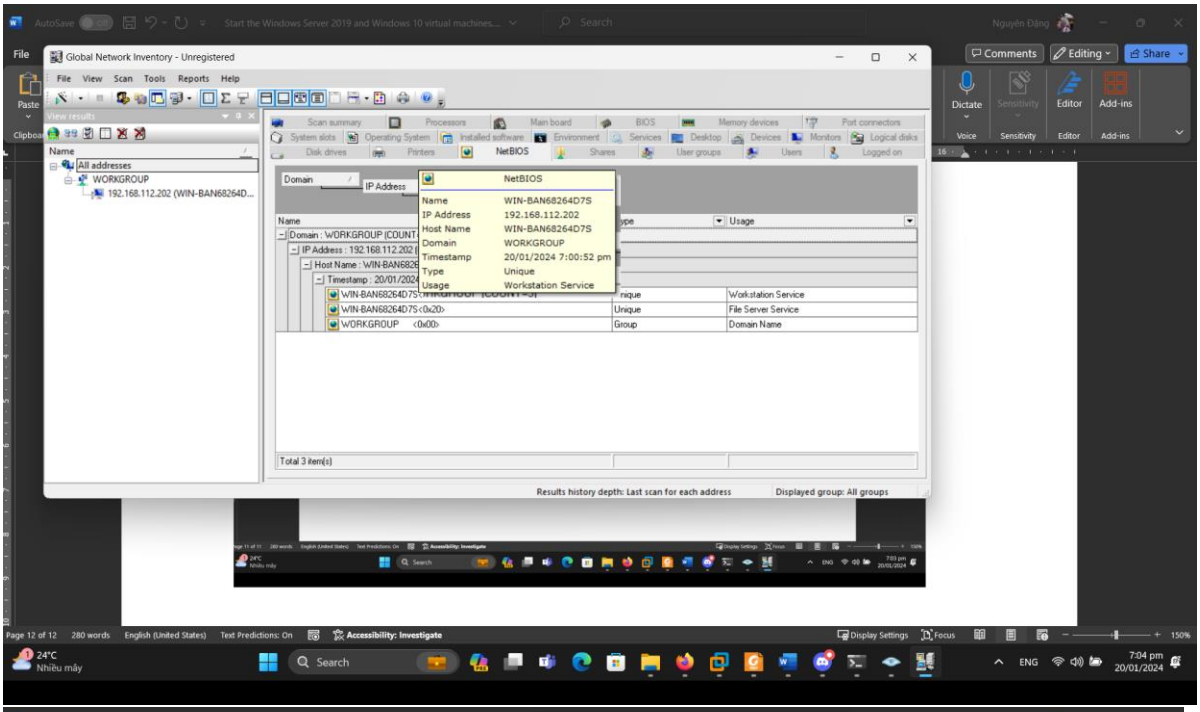
After scanning, the result show below:

