Pentesting

Security Project report

Moeez Javed	BCS203213
Fouzan Sohail	BCS203168
Saeed Anwar	BCS203227
Ali Abbas Khan	BCS203124

Lecturer:

Ms. Yafra Khan

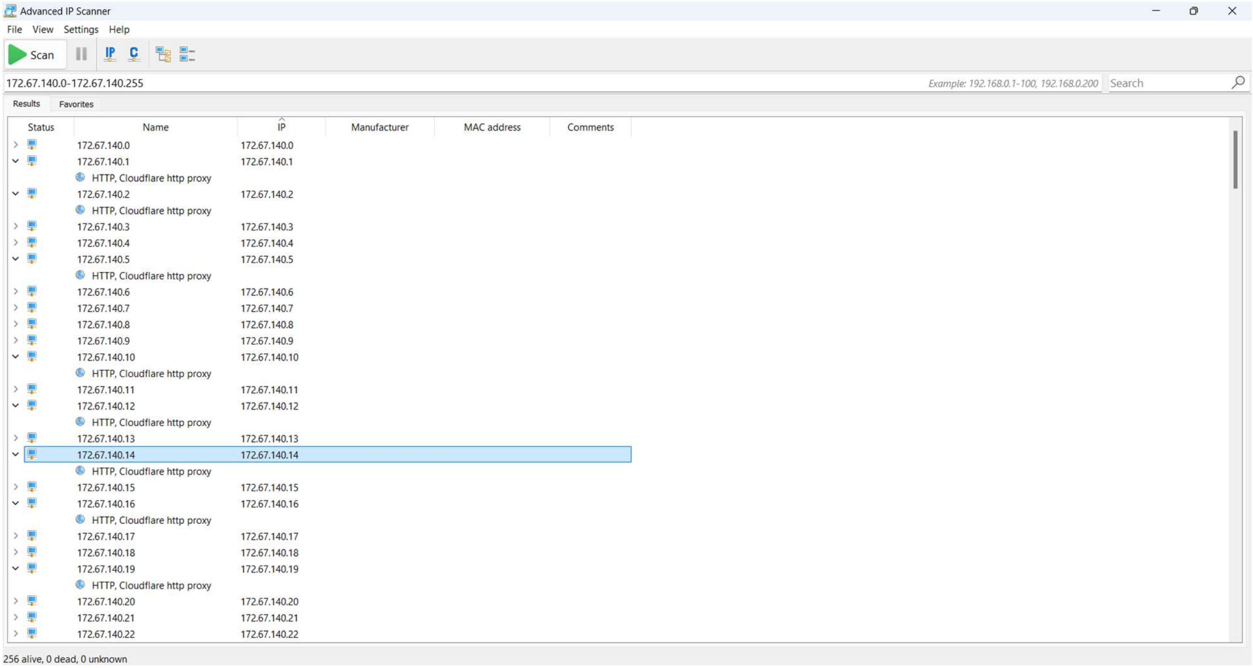
1.Project Overview

Angry IP Scanner offers swift and detailed network scanning capabilities, Nmap's OS detection feature enhances reconnaissance efforts, and FPing efficiently assesses host reachability, collectively serving as essential tools for network management and security.

Advanced IP Scanner

Advanced IP Scanner is a free network scanning tool developed by Famatech. It allows users to scan their local network and retrieve information about connected devices, including their IP addresses, MAC addresses, and network shares. The software also provides additional features such as remote control capabilities, Wake-On-LAN support, and the ability to shut down computers remotely. Advanced IP Scanner is designed to be user-friendly and efficient, making it a popular choice for network administrators and home users alike.

Screenshot:



172.67.140.0-172.67.140.255

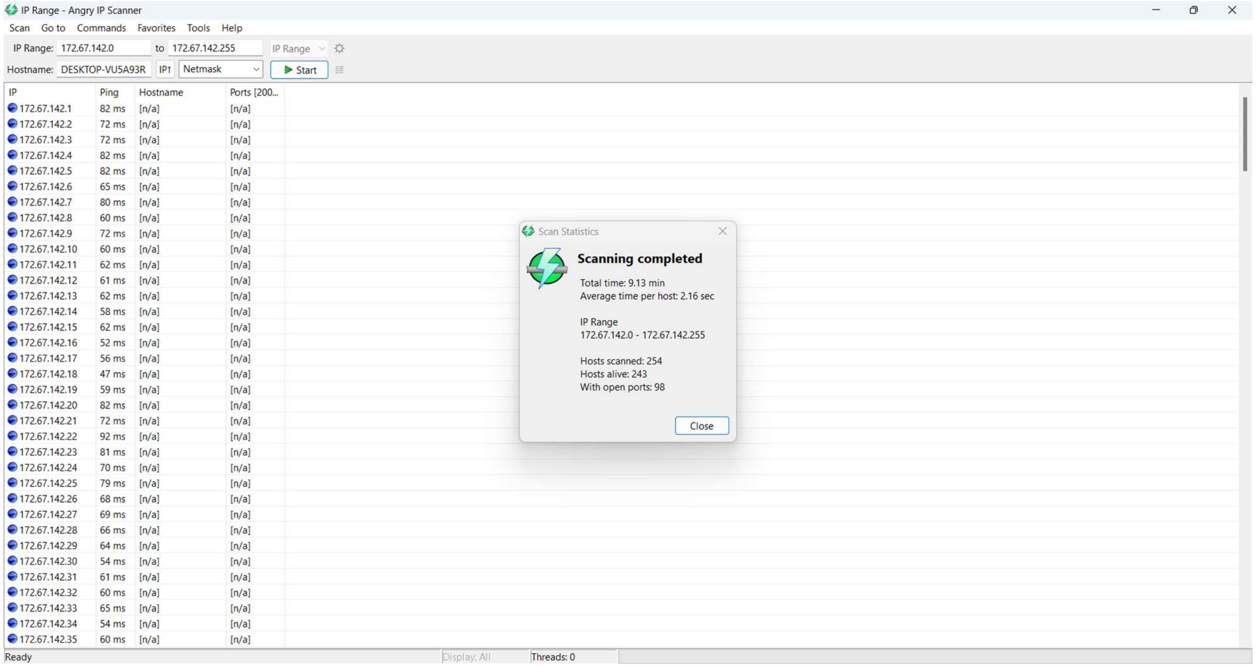
Status	Name	IP	Manufacturer	MAC address	Comments
	172.67.140.0	172.67.140.0			
	172.67.140.1	172.67.140.1			
	HTTP, Cloudflare http proxy				
	172.67.140.2	172.67.140.2			
	HTTP, Cloudflare http proxy				
	172.67.140.3	172.67.140.3			
	172.67.140.4	172.67.140.4			
	172.67.140.5	172.67.140.5			
	HTTP, Cloudflare http proxy				
	172.67.140.6	172.67.140.6			
	172.67.140.7	172.67.140.7			
	172.67.140.8	172.67.140.8			
	172.67.140.9	172.67.140.9			
	172.67.140.10	172.67.140.10			
	HTTP, Cloudflare http proxy				
	172.67.140.11	172.67.140.11			
	172.67.140.12	172.67.140.12			
	HTTP, Cloudflare http proxy				
	172.67.140.13	172.67.140.13			
	172.67.140.14	172.67.140.14			
	HTTP, Cloudflare http proxy				
	172.67.140.15	172.67.140.15			
	172.67.140.16	172.67.140.16			
	HTTP, Cloudflare http proxy				
	172.67.140.17	172.67.140.17			
	172.67.140.18	172.67.140.18			
	172.67.140.19	172.67.140.19			
	HTTP, Cloudflare http proxy				
	172.67.140.20	172.67.140.20			
	172.67.140.21	172.67.140.21			
	172.67.140.22	172.67.140.22			

