Sadiq Sonalkar

Assignment 2

VULNERABILTIY REPORT

Vulnerability Scanning

Target: Skullcandy.com

Table of Contents:

Findings:

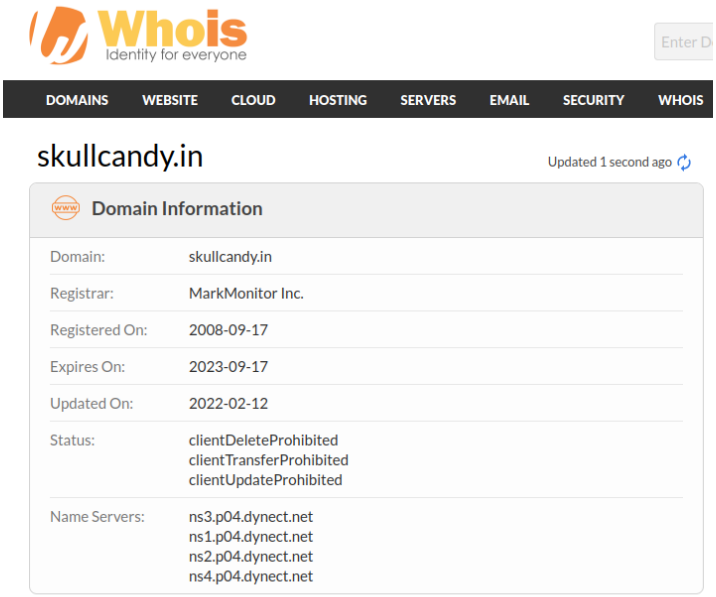
The vulnerability found are very low-level threats which can be fixed easily. The vulnerability found are not yet a threat but it can be a threat.

Determination the scope:

The scope of this test is to identify and scan the vulnerabilities of the given target. Also if any vulnerability are found then what is the solution to solve the vulnerability which was found.

Information Gathering:

1. **Whois Lookup:** With the help of whois lookup we identify the domain name, the domain registration date, expiration date, the date domain name was updated, etc.

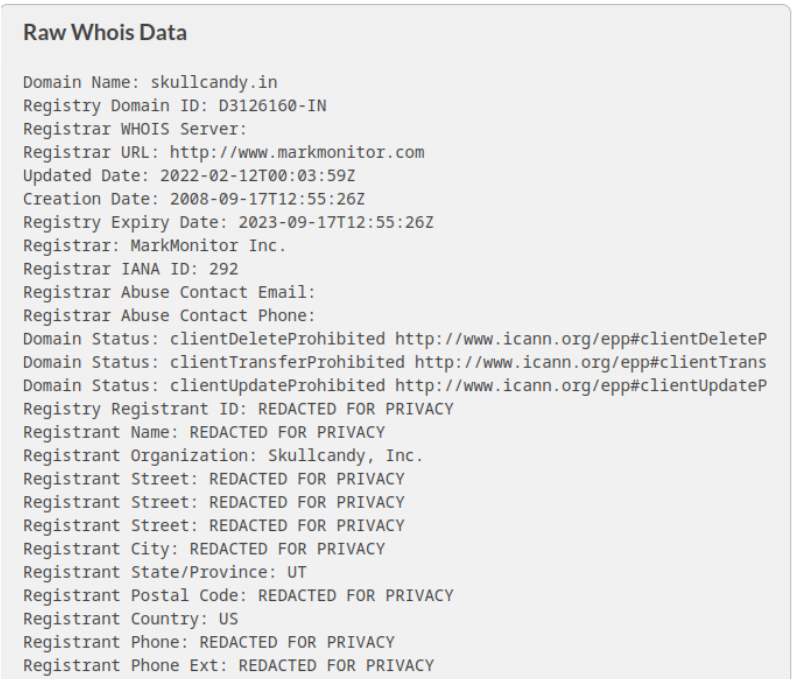


skullcandy.in

Domain Information

Domain:	skullcandy.in
Registrar:	MarkMonitor Inc.
Registered On:	2008-09-17
Expires On:	2023-09-17
Updated On:	2022-02-12
Status:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	ns3.p04.dynect.net ns1.p04.dynect.net ns2.p04.dynect.net ns4.p04.dynect.net

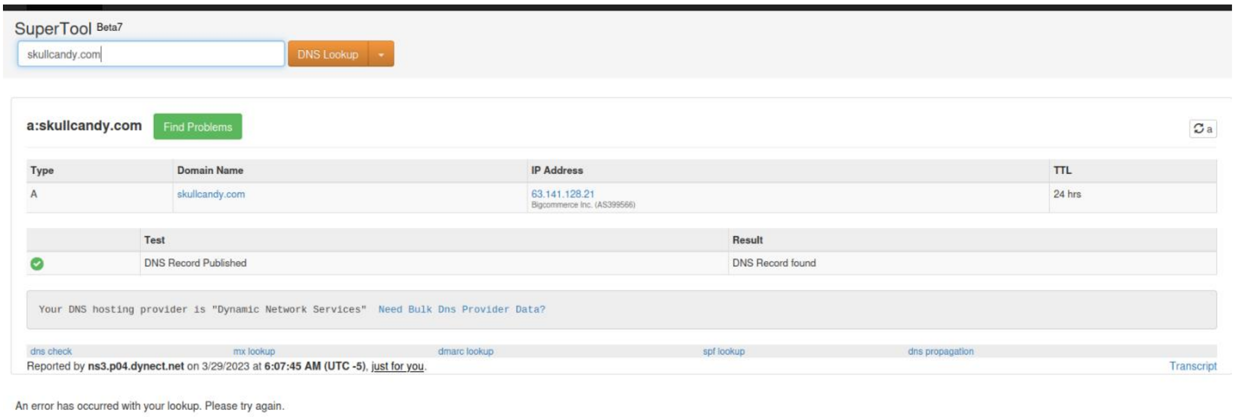
We will also get raw whois data:



Raw Whois Data

```
Domain Name: skullcandy.in
Registry Domain ID: D3126160-IN
Registrar WHOIS Server:
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-02-12T00:03:59Z
Creation Date: 2008-09-17T12:55:26Z
Registry Expiry Date: 2023-09-17T12:55:26Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteP
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTrans
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateP
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Skullcandy, Inc.
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: UT
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
```

2. **DNS Lookup:** With the help of DNS lookup we got the IP Address of our target. It is very important to obtain the IP Address.



Type	Domain Name	IP Address	TTL
A	skullcandy.com	63.141.128.21 Bigcommerce Inc. (AS399566)	24 hrs

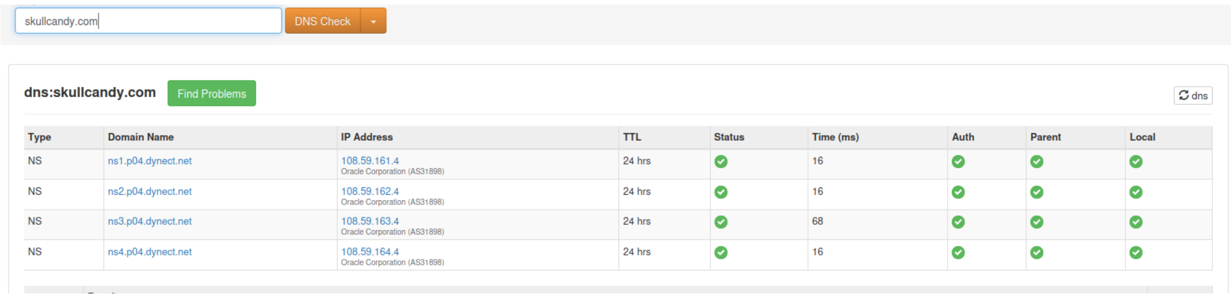
	Test	Result
✓	DNS Record Published	DNS Record found

```
Your DNS hosting provider is "Dynamic Network Services"  Need Bulk Dns Provider Data?
```

Reported by **ns3.p04.dynect.net** on 3/29/2023 at **6:07:45 AM (UTC -5)**, just for you.

An error has occurred with your lookup. Please try again.