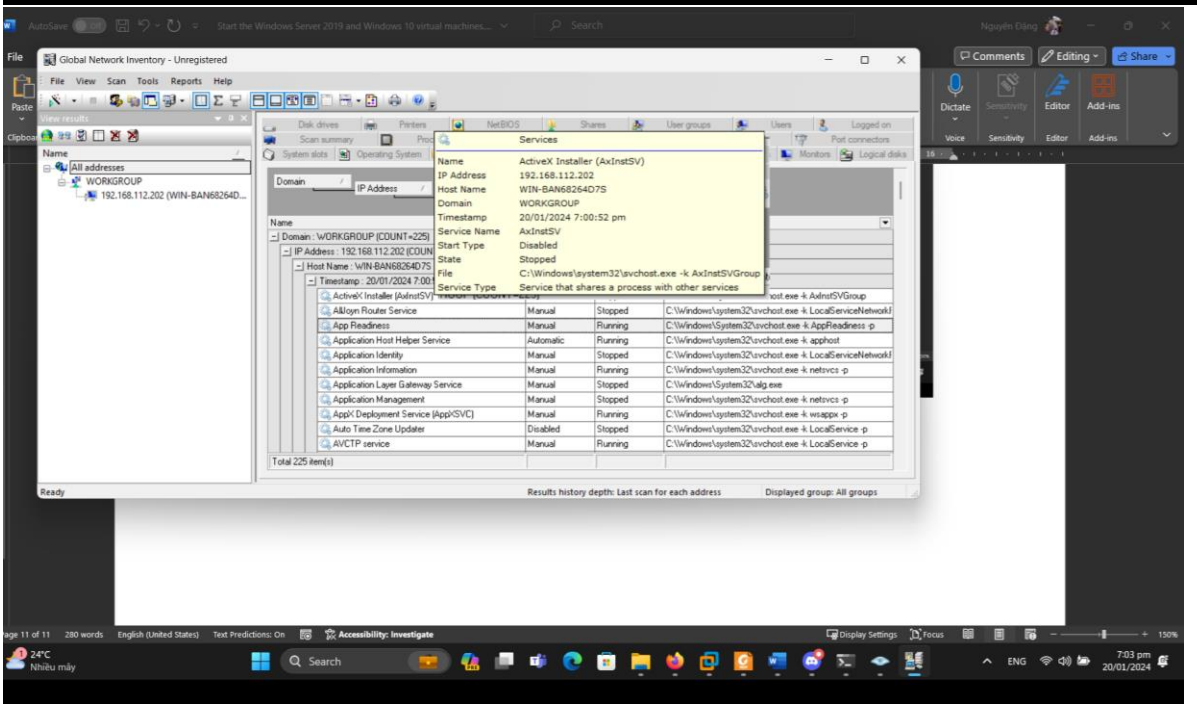


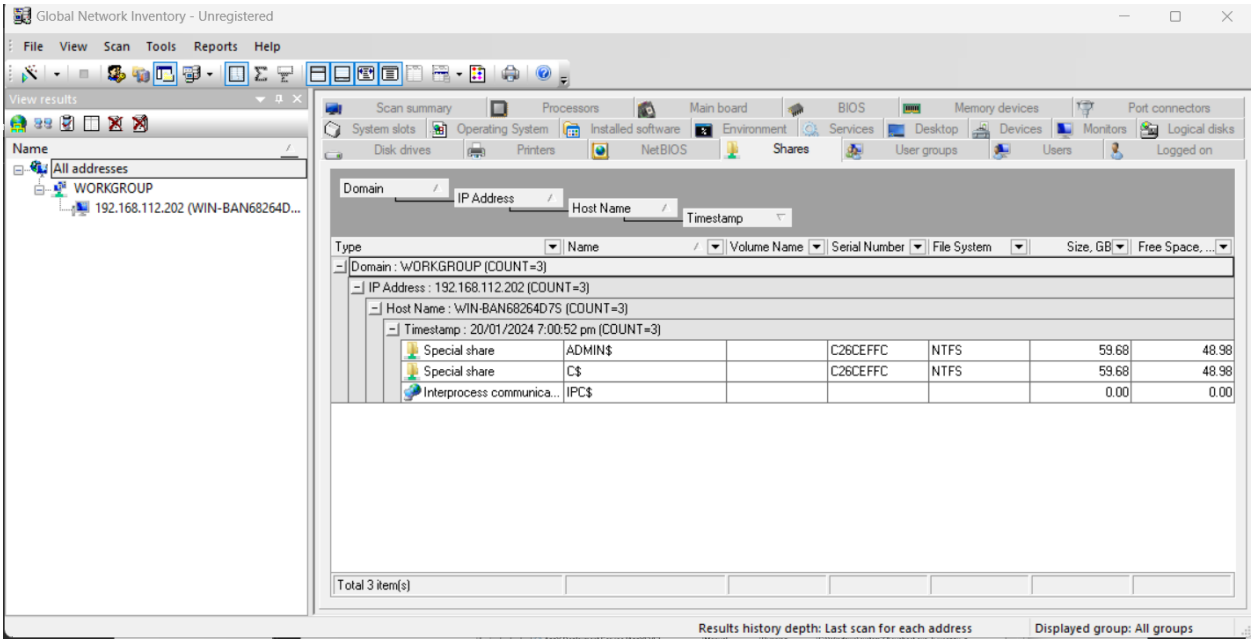
Watching bios, Operating system.,netbios, user groups,Users, Services,Installed software,Shares

