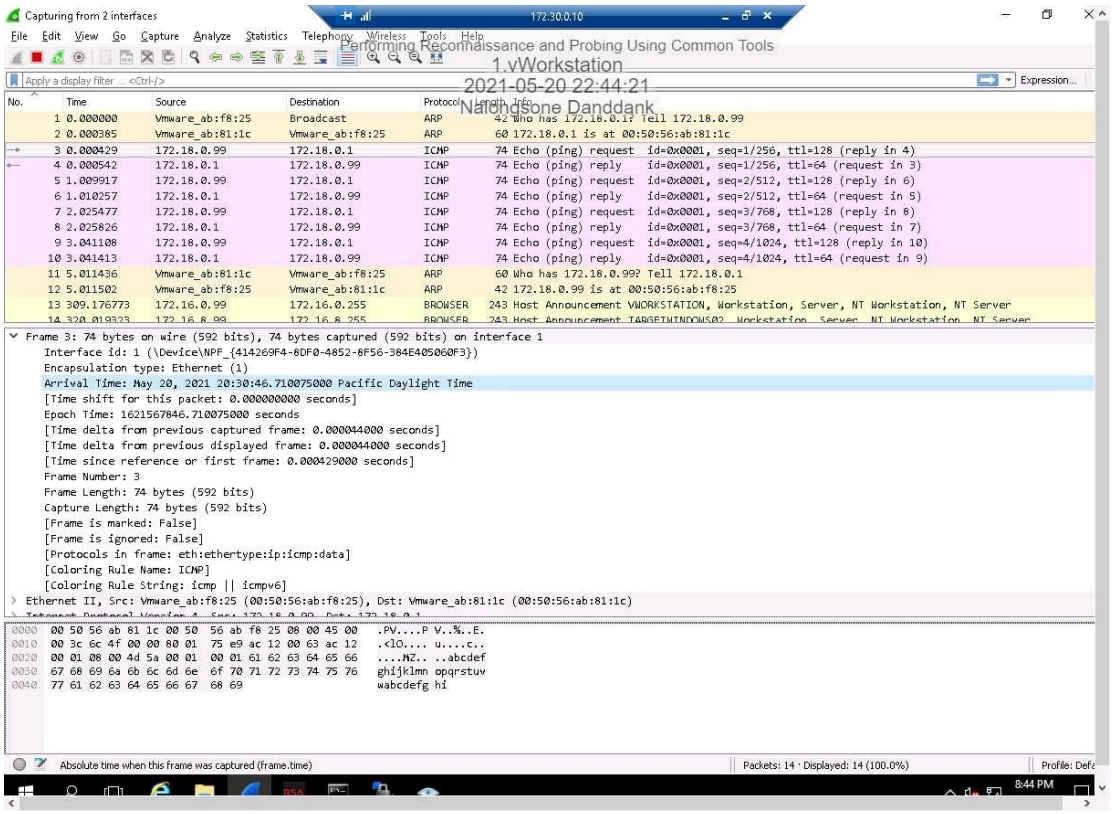
Nalongsone Danddank Student ID : 14958950 StarID: jf3893pd
Email: nalongsone.danddank@my.metrostate.edu\

