Assignment 1

Name : Bhargava Sai Jetti
College : Dr.Lankapalli Bullayya College
Regd.No : 721128805292
Date : 16/02/2024

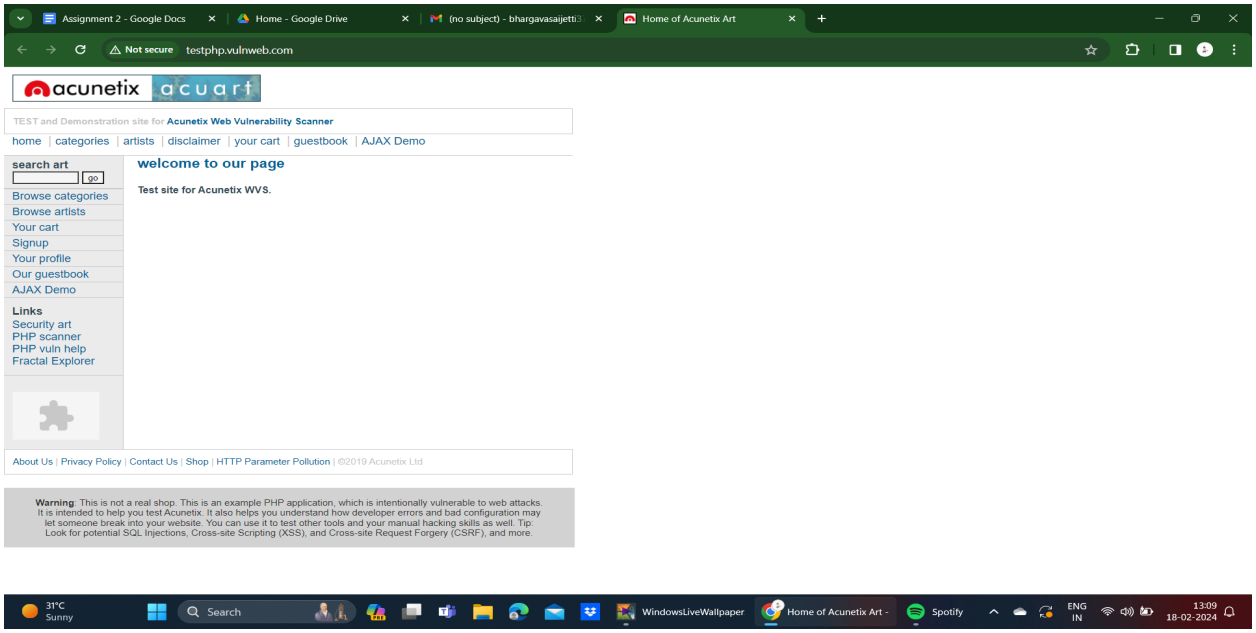
What is Footprinting?

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/



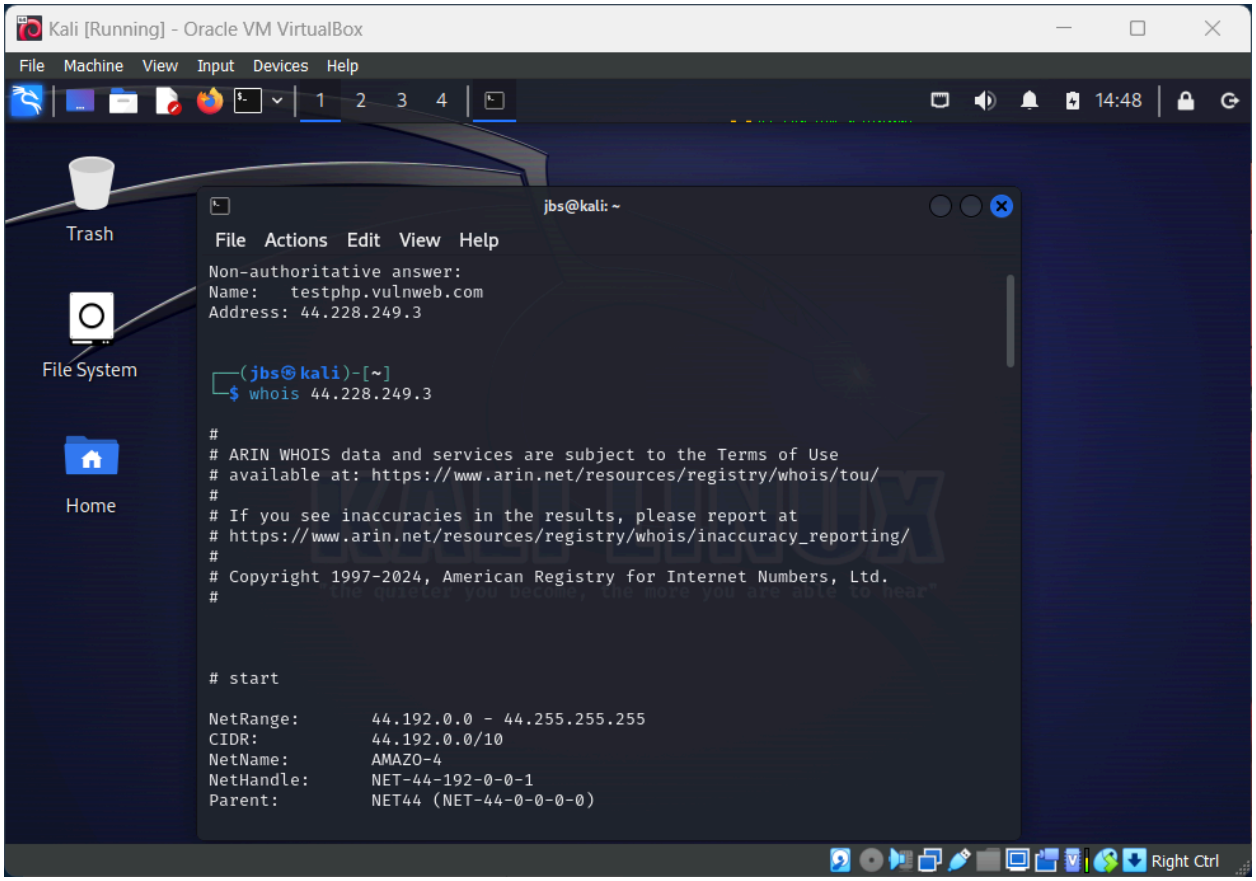
- **By using various tools & techniques such “whois” lookup, Google dorking, website analysis tools , and social engineering techniques the information is gathered about the target website .**

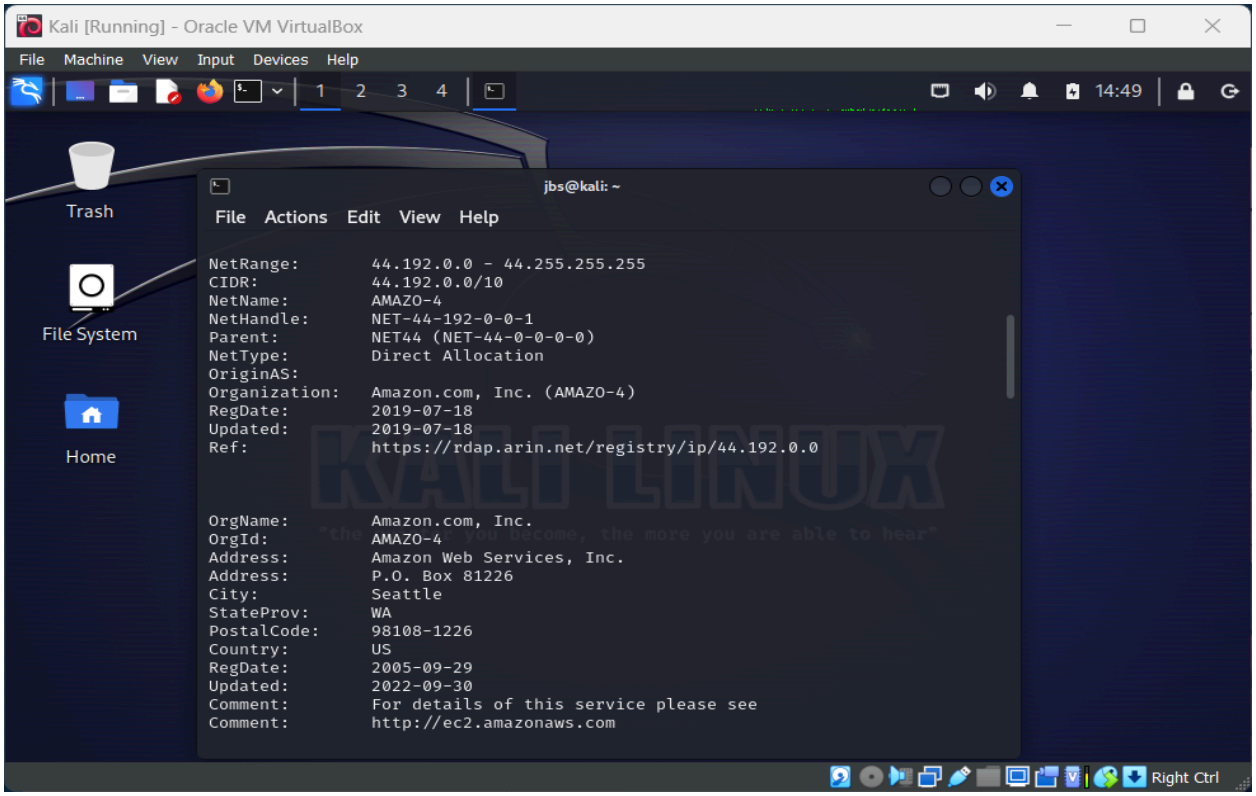
