Assignment 1

Name :Kambala Raj Kumar
College :Dr.Lankapalli Bullayya College
Regd.No :721128805335
Date :16/02/2024

What is Footprinting ?

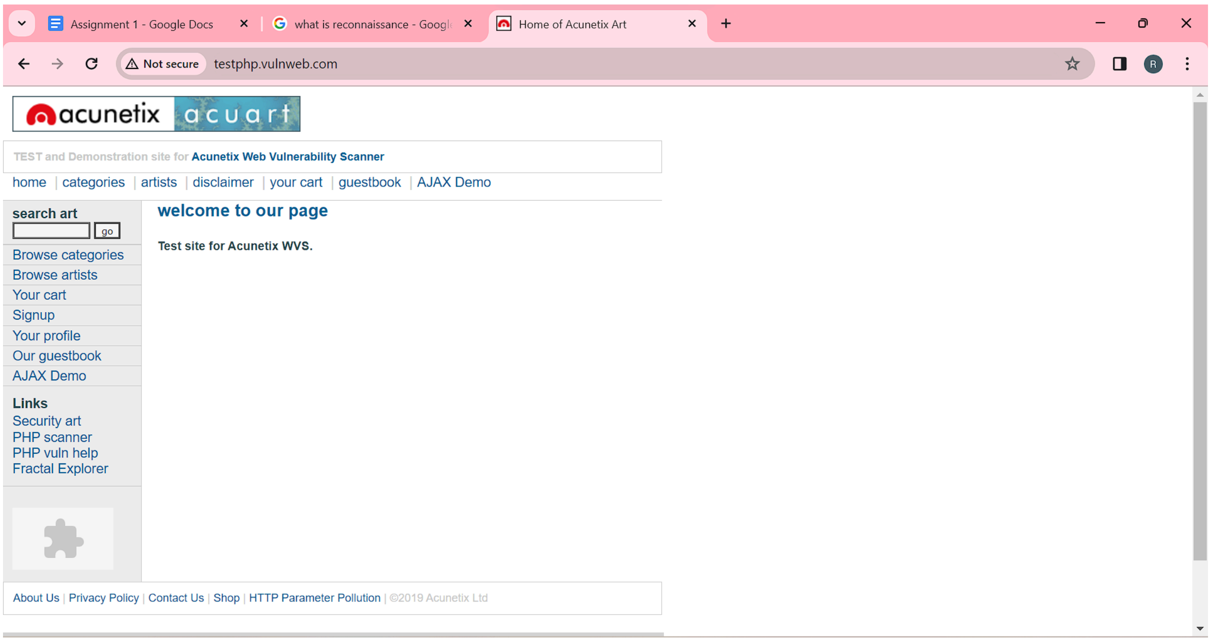
The process of cybersecurity footprinting involves profiling organisations and collecting data about the network, host, employees and third-party partners.There are two types of footprinting as follows below. Active Footprinting: Active footprinting means performing footprinting by getting in direct touch with the target machine. Passive Footprinting: Passive footprinting means collecting information about a system located at a remote distance from the attacker.

What is Reconnaissance?

Reconnaissance, often referred to as 'cyber reconnaissance' or 'cyber intelligence gathering', is the process of collecting information about potential targets, vulnerabilities, and attack vectors.Purpose: Reconnaissance and surveillance provides the commander with the information he needs to accomplish his mission. This information includes data on the terrain, weather, and the threat. R&S also provides early warning and security to the force and denies the threat information about friendly forces.

The Website to Perform Footprinting and Reconnaissance is -

http://testphp.vulnweb.com/



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

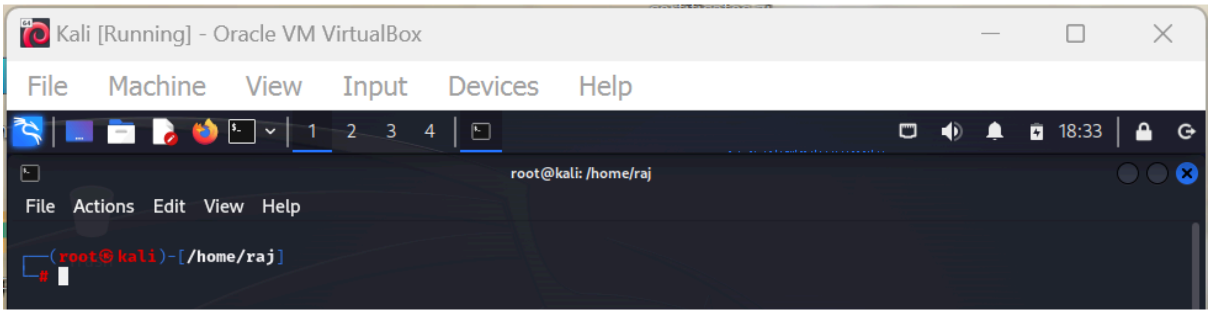
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

welcome to our page

Test site for Acunetix WVS.

