

Lab #1 Report

Frame detail for ICMP traffic

Capturing from 2 interfaces

File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

Performing Reconnaissance and Probing Using Common Tools

1.vWorkstation

2021-05-20 22:44:21

Apply a display filter ... <Ctrl+>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Vmware_ab:f8:25	Broadcast	ARP	42	Who has 172.18.0.1 tell 172.18.0.99
2	0.000385	Vmware_ab:f8:25	Vmware_ab:f8:25	ARP	60	172.18.0.1 is at 00:50:56:ab:81:1c
3	0.000429	172.18.0.99	172.18.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 4)
4	0.000542	172.18.0.1	172.18.0.99	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 3)
5	0.009917	172.18.0.99	172.18.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 6)
6	0.010257	172.18.0.1	172.18.0.99	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 5)
7	0.025477	172.18.0.99	172.18.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 8)
8	0.025826	172.18.0.1	172.18.0.99	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 7)
9	0.041108	172.18.0.99	172.18.0.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 10)
10	0.041413	172.18.0.1	172.18.0.99	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 9)
11	5.011436	Vmware_ab:81:1c	Vmware_ab:f8:25	ARP	60	Who has 172.18.0.99? Tell 172.18.0.1
12	5.011502	Vmware_ab:f8:25	Vmware_ab:81:1c	ARP	42	172.18.0.99 is at 00:50:56:ab:f8:25
13	309.176773	172.16.0.99	172.16.0.255	BROWSER	243	Host Announcement vWORKSTATION, Workstation, Server, NT Workstation, Server, NT Workstation, Server, NT Workstation, NT Server
14	320.019323	172.16.0.99	172.16.0.255	BROWSER	243	Host Announcement TARGETNTWINDOWS02, Workstation, Server, NT Workstation, Server, NT Workstation, NT Server

Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 1

Interface 1: (DeviceNPF_{414269F4-8DF0-4E52-8F56-384E405060F3})

Encapsulation type: Ethernet (1)

Arrival Time: May 20, 2021 20:30:46.710075000 Pacific Daylight Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1621567846.710075000 seconds

[Time delta from previous captured frame: 0.0000044000 seconds]

[Time delta from previous displayed frame: 0.0000044000 seconds]

[Time since reference or first frame: 0.000429000 seconds]

Frame Number: 3

Frame Length: 74 bytes (592 bits)

Capture Length: 74 bytes (592 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp || icmpv6]

> Ethernet II, Src: Vmware_ab:f8:25 (00:50:56:ab:f8:25), Dst: Vmware_ab:81:1c (00:50:56:ab:81:1c)

Absolute time when this frame was captured (frame.time): 2021-05-20 20:30:46.710075000

Packets: 14 · Displayed: 14 (100.0%)

Profile: Default

8:44 PM

Demo Collection viewed in NetWitness Investigator

NetWitness Investigator 1.0

Collection Edit View Bookmarks History Help

Performing Reconnaissance and Probing Using Common Tools

1.vWorkstation

2021-05-20 23:01:34

Nalongsone Danddank

< 2008-11-14 14:50

2008-11-14 15:06 :

Crypto (1 item)
rsa-with-rc4-128-md5 (1)

Database Name (5 items)
msdb (1) - master (1) - fe_db (1) - discovery_db (1) - ? (1)

Group (2 items)
#omega (1) - #it (1)

Referer [open]

Ethernet Source (8 items)
00:16:CB:9E:16:A8 (20) - 00:11:0A:A4:3C:98 (3) - 00:0B:DB:0F:46:C1 (3) - 00:B0:D0:A5:87:AB (1) - 00:50:DA:04:E7:F7 (1) - 00:1F:C6:2B:FA:F6 (1) - 00:1A:70:8E:69:0D (1) - 00:01:03:C5:66:6A (1)

Ethernet Destination (5 items)
00:1A:70:8E:69:0D (26) - 00:05:32:83:23:CF (2) - 00:A0:CC:51:A9:C9 (1) - 00:0F:B5:0E:B5:A3 (1) - 00:04:F2:05:6C:CO (1)

IP Aliases [open]

SQL Query [open]

The following report(s) contain 0 results for the active query:

Decoder, Source, Alerts, Risk, Informational, Risk Suspicious, Risk Warning, Source IPv6 Address, Destination IPv6 address, Errors, Forensic Fingerprint, Server Application, Operating System, Versions, Browsers, Languages, Found Search, Active Directory Username Source, Active Directory Username Destination, Active Directory Workstation Source, Active Directory Workstation Destination, Active Directory Domain Source, Active Directory Domain Destination, Source Domain, IPv6 Protocol, Organization, Source Filename, Site Category, Alert ID, IP Address, Destination Port, Source User Account, Destination User Account, Virus Name, Device Type, Device IP, Device IPv6, Device Host, Device Class, Device Address, Device Name, Event Type, Event Source, Event Description, Event Subject, Event Activity, Event Theme, Event Outcome, Event Category Name, Parse Error, Reference ID, Message, Result Code, Logon Type, Message ID, Process, Object Name, Object Type, Source E-mail Address, Destination E-mail Address, Policy Name, Category, Filter, Access Point

9:01 PM
5/20/2021

Vulnerability report

172.30.0.10 Performing Reconnaissance and Probing Using Common Tools 1.vWorkstation 2021-05-20 23:26:57 administrator

Nalongsone_51_BasicScan CURRENT RESULTS TODAY AT 9:20 PM

Scans > Hosts Vulnerabilities 24 Notes History

Severity	Plugin Name	Plugin Family	Count
MEDIUM	SSH Weak Algorithms Supported	Misc.	1
MEDIUM	Terminal Services Doesn't Use Network Level Authenti...	Misc.	1
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1
LOW	SSH Weak MAC Algorithms Enabled	Misc.	1
INFO	RPC Services Enumeration	Service detection	4
INFO	Nessus SYN scanner	Port scanners	3
INFO	Backported Security Patch Detection (SSH)	General	1
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	mDNS Detection (Local Network)	Service detection	1
INFO	Nessus Scan Information	Settings	1

Scan Details

Name: Nalongsone_51_BasicScan
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Folder: My Scans
Start: Today at 9:20 PM
End: Today at 9:23 PM
Elapsed: 3 minutes
Targets: 172.30.0.11