Step 1 - Open kali linux

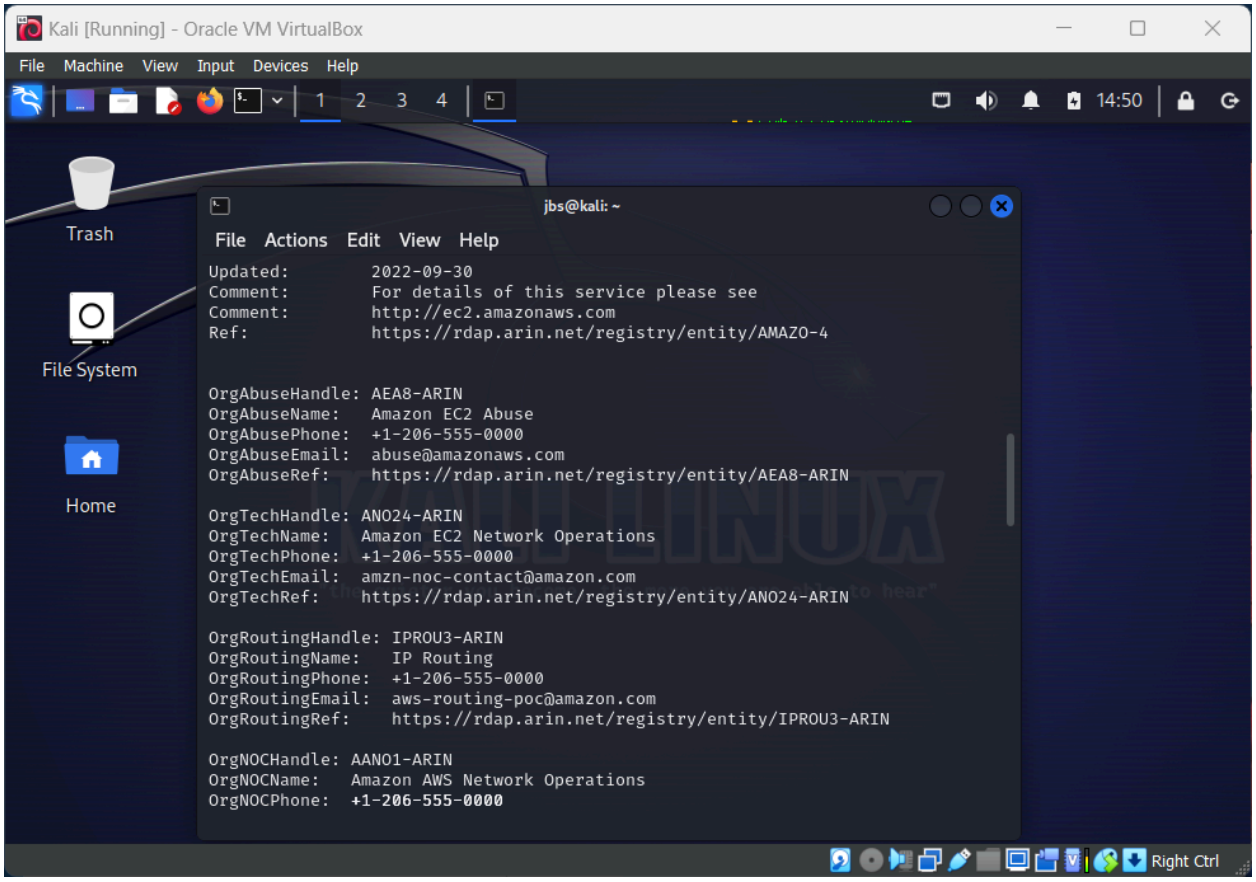
Step 2 - Open Terminal emulator in kali linux.
In there use **“nslookup”** command for the site - “testphp.vulnweb.com”

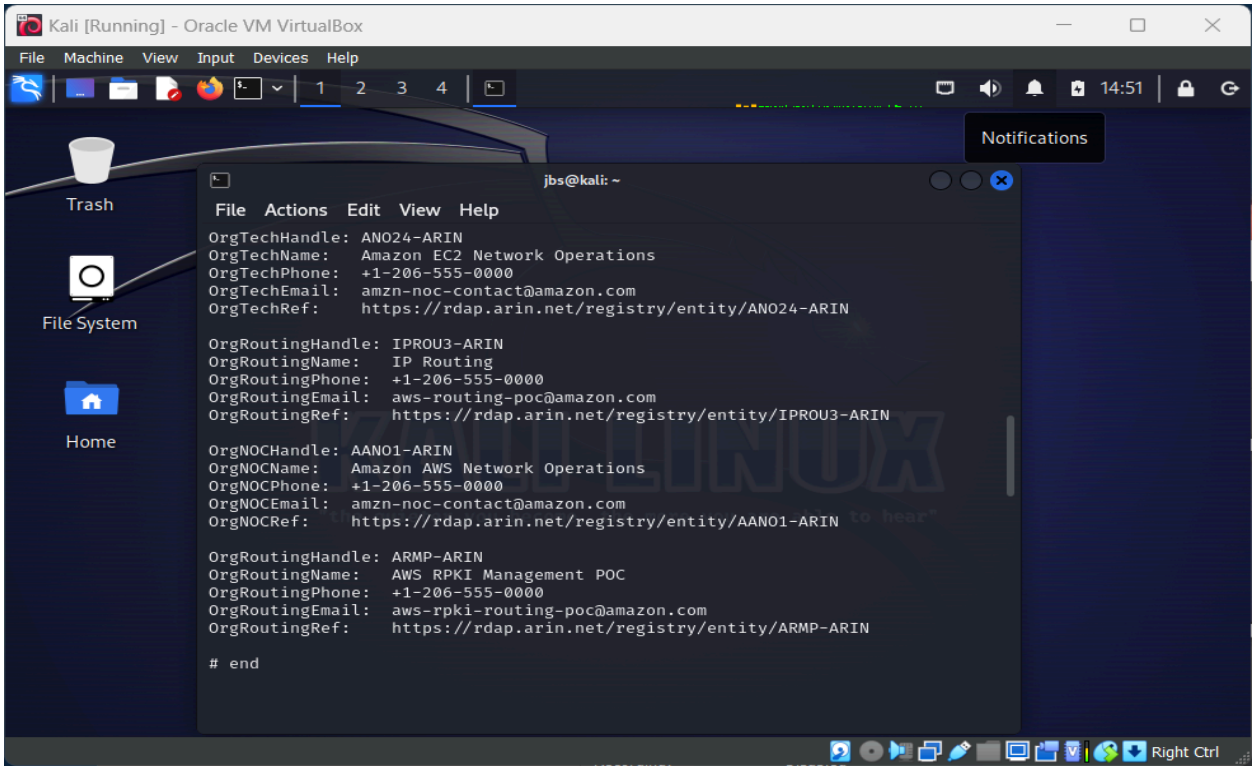
```
┌──(jbs㉿kali)-[~]
└─$ nslookup testphp.vulnweb.com
;; communications error to 192.168.91.163#53: timed out
Server:         192.168.91.163
Address:        192.168.91.163#53

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

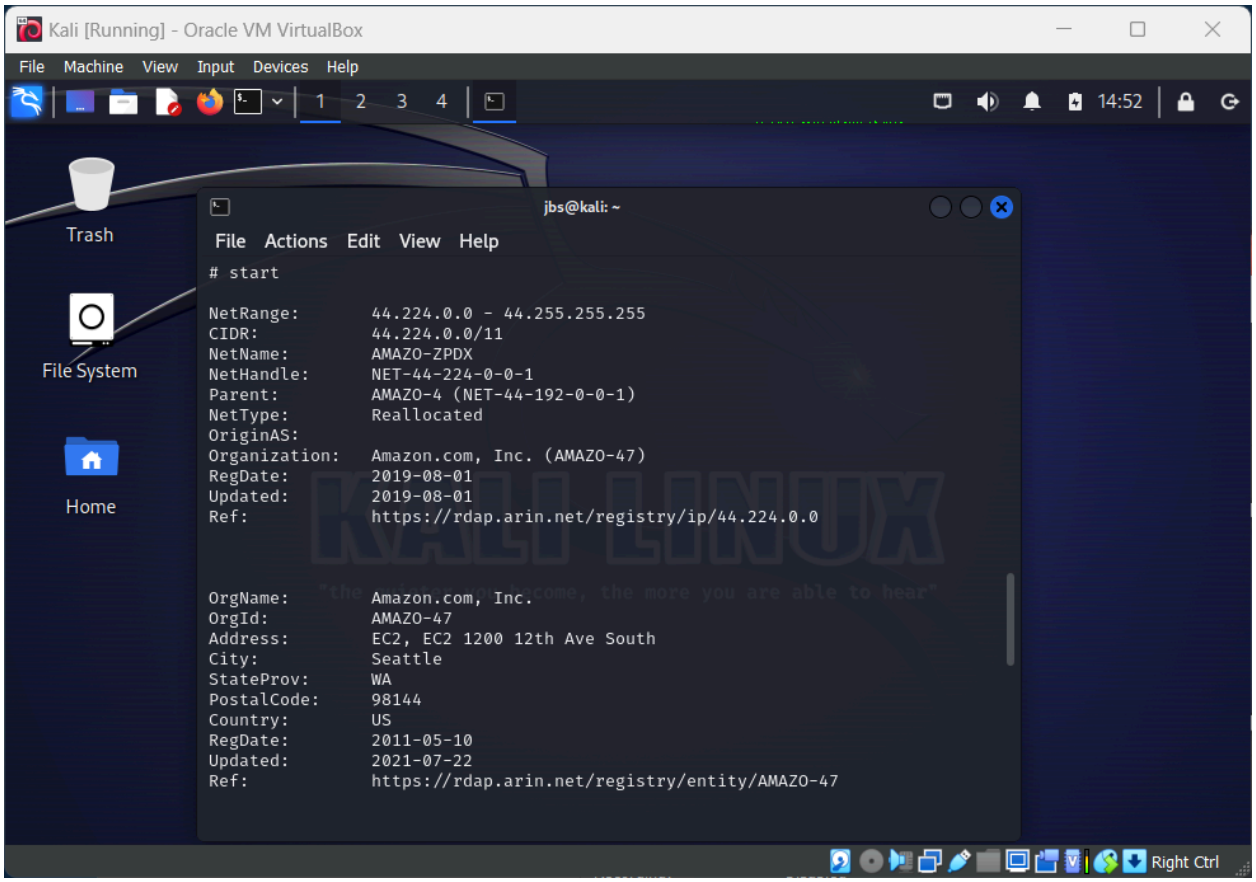
Step 3 - Copy the address and use **“whois”** command for getting data as follows