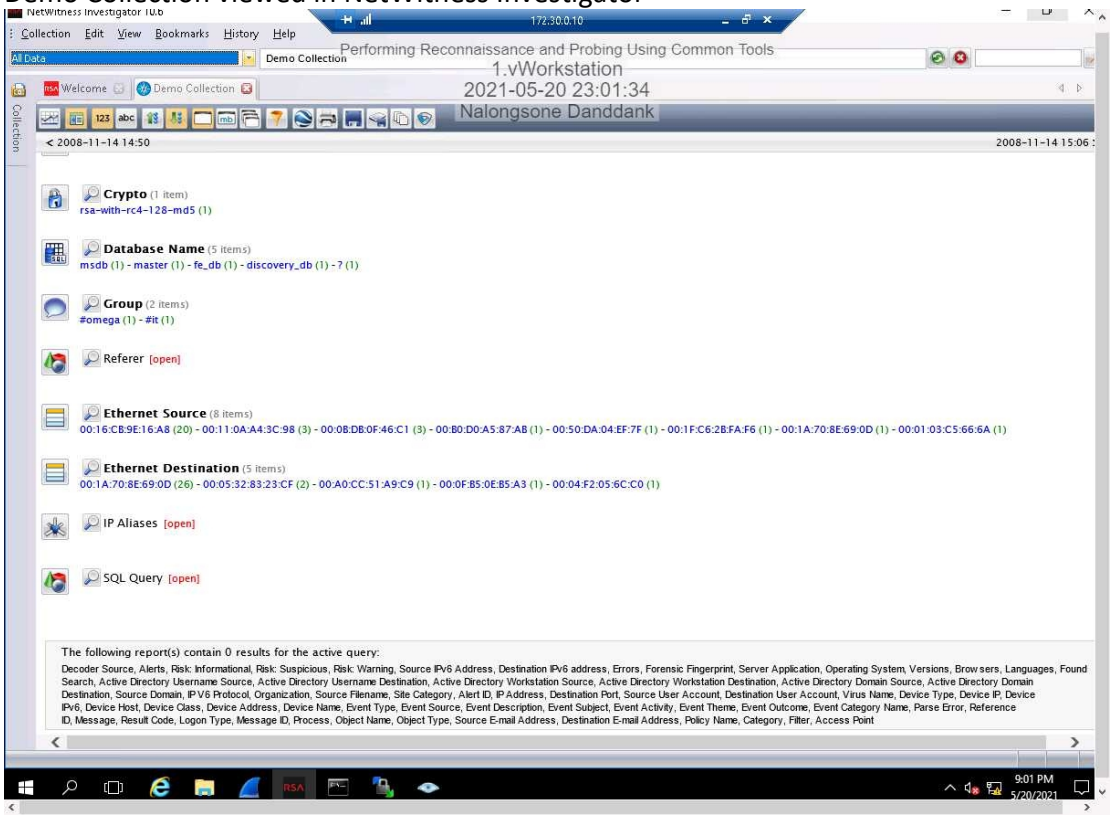
ICS382/CYBR332-51 —Computer Security

Lab #1 Report

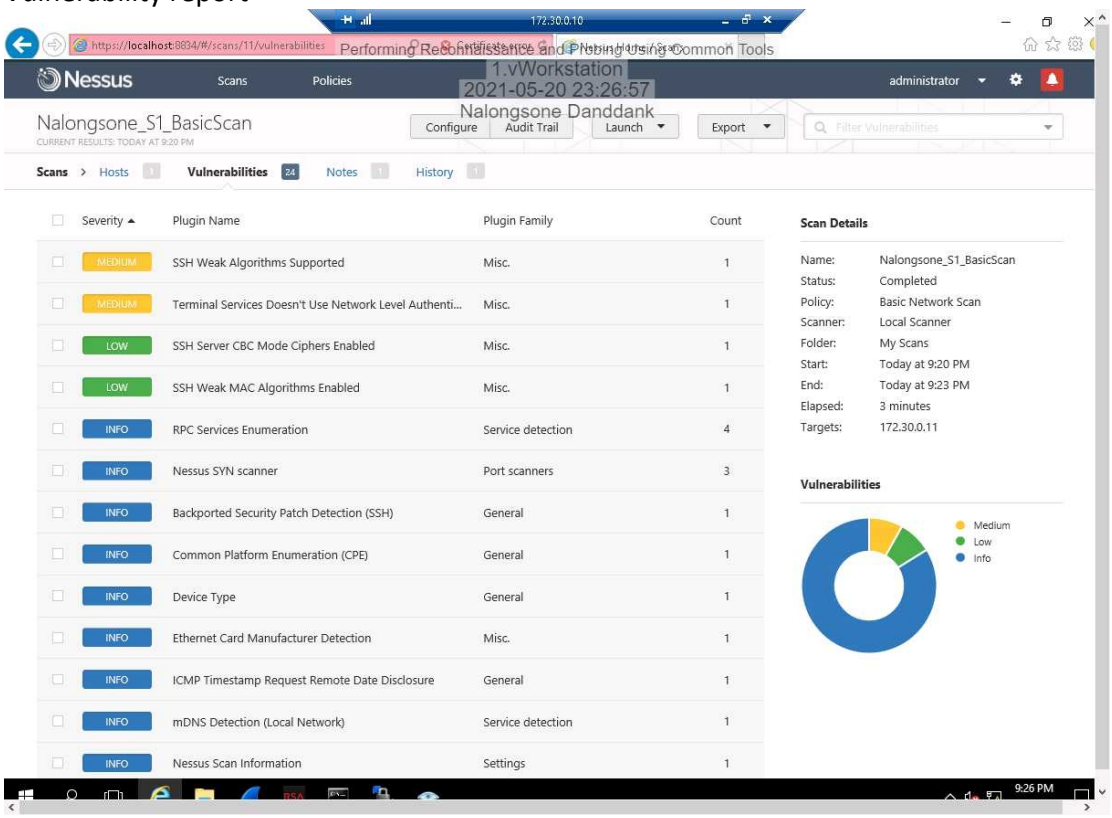
Frame detail for ICMP traffic

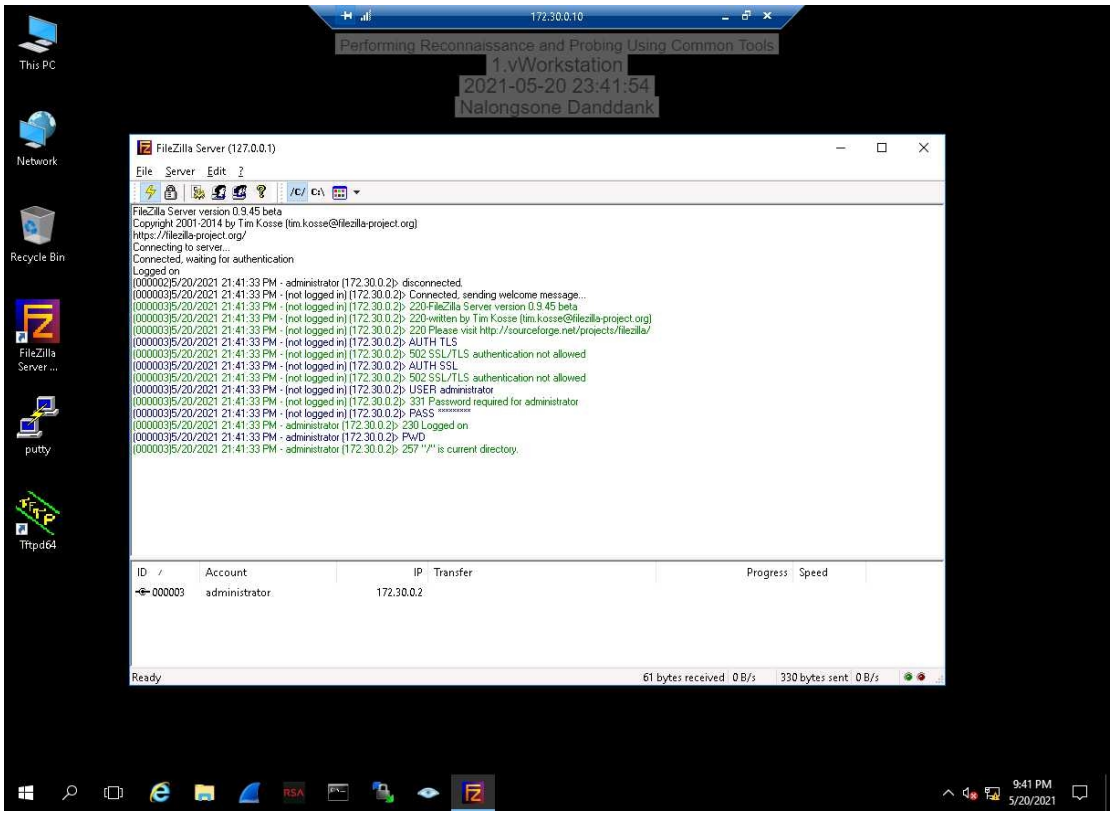


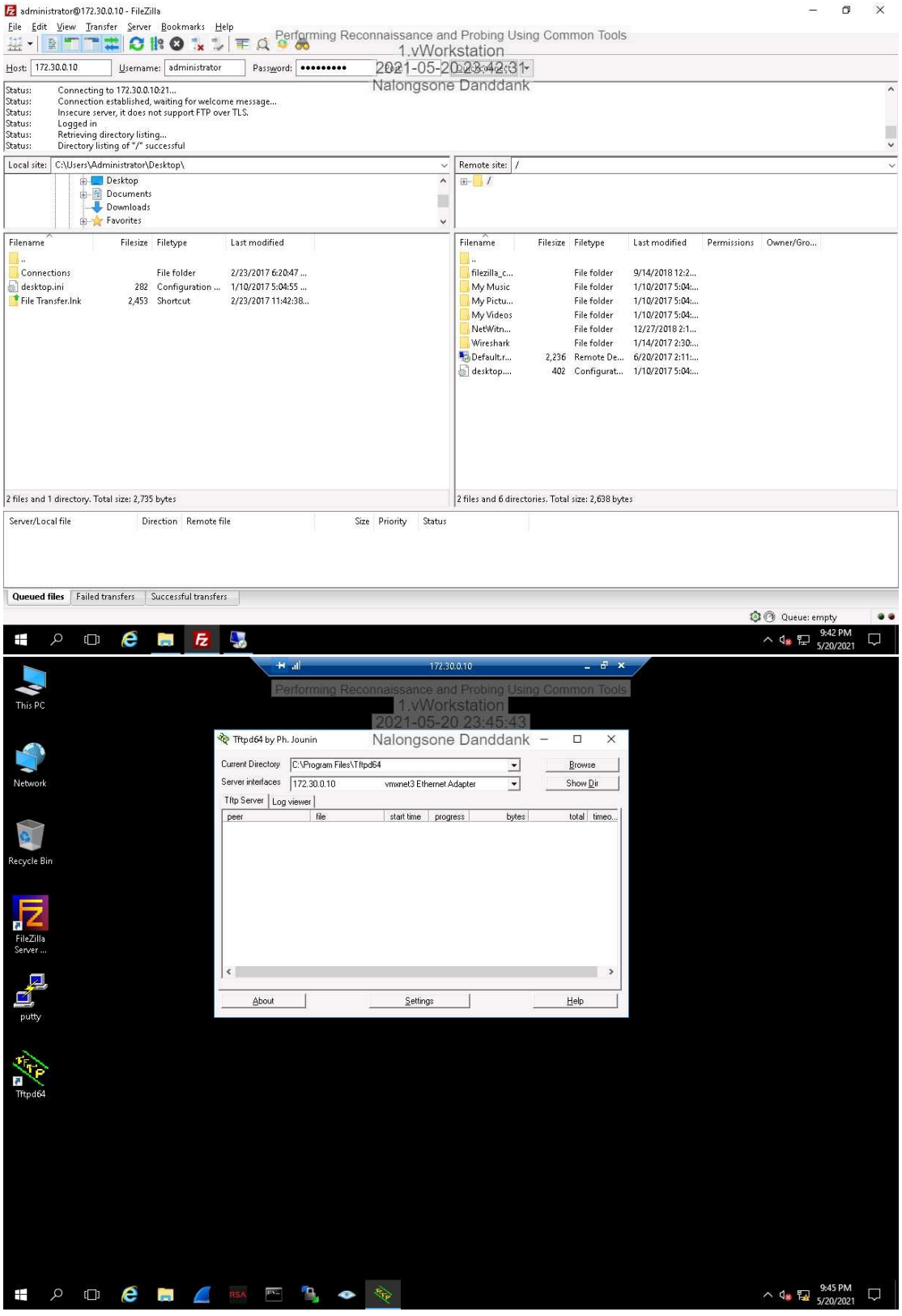
Demo Collection viewed in NetWitness Investigator

