

Assignment 1

Name : Bhargava Sai Jetti

College : Dr.Lankapalli Bullayya College

Regd.No : 721128805292

Date : 16/02/2024

What is Footprinting?

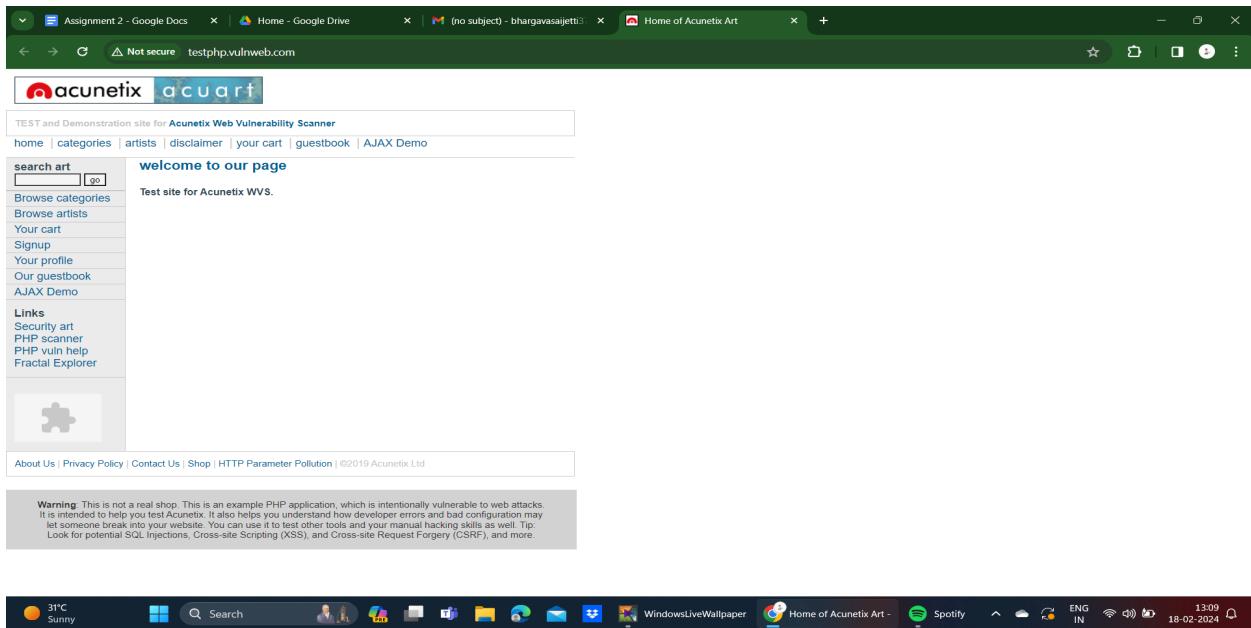
Footprinting is the process of gathering information about a target system or network to create a profile or "footprint" of its infrastructure, services, and security posture. This information can include details about the organization's domain names, IP addresses, network topology, employee names, email addresses, and more. Footprinting techniques often involve passive information gathering through sources like search engines, social media, public databases, and company websites.

What is Reconnaissance?

Reconnaissance, also known as "recon," is the active process of scanning and probing a target system or network to gather additional information beyond what is available through passive footprinting.

Reconnaissance activities typically involve techniques such as network scanning, port scanning, banner grabbing, and vulnerability scanning to identify potential points of entry or weaknesses in the target's defenses. The goal of reconnaissance is to obtain detailed insights into the target's infrastructure, services, and security vulnerabilities to aid in further analysis or exploitation.

The website to perform Footprinting & Reconnaissance is - <http://testphp.vulnweb.com/>



- By using various tools & techniques such “whois” lookup, Google dorking, website analysis tools , and social engineering techniques the information is gathered about the target website .