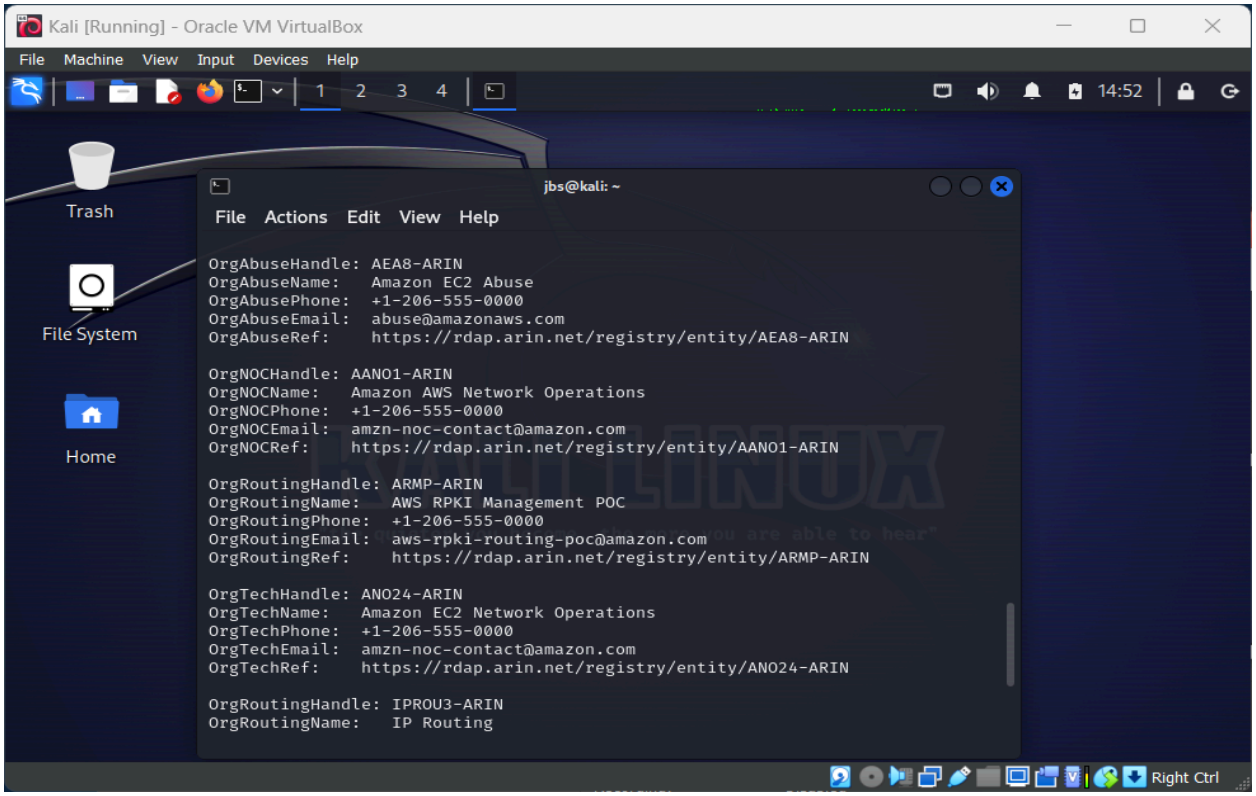


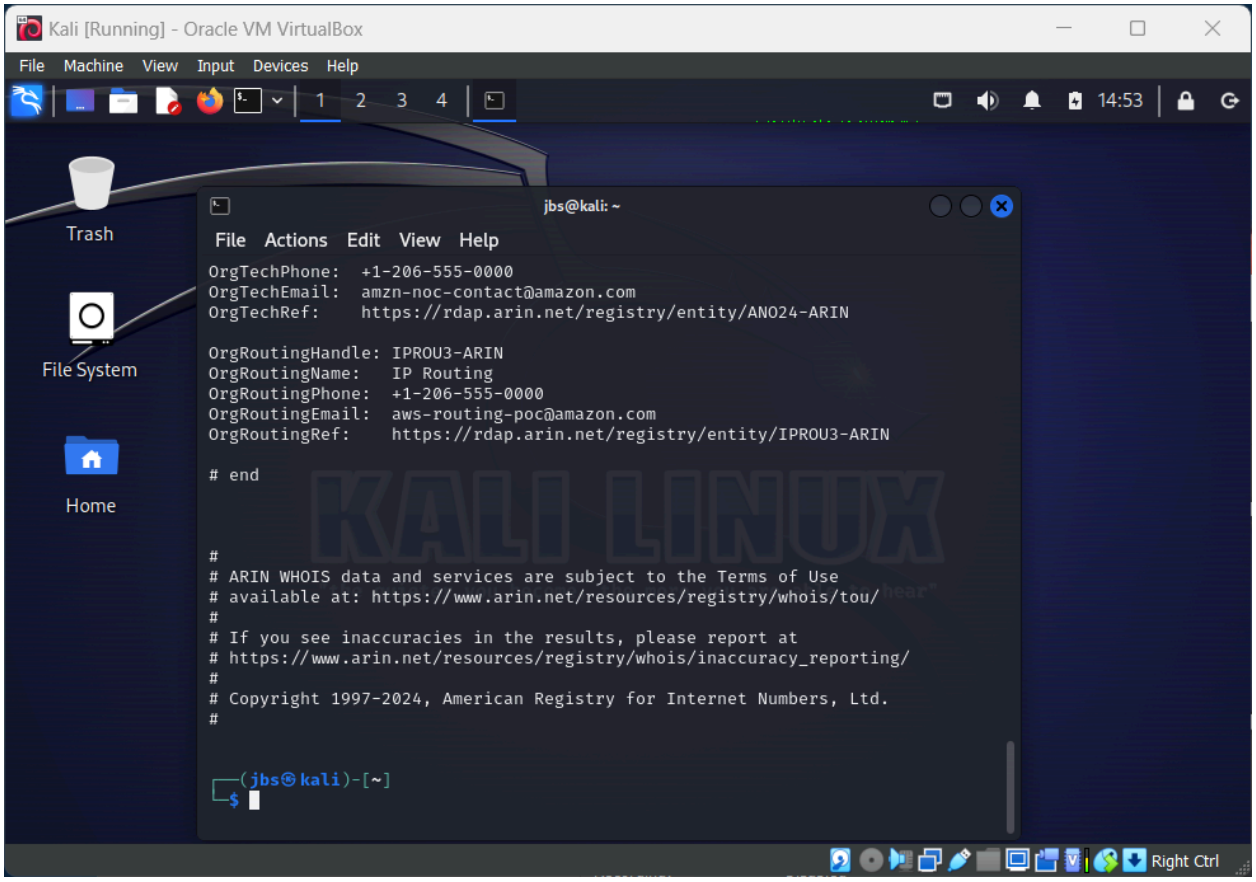

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
14:49
Trash
File System
Home
jbs@kali: ~
File Actions Edit View Help
NetRange: 44.192.0.0 - 44.255.255.255
CIDR: 44.192.0.0/10
NetName: AMAZO-4
NetHandle: NET-44-192-0-0-1
Parent: NET44 (NET-44-0-0-0-0)
NetType: Direct 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
Right Ctrl


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
14:50