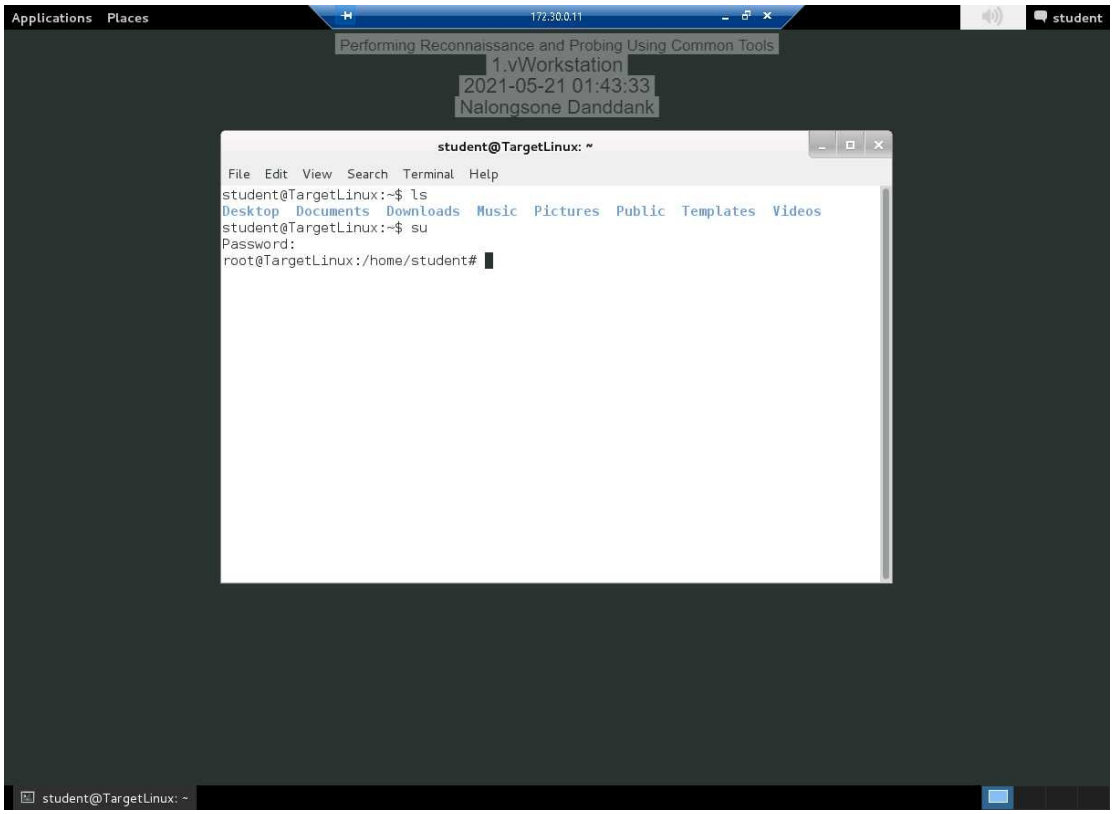


Vulnerability report

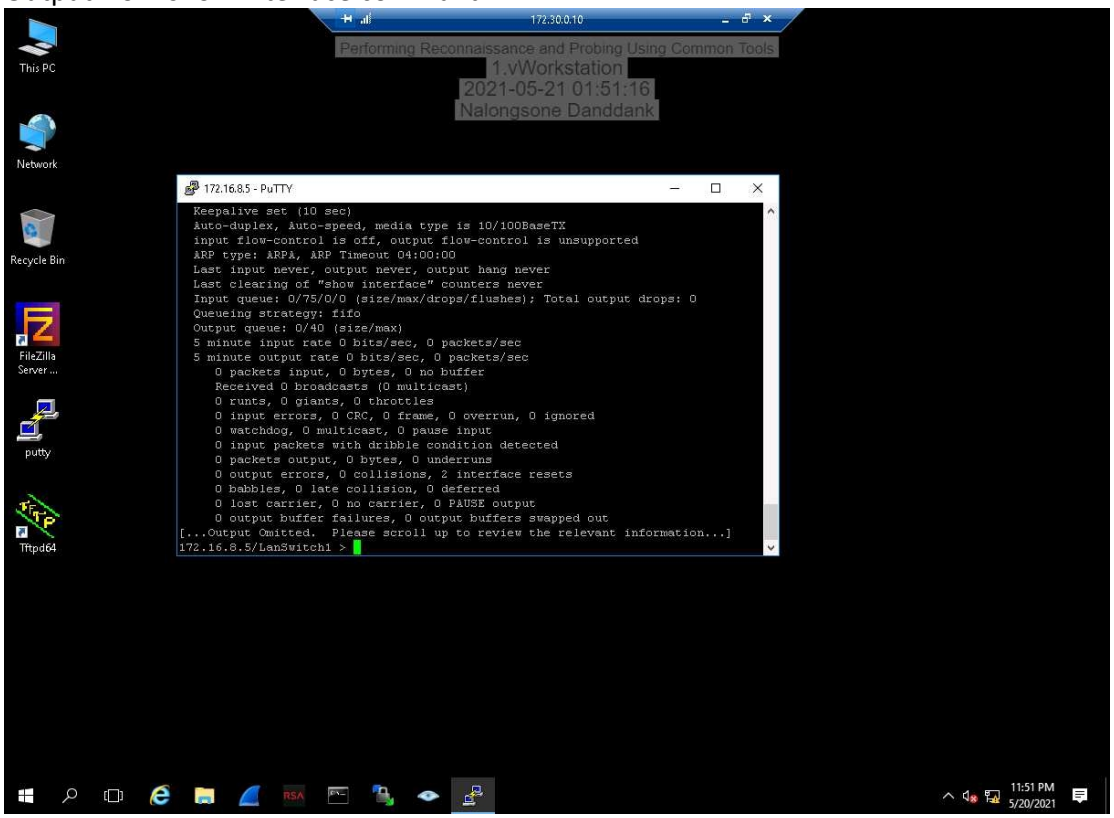


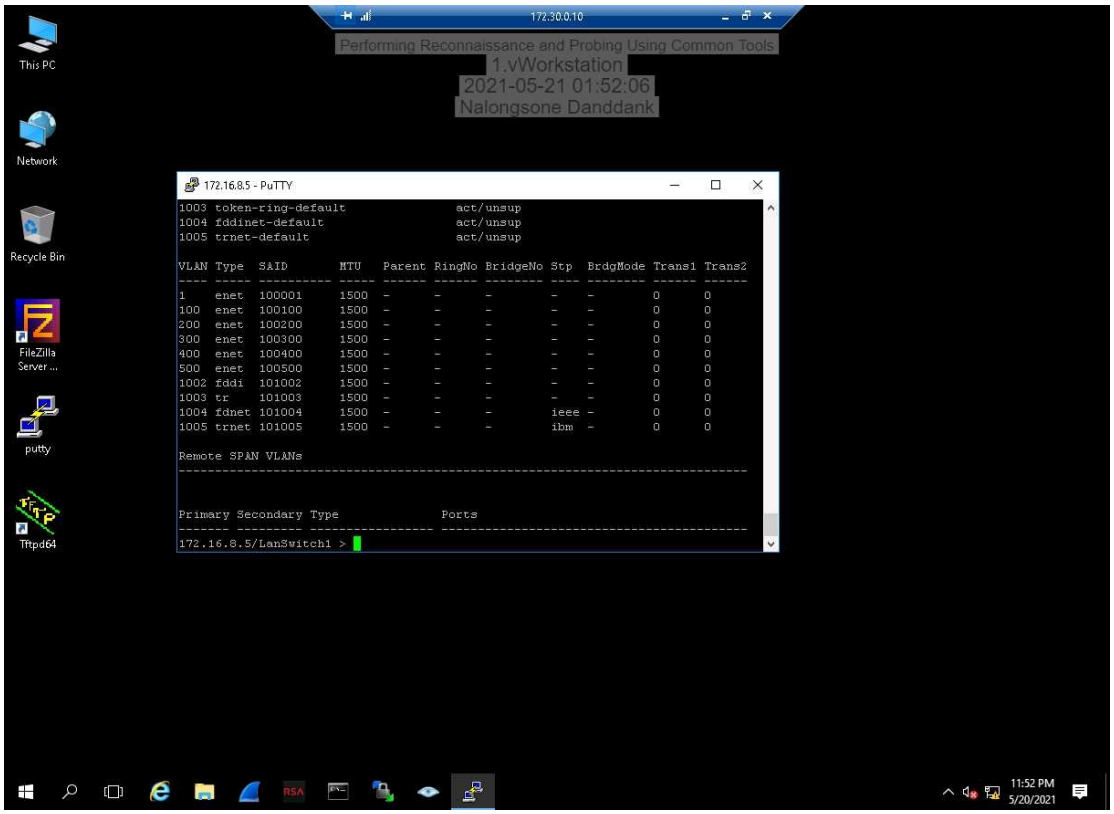


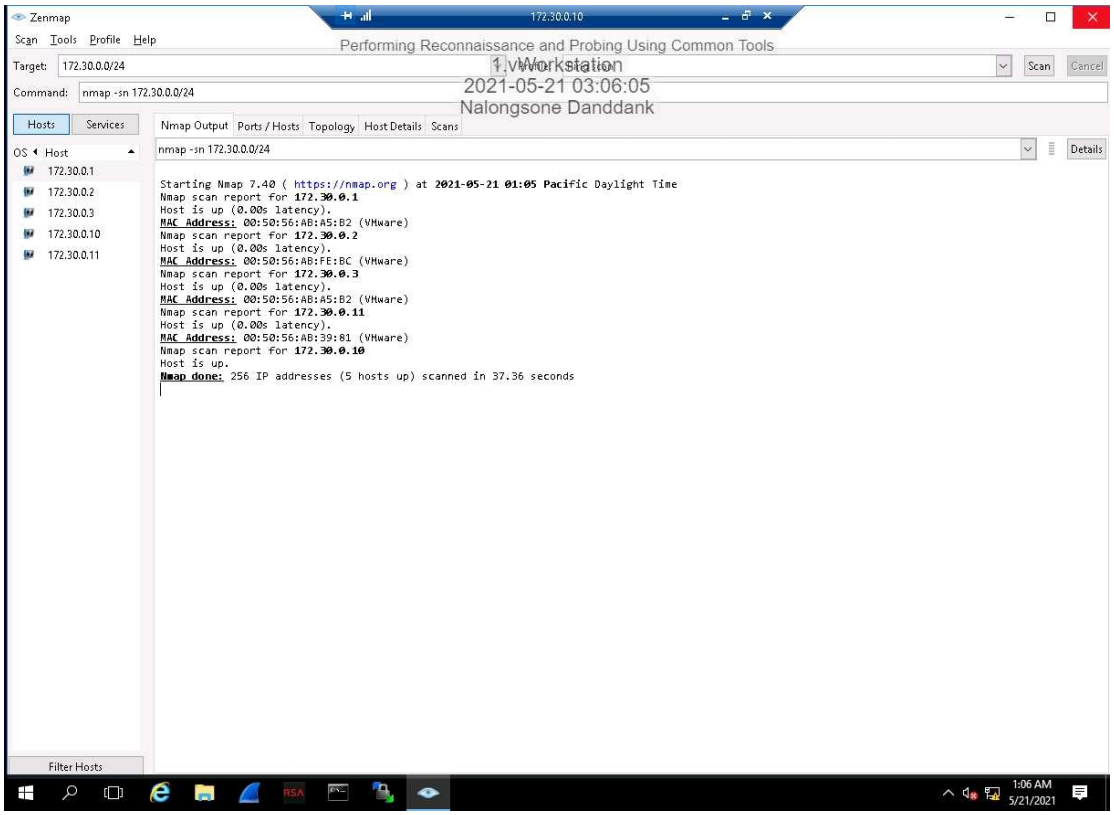

administrator@172.30.0.10 - FileZilla
File Edit View Transfer Server Bookmarks Help
Performing Reconnaissance and Probing Using Common Tools
1.vWorkstation
2021-05-20 23:42:31
Nalongsone Danddank
Host: 172.30.0.10 Username: administrator Password:
Status: Connecting to 172.30.0.10:21...
Status: Connection established, waiting for welcome message...
Status: Insecure server, it does not support FTP over TLS.
Status: Logged in
Status: Retrieving directory listing...
Status: Directory listing of "/" successful
Local site: C:\Users\Administrator\Desktop\
Remote site: /
Desktop
Documents
Downloads
Favorites
Filename Filesize Filetype Last modified
Connections File folder 2/23/2017 6:20:47 ...
desktop.ini 282 Configuration ... 1/10/2017 5:04:55 ...
File Transfer.lnk 2,453 Shortcut 2/23/2017 11:42:38...
2 files and 1 directory. Total size: 2,735 bytes