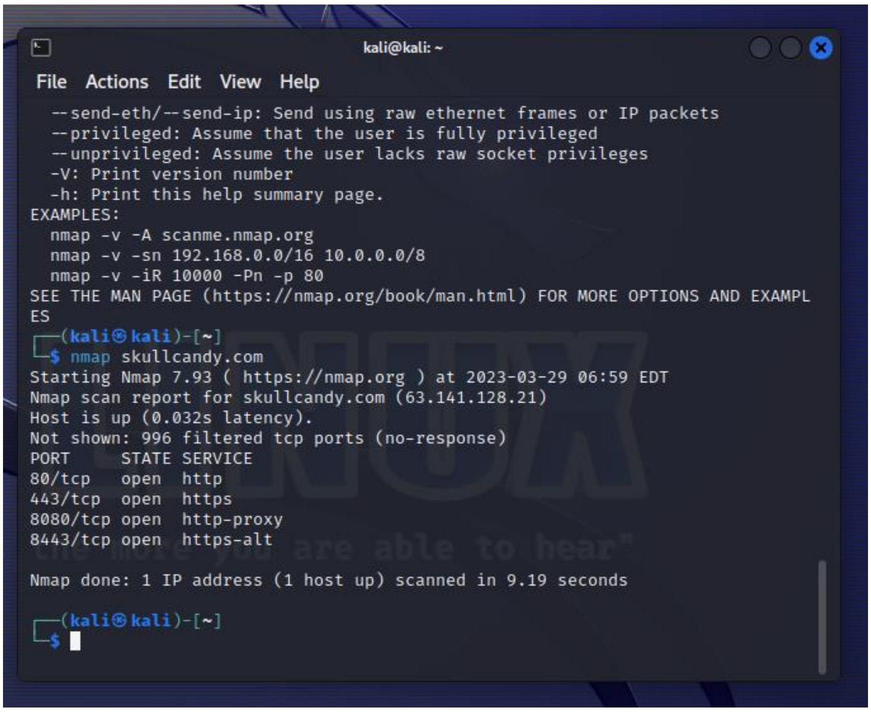
3. **DNS Check:** Then with the help of DNS check we get the name server domain as well as their IP Address.



Type	Domain Name	IP Address	TTL	Status	Time (ms)	Auth	Parent	Local
NS	ns1.p04.dynect.net	108.59.161.4 Oracle Corporation (AS31898)	24 hrs	✓	16	✓	✓	✓
NS	ns2.p04.dynect.net	108.59.162.4 Oracle Corporation (AS31898)	24 hrs	✓	16	✓	✓	✓
NS	ns3.p04.dynect.net	108.59.163.4 Oracle Corporation (AS31898)	24 hrs	✓	68	✓	✓	✓
NS	ns4.p04.dynect.net	108.59.164.4 Oracle Corporation (AS31898)	24 hrs	✓	16	✓	✓	✓

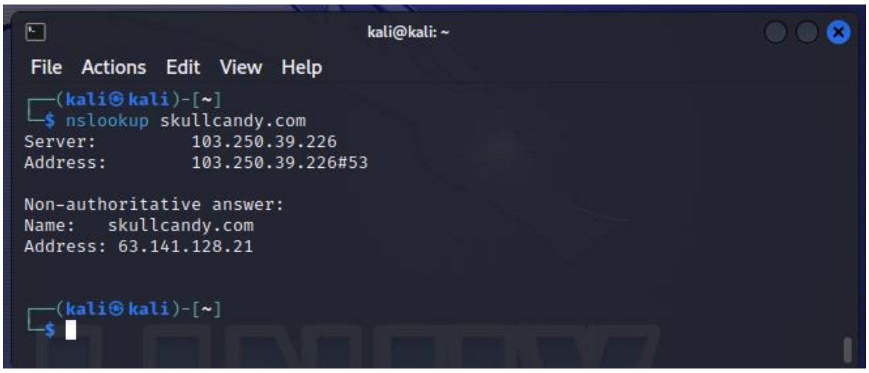
4. Using NMAP:

a. NMAP Scan: Will return IP Address and some information



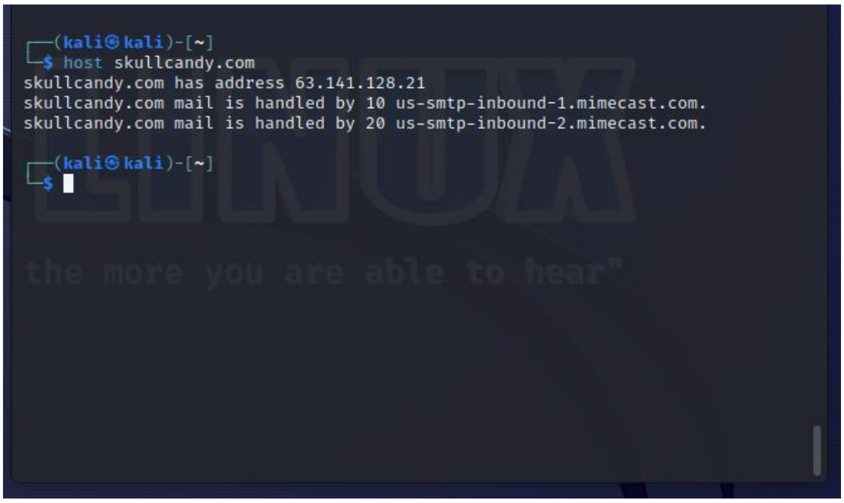
```
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPL
ES
┌──(kali㉿kali)-[~]
└─$ nmap skullcandy.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-29 06:59 EDT
Nmap scan report for skullcandy.com (63.141.128.21)
Host is up (0.032s 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

Nmap done: 1 IP address (1 host up) scanned in 9.19 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

b. Nslookup: Will return the name server and it's IP Address



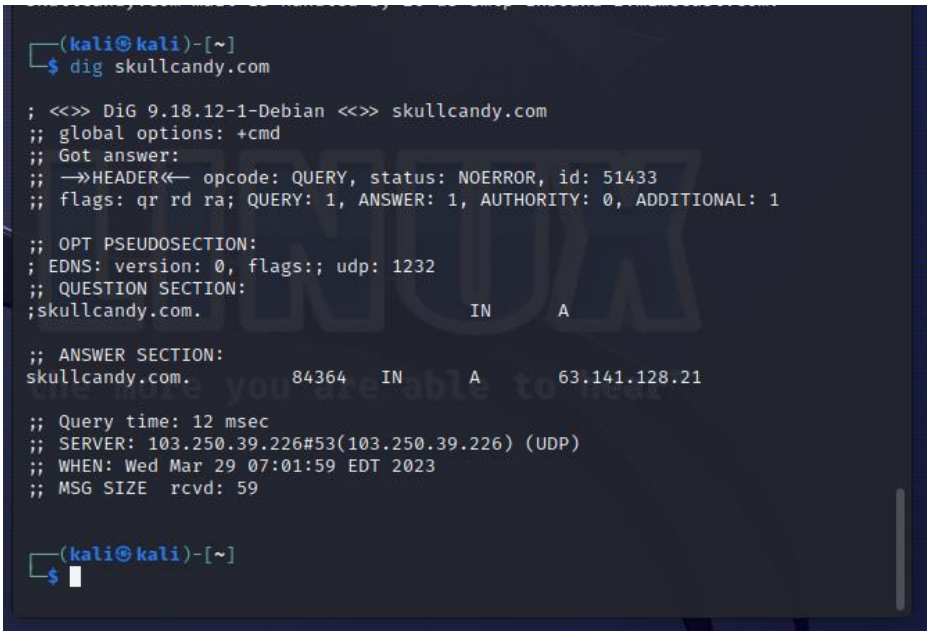
```
┌──(kali㉿kali)-[~]
└─$ nslookup skullcandy.com
Server:         103.250.39.226
Address:        103.250.39.226#53

Non-authoritative answer:
Name:   skullcandy.com
Address: 63.141.128.21


┌──(kali㉿kali)-[~]
└─$ 
```

c. Host: Will give us the SMTP inbound.



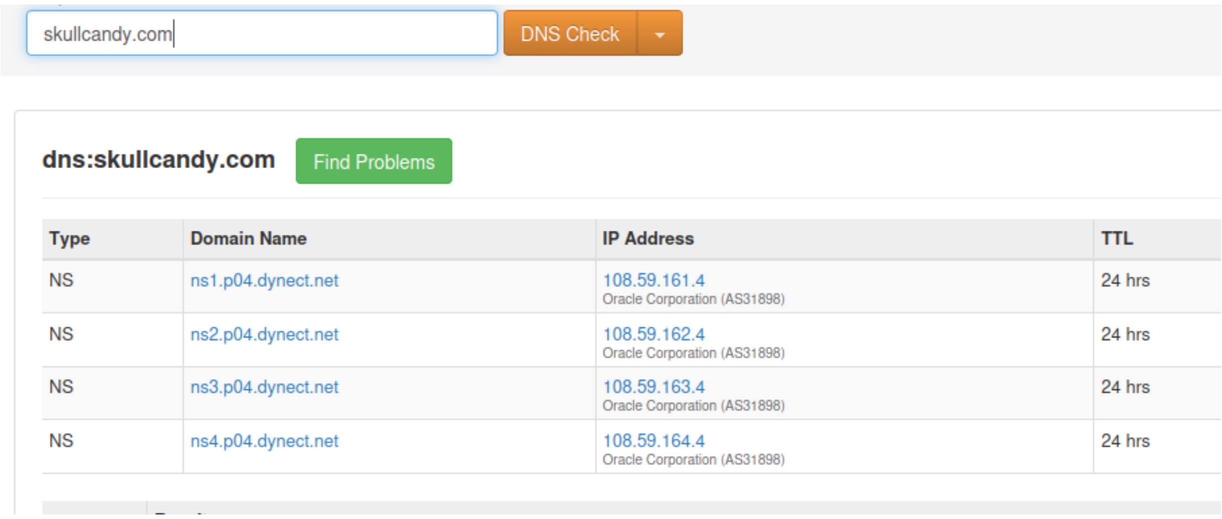
```
┌──(kali㉿kali)-[~]
└─$ host skullcandy.com
skullcandy.com has address 63.141.128.21
skullcandy.com mail is handled by 10 us-smtp-inbound-1.mimecast.com.
skullcandy.com mail is handled by 20 us-smtp-inbound-2.mimecast.com.