Step 1 - Open kali linux



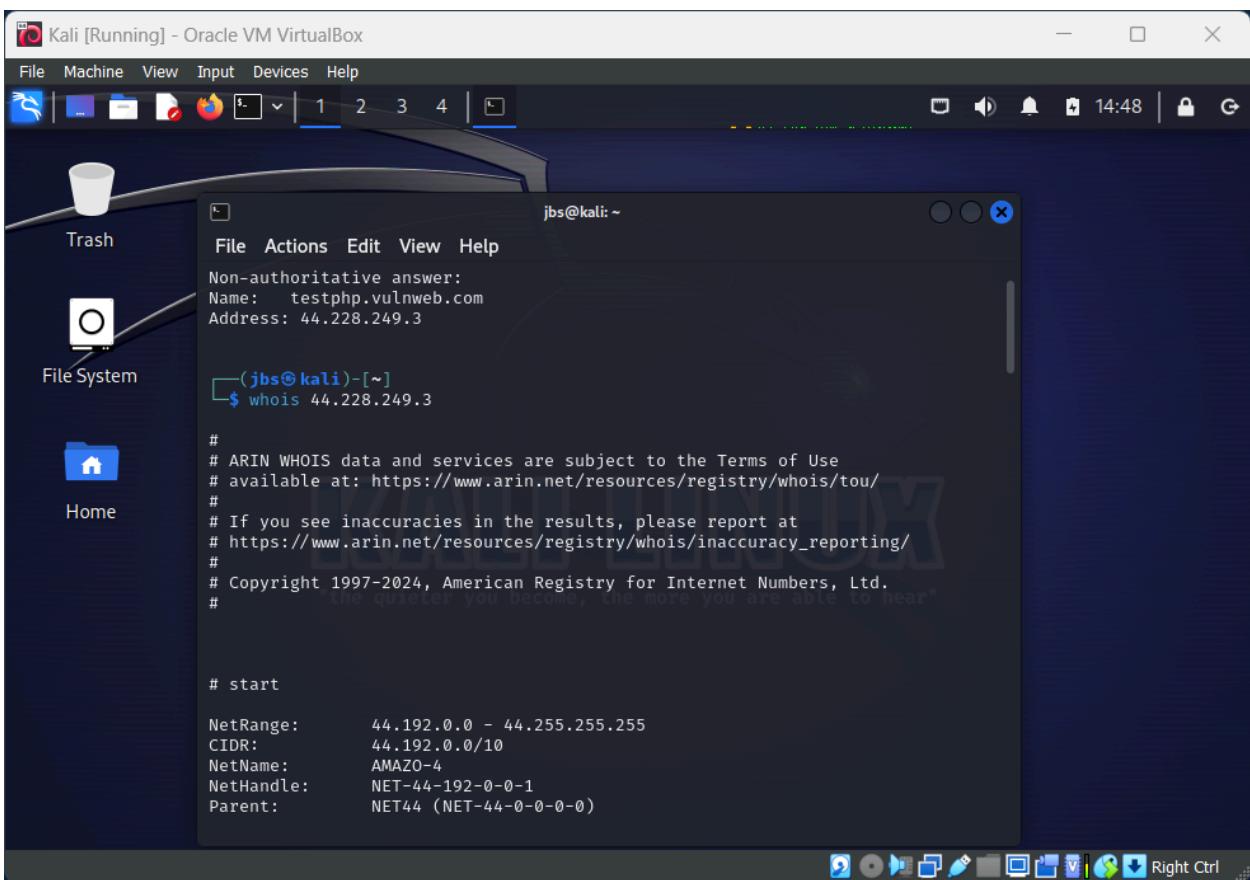
Step 2 - Open Terminal emulator in kali linux.