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: 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: 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
Right Ctrl


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
14:51
Notifications
Trash
File System
Home
jbs@kali: ~
File Actions Edit View Help
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: 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
OrgNOCEmail: amzn-noc-contact@amazon.com
OrgNOCRef: https://rdap.arin.net/registry/entity/AANO1-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
Right Ctrl

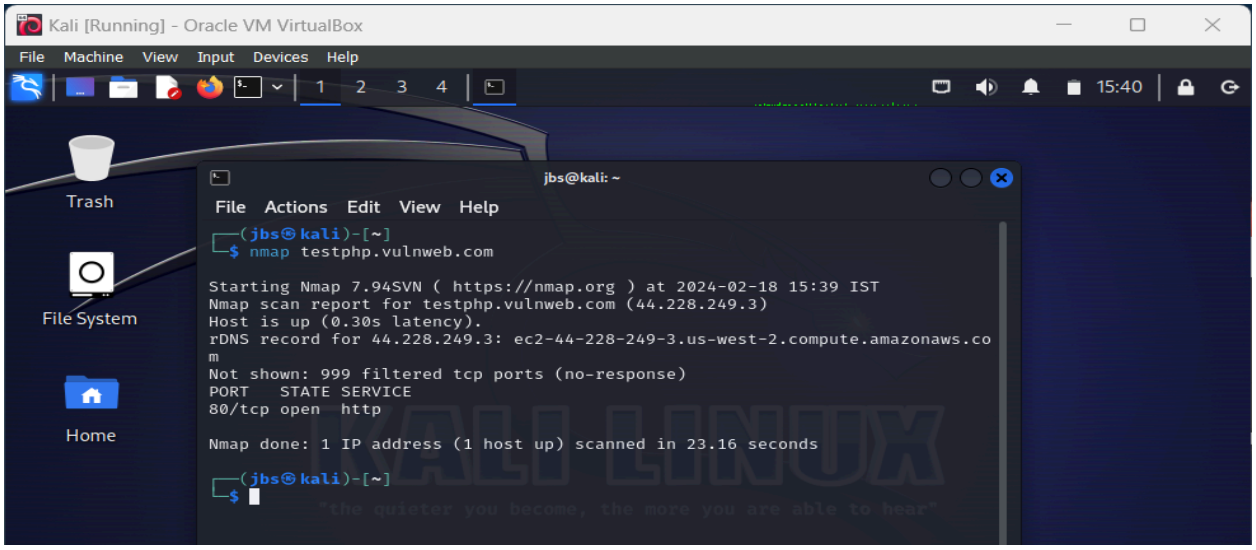

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
14:52
Trash
File System
Home
jbs@kali: ~
File Actions Edit View Help
start
NetRange: 44.224.0.0 - 44.255.255.255
CIDR: 44.224.0.0/11
NetName: AMAZO-ZPDX
NetHandle: NET-44-224-0-0-1
Parent: AMAZO-4 (NET-44-192-0-0-1)
NetType: 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: 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
Right Ctrl


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