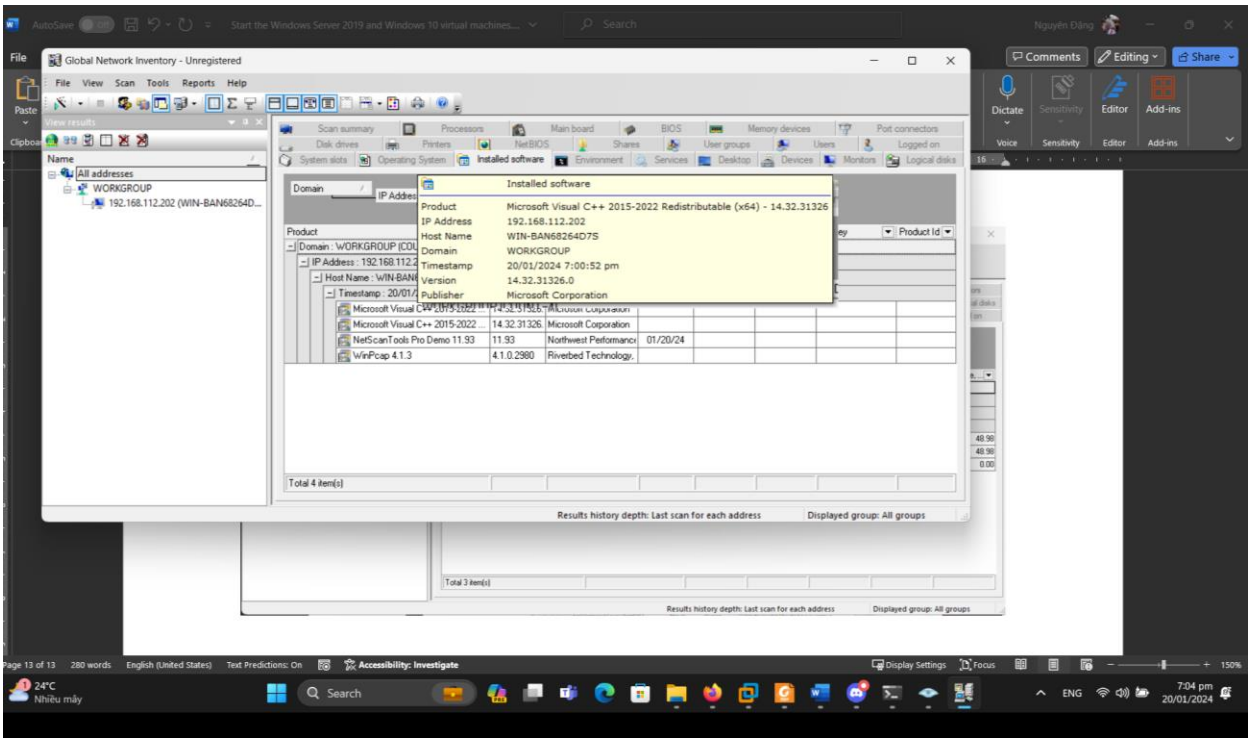

Global Network Inventory - Unregistered
BIOS
Name VMW201.00V.20648489.B64.2210180829
IP Address 192.168.112.202
Host Name WIN-BAN68264D7S
Domain WORKGROUP
Timestamp 20/01/2024 7:00:52 pm
Serial Number VMware-56 4d 78 23 1d 02 ba 9e-1f da f1 48 e8 13 a0 0e
Manufacturer VMware, Inc.
Release Date 20221018
Version INTEL - 6040000
SMBIOS Present Yes
SMBIOS BIOS Version VMW201.00V.20648489.B64.2210180829
SMBIOS Major Version 2
SMBIOS Minor Version 7
WORKGROUP
192.168.112.202 (WIN-BAN68264D...
Total 1 item(s)
Results history depth: Last scan for each address
Displayed group: All groups


Global Network Inventory - Unregistered
Operating System
Type WINNT
IP Address 192.168.112.202
Host Name WIN-BAN68264D7S
Domain WORKGROUP
Timestamp 20/01/2024 7:00:52 pm
Name Windows Server 2019 Standard
Build Number 9200
Registered User Windows User
WORKGROUP
192.168.112.202 (WIN-BAN68264D...
Total 1 item(s)
Results history depth: Last scan for each address
Displayed group: All groups