In there use “**nslookup**” command for the site - “testphp.vulnweb.com”

```
(jbs㉿kali)-[~]
$ nslookup testphp.vulnweb.com
;; communications error to 192.168.91.163#53: timed out
Server:      192.168.91.163
Address:     192.168.91.163#53

Non-authoritative answer:
Name:  testphp.vulnweb.com
Address: 44.228.249.3
```

Step 3 - Copy the address and use “**whois**” command for getting data as follows



The screenshot shows a Kali Linux desktop environment. A terminal window titled "jbs@kali: ~" is open, displaying the output of a "nslookup" command for "testphp.vulnweb.com". It shows a "communications error" due to a timeout. Below this, a "whois" command is run against the IP address 44.228.249.3, which returns ARIN WHOIS data. The data includes the NetRange (44.192.0.0 - 44.255.255.255), CIDR (44.192.0.0/10), NetName (AMAZO-4), NetHandle (NET-44-192-0-0-1), and Parent (NET44 (NET-44-0-0-0-0)). A file manager window is also visible in the background, showing a "File System" tree with icons for Trash, Home, and a folder named "File System". The desktop interface includes a dock at the bottom with various application icons.

```
jbs@kali: ~
$ nslookup testphp.vulnweb.com
;; communications error to 192.168.91.163#53: timed out
Server:      192.168.91.163
Address:     192.168.91.163#53

Non-authoritative answer:
Name:  testphp.vulnweb.com
Address: 44.228.249.3

(jbs㉿kali)-[~]
$ whois 44.228.249.3

#
# 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.
#           "The quieter you become, the more you are able to hear"

#
# start

NetRange:      44.192.0.0 - 44.255.255.255
CIDR:         44.192.0.0/10
NetName:       AMAZO-4
NetHandle:    NET-44-192-0-0-1
Parent:        NET44 (NET-44-0-0-0-0)
```

```
Kali [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Trash  
File System  
Home  
jbs@kali: ~  
File Actions Edit View Help  
NetRange: 44.192.0.0 - 44.255.255.255  
CIDR: 44.192.0.0/10  
NetName: AMAZO-4  
NetHandle: NET-44-192-0-0-1  
Parent: NET44 (NET-44-0-0-0-0)  
NetType: Direct Allocation  
OriginAS:  
Organization: Amazon.com, Inc. (AMAZO-4)  
RegDate: 2019-07-18  
Updated: 2019-07-18  
Ref: https://rdap.arin.net/registry/ip/44.192.0.0  
  
OrgName: Amazon.com, Inc.  
OrgId: AMAZO-4  