14:52
Trash
File System
Home
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: AANO1-ARIN
OrgNOCName: Amazon AWS Network Operations
OrgNOCPhone: +1-206-555-0000
OrgNOCEmail: amzn-noc-contact@amazon.com
OrgNOCRef: https://rdap.arin.net/registry/entity/AANO1-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: IPROU3-ARIN
OrgRoutingName: IP Routing
Right Ctrl

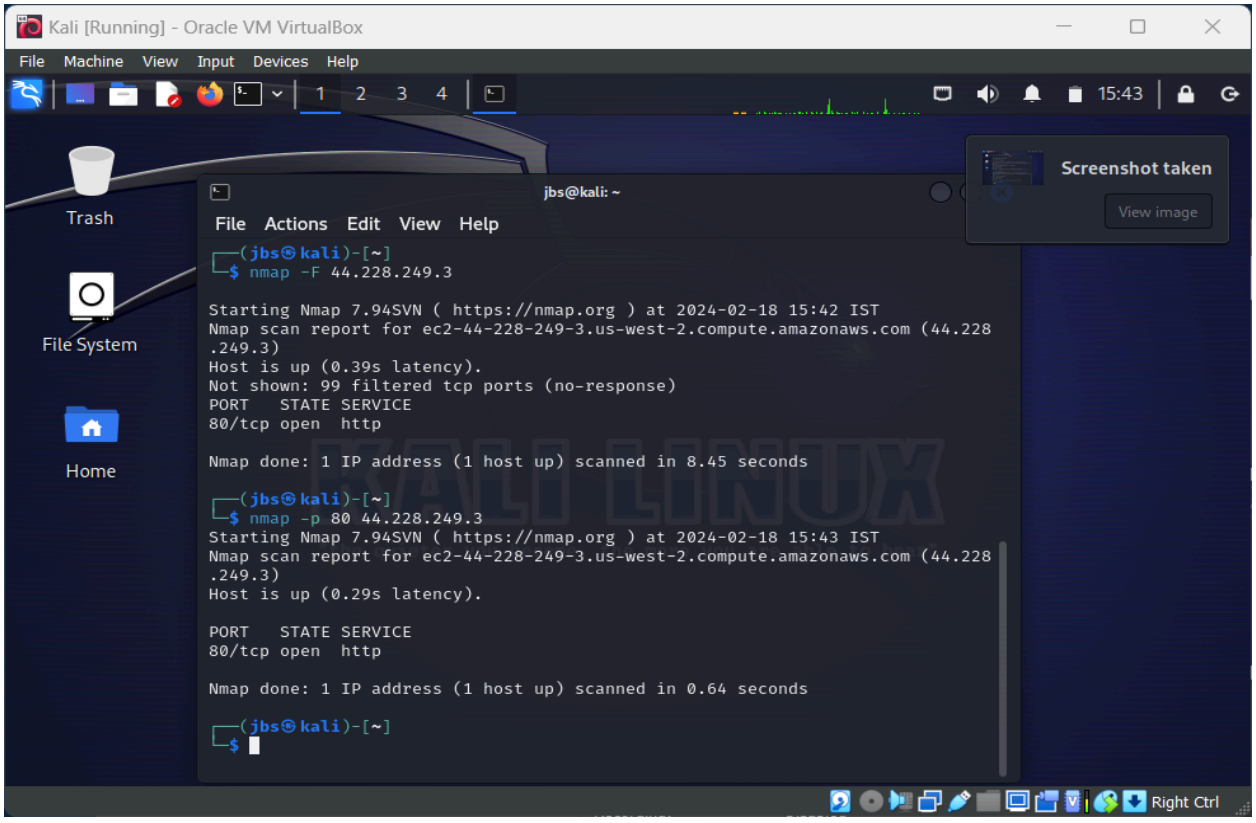

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
14:53
Trash
File System
Home
jbs@kali: ~
File Actions Edit View Help