┌──(kali㉿kali)-[~]
└─$ 
```

d. **Dig:** Will give us more information about the target.



```
┌──(kali㉿kali)-[~]
└─$ dig skullcandy.com

; <<>> DiG 9.18.12-1-Debian <<>> skullcandy.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51433
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;skullcandy.com.                IN      A

;; ANSWER SECTION:
skullcandy.com.         84364   IN      A       63.141.128.21

;; Query time: 12 msec
;; SERVER: 103.250.39.226#53(103.250.39.226) (UDP)
;; WHEN: Wed Mar 29 07:01:59 EDT 2023
;; MSG SIZE  rcvd: 59

┌──(kali㉿kali)-[~]
└─$ 
```

These are the DNS server of skullcandy.



skullcandy.com

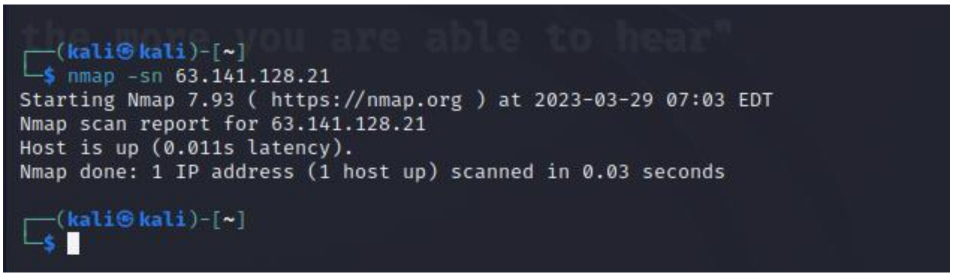
dns:skullcandy.com

Type	Domain Name	IP Address	TTL
NS	ns1.p04.dynect.net	108.59.161.4 Oracle Corporation (AS31898)	24 hrs
NS	ns2.p04.dynect.net	108.59.162.4 Oracle Corporation (AS31898)	24 hrs
NS	ns3.p04.dynect.net	108.59.163.4 Oracle Corporation (AS31898)	24 hrs
NS	ns4.p04.dynect.net	108.59.164.4 Oracle Corporation (AS31898)	24 hrs

DNS servers connect the organization website to the outside world. Exploitation of these servers may lead to malicious usage of the organization web and mail servers.

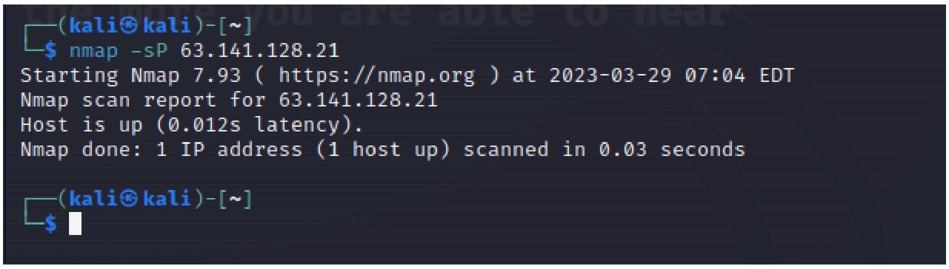
Scanning using NMAP Commands:

1. **Nmap -sn IP Address:** Will check whether Server/Host is Up or not



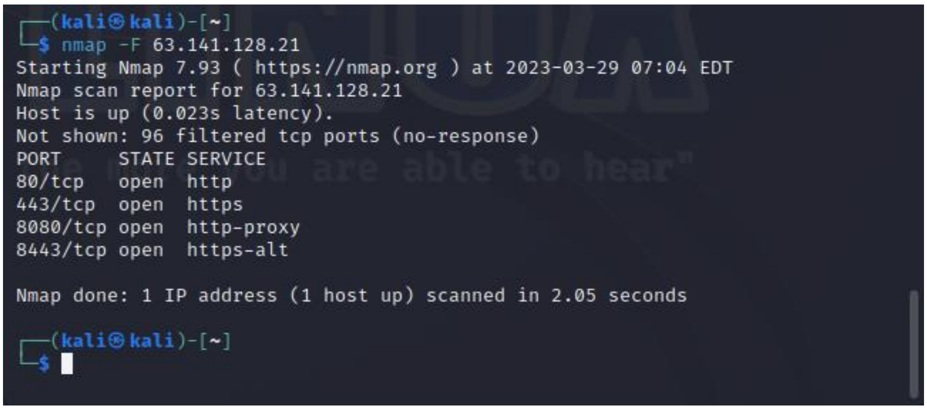
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 63.141.128.21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-29 07:03 EDT
Nmap scan report for 63.141.128.21
Host is up (0.011s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

2. **Nmap -sP IP Address:** Will ping the Server.



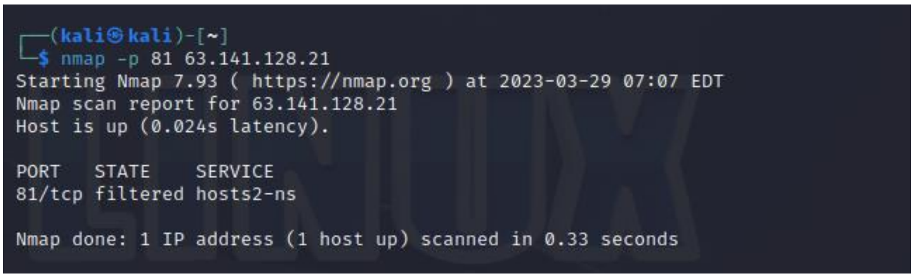
```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 63.141.128.21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-29 07:04 EDT
Nmap scan report for 63.141.128.21
Host is up (0.012s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

3. **Nmap -F IP Address:** Will do a Fast Scan on the server and will show open ports.



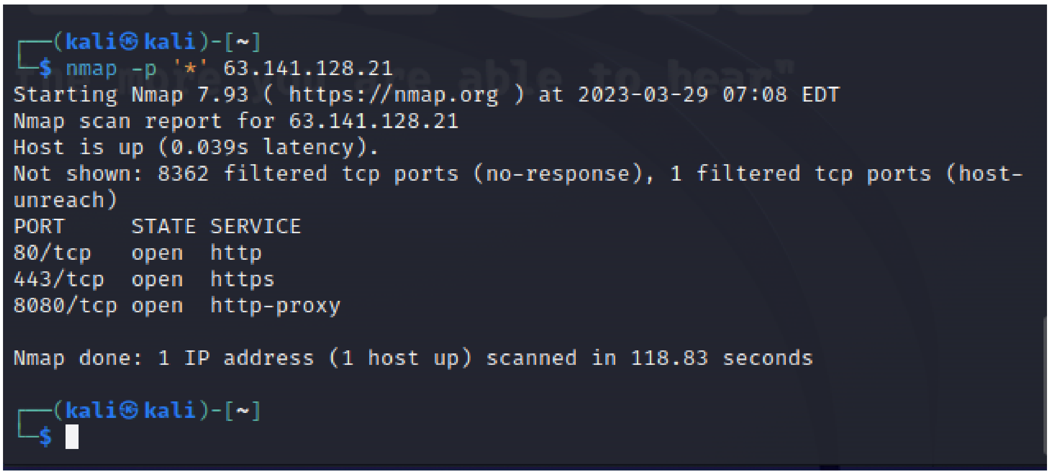
```
┌──(kali㉿kali)-[~]
└─$ nmap -F 63.141.128.21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-29 07:04 EDT
Nmap scan report for 63.141.128.21
Host is up (0.023s latency).
Not shown: 96 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

4. **Nmap -p port number IP Address:** Will scan a particular port number.



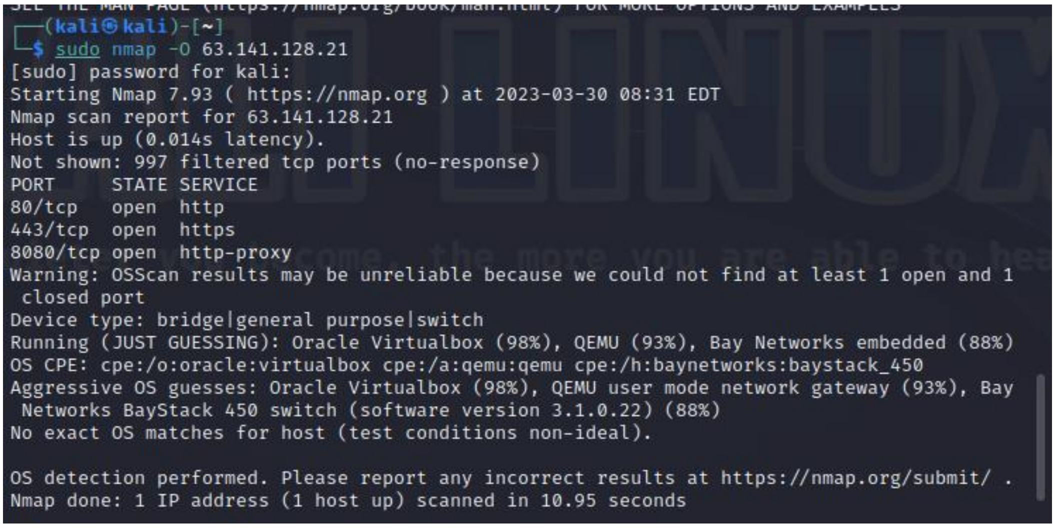
```
┌──(kali㉿kali)-[~]
└─$ nmap -p 81 63.141.128.21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-29 07:07 EDT
Nmap scan report for 63.141.128.21
Host is up (0.024s latency).