Address: Amazon Web Services, Inc.  
Address: P.O. Box 81226  
City: Seattle  
StateProv: WA  
PostalCode: 98108-1226  
Country: US  
RegDate: 2005-09-29  
Updated: 2022-09-30  
Comment: For details of this service please see  
Comment: http://ec2.amazonaws.com  
jbs@kali: ~
```

```
Kali [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Trash  
File System  
Home  
jbs@kali: ~  
File Actions Edit View Help  
Updated: 2022-09-30  
Comment: For details of this service please see  
Comment: http://ec2.amazonaws.com  
Ref: https://rdap.arin.net/registry/entity/AMAZO-4  
  
OrgAbuseHandle: AEA8-ARIN  
OrgAbuseName: Amazon EC2 Abuse  
OrgAbusePhone: +1-206-555-0000  
OrgAbuseEmail: abuse@amazonaws.com  
OrgAbuseRef: https://rdap.arin.net/registry/entity/AEA8-ARIN  
  
OrgTechHandle: AN024-ARIN  
OrgTechName: Amazon EC2 Network Operations  
OrgTechPhone: +1-206-555-0000  
OrgTechEmail: amzn-noc-contact@amazon.com  
OrgTechRef: https://rdap.arin.net/registry/entity/AN024-ARIN  
  
OrgRoutingHandle: IPROU3-ARIN  
OrgRoutingName: IP Routing  
OrgRoutingPhone: +1-206-555-0000  
OrgRoutingEmail: aws-routing-poc@amazon.com  
OrgRoutingRef: https://rdap.arin.net/registry/entity/IPROU3-ARIN  
  
OrgNOCHandle: AANO1-ARIN  
OrgNOCName: Amazon AWS Network Operations  
OrgNOCPhone: +1-206-555-0000  
jbs@kali: ~
```

```
Kali [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Trash  
File System  
Home  
Notifications  
File Actions Edit View Help  
jbs@kali: ~  
OrgTechHandle: AN024-ARIN  
OrgTechName: Amazon EC2 Network Operations  
OrgTechPhone: +1-206-555-0000  
OrgTechEmail: amzn-noc-contact@amazon.com  
OrgTechRef: https://rdap.arin.net/registry/entity/AN024-ARIN  
  
OrgRoutingHandle: IPROU3-ARIN  
OrgRoutingName: IP Routing  
OrgRoutingPhone: +1-206-555-0000  
OrgRoutingEmail: aws-routing-poc@amazon.com  
OrgRoutingRef: https://rdap.arin.net/registry/entity/IPROU3-ARIN  
  
OrgNOCHandle: AAN01-ARIN  
OrgNOCName: Amazon AWS Network Operations  
OrgNOCPhone: +1-206-555-0000  
OrgNOCEmail: amzn-noc-contact@amazon.com  
OrgNOCRef: https://rdap.arin.net/registry/entity/AAN01-ARIN  
  
OrgRoutingHandle: ARMP-ARIN  
OrgRoutingName: AWS RPKI Management POC  
OrgRoutingPhone: +1-206-555-0000  
OrgRoutingEmail: aws-rpki-routing-poc@amazon.com  