Filename Filesize Filetype Last modified Permissions Owner/Gro...
filezilla_c... File folder 9/14/2018 12:2...
My Music File folder 1/10/2017 5:04:...
My Pictu... File folder 1/10/2017 5:04:...
My Videos File folder 1/10/2017 5:04:...
NetWitn... File folder 12/27/2018 2:1...
Wireshark File folder 1/14/2017 2:30:...
Default.r... 2,236 Remote De... 6/20/2017 2:11:...
desktop.... 402 Configurat... 1/10/2017 5:04:...
2 files and 6 directories. Total size: 2,638 bytes
Server/Local file Direction Remote file Size Priority Status
Queued files Failed transfers Successful transfers
Queue: empty
9:42 PM
5/20/2021
172.30.0.10
Performing Reconnaissance and Probing Using Common Tools
1.vWorkstation
2021-05-20 23:45:43
Nalongsone Danddank
This PC
Network
Recycle Bin
FileZilla Server ...
putty
Tftpd64
Tftpd64 by Ph. Jounin
Current Directory C:\Program Files\Tftpd64
Browse
Server interfaces 172.30.0.10 vmxnet3 Ethernet Adapter
Show Dir
Tftp Server Log viewer
peer file start time progress bytes total timeo...
About Settings Help
9:45 PM
5/20/2021