PORT   STATE    SERVICE
81/tcp filtered hosts2-ns

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

5. **Nmap -p '*' IP Address:** Will scan all the open ports.



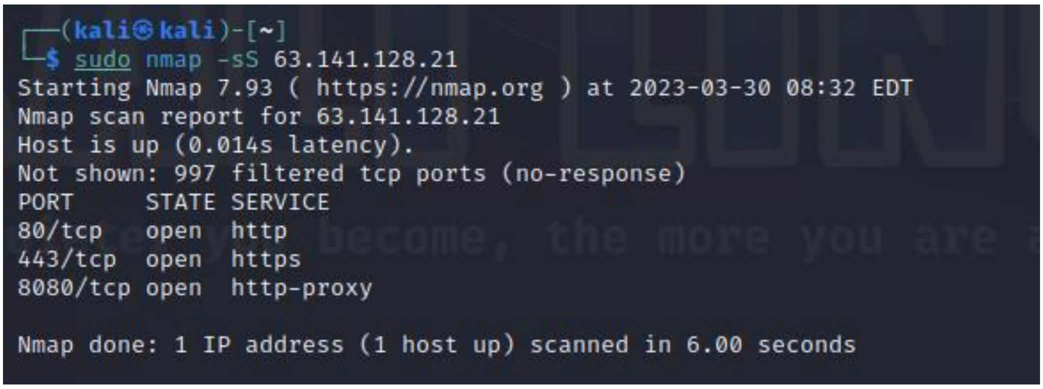
```
┌──(kali㉿kali)-[~]
└─$ nmap -p '*' 63.141.128.21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-29 07:08 EDT
Nmap scan report for 63.141.128.21
Host is up (0.039s latency).
Not shown: 8362 filtered tcp ports (no-response), 1 filtered tcp ports (host-
unreach)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 118.83 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

6. **Sudo Nmap -O IP Address:** Will return the operating system being used. It requires root privileges. So we use sudo.



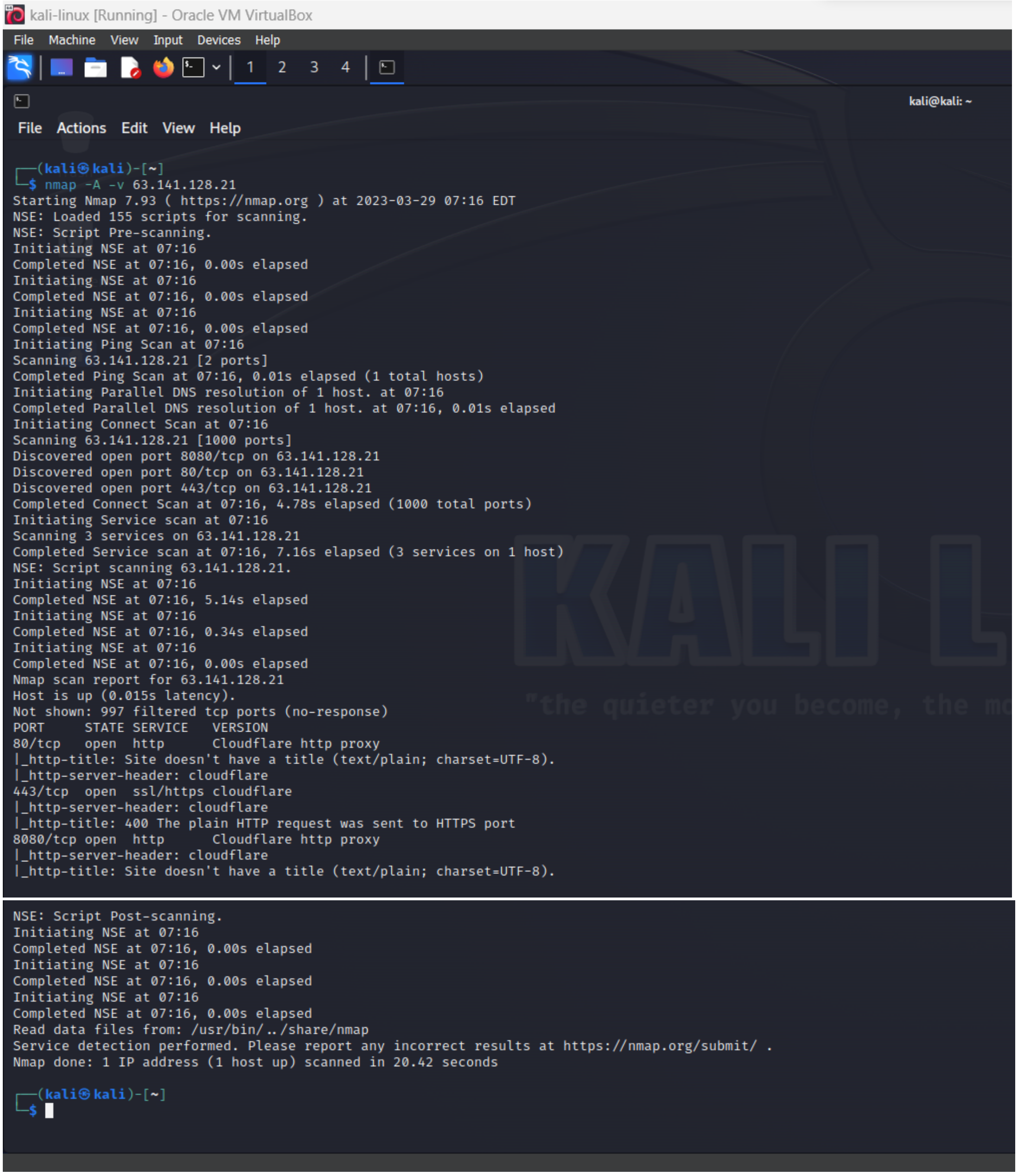
```
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 63.141.128.21
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-30 08:31 EDT
Nmap scan report for 63.141.128.21
Host is up (0.014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%), Bay Networks embedded (88%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%), Bay
 Networks BayStack 450 switch (software version 3.1.0.22) (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 10.95 seconds
```

7. **Nmap -sS IP Address:** Will perform a stealth scan.



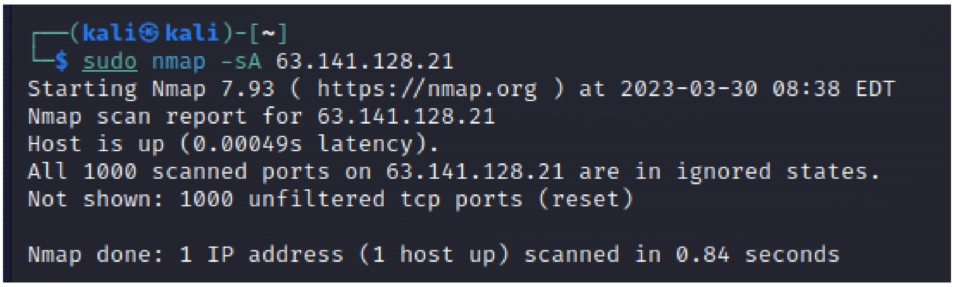
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 63.141.128.21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-30 08:32 EDT
Nmap scan report for 63.141.128.21
Host is up (0.014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 6.00 seconds
```