256 alive, 0 dead, 0 unknown

Angry IP Scanner

Angry IP Scanner is a powerful and lightweight network scanner designed to swiftly scan IP addresses and ports on local and remote networks. It provides detailed information about network devices, including hostname, MAC address, and open ports, aiding in network troubleshooting, security assessments, and system administration tasks. Its user-friendly interface and customizable scanning options make it a popular choice for both novice and advanced users.

Screenshot:



IP Range: 172.67.142.0 to 172.67.142.255

Hostname: DESKTOP-VU5A93R IP↑ Netmask

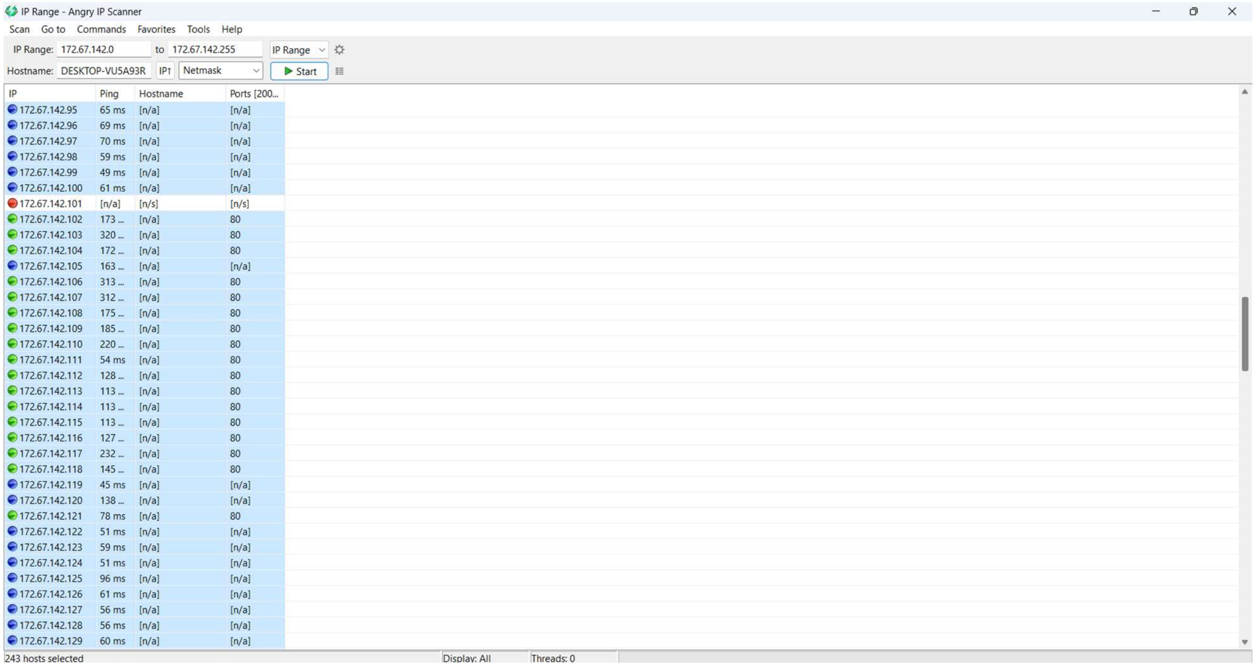
IP	Ping	Hostname	Ports [200...
172.67.142.1	82 ms	[n/a]	[n/a]
172.67.142.2	72 ms	[n/a]	[n/a]
172.67.142.3	72 ms	[n/a]	[n/a]
172.67.142.4	82 ms	[n/a]	[n/a]
172.67.142.5	82 ms	[n/a]	[n/a]
172.67.142.6	65 ms	[n/a]	[n/a]
172.67.142.7	80 ms	[n/a]	[n/a]
172.67.142.8	60 ms	[n/a]	[n/a]
172.67.142.9	72 ms	[n/a]	[n/a]
172.67.142.10	60 ms	[n/a]	[n/a]
172.67.142.11	62 ms	[n/a]	[n/a]
172.67.142.12	61 ms	[n/a]	[n/a]
172.67.142.13	62 ms	[n/a]	[n/a]
172.67.142.14	58 ms	[n/a]	[n/a]
172.67.142.15	62 ms	[n/a]	[n/a]
172.67.142.16	52 ms	[n/a]	[n/a]
172.67.142.17	56 ms	[n/a]	[n/a]
172.67.142.18	47 ms	[n/a]	[n/a]
172.67.142.19	59 ms	[n/a]	[n/a]
172.67.142.20	82 ms	[n/a]	[n/a]
172.67.142.21	72 ms	[n/a]	[n/a]
172.67.142.22	92 ms	[n/a]	[n/a]
172.67.142.23	81 ms	[n/a]	[n/a]
172.67.142.24	70 ms	[n/a]	[n/a]
172.67.142.25	79 ms	[n/a]	[n/a]
172.67.142.26	68 ms	[n/a]	[n/a]
172.67.142.27	69 ms	[n/a]	[n/a]
172.67.142.28	66 ms	[n/a]	[n/a]
172.67.142.29	64 ms	[n/a]	[n/a]
172.67.142.30	54 ms	[n/a]	[n/a]
172.67.142.31	61 ms	[n/a]	[n/a]
172.67.142.32	60 ms	[n/a]	[n/a]
172.67.142.33	65 ms	[n/a]	[n/a]
172.67.142.34	54 ms	[n/a]	[n/a]
172.67.142.35	60 ms	[n/a]	[n/a]