Vulnerabilities

Medium
Low
Info

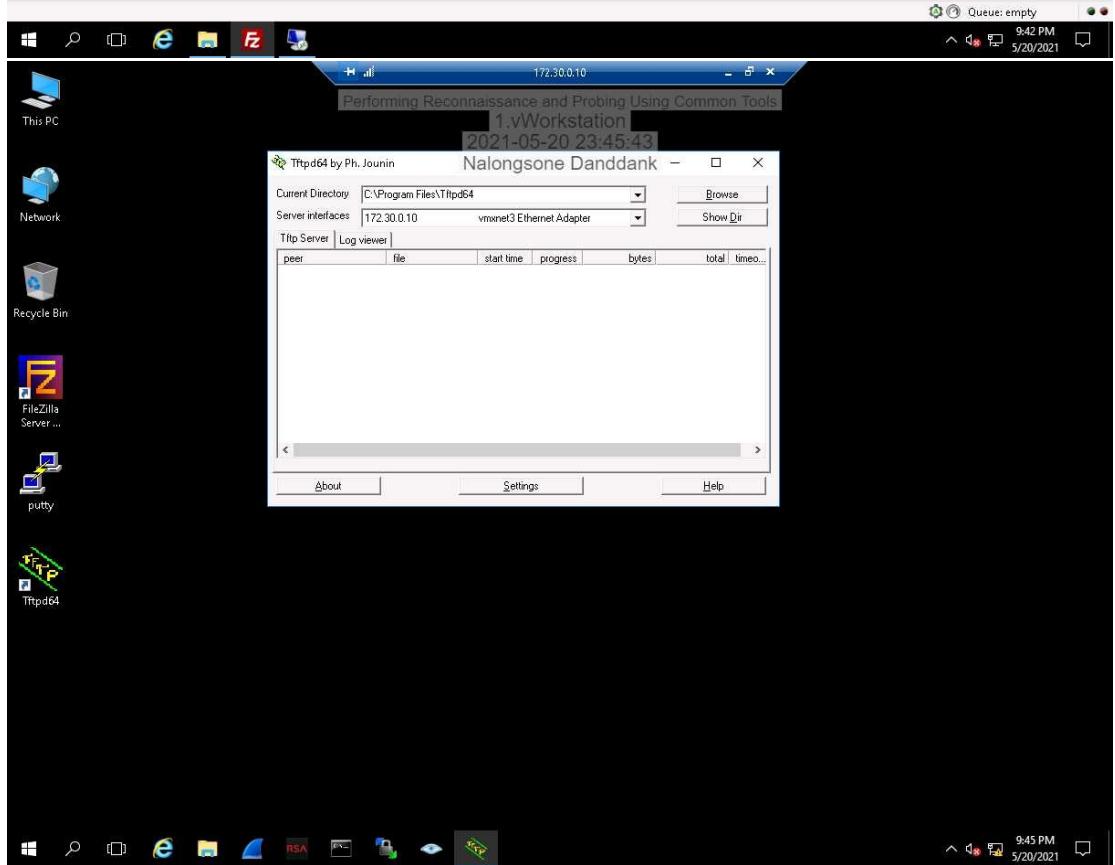
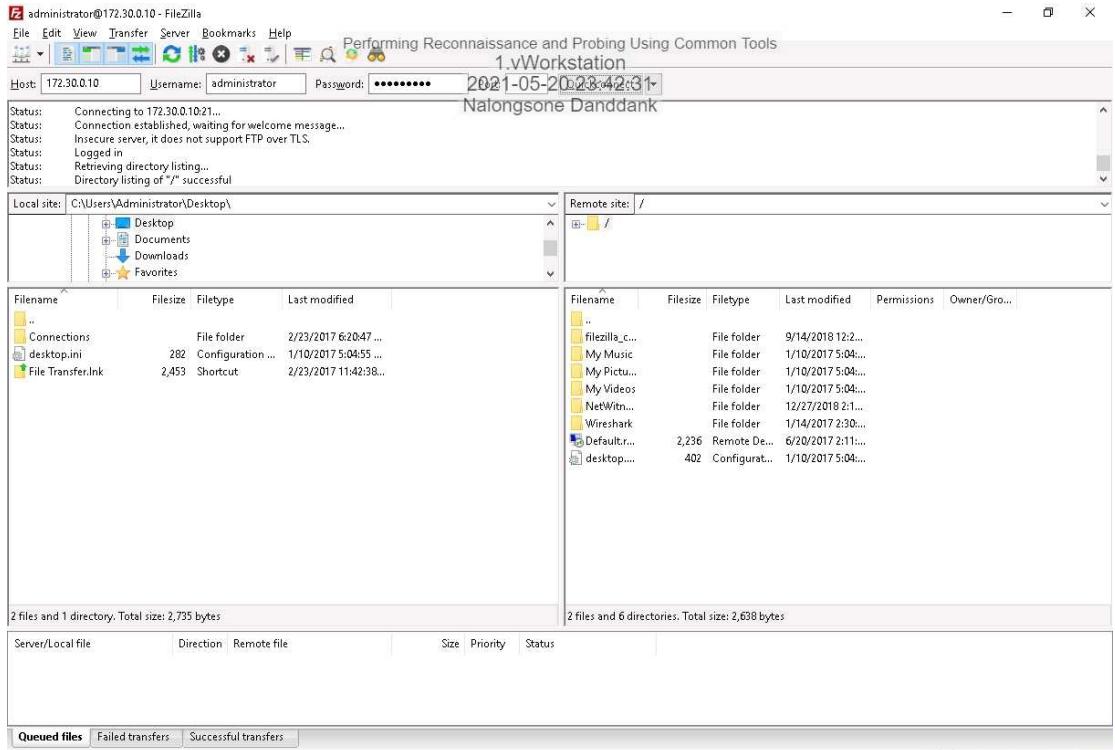
172.30.0.10 Performing Reconnaissance and Probing Using Common Tools 1.vWorkstation 2021-05-20 23:41:54 Nalongsone Danddank

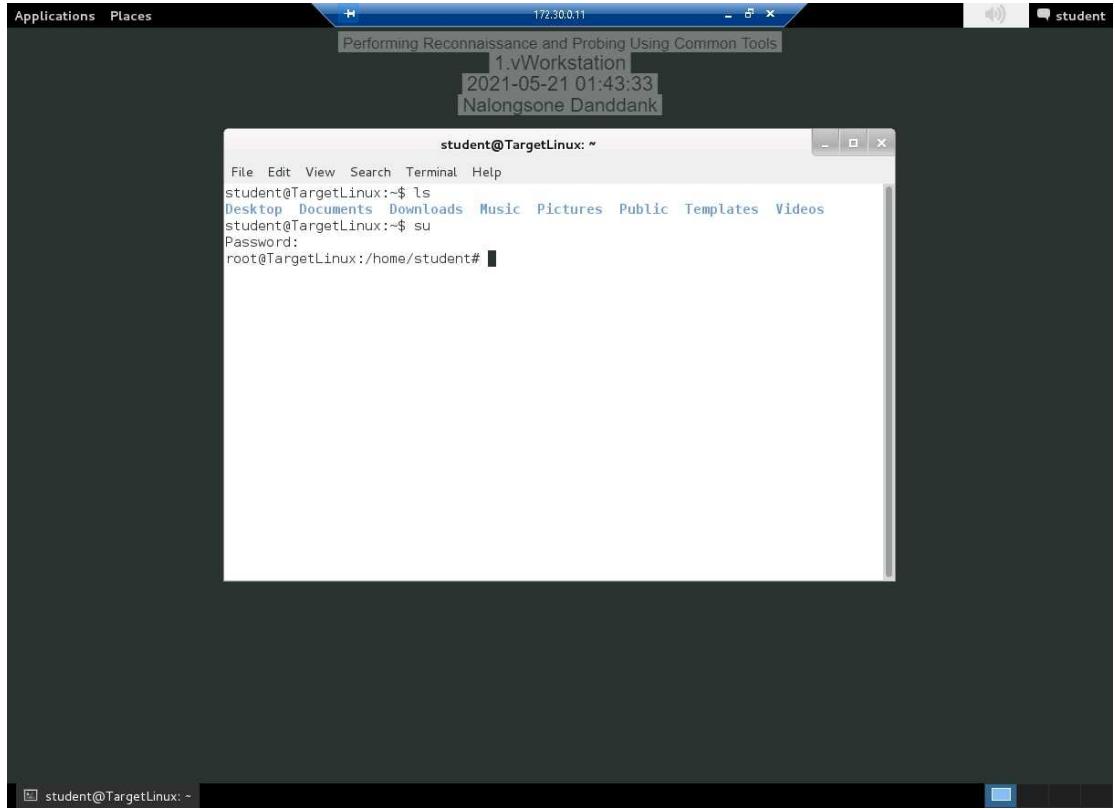
This PC Network Recycle Bin FileZilla Server (127.0.0.1) File Server Edit ? /c/ c:\