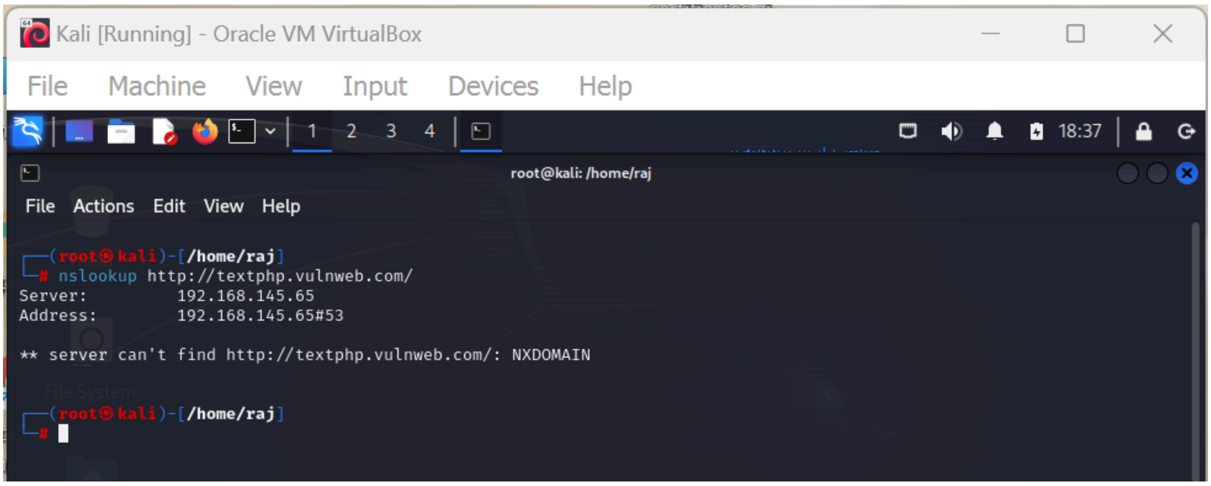
About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd

Step 1:open kali linux and change to root user


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:33
root@kali: /home/raj
File Actions Edit View Help

```
┌──(root㉿kali)-[/home/raj]
└─# 
```