OrgTechPhone: +1-206-555-0000
OrgTechEmail: amzn-noc-contact@amazon.com
OrgTechRef: https://rdap.arin.net/registry/entity/ANO24-ARIN
OrgRoutingHandle: 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
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)-[~]
$
Right Ctrl

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



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



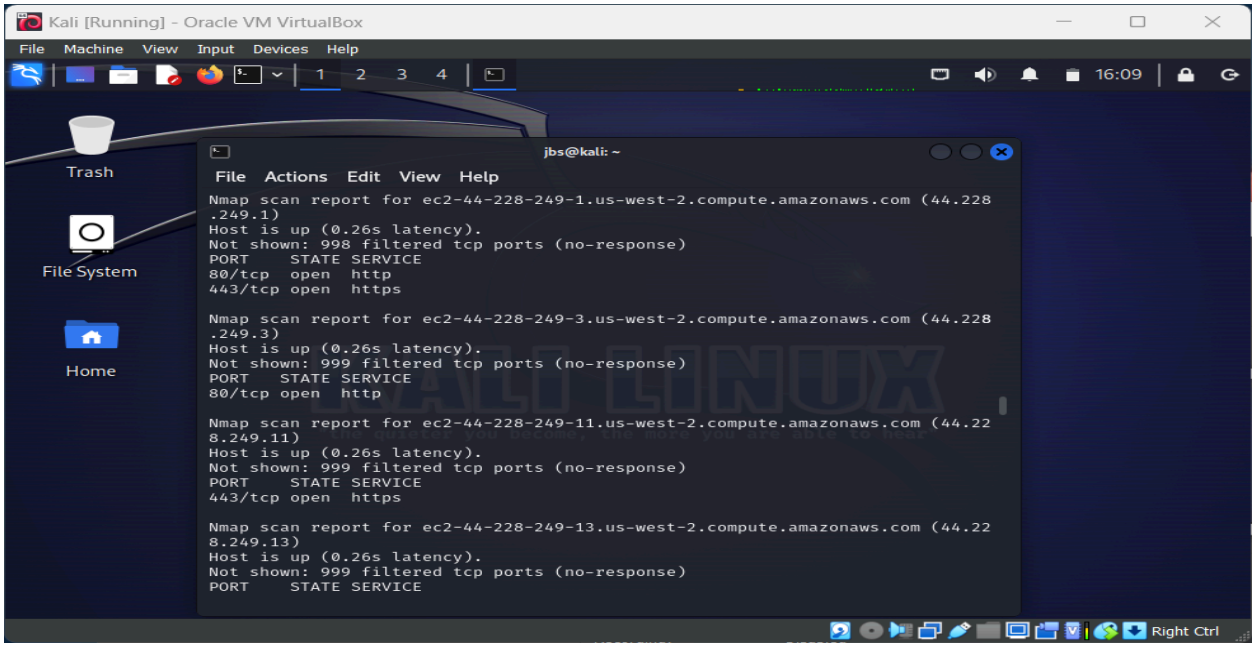
- We used **“-A”** to scan aggressively in detail and we also got one extra column **“VERSION”**.