FileZilla Server version 0.9.45 beta Copyright 2001-2014 by Tim Kosse (tim.kosse@filezilla-project.org) https://filezilla-project.org/ Connected to server. Connected to server. Connected, waiting for authentication Logged on [000002] [5/20/2021 21:41:33 PM] - administrator [172.30.0.2] disconnected. [000003] [5/20/2021 21:41:33 PM] - (not logged in) [172.30.0.2] - Connected, sending welcome message... [000004] [5/20/2021 21:41:33 PM] - (not logged in) [172.30.0.2] - 220 FileZilla Server version 0.9.45 beta [000005] [5/20/2021 21:41:33 PM] - (not logged in) [172.30.0.2] - 220 Please visit http://sourceforge.net/projects/filezilla/ [000006] [5/20/2021 21:41:33 PM] - (not logged in) [172.30.0.2] - AUTH TLS [000007] [5/20/2021 21:41:33 PM] - (not logged in) [172.30.0.2] - 502 SSL/TLS authentication not allowed [000008] [5/20/2021 21:41:33 PM] - (not logged in) [172.30.0.2] - AUTH SSL [000009] [5/20/2021 21:41:33 PM] - (not logged in) [172.30.0.2] - 502 SSL/TLS authentication not allowed [00000A] [5/20/2021 21:41:33 PM] - (not logged in) [172.30.0.2] - USER administrator [00000B] [5/20/2021 21:41:33 PM] - (not logged in) [172.30.0.2] - 33 Password required for administrator [00000C] [5/20/2021 21:41:33 PM] - (not logged in) [172.30.0.2] - PASS [00000D] [5/20/2021 21:41:33 PM] - administrator [172.30.0.2] - 230 Logged on [00000E] [5/20/2021 21:41:33 PM] - administrator [172.30.0.2] - PWD [00000F] [5/20/2021 21:41:33 PM] - administrator [172.30.0.2] - 257 "/" is current directory.