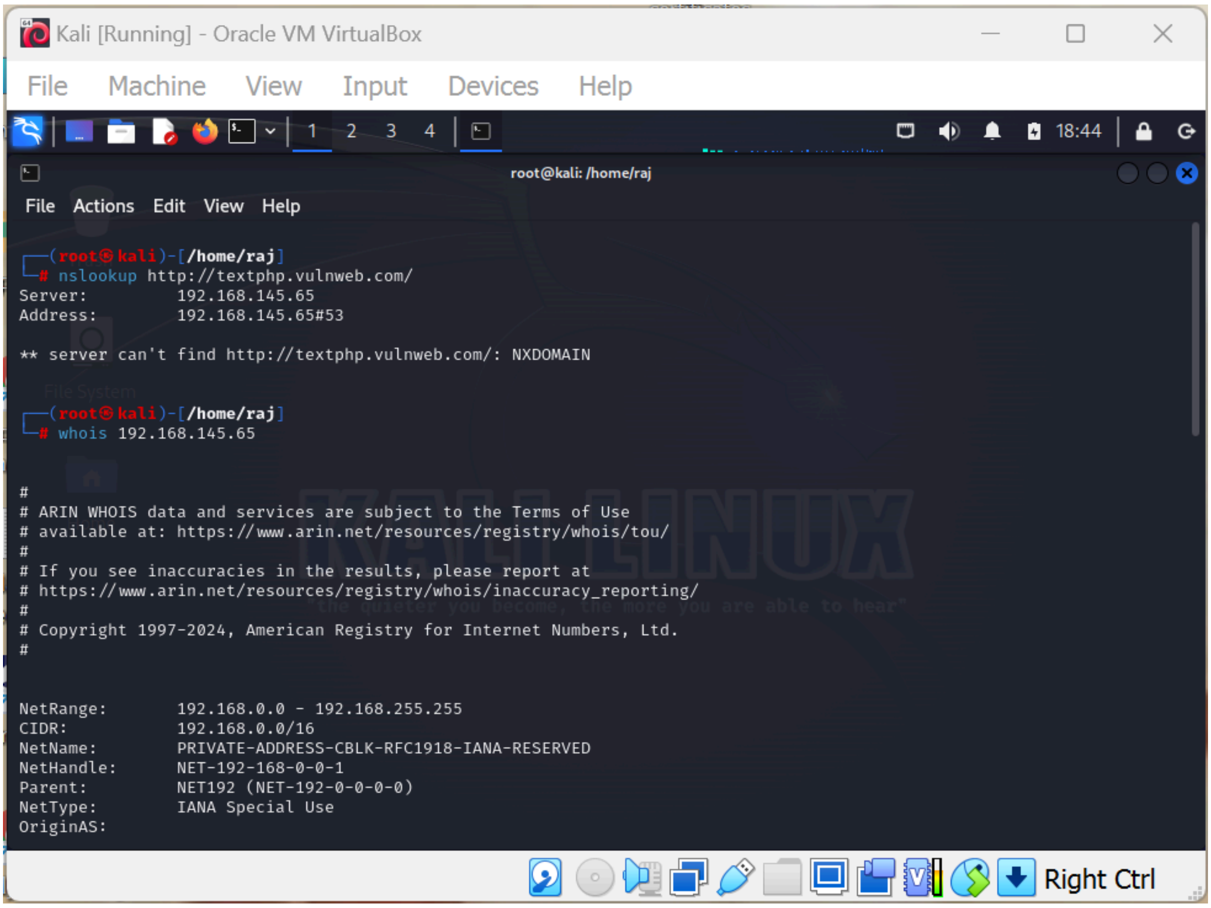
Step 2:use nslookup on the target


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:37
root@kali: /home/raj
File Actions Edit View Help

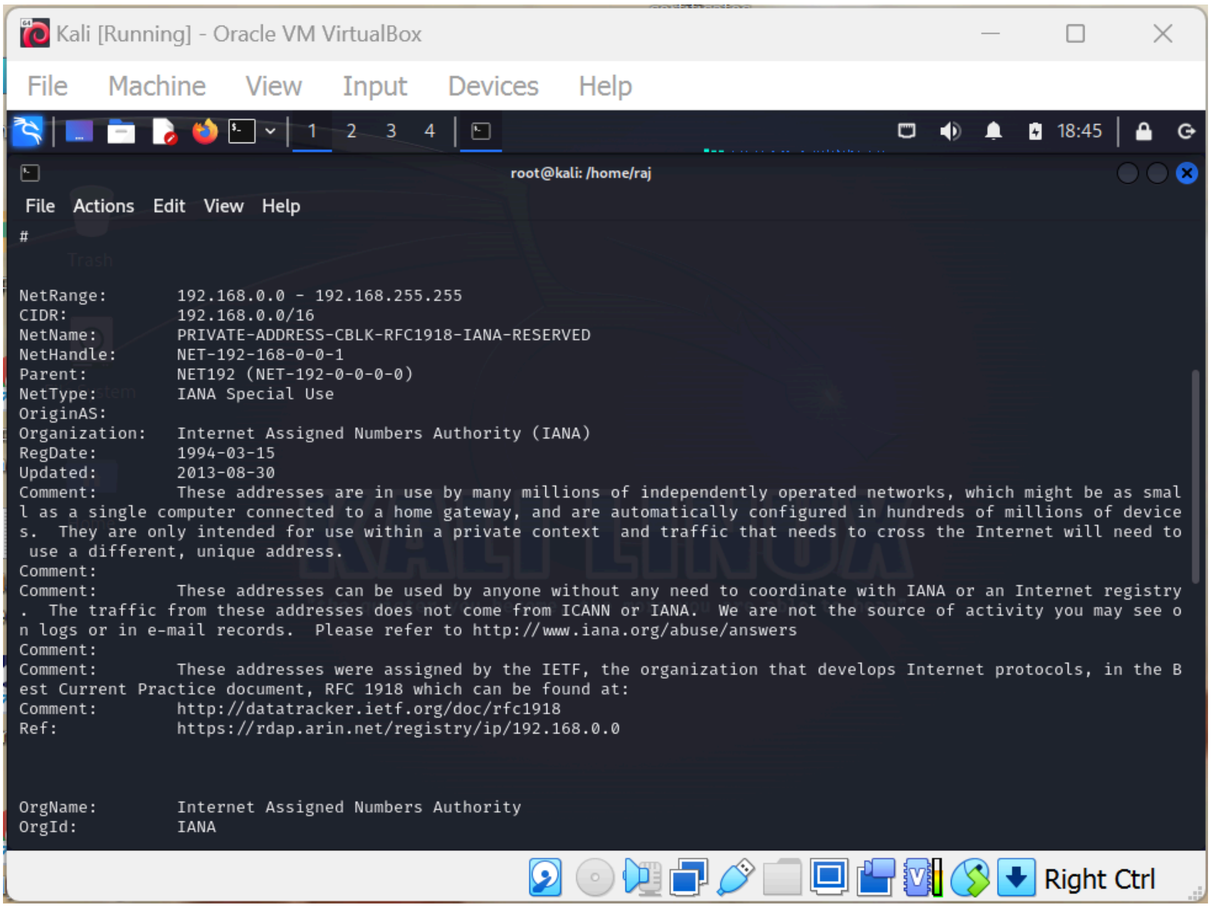
```
┌──(root㉿kali)-[/home/raj]
└─# nslookup http://textphp.vulnweb.com/
Server:         192.168.145.65
Address:        192.168.145.65#53

** server can't find http://textphp.vulnweb.com/: NXDOMAIN

┌──(root㉿kali)-[/home/raj]
└─# 
```