OrgRoutingRef: https://rdap.arin.net/registry/entity/ARMP-ARIN  
  
# end
```

```
Kali [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
Trash  
File System  
Home  
jbs@kali: ~  
File Actions Edit View Help  
# start  
  
NetRange: 44.224.0.0 - 44.255.255.255  
CIDR: 44.224.0.0/11  
NetName: AMAZO-ZPDX  
NetHandle: NET-44-224-0-0-1  
Parent: AMAZO-4 (NET-44-192-0-0-1)  
NetType: Reallocated  
OriginAS:  
Organization: Amazon.com, Inc. (AMAZO-47)  
RegDate: 2019-08-01  
Updated: 2019-08-01  
Ref: https://rdap.arin.net/registry/ip/44.224.0.0  
  
OrgName: "the Amazon.com, Inc.  
OrgId: AMAZO-47  
Address: EC2, EC2 1200 12th Ave South  
City: Seattle  
StateProv: WA  
PostalCode: 98144  
Country: US  
RegDate: 2011-05-10  
Updated: 2021-07-22  
Ref: https://rdap.arin.net/registry/entity/AMAZO-47
```

```
jbs@kali: ~
File Actions Edit View Help
OrgAbuseHandle: AEA8-ARIN
OrgAbuseName: Amazon EC2 Abuse
OrgAbusePhone: +1-206-555-0000
OrgAbuseEmail: abuse@amazonaws.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/AEA8-ARIN

OrgNOCHandle: AAN01-ARIN
OrgNOCName: Amazon AWS Network Operations
OrgNOCPhone: +1-206-555-0000
OrgNOCEmail: amzn-noc-contact@amazon.com
OrgNOCRef: https://rdap.arin.net/registry/entity/AAN01-ARIN

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName: AWS RPKI Management POC
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-rpki-routing-poc@amazon.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/ARMP-ARIN

OrgTechHandle: ANO24-ARIN
OrgTechName: Amazon EC2 Network Operations
OrgTechPhone: +1-206-555-0000
OrgTechEmail: amzn-noc-contact@amazon.com
OrgTechRef: https://rdap.arin.net/registry/entity/ANO24-ARIN

OrgRoutingHandle: IPROUT3-ARIN
OrgRoutingName: IP Routing
```

```
jbs@kali: ~
File Actions Edit View Help
OrgTechPhone: +1-206-555-0000
OrgTechEmail: amzn-noc-contact@amazon.com
OrgTechRef: https://rdap.arin.net/registry/entity/ANO24-ARIN

OrgRoutingHandle: IPROUT3-ARIN
OrgRoutingName: IP Routing
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-routing-poc@amazon.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/IPROUT3-ARIN

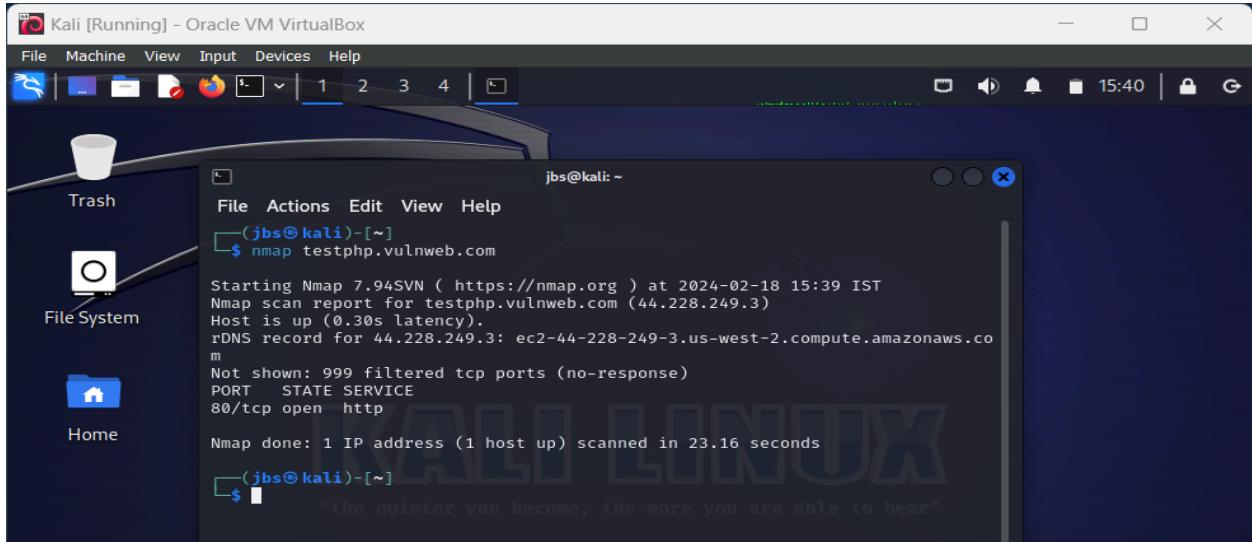
# end

#
# 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.
#

(jbs@kali)-[~]
$
```