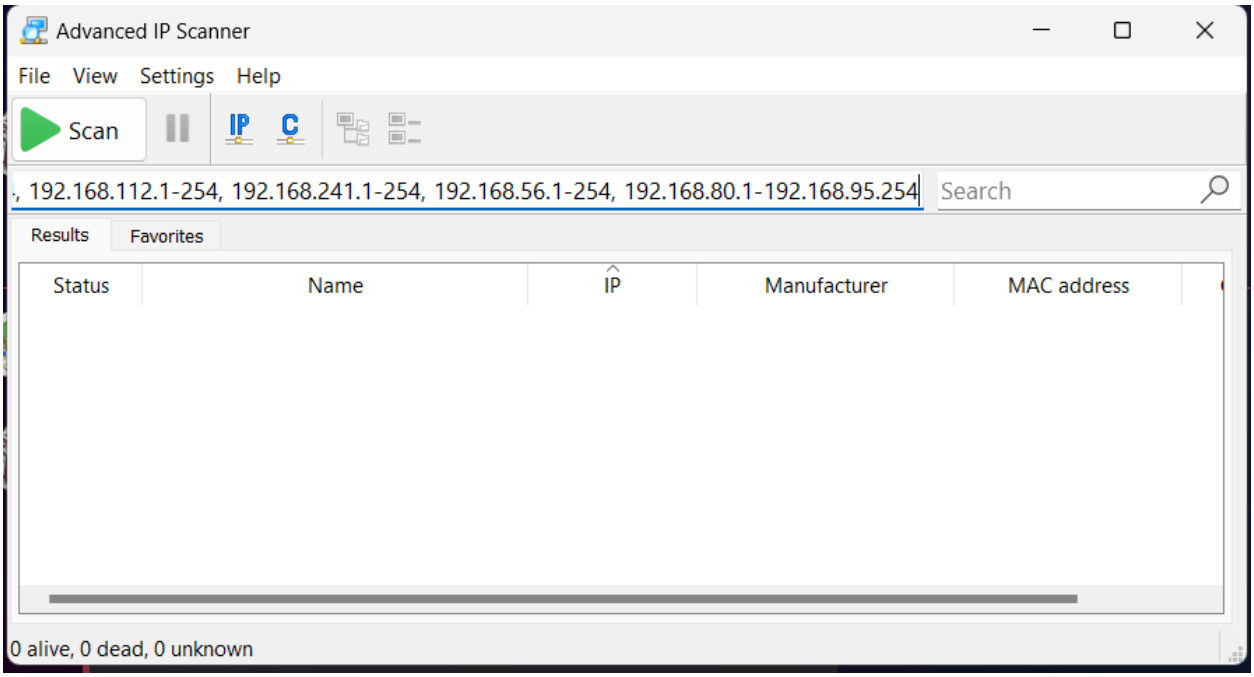

Global Network Inventory - Unregistered
NetBIOS
Name WIN-BAN68264D7S
IP Address 192.168.112.202
Host Name WIN-BAN68264D7S
Domain WORKGROUP
Timestamp 20/01/2024 7:00:52 pm
Type Unique
Usage Workstation Service
Total 3 item(s)
Results history depth: Last scan for each address
Displayed group: All groups


Global Network Inventory - Unregistered
Services
Name ActiveX Installer (AxInstSV)
IP Address 192.168.112.202
Host Name WIN-BAN68264D7S
Domain WORKGROUP
Timestamp 20/01/2024 7:00:52 pm
Service Name AxInstSV
Start Type Disabled
State Stopped
File C:\Windows\system32\svchost.exe -k AxInstSVGroup
Service Type Service that shares a process with other services
Total 225 item(s)
Ready
Results history depth: Last scan for each address
Displayed group: All groups