We got the server IP as shown above

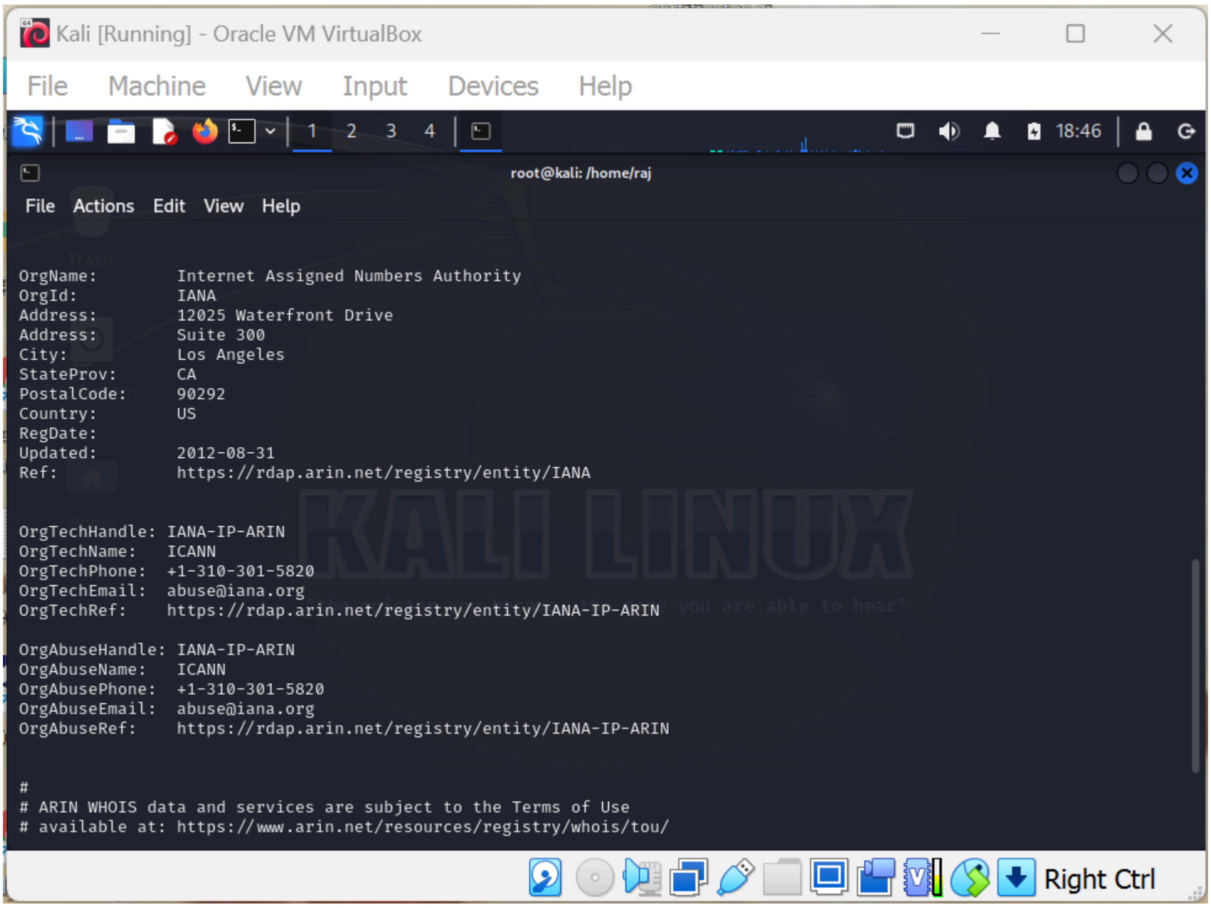
Step 3:now use whois command to gather information