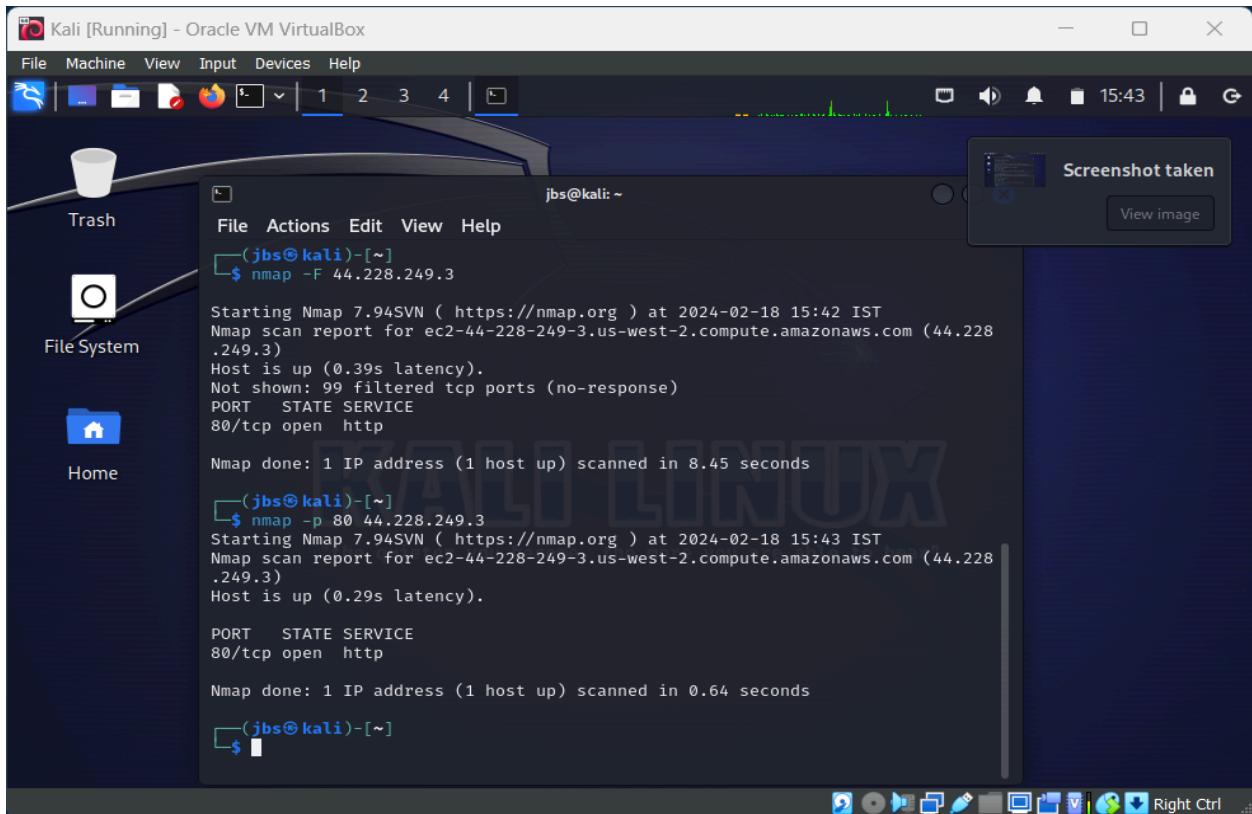
So, we got a lot of information as shown in the pictures above. Therefore Footprinting & Reconnaissance are performed using “**whois**” command