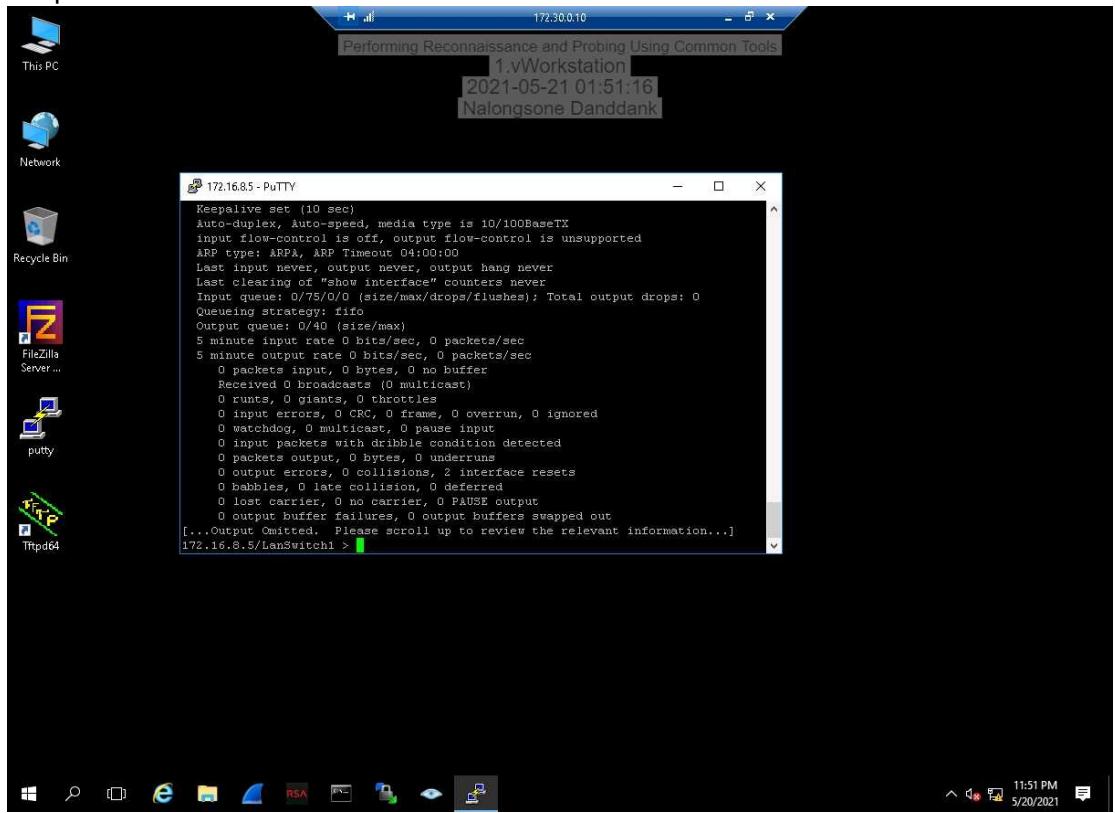
ID	Account	IP	Transfer	Progress	Speed
000003	administrator	172.30.0.2			