Scanning completed

Total time: 9.13 min
Average time per host: 2.16 sec

IP Range
172.67.142.0 - 172.67.142.255

Hosts scanned: 254
Hosts alive: 243
With open ports: 98


IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help

IP Range: 172.67.142.0 to 172.67.142.255 IP Range

Hostname: DESKTOP-VU5A93R IP↑ Netmask

IP	Ping	Hostname	Ports [200...
172.67.142.95	65 ms	[n/a]	[n/a]
172.67.142.96	69 ms	[n/a]	[n/a]
172.67.142.97	70 ms	[n/a]	[n/a]
172.67.142.98	59 ms	[n/a]	[n/a]
172.67.142.99	49 ms	[n/a]	[n/a]
172.67.142.100	61 ms	[n/a]	[n/a]
172.67.142.101	[n/a]	[n/s]	[n/s]
172.67.142.102	173 ...	[n/a]	80
172.67.142.103	320 ...	[n/a]	80
172.67.142.104	172 ...	[n/a]	80
172.67.142.105	163 ...	[n/a]	[n/a]
172.67.142.106	313 ...	[n/a]	80
172.67.142.107	312 ...	[n/a]	80
172.67.142.108	175 ...	[n/a]	80
172.67.142.109	185 ...	[n/a]	80
172.67.142.110	220 ...	[n/a]	80
172.67.142.111	54 ms	[n/a]	80
172.67.142.112	128 ...	[n/a]	80
172.67.142.113	113 ...	[n/a]	80
172.67.142.114	113 ...	[n/a]	80
172.67.142.115	113 ...	[n/a]	80
172.67.142.116	127 ...	[n/a]	80
172.67.142.117	232 ...	[n/a]	80
172.67.142.118	145 ...	[n/a]	80
172.67.142.119	45 ms	[n/a]	[n/a]
172.67.142.120	138 ...	[n/a]	[n/a]
172.67.142.121	78 ms	[n/a]	80
172.67.142.122	51 ms	[n/a]	[n/a]
172.67.142.123	59 ms	[n/a]	[n/a]
172.67.142.124	51 ms	[n/a]	[n/a]
172.67.142.125	96 ms	[n/a]	[n/a]
172.67.142.126	61 ms	[n/a]	[n/a]
172.67.142.127	56 ms	[n/a]	[n/a]
172.67.142.128	56 ms	[n/a]	[n/a]
172.67.142.129	60 ms	[n/a]	[n/a]