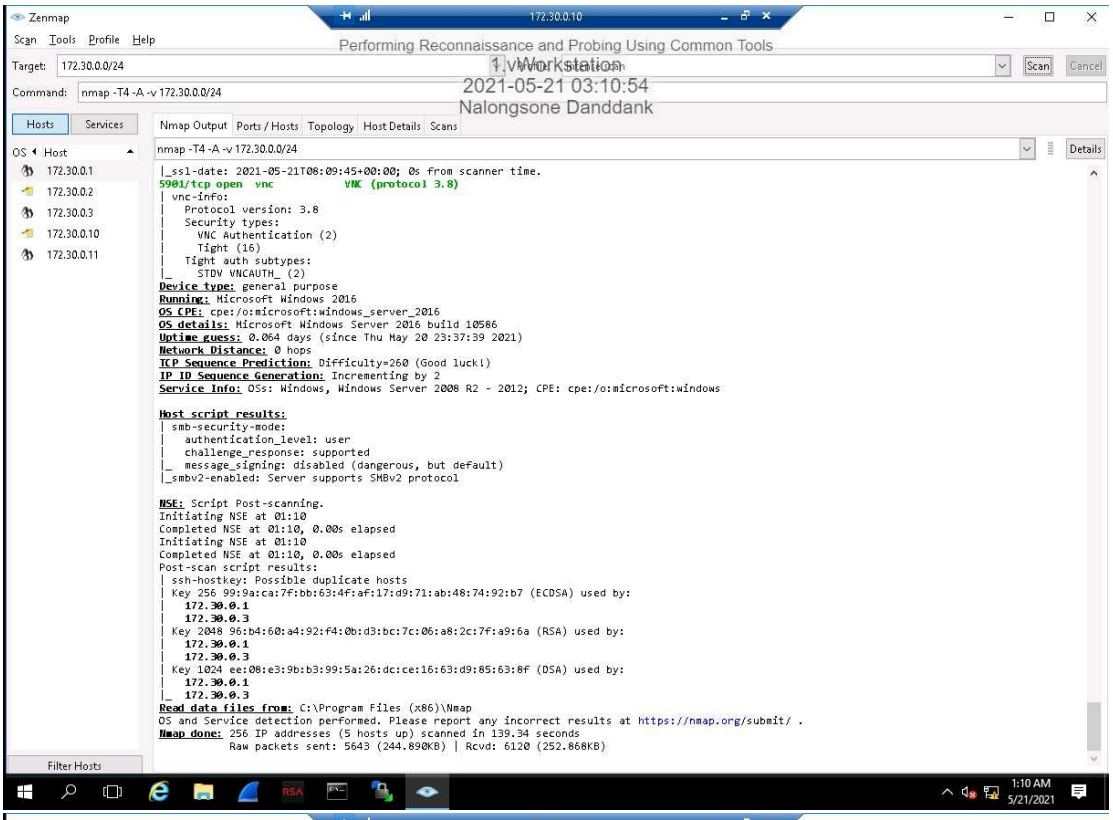
Output from show interface command

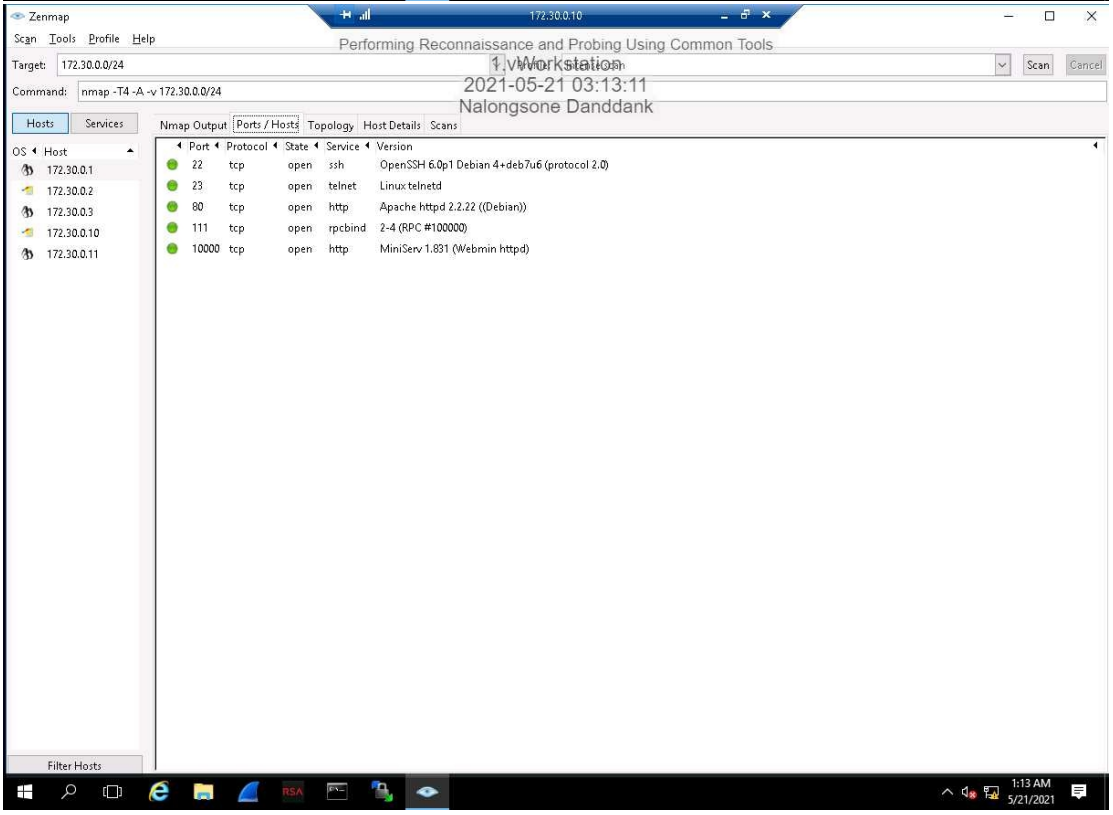


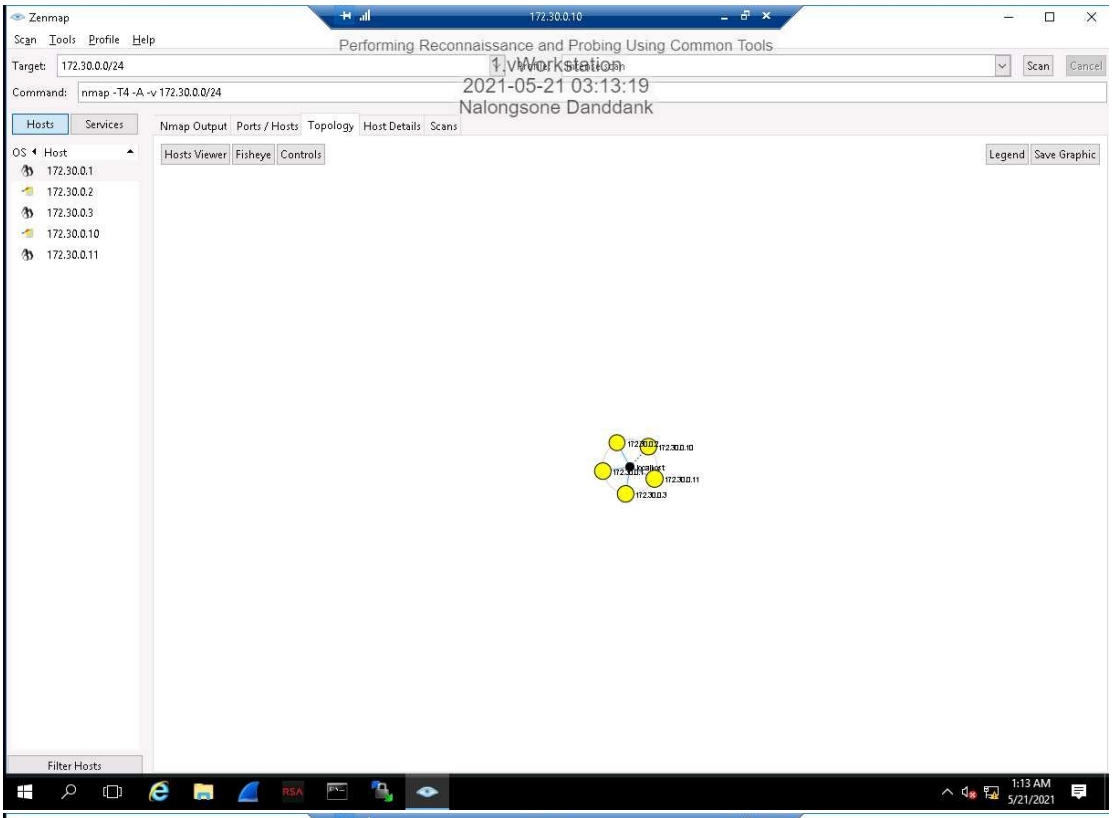


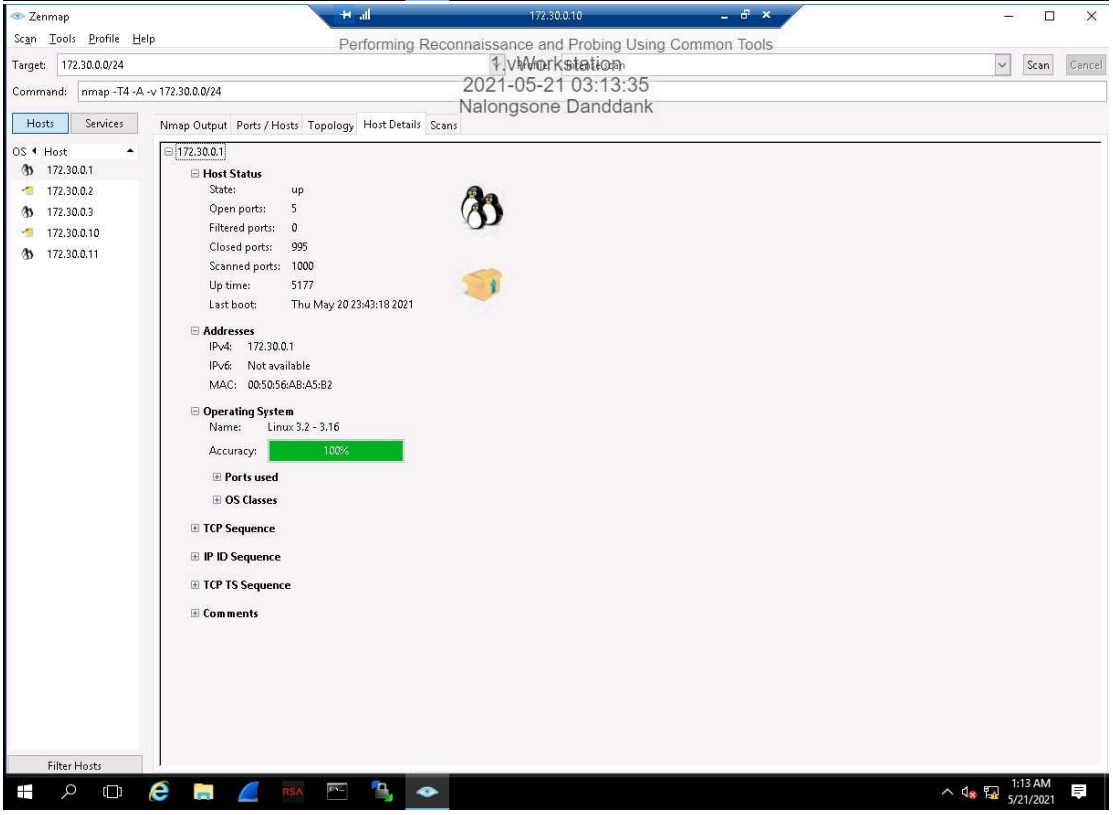


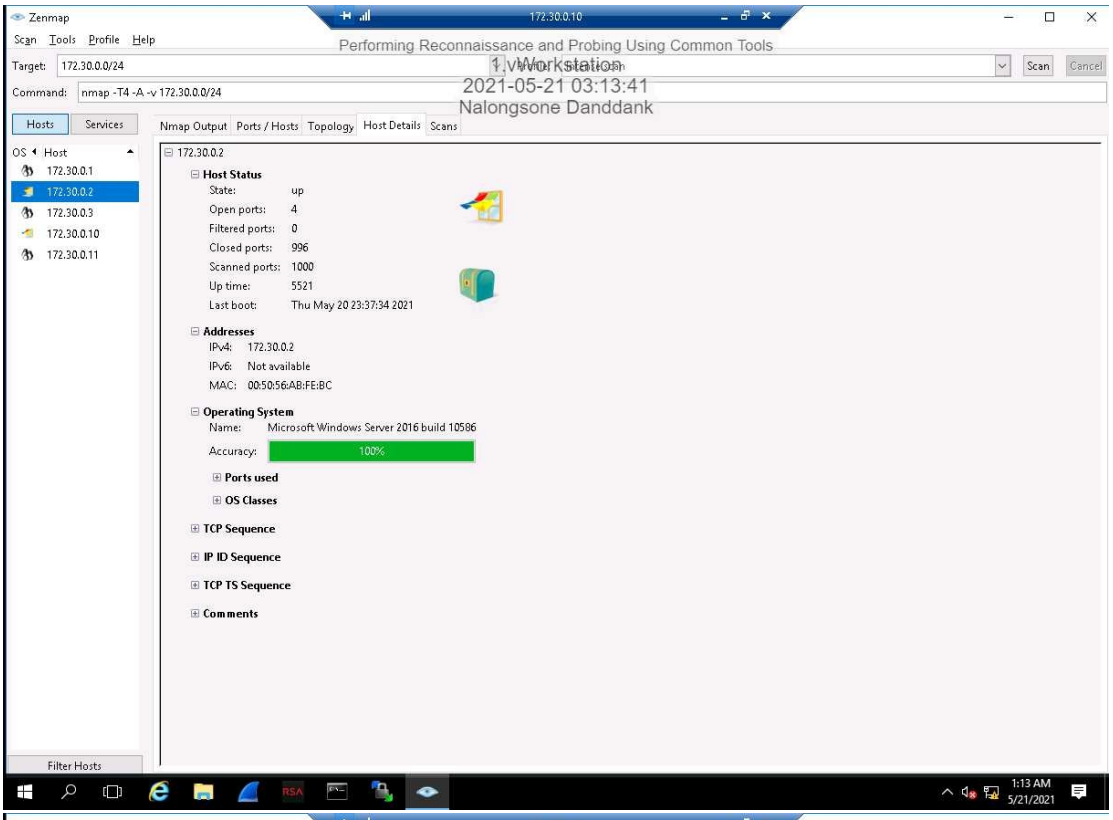
Intense scan

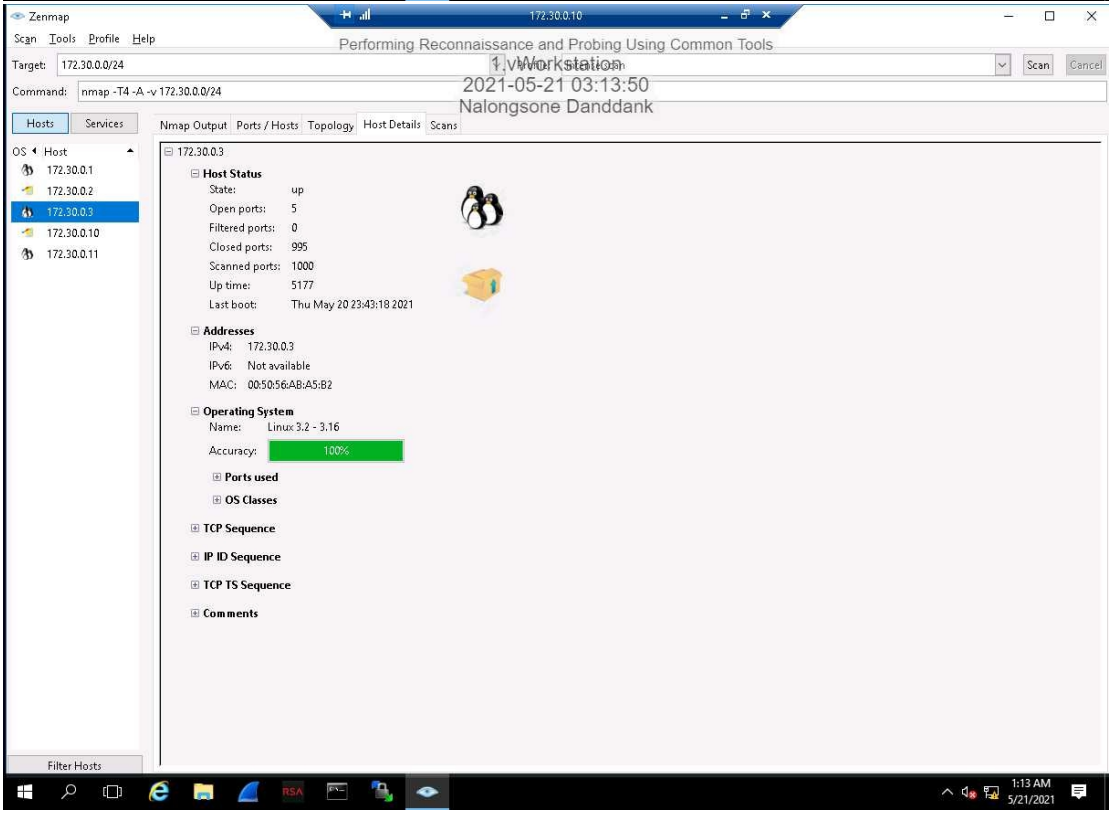

Zenmap
172.30.0.10
Scan Tools Profile Help
Performing Reconnaissance and Probing Using Common Tools
1 Workstation
2021-05-21 03:10:54
Nalongsone Danddank
Target: 172.30.0.0/24
Command: nmap -T4 -A -v 172.30.0.0/24
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
172.30.0.1
172.30.0.2
172.30.0.3
172.30.0.10
172.30.0.11
Details
|_ssl-date: 2021-05-21T08:09:45+00:00; 0s from scanner time.
5901/tcp open vnc VNC (protocol 3.8)
| vnc-info:
| Protocol version: 3.8
| Security types:
| VNC Authentication (2)
| Tight (16)
| Tight auth subtypes:
|_ STDV VNCAUTH_ (2)
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 build 10586
Uptime guess: 0.064 days (since Thu May 20 23:37:39 2021)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incrementing by 2
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
Host script results:
| smb-security-mode:
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol
NSE: Script Post-scanning.
Initiating NSE at 01:10
Completed NSE at 01:10, 0.00s elapsed
Initiating NSE at 01:10
Completed NSE at 01:10, 0.00s elapsed
Post-scan script results:
| ssh-hostkey: Possible duplicate hosts
| Key 256 99:9a:ca:7f:bb:63:4f:af:17:d9:71:ab:48:74:92:b7 (ECDSA) used by:
| 172.30.0.1
| 172.30.0.3
| Key 2048 96:b4:60:a4:92:f4:0b:d3:bc:7c:06:a8:2c:7f:a9:6a (RSA) used by:
| 172.30.0.1
| 172.30.0.3
| Key 1024 ee:08:e3:9b:b3:99:5a:26:dc:ce:16:63:d9:85:63:8f (DSA) used by:
| 172.30.0.1
|_ 172.30.0.3
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: 256 IP addresses (5 hosts up) scanned in 139.34 seconds
Raw packets sent: 5643 (244.890KB) | Rcvd: 6120 (252.868KB)
Filter Hosts
1:10 AM
5/21/2021