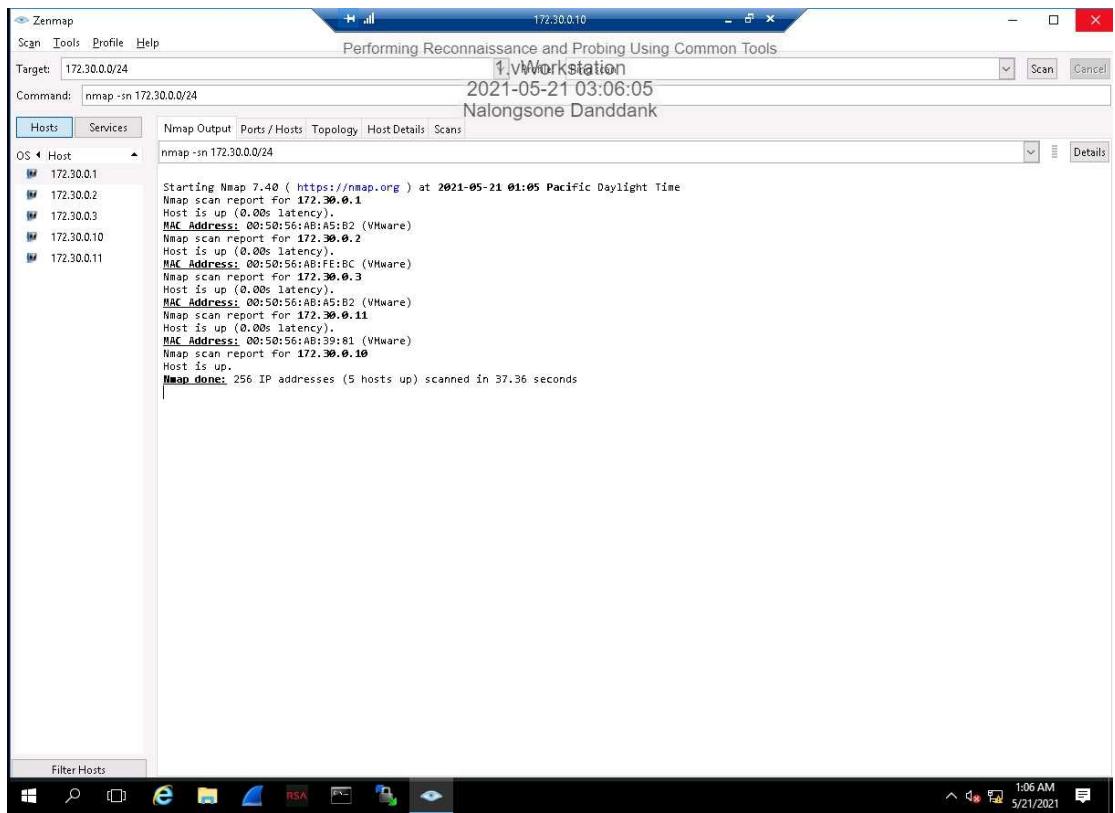
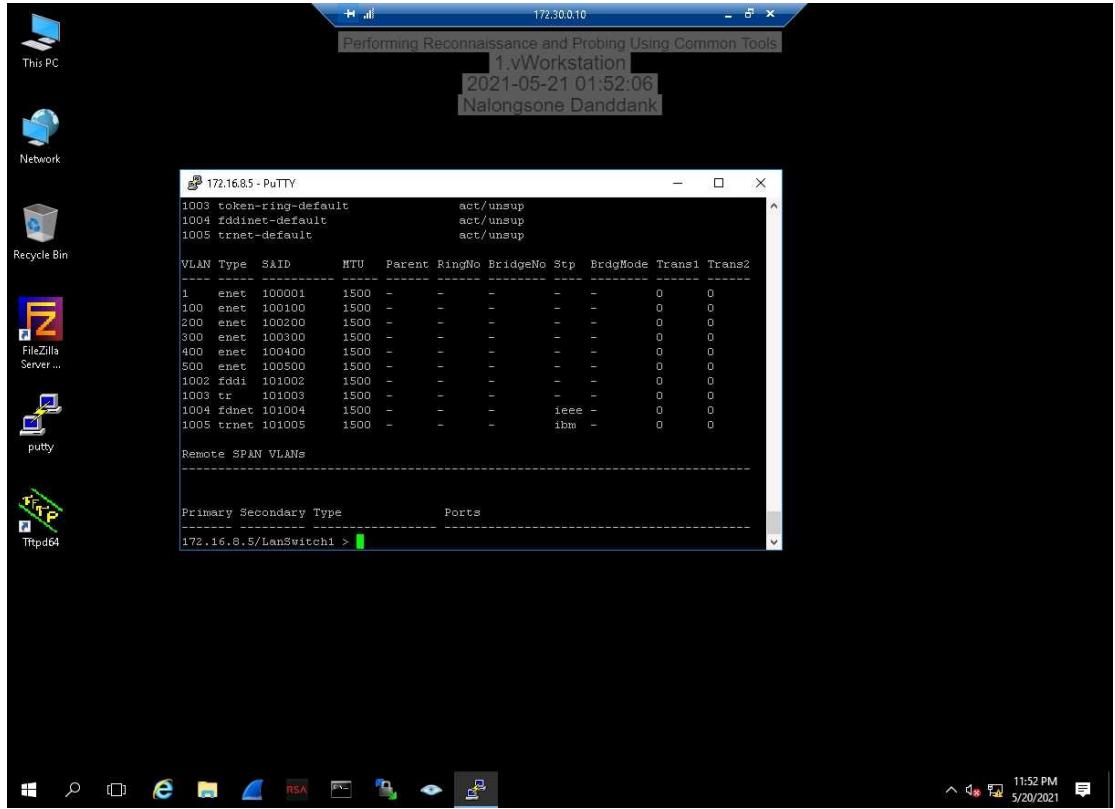
Ready 61 bytes received: 0 B/s 330 bytes sent: 0 B/s 9:41 PM 5/20/2021





Output from show interface command





Intense scan

Zenmap

Scan Tools Profile Help

Target: 172.30.0.0/24

Command: nmap -T4 -A -v 172.30.0.0/24

1 Workstation 2021-05-21 03:10:54 Nalongsone Danddank

Hosts **Services** Nmap Output Ports/Hosts Topology Host Details Scans

```
nmap -T4 -A -v 172.30.0.0/24
[...]
|_s1-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:7fb:b1:63:4f: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:d1:c1:16:63: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 (244.89KB) | Rcvd: 6120 (252.86KB)
```