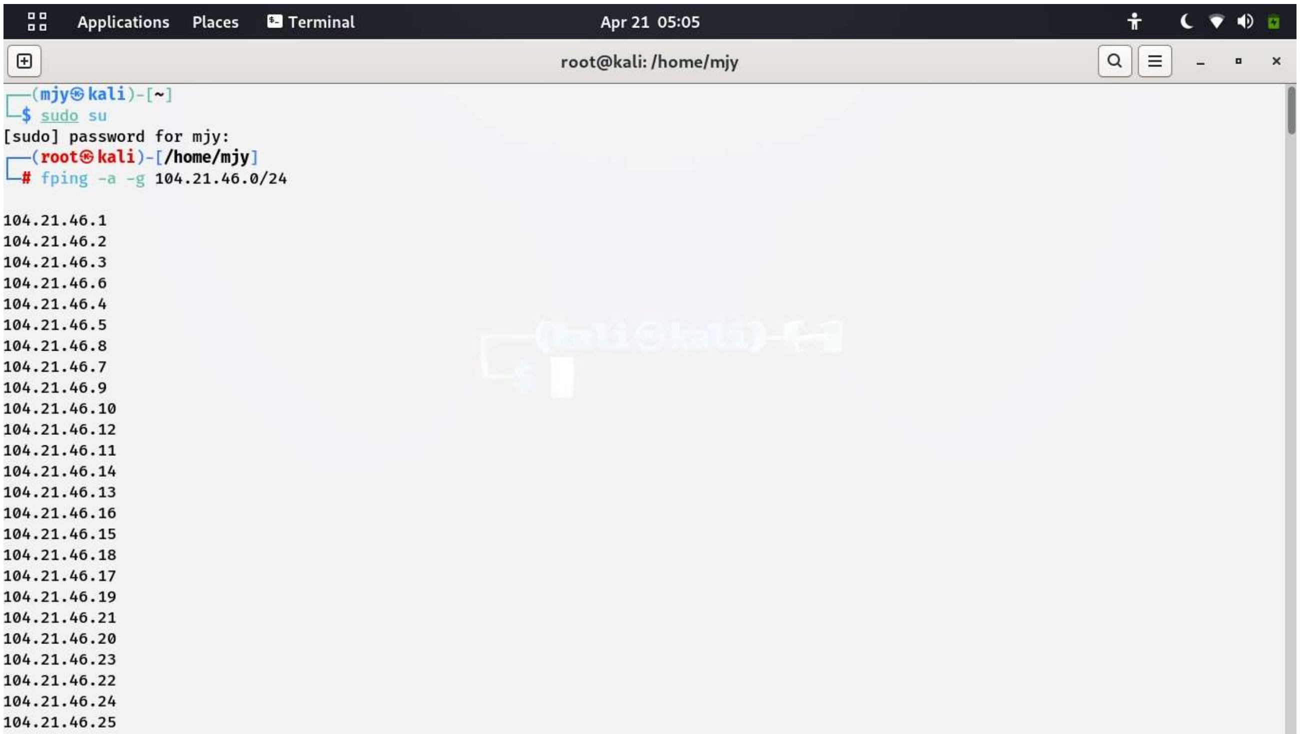
243 hosts selected   Display: All   Threads: 0

Fping:

Fping is a command-line network diagnostic tool used to check the reachability of multiple hosts in an IP network. Unlike traditional ping utilities, which typically only send ICMP echo requests to a single host at a time, FPing sends ICMP echo requests to multiple hosts simultaneously, providing a faster and more efficient way to assess the connectivity status of multiple hosts.

Fping -a -g 104.21.46.0/24

Screenshot:

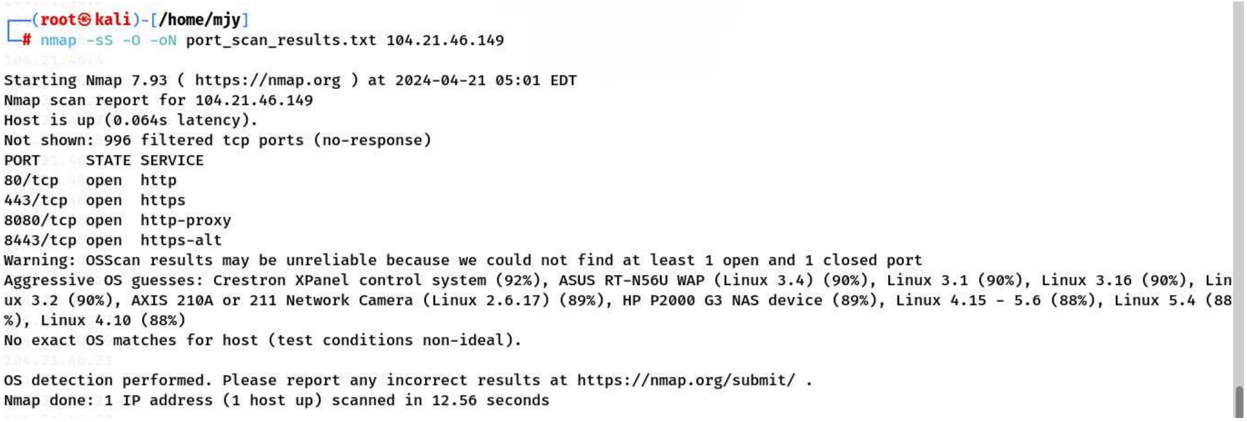


```
┌──(mjy㉿kali)-[~]
└─$ sudo su
[sudo] password for mjy:
┌──(root㉿kali)-[/home/mjy]
└─# fping -a -g 104.21.46.0/24

104.21.46.1
104.21.46.2
104.21.46.3
104.21.46.6
104.21.46.4
104.21.46.5
104.21.46.8
104.21.46.7
104.21.46.9
104.21.46.10
104.21.46.12
104.21.46.11
104.21.46.14
104.21.46.13
104.21.46.16
104.21.46.15
104.21.46.18
104.21.46.17
104.21.46.19
104.21.46.21
104.21.46.20
104.21.46.23
104.21.46.22
104.21.46.24
104.21.46.25
```

OS Detection:

Nmap -nS -o -nN port_scan_results.txt 104.21.45.149

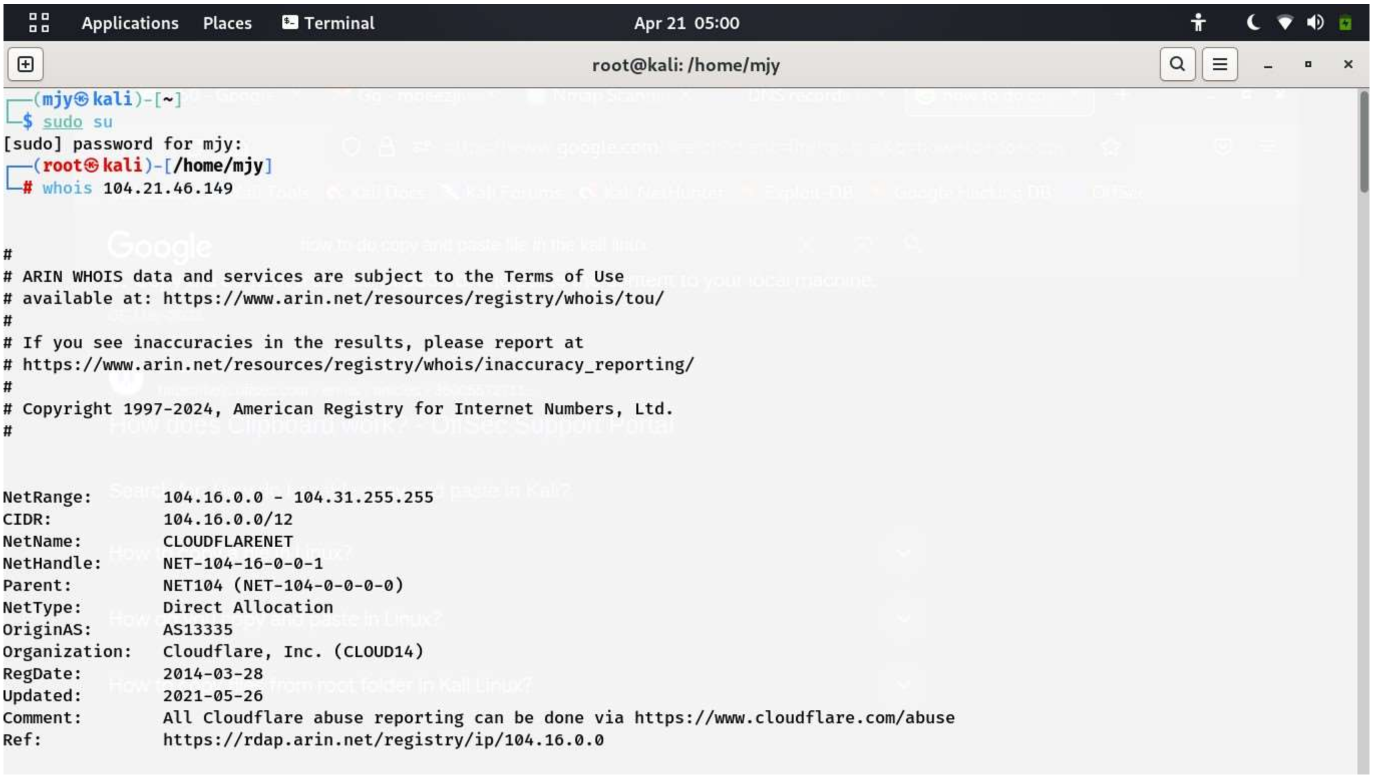
Screenshot:



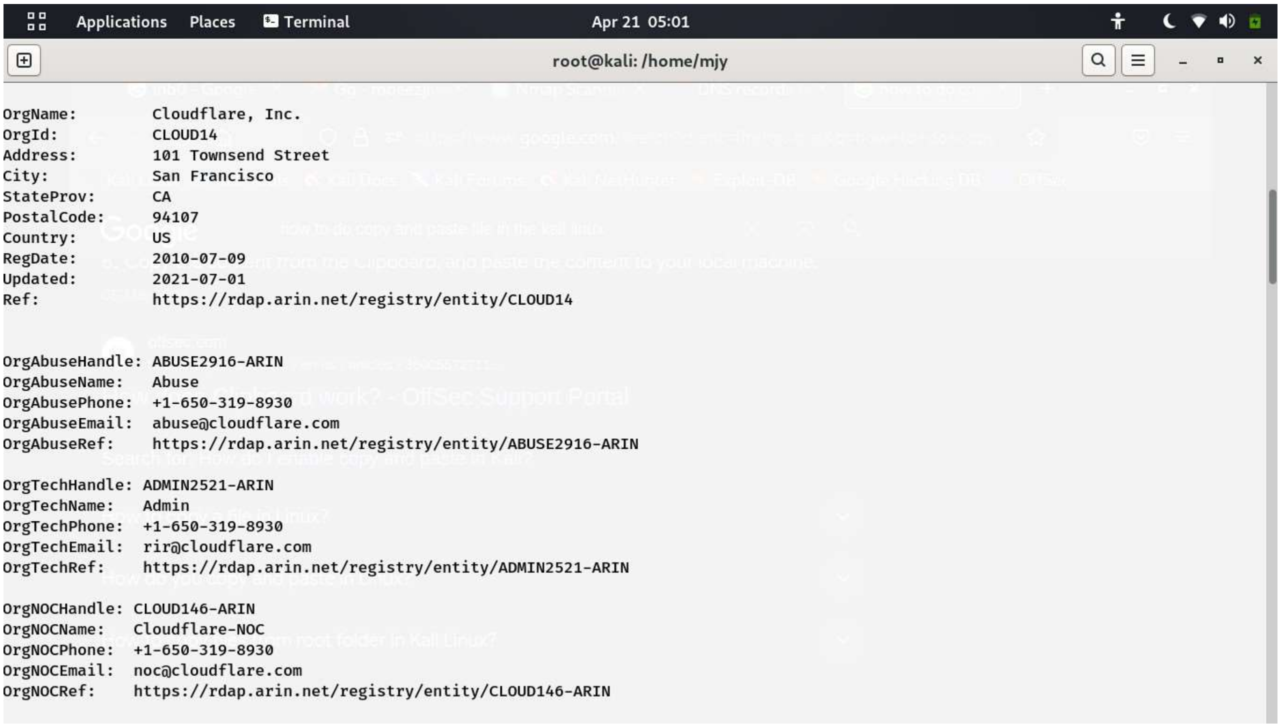
```
┌──(root㉿kali)-[/home/mjy]
└─# nmap -sS -O -oN port_scan_results.txt 104.21.46.149

Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-21 05:01 EDT
Nmap scan report for 104.21.46.149
Host is up (0.064s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Crestron XPanel control system (92%), ASUS RT-N56U WAP (Linux 3.4) (90%), Linux 3.1 (90%), Linux 3.16 (90%), Lin
ux 3.2 (90%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (89%), HP P2000 G3 NAS device (89%), Linux 4.15 - 5.6 (88%), Linux 5.4 (88
%), Linux 4.10 (88%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.56 seconds
```