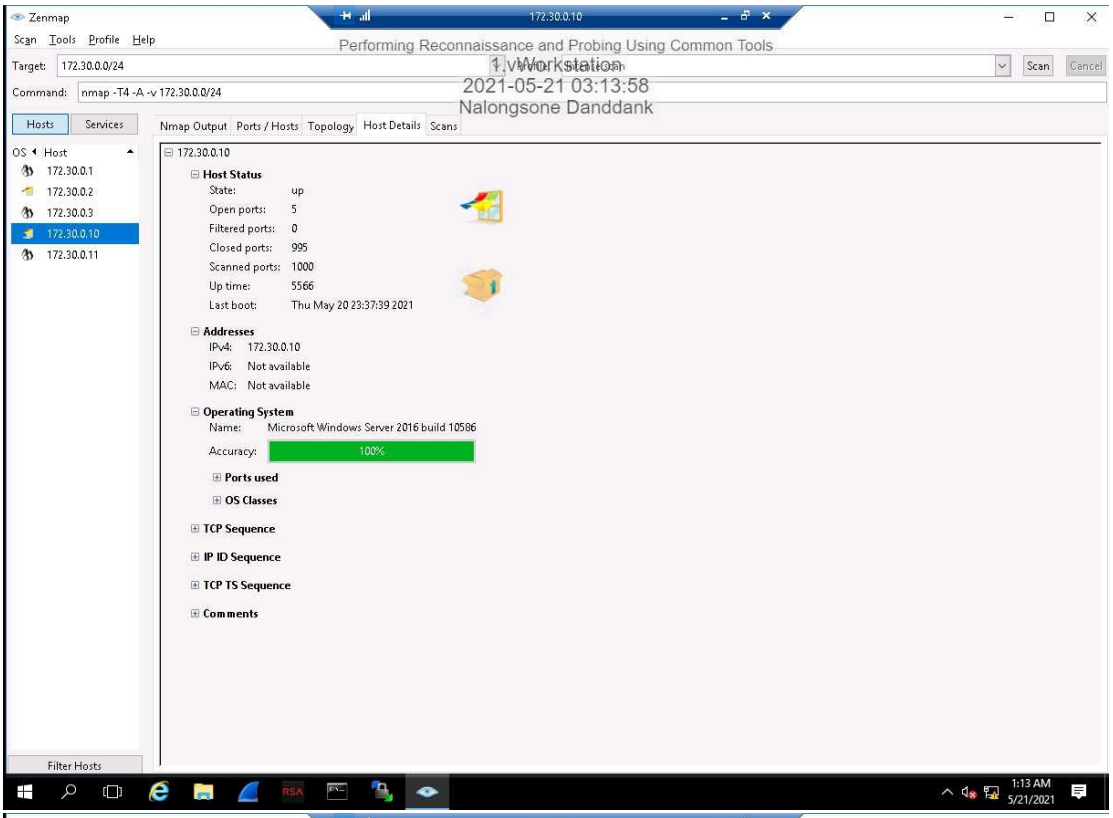

Zenmap
172.30.0.10
Scan Tools Profile Help
Performing Reconnaissance and Probing Using Common Tools
1 Workstation
2021-05-21 03:13:11
Nalongsone Danddank
Target: 172.30.0.0/24
Command: nmap -T4 -A -v 172.30.0.0/24
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
172.30.0.1
172.30.0.2
172.30.0.3
172.30.0.10
172.30.0.11
Port Protocol State Service Version
22 tcp open ssh OpenSSH 6.0p1 Debian 4+deb7u6 (protocol 2.0)
23 tcp open telnet Linux telnetd
80 tcp open http Apache httpd 2.2.22 ((Debian))
111 tcp open rpcbind 2-4 (RPC #100000)
10000 tcp open http MiniServ 1.831 (Webmin httpd)
Filter Hosts
1:13 AM
5/21/2021


Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Command: nmap -T4 -A -v 172.30.0.0/24
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
172.30.0.1
172.30.0.2
172.30.0.3
172.30.0.10
172.30.0.11
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
Filter Hosts
Performing Reconnaissance and Probing Using Common Tools
1 Workstation
2021-05-21 03:13:19
Nalongsone Danddank
1:13 AM
5/21/2021

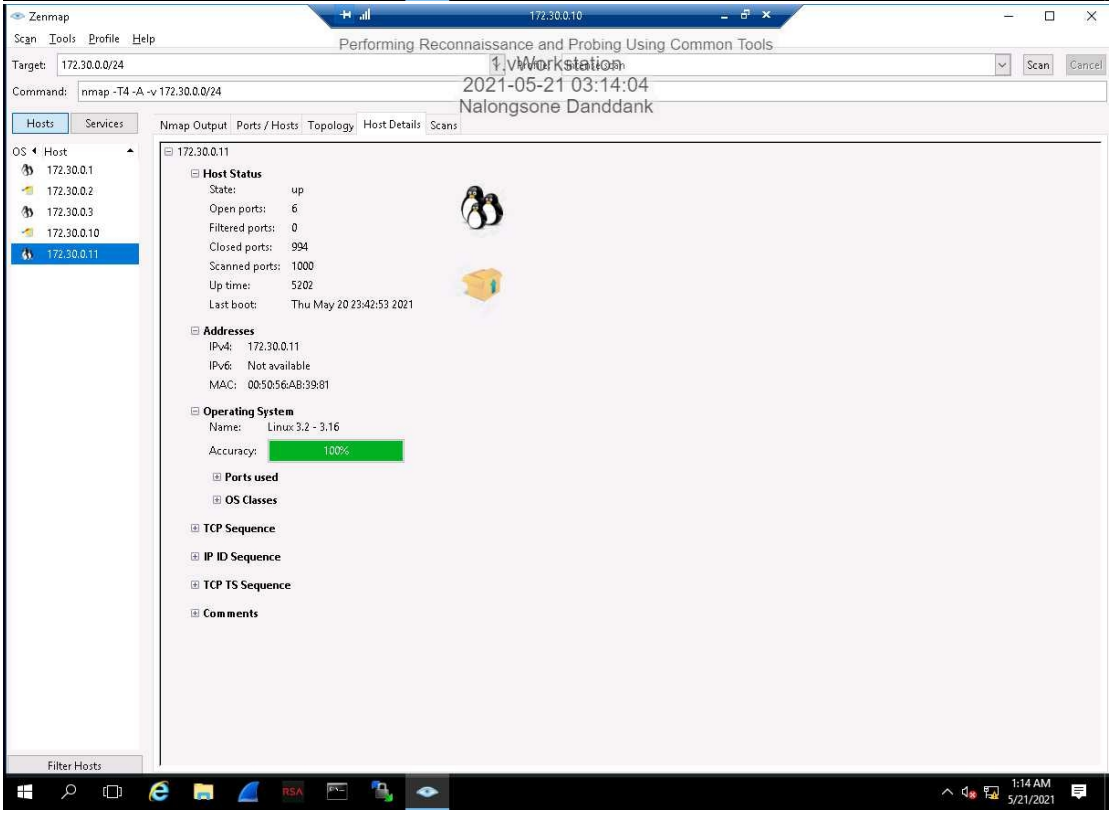

Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Command: nmap -T4 -A -v 172.30.0.0/24
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
172.30.0.1
172.30.0.2
172.30.0.3
172.30.0.10
172.30.0.11
Host Status
State: up
Open ports: 5
Filtered ports: 0
Closed ports: 995
Scanned ports: 1000
Up time: 5177
Last boot: Thu May 20 23:43:18 2021
Addresses
IPv4: 172.30.0.1
IPv6: Not available
MAC: 00:50:56:AB:A5:B2
Operating System
Name: Linux 3.2 - 3.16
Accuracy: 100%
Ports used
OS Classes
TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments
Filter Hosts
Performing Reconnaissance and Probing Using Common Tools
1 Workstation
2021-05-21 03:13:35
Nalongsone Danddank
1:13 AM
5/21/2021


Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Command: nmap -T4 -A -v 172.30.0.0/24
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS Host
172.30.0.1
172.30.0.2
172.30.0.3
172.30.0.10
172.30.0.11
172.30.0.2
Host Status
State: up
Open ports: 4
Filtered ports: 0
Closed ports: 996
Scanned ports: 1000
Up time: 5521
Last boot: Thu May 20 23:37:34 2021
Addresses
IPv4: 172.30.0.2
IPv6: Not available
MAC: 00:50:56:AB:FE:BC
Operating System
Name: Microsoft Windows Server 2016 build 10586
Accuracy: 100%
Ports used
OS Classes
TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments
Filter Hosts
Performing Reconnaissance and Probing Using Common Tools
1 vWorkstation
2021-05-21 03:13:41
Nalongsone Danddank
1:13 AM
5/21/2021