Filter Hosts

172.30.0.10 1:10 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

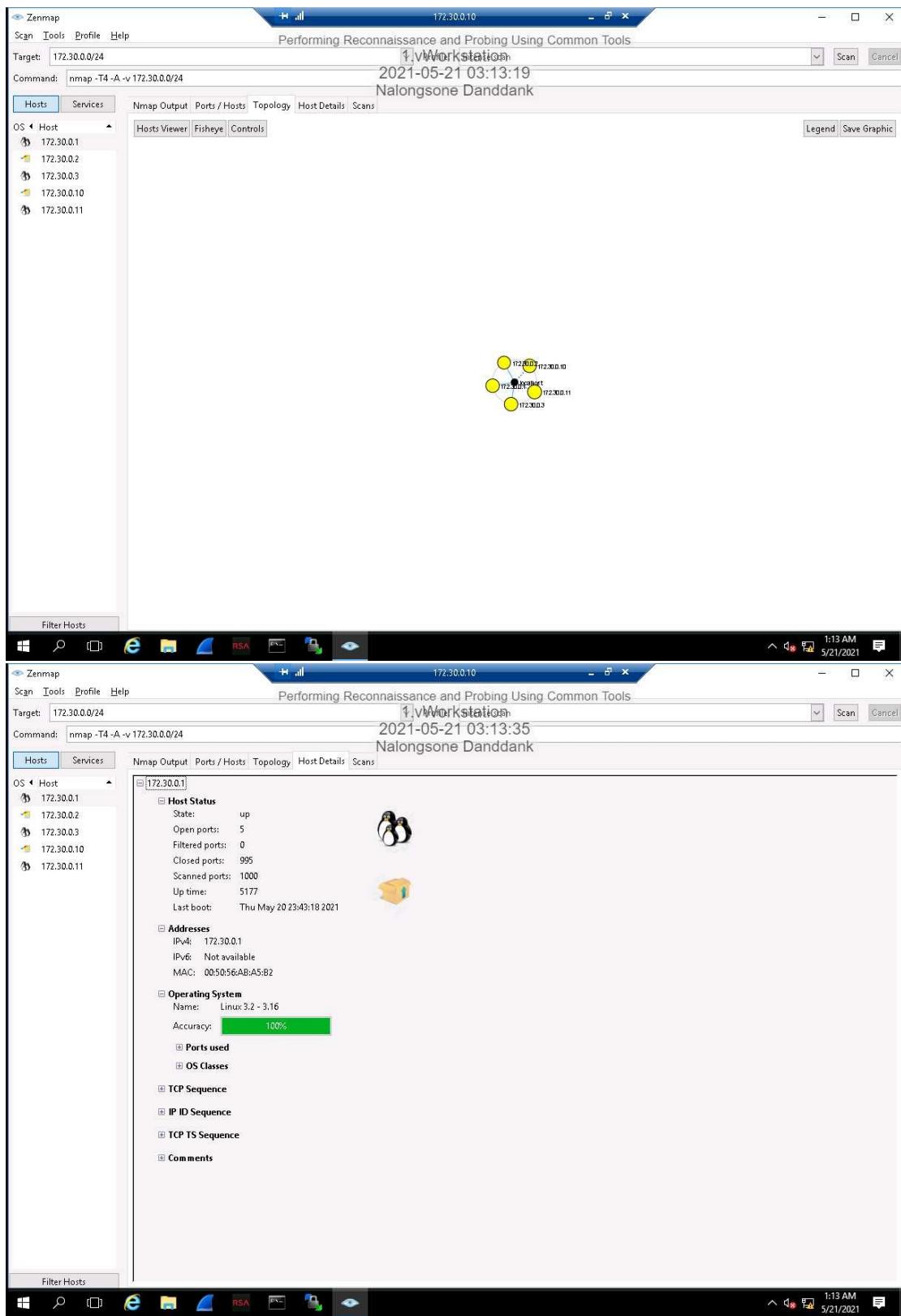
1 Workstation 2021-05-21 03:13:11 Nalongsone Danddank

Hosts **Services** Nmap Output **Ports/Hosts** Topology Host Details Scans

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 #10000)
10000	tcp	open	http	MiniServ 1.831 (Webmin httpd)

Filter Hosts

172.30.0.10 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

1 Workstation
2021-05-21 03:13:41
Nalongsone Danddank

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

172.30.0.10

1 Workstation
2021-05-21 03:13:50
Nalongsone Danddank

Scan Tools Profile Help

Target: 172.30.0.0/24

Command: nmap -T4 -A -v 172.30.0.0/24

1 Workstation
2021-05-21 03:13:50
Nalongsone Danddank

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

172.30.0.10

1 Workstation
2021-05-21 03:13:50
Nalongsone Danddank

Scan Tools Profile Help

Target: 172.30.0.0/24

Command: nmap -T4 -A -v 172.30.0.0/24

1 Workstation
2021-05-21 03:13:50
Nalongsone Danddank

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

Zenmap

Scan Tools Profile Help

Target: 172.30.0.0/24

Command: nmap -T4 -A -v 172.30.0.0/24

1 Workstation
2021-05-21 03:13:58
Nalongsone Danddank

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

172.30.0.10

Host Status

State:	up
Open ports:	5
Filtered ports:	0
Closed ports:	995
Scanned ports:	1000
Up time:	5566
Last boot:	Thu May 20 23:37:39 2021