TO Find DNS:

Whois 104.21.46.149



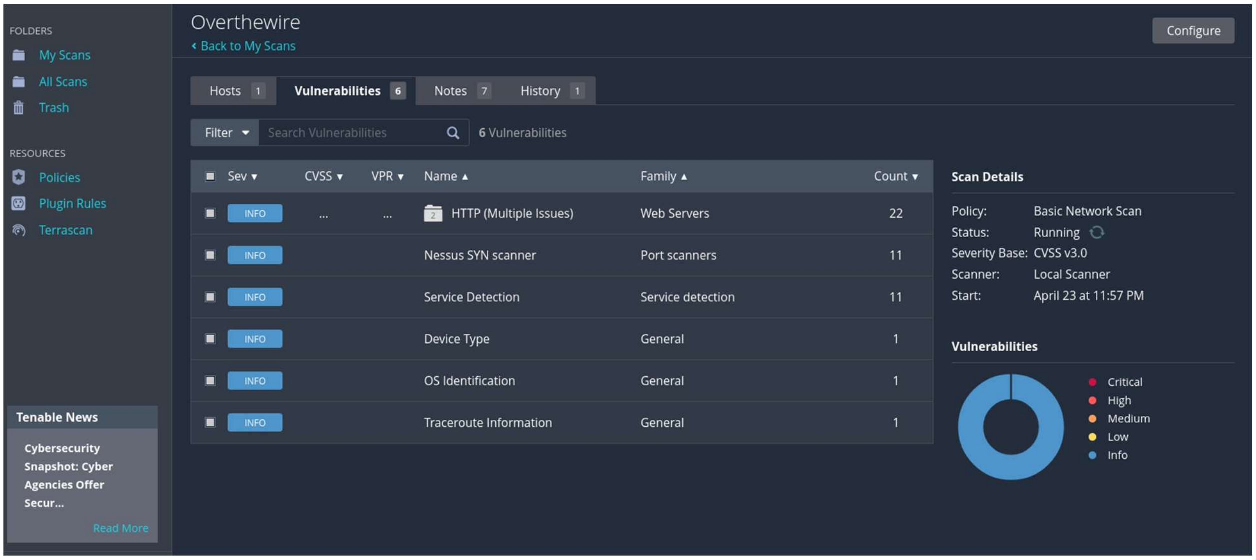
```
┌──(mjy㉿kali)-[~]
└─$ sudo su
[sudo] password for mjy:
┌──(root㉿kali)-[/home/mjy]
└─# whois 104.21.46.149


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#


NetRange:       104.16.0.0 - 104.31.255.255
CIDR:           104.16.0.0/12
NetName:        CLOUDFLARENET
NetHandle:      NET-104-16-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS13335
Organization:   Cloudflare, Inc. (CLOUD14)
RegDate:        2014-03-28
Updated:        2021-05-26
Comment:        All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse
Ref:            https://rdap.arin.net/registry/ip/104.16.0.0
```



```
OrgName:        Cloudflare, Inc.
OrgId:          CLOUD14
Address:        101 Townsend Street
City:           San Francisco
StateProv:      CA
PostalCode:     94107
Country:        US
RegDate:        2010-07-09
Updated:        2021-07-01
Ref:            https://rdap.arin.net/registry/entity/CLOUD14


OrgAbuseHandle: ABUSE2916-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-319-8930
OrgAbuseEmail:  abuse@cloudflare.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

OrgTechHandle: ADMIN2521-ARIN
OrgTechName:   Admin
OrgTechPhone:  +1-650-319-8930
OrgTechEmail:  rir@cloudflare.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ADMIN2521-ARIN

OrgNOCHandle: CLOUD146-ARIN
OrgNOCName:   Cloudflare-NOC
OrgNOCPhone:  +1-650-319-8930
OrgNOCEmail:  noc@cloudflare.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/CLOUD146-ARIN
```

Nessus:

Nessus is a comprehensive vulnerability scanning and assessment tool designed to identify security weaknesses within computer systems, networks, and infrastructure. Developed by Tenable, Nessus is widely recognized for its robust features and extensive database of known vulnerabilities.