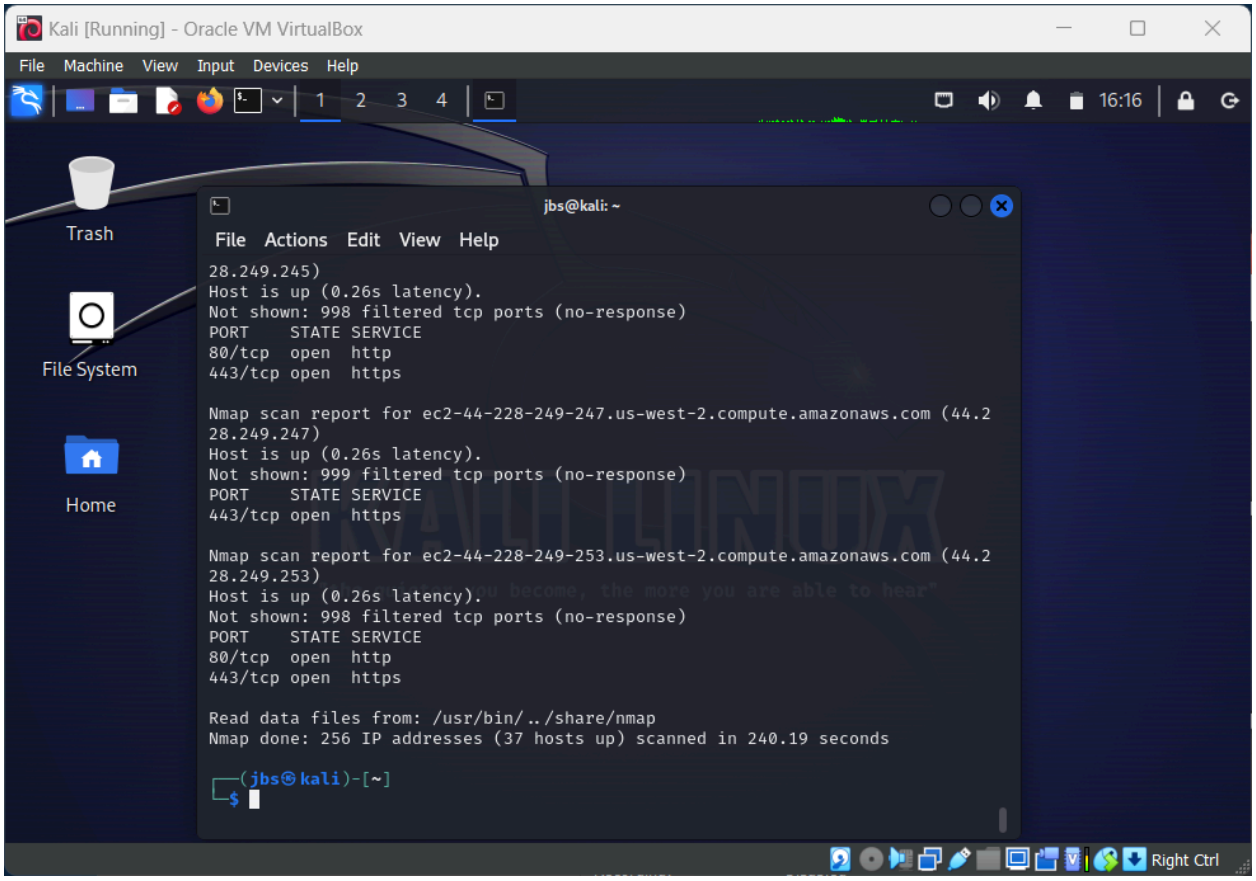
```
Nmap done: 1 IP address (1 host up) scanned in 30.80 seconds

┌──(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,





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