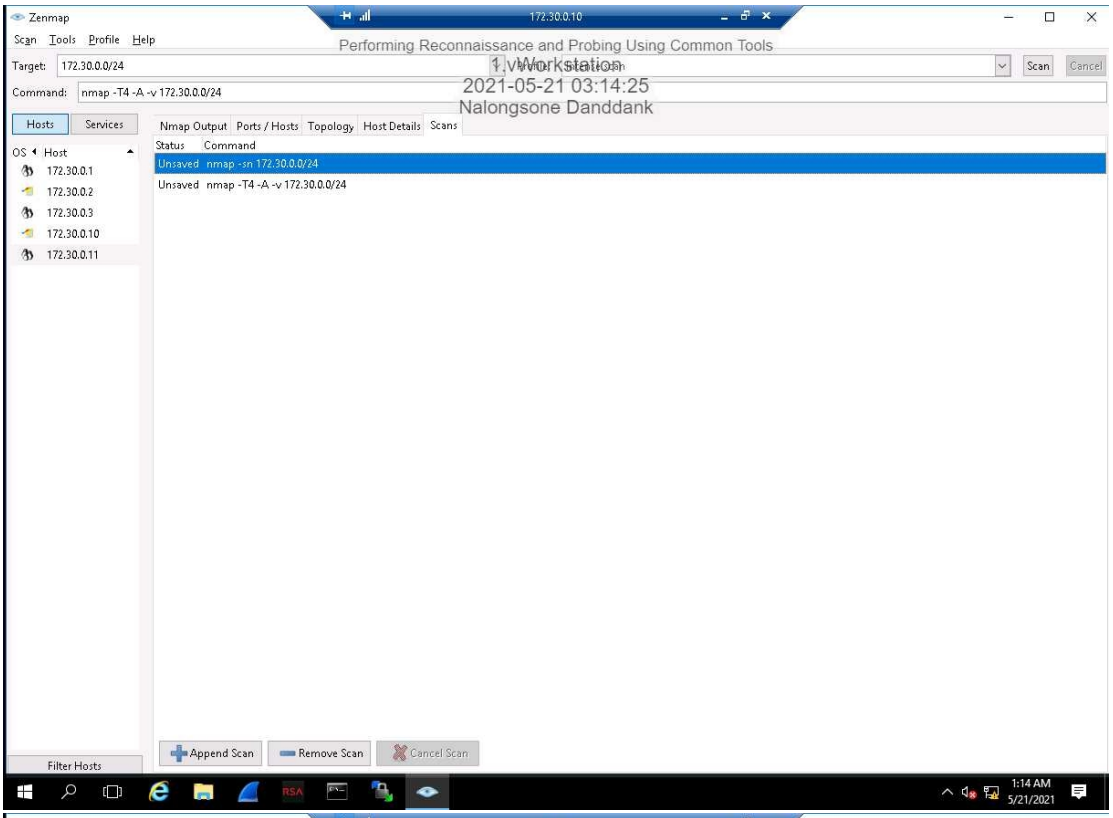

Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Command: nmap -T4 -A -v 172.30.0.0/24
Scan
Cancel
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS Host
172.30.0.1
172.30.0.2
172.30.0.3
172.30.0.10
172.30.0.11
172.30.0.3
Host Status
State: up
Open ports: 5
Filtered ports: 0
Closed ports: 995
Scanned ports: 1000
Up time: 5177
Last boot: Thu May 20 23:43:18 2021
Addresses
IPv4: 172.30.0.3
IPv6: Not available
MAC: 00:50:56:AB:A5:B2
Operating System
Name: Linux 3.2 - 3.16
Accuracy: 100%
Ports used
OS Classes
TCP Sequence
IP ID Sequence
TCP TS Sequence
Comments
Filter Hosts
Performing Reconnaissance and Probing Using Common Tools
1 vWorkstation
2021-05-21 03:13:50
Nalongsone Danddank
1:13 AM
5/21/2021

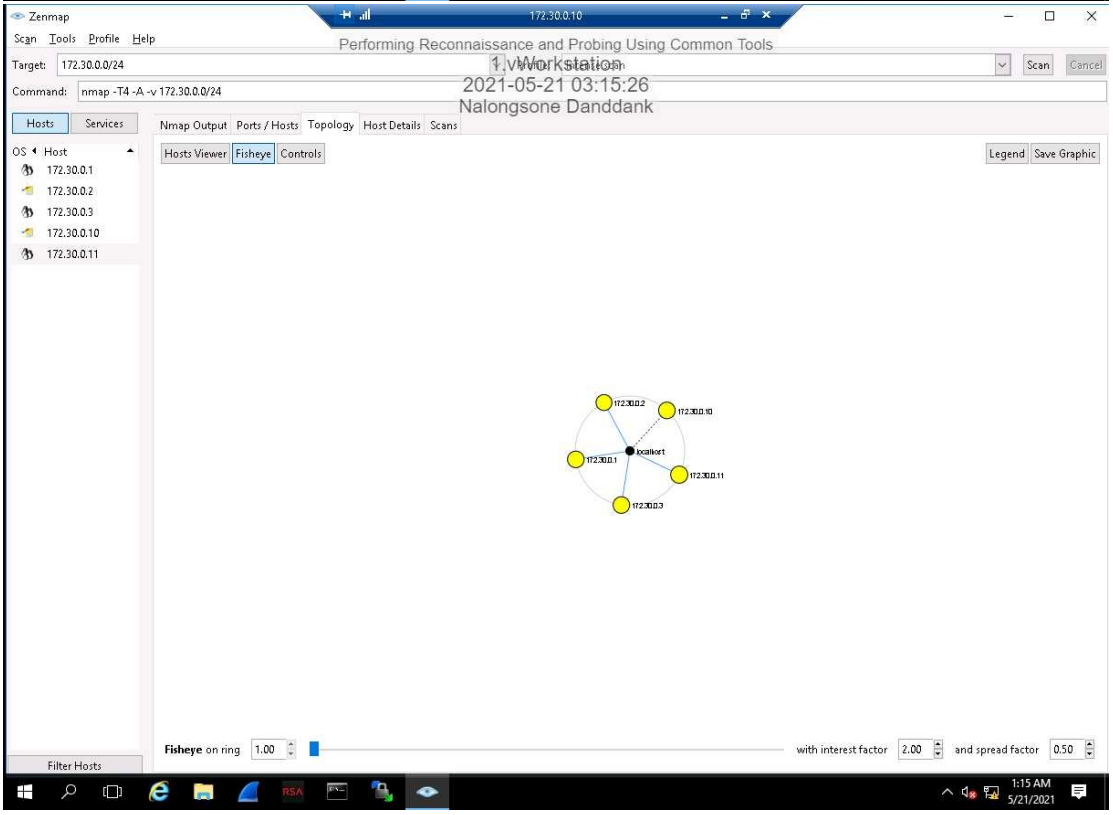


Performing Reconnaissance and Probing Using Common Tools
1 vWorkstation
2021-05-21 03:13:58
Nalongsone Danddank



Performing Reconnaissance and Probing Using Common Tools
1 vWorkstation
2021-05-21 03:14:04
Nalongsone Danddank


Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Command: nmap -T4 -A -v 172.30.0.0/24
Scan
Cancel
Hosts
Services
OS Host
172.30.0.1
172.30.0.2
172.30.0.3
172.30.0.10
172.30.0.11
Nmap Output Ports / Hosts Topology Host Details Scans
Status Command
Unsaved nmap -sn 172.30.0.0/24
Unsaved nmap -T4 -A -v 172.30.0.0/24
Append Scan
Remove Scan
Cancel Scan
Filter Hosts
Performing Reconnaissance and Probing Using Common Tools
1 Workstation
2021-05-21 03:14:25
Nalongsone Danddank
1:14 AM
5/21/2021


Zenmap
Scan Tools Profile Help
Target: 172.30.0.0/24
Command: nmap -T4 -A -v 172.30.0.0/24
Scan
Cancel
Hosts
Services
OS Host
172.30.0.1
172.30.0.2
172.30.0.3
172.30.0.10
172.30.0.11
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
Legend Save Graphic
localhost
Fisheye on ring 1.00
with interest factor 2.00
and spread factor 0.50
Filter Hosts
Performing Reconnaissance and Probing Using Common Tools
1 Workstation
2021-05-21 03:15:26
Nalongsone Danddank
1:15 AM
5/21/2021

Resized Fisheye Bubble Chart