Overthewire

‹ Back to My Scans

6 Vulnerabilities

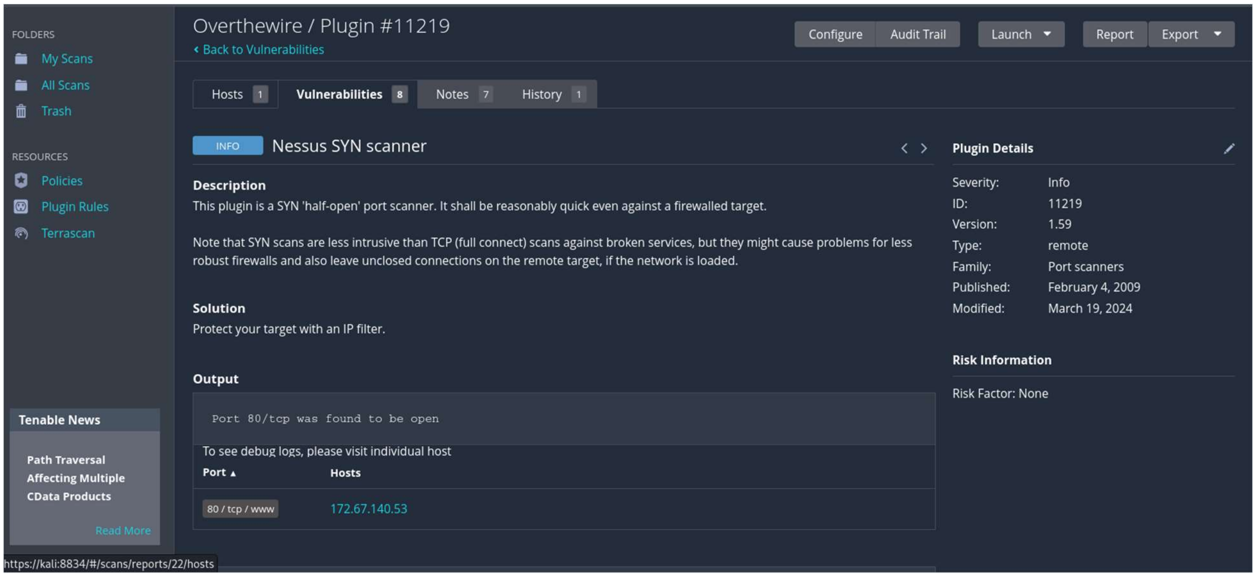
	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾
■	INFO	...	...	2 HTTP (Multiple Issues)	Web Servers	22
■	INFO			Nessus SYN scanner	Port scanners	11
■	INFO			Service Detection	Service detection	11
■	INFO			Device Type	General	1
■	INFO			OS Identification	General	1
■	INFO			Traceroute Information	General	1

Scan Details

Policy:	Basic Network Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	April 23 at 11:57 PM

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info



Overthewire / Plugin #11219

‹ Back to Vulnerabilities

INFO Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

```
Port 80/tcp was found to be open
```

To see debug logs, please visit individual host

Port ▴	Hosts
80 / tcp / www	172.67.140.53

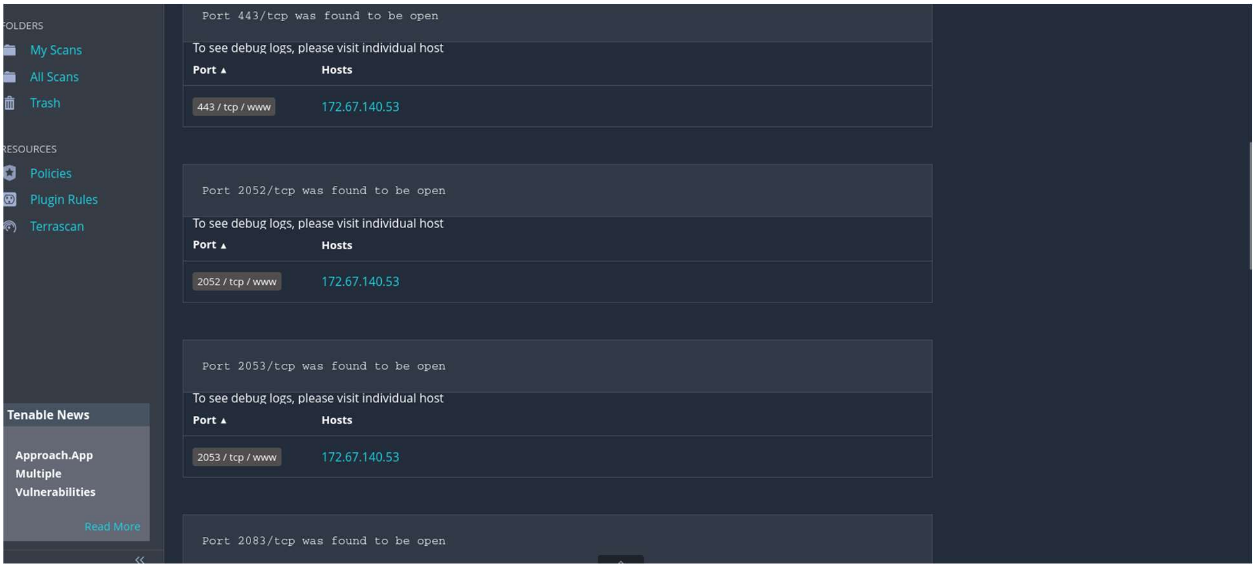
Plugin Details

Severity:	Info
ID:	11219
Version:	1.59
Type:	remote
Family:	Port scanners
Published:	February 4, 2009
Modified:	March 19, 2024

Risk Information

Risk Factor: None

https://kali:8834/#/scans/reports/22/hosts



```
Port 443/tcp was found to be open
```

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp / www	172.67.140.53

```
Port 2052/tcp was found to be open
```