8. **Nmap -A -v IP Address:** Intense scan. It will perform various scans. Will give details about the port no., State of the port, Service running on that port and the version.


kali-linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
KALI L
"the quieter you become, the mo

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -v 63.141.128.21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-29 07:16 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:16
Completed NSE at 07:16, 0.00s elapsed
Initiating NSE at 07:16
Completed NSE at 07:16, 0.00s elapsed
Initiating NSE at 07:16
Completed NSE at 07:16, 0.00s elapsed
Initiating Ping Scan at 07:16
Scanning 63.141.128.21 [2 ports]
Completed Ping Scan at 07:16, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:16
Completed Parallel DNS resolution of 1 host. at 07:16, 0.01s elapsed
Initiating Connect Scan at 07:16
Scanning 63.141.128.21 [1000 ports]
Discovered open port 8080/tcp on 63.141.128.21
Discovered open port 80/tcp on 63.141.128.21
Discovered open port 443/tcp on 63.141.128.21
Completed Connect Scan at 07:16, 4.78s elapsed (1000 total ports)
Initiating Service scan at 07:16
Scanning 3 services on 63.141.128.21
Completed Service scan at 07:16, 7.16s elapsed (3 services on 1 host)
NSE: Script scanning 63.141.128.21.
Initiating NSE at 07:16
Completed NSE at 07:16, 5.14s elapsed
Initiating NSE at 07:16
Completed NSE at 07:16, 0.34s elapsed
Initiating NSE at 07:16
Completed NSE at 07:16, 0.00s elapsed
Nmap scan report for 63.141.128.21
Host is up (0.015s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE   VERSION
80/tcp   open  http      Cloudflare http proxy
|_http-title: Site doesn't have a title (text/plain; charset=UTF-8).
|_http-server-header: cloudflare
443/tcp  open  ssl/https cloudflare
|_http-server-header: cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
8080/tcp open  http      Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: Site doesn't have a title (text/plain; charset=UTF-8).

NSE: Script Post-scanning.
Initiating NSE at 07:16
Completed NSE at 07:16, 0.00s elapsed
Initiating NSE at 07:16
Completed NSE at 07:16, 0.00s elapsed
Initiating NSE at 07:16
Completed NSE at 07:16, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.42 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

9. **Nmap -sA IP Address:** Will check for firewall on the ports.