Now let's use “nmap” command



```
jbs@kali: ~
File Actions Edit View Help
(jbs@kali)-[~]
$ nmap testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 15:39 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.30s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.co
m
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 23.16 seconds
(jbs@kali)-[~]
```

- We got one open port
- Along with “nmap” we use “**-F**” to speed up scanning & “**-p+port_number**” to scan specific port



```
jbs@kali: ~
File Actions Edit View Help
(jbs@kali)-[~]
$ nmap -F 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 15:42 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228
.249.3)
Host is up (0.39s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 8.45 seconds
(jbs@kali)-[~]
$ nmap -p 80 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 15:43 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228
.249.3)
Host is up (0.29s latency).

PORT      STATE SERVICE
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
(jbs@kali)-[~]
```

- We used “-A” to scan aggressively in detail and we also got one extra column “VERSION”.

```
Nmap done: 1 IP address (1 host up) scanned in 30.80 seconds

[jbs@kali:~]
$ nmap -A 44.228.249.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 15:49 IST
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.64% done; ETC: 15:50 (0:00:00 remaining)
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228
.249.3)
Host is up (0.31s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.19.0

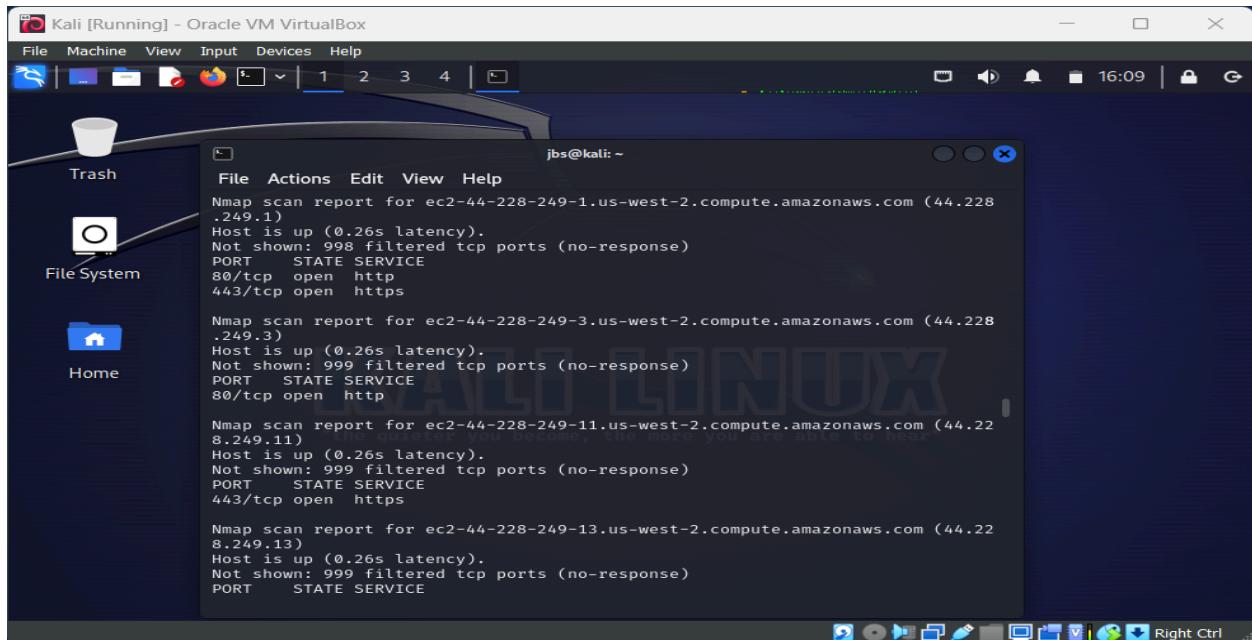
Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.93 seconds

[jbs@kali:~]
$
```

- We used a specific command “**address/24**” as follows to check for the others devices/users on the network

```
[jbs@kali:~]
$ nmap 44.228.249.3/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 15:55 IST
```

- We get the data related to the other user devices & also along with their IP-address, but it takes time for output and it performs a long scan,



The screenshot shows a Kali Linux desktop environment with several windows open. One window is a terminal window titled 'jbs@kali: ~' displaying Nmap scan reports for four different IP addresses: 44.228.249.1, 44.228.249.3, 44.228.249.11, and 44.228.249.13. Each report shows the host is up with low latency, no response for many ports, and open ports 80/tcp (http) and 443/tcp (https). Another window shows a file manager with icons for Trash, File System, and Home. The desktop background has a faint watermark of the word 'KALI'.

```
jbs@kali: ~
File Actions Edit View Help
Nmap scan report for ec2-44-228-249-1.us-west-2.compute.amazonaws.com (44.228
.249.1)
Host is up (0.26s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228
.249.3)
Host is up (0.26s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for ec2-44-228-249-11.us-west-2.compute.amazonaws.com (44.22
8.249.11)
Host is up (0.26s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
443/tcp   open  https

Nmap scan report for ec2-44-228-249-13.us-west-2.compute.amazonaws.com (44.22
8.249.13)
Host is up (0.26s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
```

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Trash

File System

Home

jbs@kali: ~

```
File Actions Edit View Help
28.249.245)
Host is up (0.26s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for ec2-44-228-249-247.us-west-2.compute.amazonaws.com (44.2
28.249.247)
Host is up (0.26s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
443/tcp   open  https

Nmap scan report for ec2-44-228-249-253.us-west-2.compute.amazonaws.com (44.2
28.249.253)
Host is up (0.26s latency).u become, the more you are able to hear'
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (37 hosts up) scanned in 240.19 seconds

(jbs@kali)-[~]
```

So, we conclude that we have found 256 IP addresses and 37 hosts are up.