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:44
root@kali: /home/raj
File Actions Edit View Help
Right Ctrl

```
┌──(root㉿kali)-[/home/raj]
└─# nslookup http://textphp.vulnweb.com/
Server:         192.168.145.65
Address:        192.168.145.65#53

** server can't find http://textphp.vulnweb.com/: NXDOMAIN

┌──(root㉿kali)-[/home/raj]
└─# whois 192.168.145.65


#
# 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:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
```

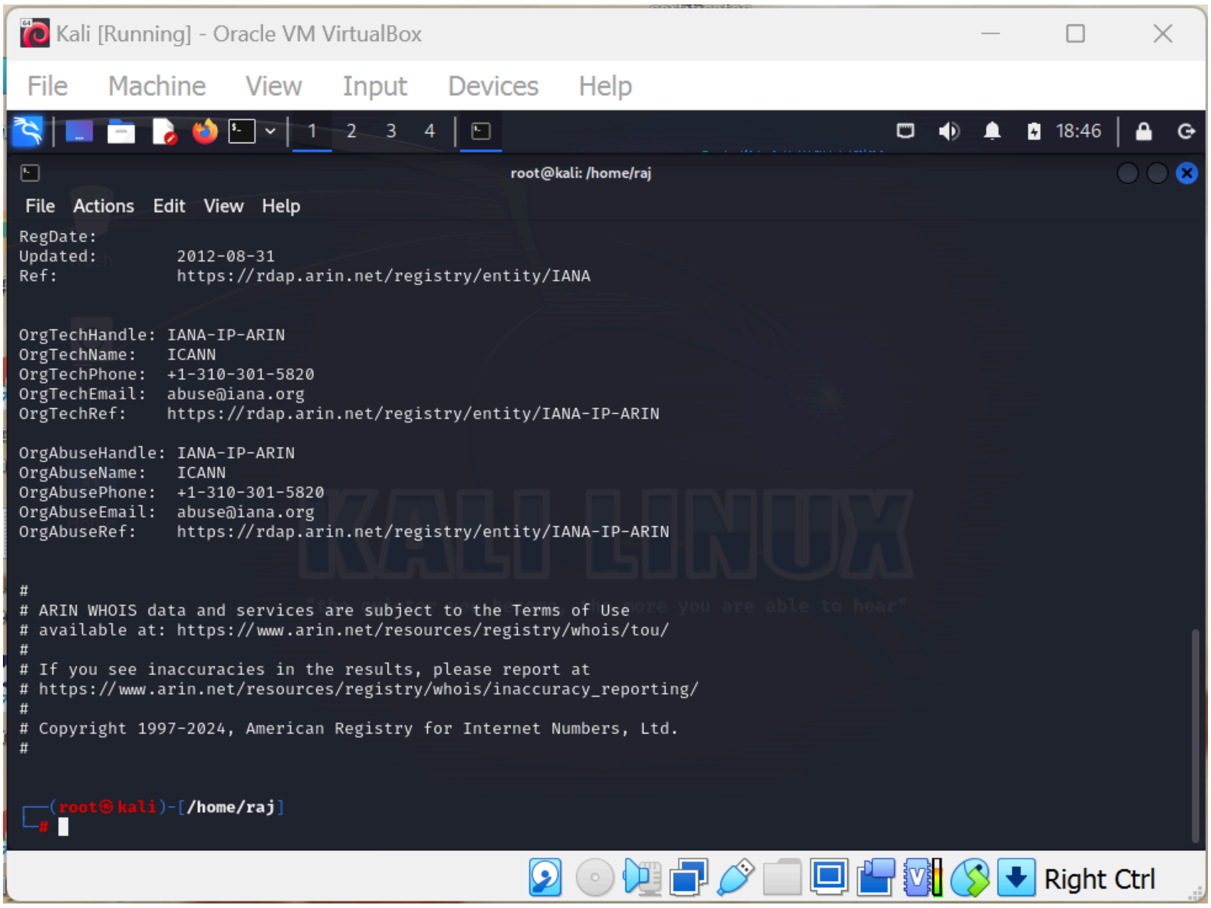

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
18:45
root@kali: /home/raj
File Actions Edit View Help
Right Ctrl

```
#


NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2013-08-30
Comment:        These addresses are in use by many millions of independently operated networks, which might be as smal
l as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of device
s.  They are only intended for use within a private context  and traffic that needs to cross the Internet will need to
 use a different, unique address.
Comment:
Comment:        These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry
.  The traffic from these addresses does not come from ICANN or IANA.  We are not the source of activity you may see o
n logs or in e-mail records.  Please refer to http://www.iana.org/abuse/answers
Comment:
Comment:        These addresses were assigned by the IETF, the organization that develops Internet protocols, in the B
est Current Practice document, RFC 1918 which can be found at:
Comment:        http://datatracker.ietf.org/doc/rfc1918
Ref:            https://rdap.arin.net/registry/ip/192.168.0.0


OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
```



Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
18:46
root@kali: /home/raj
File Actions Edit View Help
Right Ctrl

```
OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2012-08-31
Ref:            https://rdap.arin.net/registry/entity/IANA


OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
```

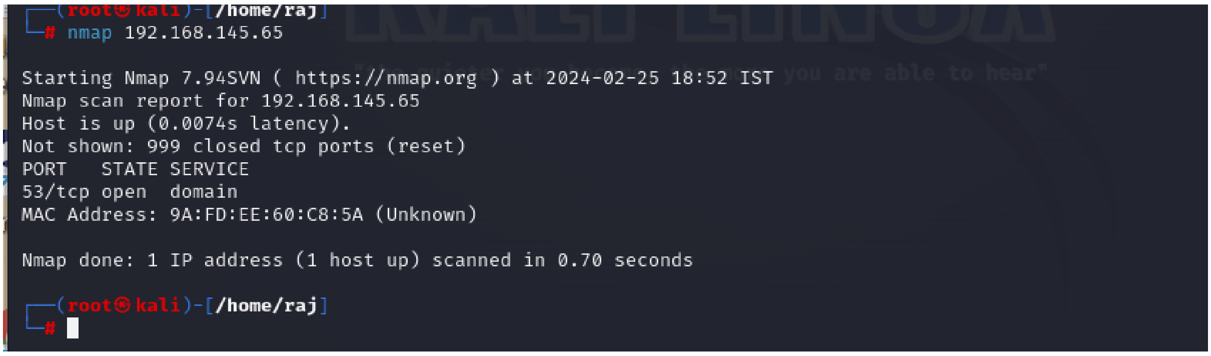


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
18:46
root@kali: /home/raj
File Actions Edit View Help
Right Ctrl

```
RegDate:
Updated:        2012-08-31
Ref:            https://rdap.arin.net/registry/entity/IANA


OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN


#
# 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.
#


┌──(root㉿kali)-[/home/raj]
└─#
```

We have gathered enough info.

Step 4:Now let use nmap command to find vulnerabilities



```
┌──(root㉿kali)-[/home/raj]
└─# nmap 192.168.145.65

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 18:52 IST
Nmap scan report for 192.168.145.65
Host is up (0.0074s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 9A:FD:EE:60:C8:5A (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds

┌──(root㉿kali)-[/home/raj]
└─# 
```

We have a open port 53

PORT 53 : The standard port for DNS is port 53. DNS client applications use the DNS protocol to query and request information from DNS servers, and the server returns the results to the client using the same port. Port 53 is used for both TCP and UDP communication.

Vulnerability : An attacker may use this flaw to inject UDP packets to the remote hosts, in spite of the presence of a firewall. Impact: While using a source port equal to 53 UDP packets may be sent by passing the remote firewall, an attacker could inject UDP packets, in spite of the presence of a firewall.