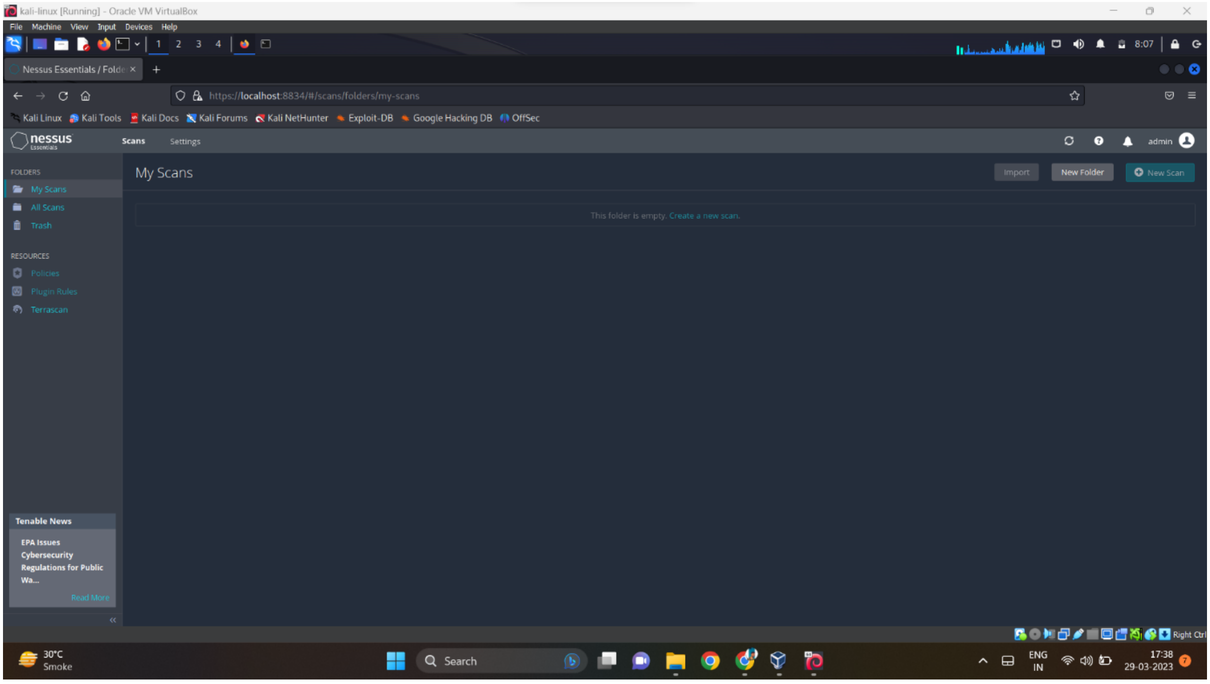


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sA 63.141.128.21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-30 08:38 EDT
Nmap scan report for 63.141.128.21
Host is up (0.00049s latency).
All 1000 scanned ports on 63.141.128.21 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
```

Scanning using Nessus Tool:

First, we have to install Nessus. Go to ‘localhost:8834’ and the Nessus will start. It will take time to download plugins. After it’s done login using username= ‘admin’ and password= ‘admin’.

You will come to this screen.



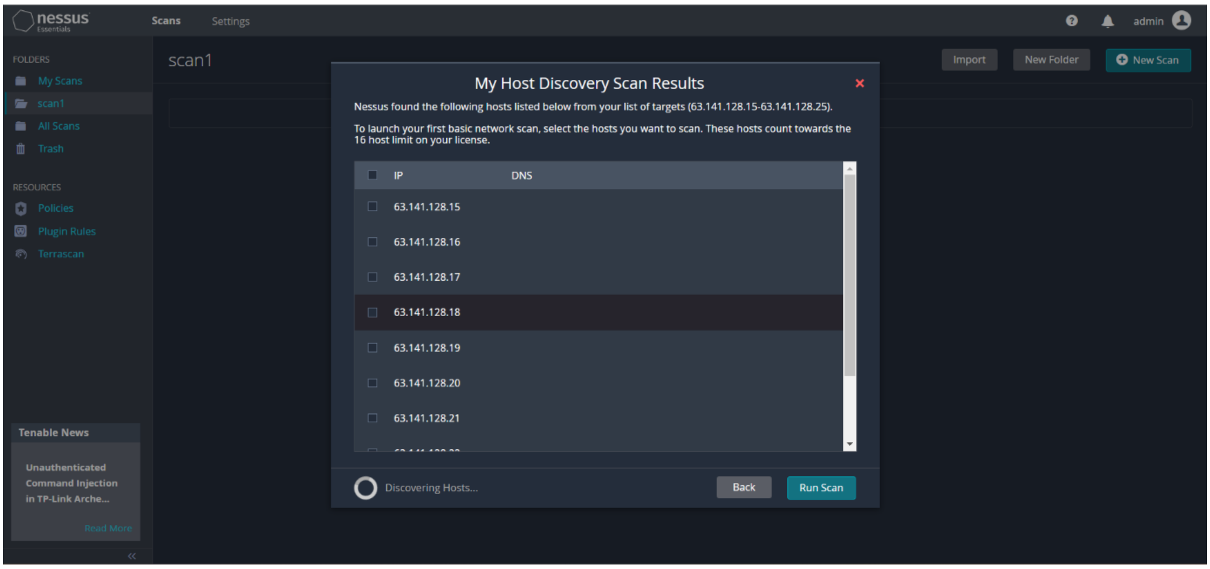
My Scans

This folder is empty. Create a new scan.

EPA Issues Cybersecurity Regulations for Public Wa...

Then you scan multiple server or host and you can even scan single host.

I’ll scan multiple host ranges from IP Address = 63.141.128.15 – 63.128.141.25



scan1

My Host Discovery Scan Results

Nessus found the following hosts listed below from your list of targets (63.141.128.15-63.141.128.25).

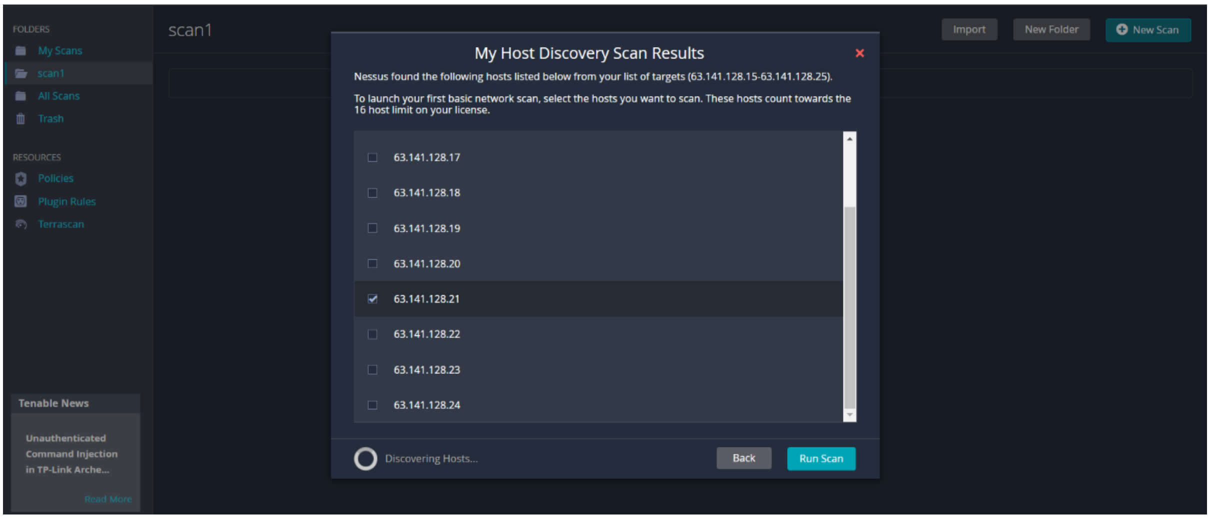
To launch your first basic network scan, select the hosts you want to scan. These hosts count towards the 16 host limit on your license.

□	IP	DNS
□	63.141.128.15	
□	63.141.128.16	
□	63.141.128.17	
□	63.141.128.18	
□	63.141.128.19	
□	63.141.128.20	
□	63.141.128.21	

Discovering Hosts...

Unauthenticated Command Injection in TP-Link Arche...

You can select a single server too.



My Host Discovery Scan Results

Nessus found the following hosts listed below from your list of targets (63.141.128.15-63.141.128.25).

To launch your first basic network scan, select the hosts you want to scan. These hosts count towards the 16 host limit on your license.

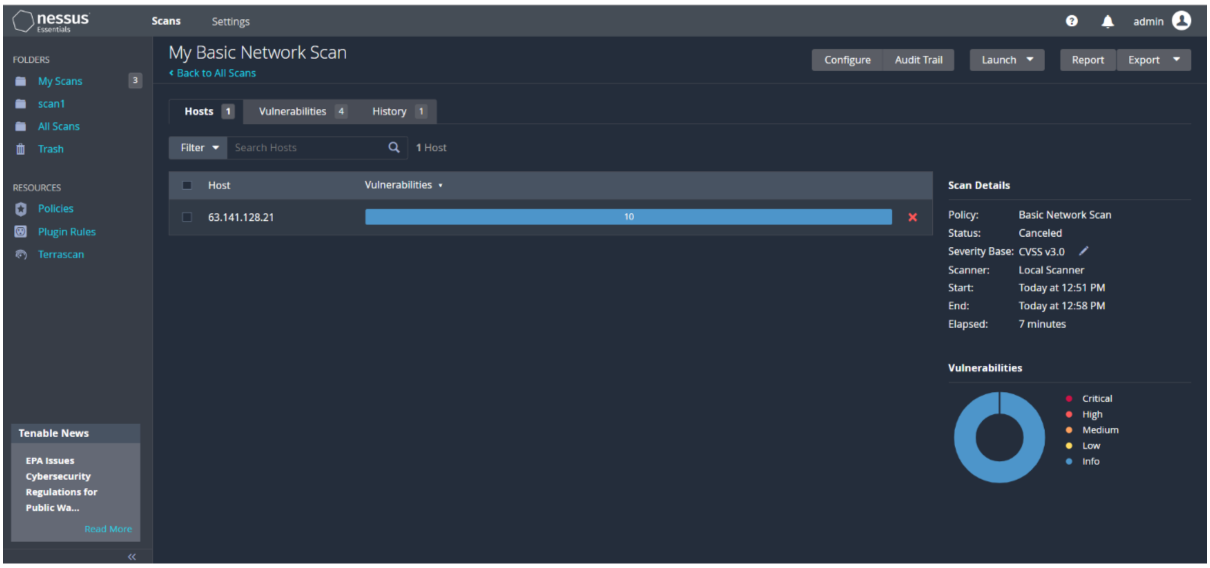
- □ 63.141.128.17
- □ 63.141.128.18
- □ 63.141.128.19
- □ 63.141.128.20
- ☑ 63.141.128.21
- □ 63.141.128.22
- □ 63.141.128.23
- □ 63.141.128.24

Discovering Hosts...

Now it will run a basic scan on the selected host.

I stopped the scan after a while and 4 very very low level vulnerability were found.

They are not vulnerability but they can be.



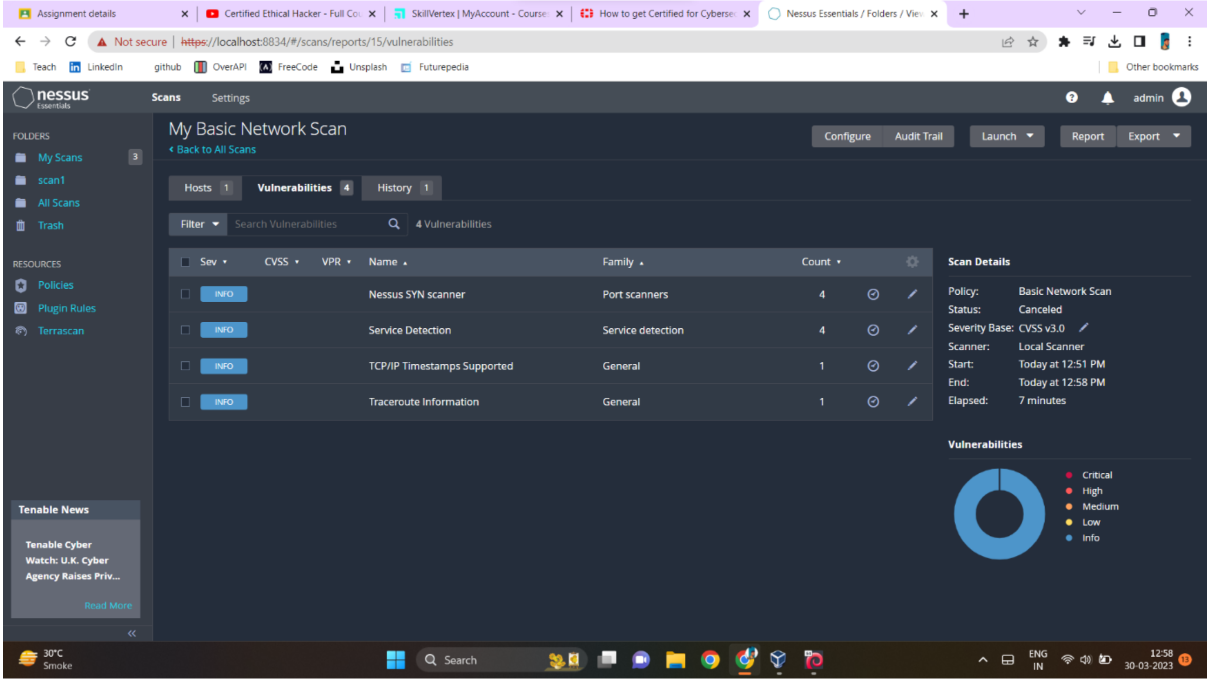
My Basic Network Scan

Host	Vulnerabilities
63.141.128.21	10

Scan Details

Policy: Basic Network Scan
Status: Canceled
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:51 PM
End: Today at 12:58 PM
Elapsed: 7 minutes

The 4 vulnerabilities were as follow:



My Basic Network Scan

‹ Back to All Scans

4 Vulnerabilities

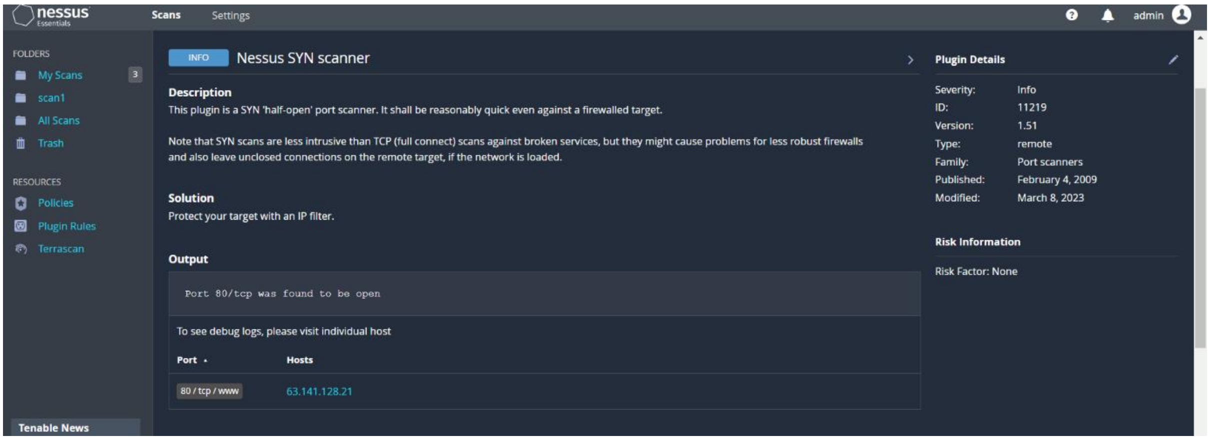
Sev	CVSS	VPR	Name	Family	Count
INFO			Nessus SYN scanner	Port scanners	4
INFO			Service Detection	Service detection	4
INFO			TCP/IP Timestamps Supported	General	1
INFO			Traceroute Information	General	1

Scan Details

Policy:	Basic Network Scan
Status:	Canceled
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 12:51 PM
End:	Today at 12:58 PM
Elapsed:	7 minutes

Vulnerabilities

The first vulnerability was Nessus SYN scanner.



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

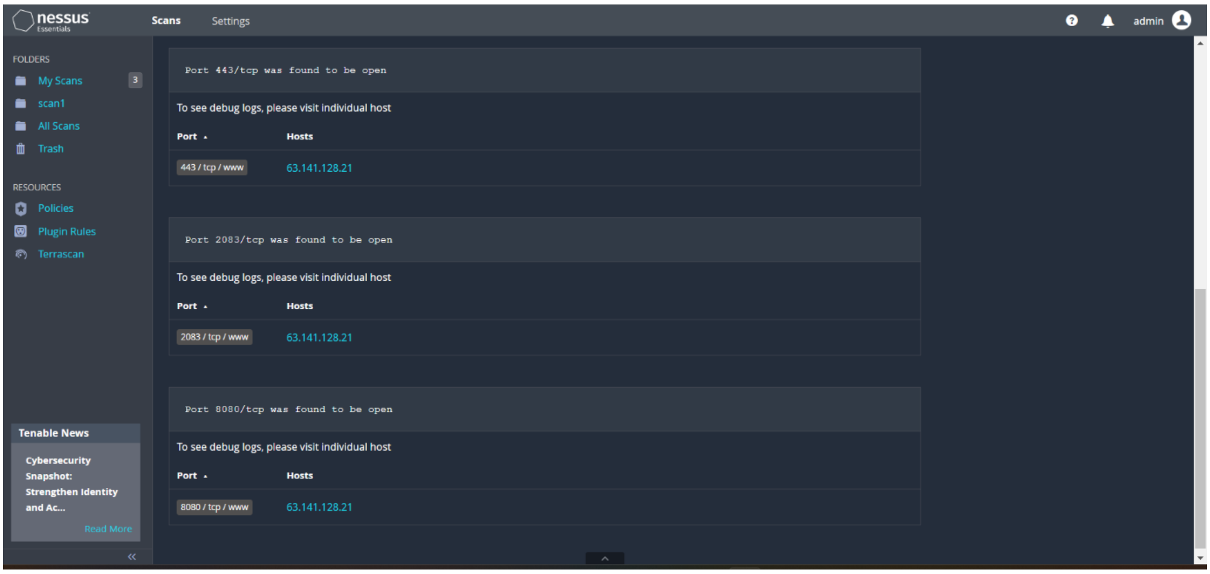
Port	Hosts
80 / tcp / www	63.141.128.21

Plugin Details

Severity:	Info
ID:	11219
Version:	1.51
Type:	remote
Family:	Port scanners
Published:	February 4, 2009
Modified:	March 8, 2023

Risk Information

Risk Factor: None



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

To see debug logs, please visit individual host

Port	Hosts
443 / tcp / www	63.141.128.21

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

To see debug logs, please visit individual host

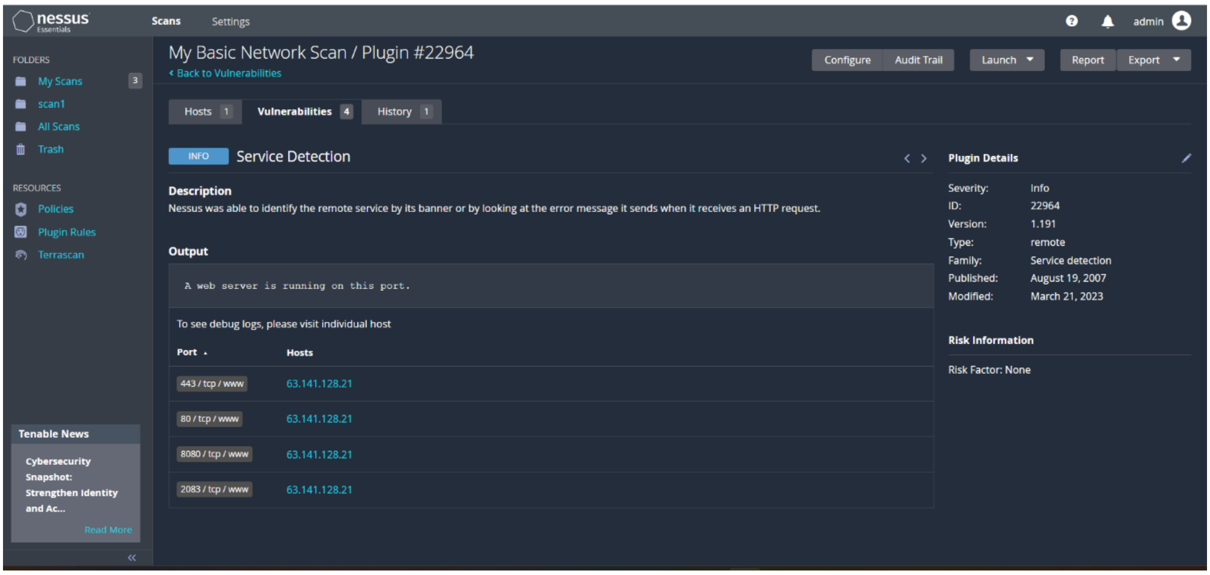
Port	Hosts
2083 / tcp / www	63.141.128.21