Addresses

IPv4:	172.30.0.10
IPv6:	Not available
MAC:	Not available

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

172.30.0.10 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

1 Workstation
2021-05-21 03:14:04
Nalongsone Danddank

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**

172.30.0.11

Host Status

State:	up
Open ports:	6
Filtered ports:	0
Closed ports:	994
Scanned ports:	1000
Up time:	5202
Last boot:	Thu May 20 23:42:53 2021

Addresses

IPv4:	172.30.0.11
IPv6:	Not available
MAC:	00:50:56:AB:39:81

Operating System

Name:	Linux 3.2 - 3.16
Accuracy:	100%

Ports used

OS Classes

TCP Sequence

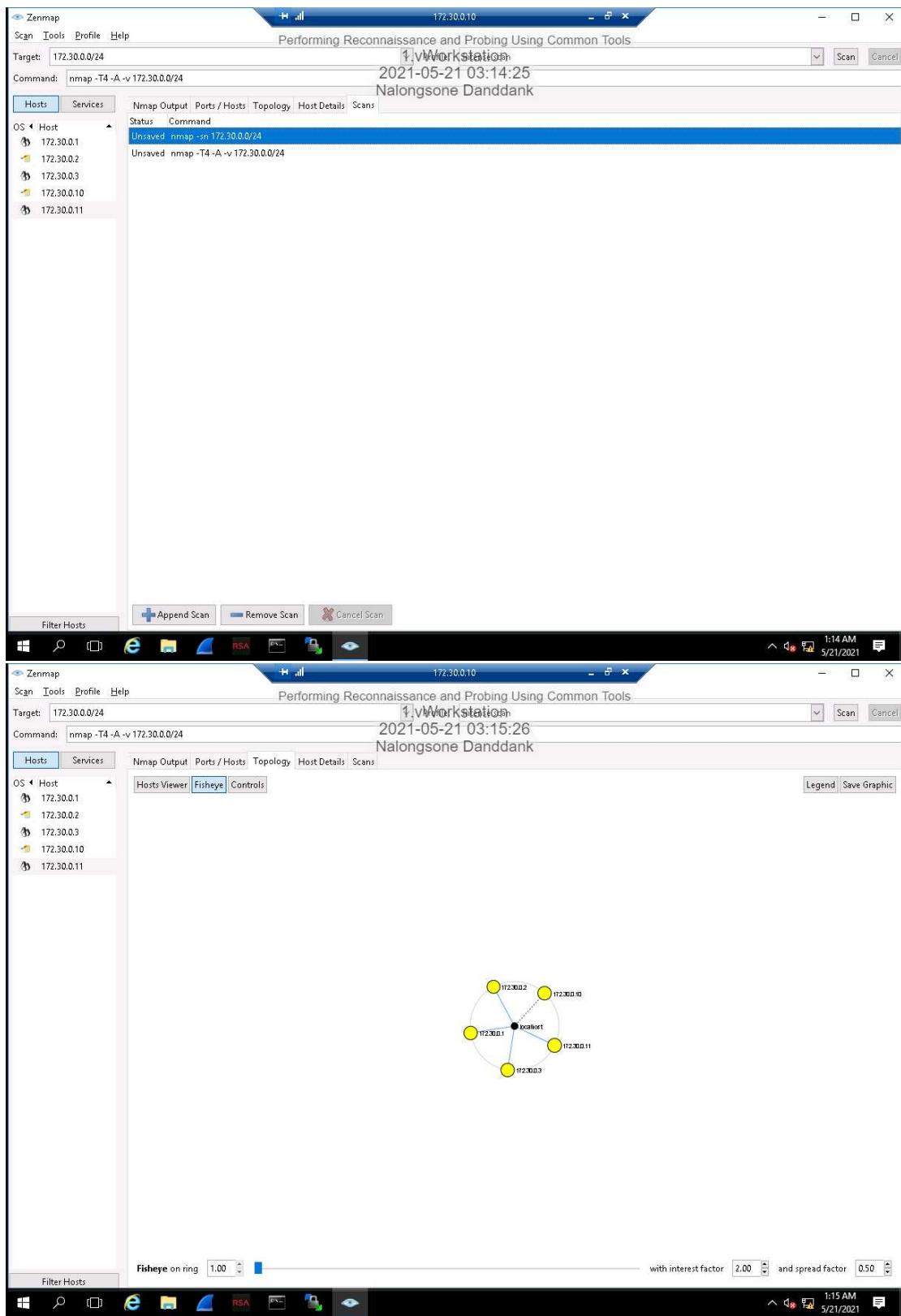
IP ID Sequence

TCP TS Sequence

Comments

Filter Hosts

172.30.0.11 1:14 AM 5/21/2021



Resized Fisheye Bubble Chart