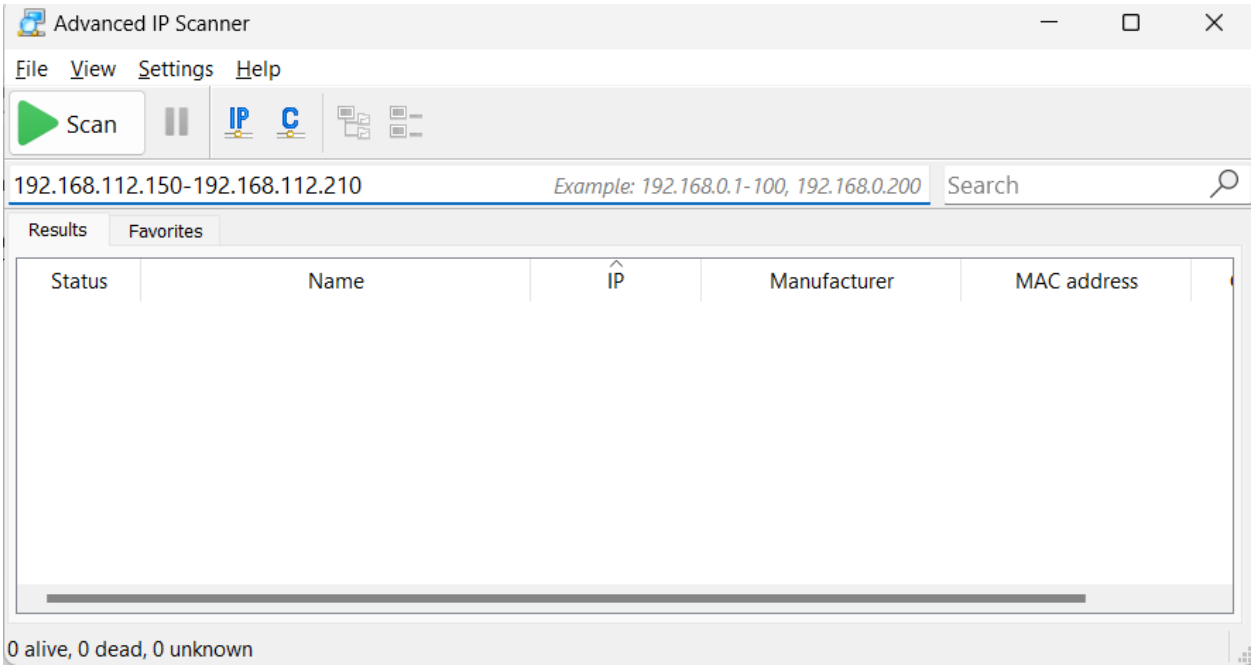




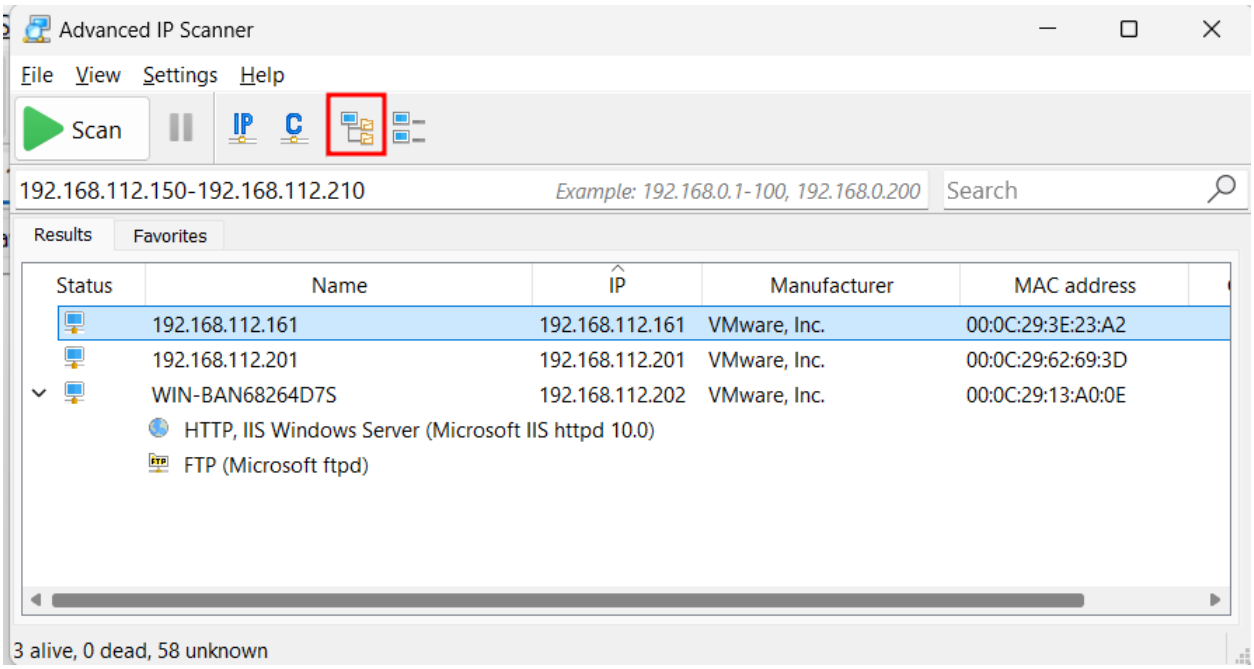
Install Advanceds IP Scanner



Scan from 192.168.112.150 to 192.168.112.210



The result can be show all the service below



Right click to see the list of available options