```
Port 8080/tcp was found to be open
```

To see debug logs, please visit individual host

Port	Hosts
8080 / tcp / www	63.141.128.21

The second vulnerability was Service Detection.



My Basic Network Scan / Plugin #22964

‹ Back to Vulnerabilities

INFO Service Detection

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Output

```
A web server is running on this port.
```

To see debug logs, please visit individual host

Port	Hosts
443 / tcp / www	63.141.128.21
80 / tcp / www	63.141.128.21
8080 / tcp / www	63.141.128.21
2083 / tcp / www	63.141.128.21

Plugin Details

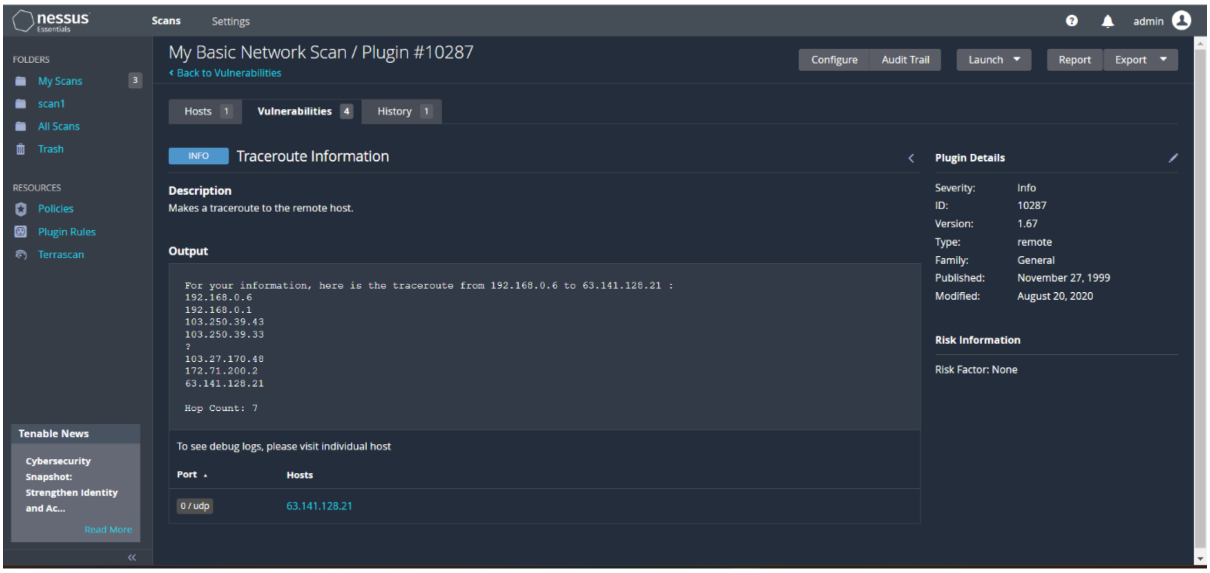
Severity:	Info
ID:	22964
Version:	1.191
Type:	remote
Family:	Service detection
Published:	August 19, 2007
Modified:	March 21, 2023

Risk Information

Risk Factor: None

The third vulnerability was TCP/IP Timestamps supported.

The fourth vulnerability was Traceroute information.



My Basic Network Scan / Plugin #10287

‹ Back to Vulnerabilities

INFO Traceroute Information

Description

Makes a traceroute to the remote host.

Output