To see debug logs, please visit individual host

Port ▴	Hosts
2052 / tcp / www	172.67.140.53

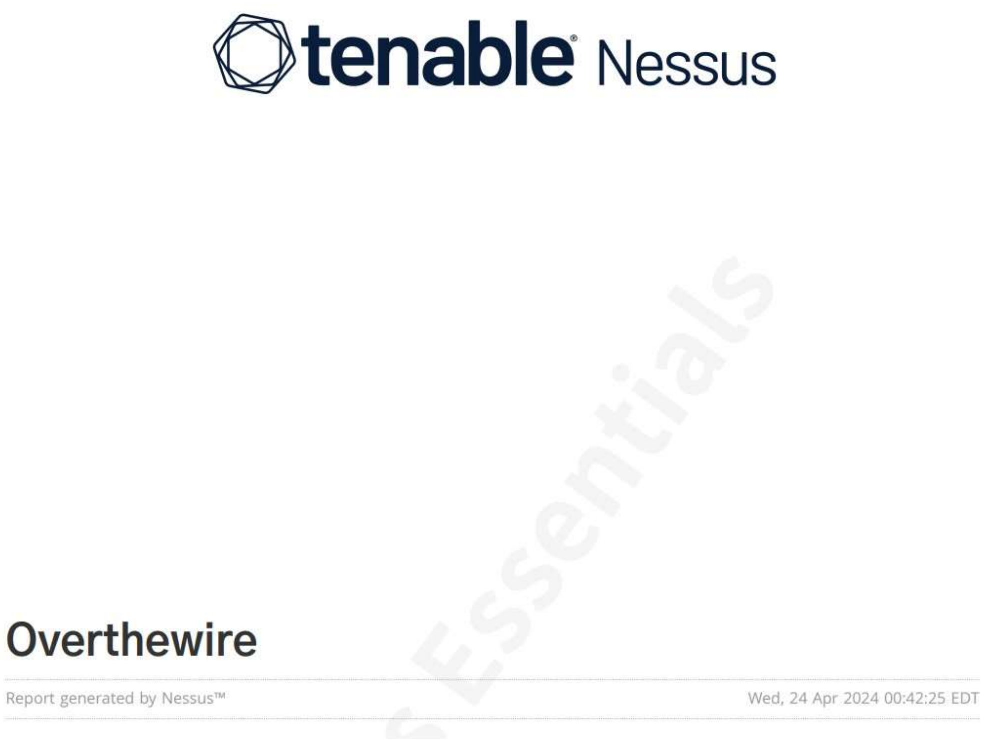
```
Port 2053/tcp was found to be open
```

To see debug logs, please visit individual host

Port ▴	Hosts
2053 / tcp / www	172.67.140.53

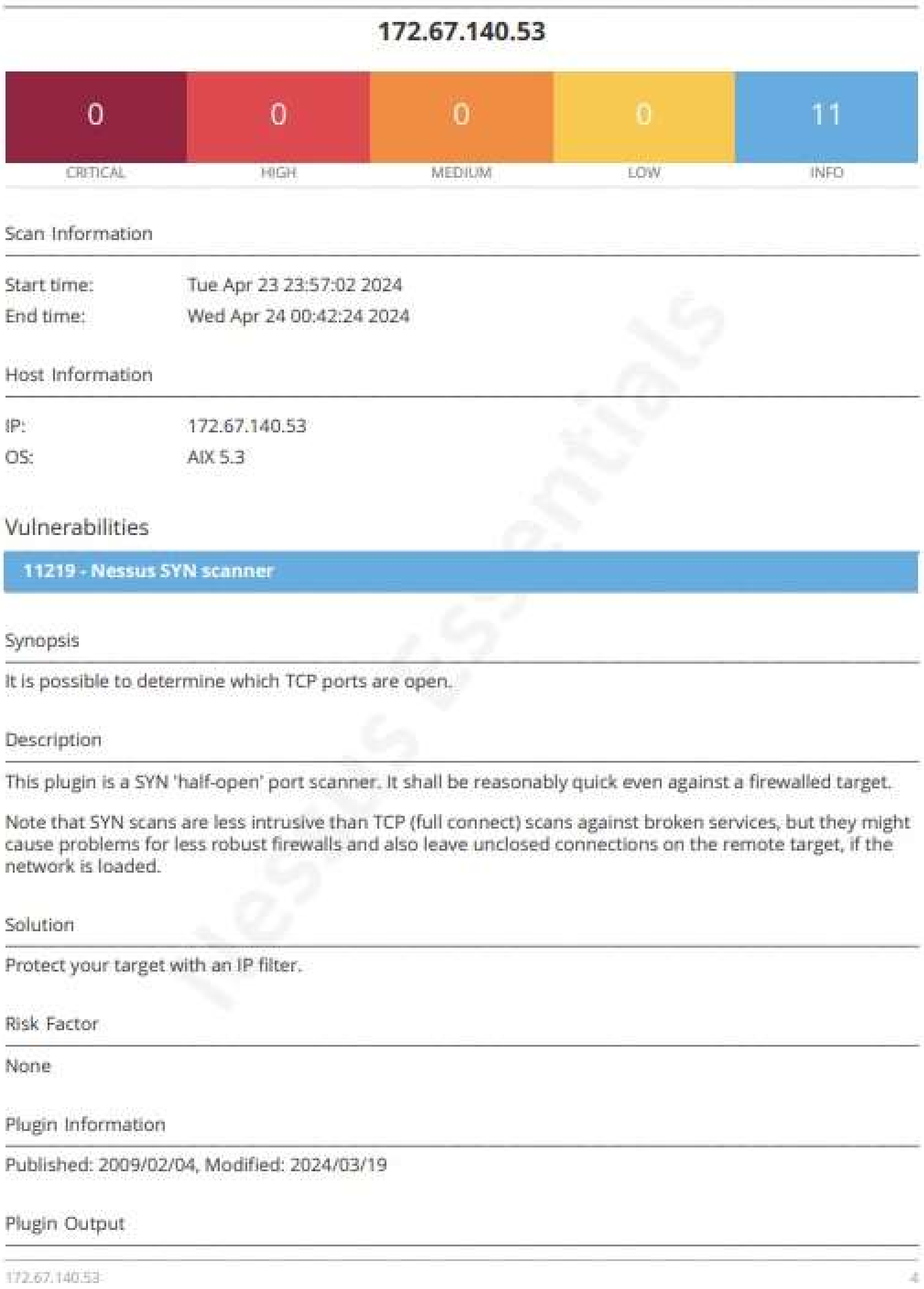
```
Port 2083/tcp was found to be open
```

Report View:



Overthewire

Report generated by Nessus™ Wed, 24 Apr 2024 00:42:25 EDT



172.67.140.53

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	11

Scan Information

Start time:	Tue Apr 23 23:57:02 2024
End time:	Wed Apr 24 00:42:24 2024

Host Information

IP:	172.67.140.53
OS:	AIX 5.3

Vulnerabilities

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2024/03/19

Plugin Output

tcp/443/www

```
Port 443/tcp was found to be open
```