```
For your information, here is the traceroute from 192.168.0.6 to 63.141.128.21 :
192.168.0.6
192.168.0.1
103.250.39.43
103.250.39.33
?
103.27.170.48
172.71.200.2
63.141.128.21

Hop Count: 7
```

To see debug logs, please visit individual host

Port	Hosts
0 / udp	63.141.128.21

Plugin Details

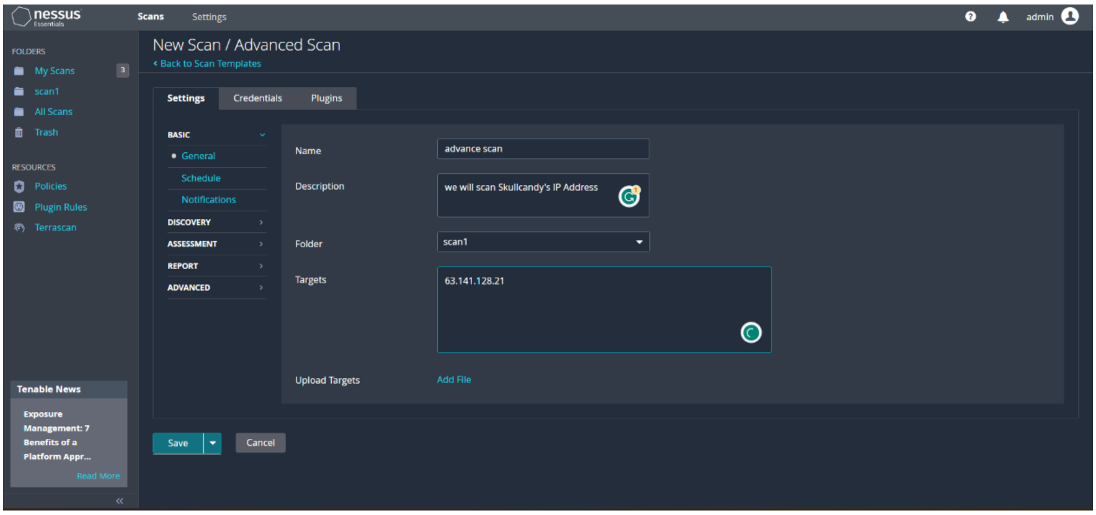
Severity:	Info
ID:	10287
Version:	1.67
Type:	remote
Family:	General
Published:	November 27, 1999
Modified:	August 20, 2020

Risk Information

Risk Factor: None

It gives us the route it followed to reach the target IP Address. And it also gives the number of hop count. i.e., the no. of network in between.

Now I'll create a advance scan on the same port.



New Scan / Advanced Scan

‹ Back to Scan Templates

Name: advance scan

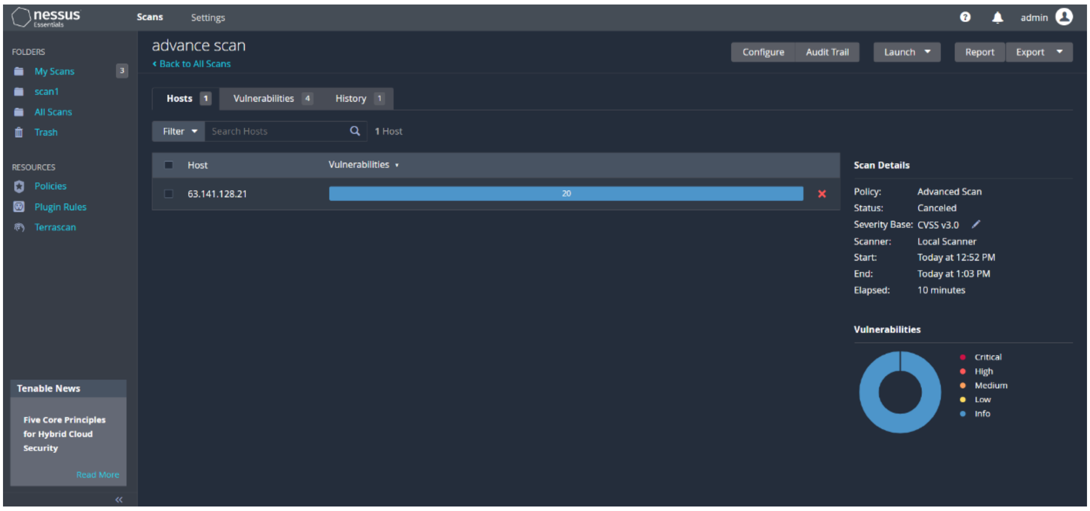
Description: we will scan Skullcandy's IP Address

Folder: scan1

Targets: 63.141.128.21

Upload Targets: Add File

The results were same for both basic and advance scan.



advance scan

‹ Back to All Scans

1 Host

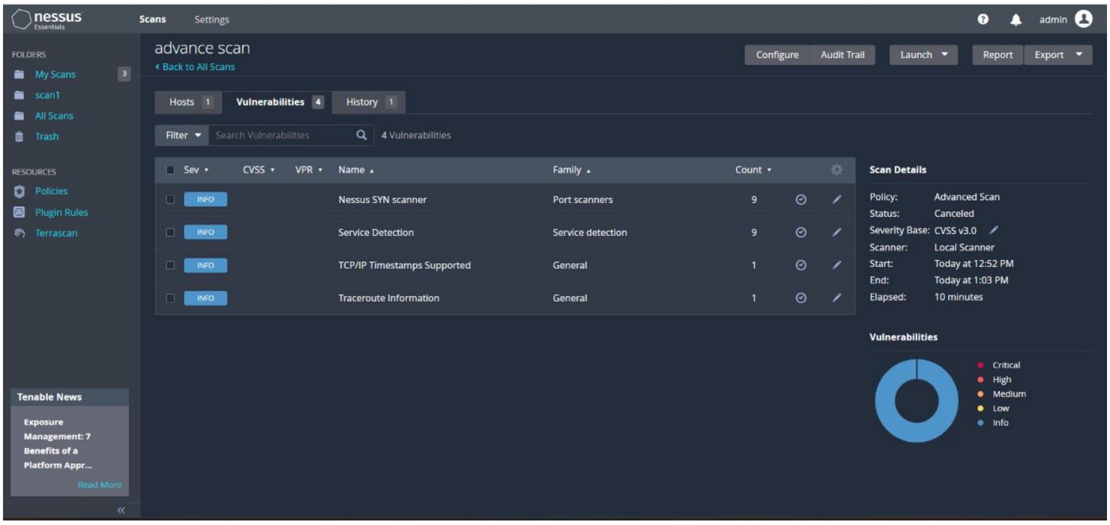
Host	Vulnerabilities
63.141.128.21	20

Scan Details

Policy:	Advanced Scan
Status:	Canceled
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 12:52 PM
End:	Today at 1:03 PM
Elapsed:	10 minutes

Vulnerabilities

The 4 same vulnerabilities were found.



advance scan

‹ Back to All Scans

4 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
INFO			Nessus SYN scanner	Port scanners	9
INFO			Service Detection	Service detection	9
INFO			TCP/IP Timestamps Supported	General	1
INFO			Traceroute Information	General	1

Scan Details

Policy:	Advanced Scan
Status:	Canceled
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 12:52 PM
End:	Today at 1:03 PM
Elapsed:	10 minutes

Vulnerabilities

So this is my vulnerability scanning report – **Sadiq Sonalkar**