

# Assignment 1

**Name :Avala Jyotheeshwar Rao**  
**College:Dr.Lankapalli Bullayya College**  
**Regd.No : 721128805286**  
**Date :16/02/2024**

## Footprinting:

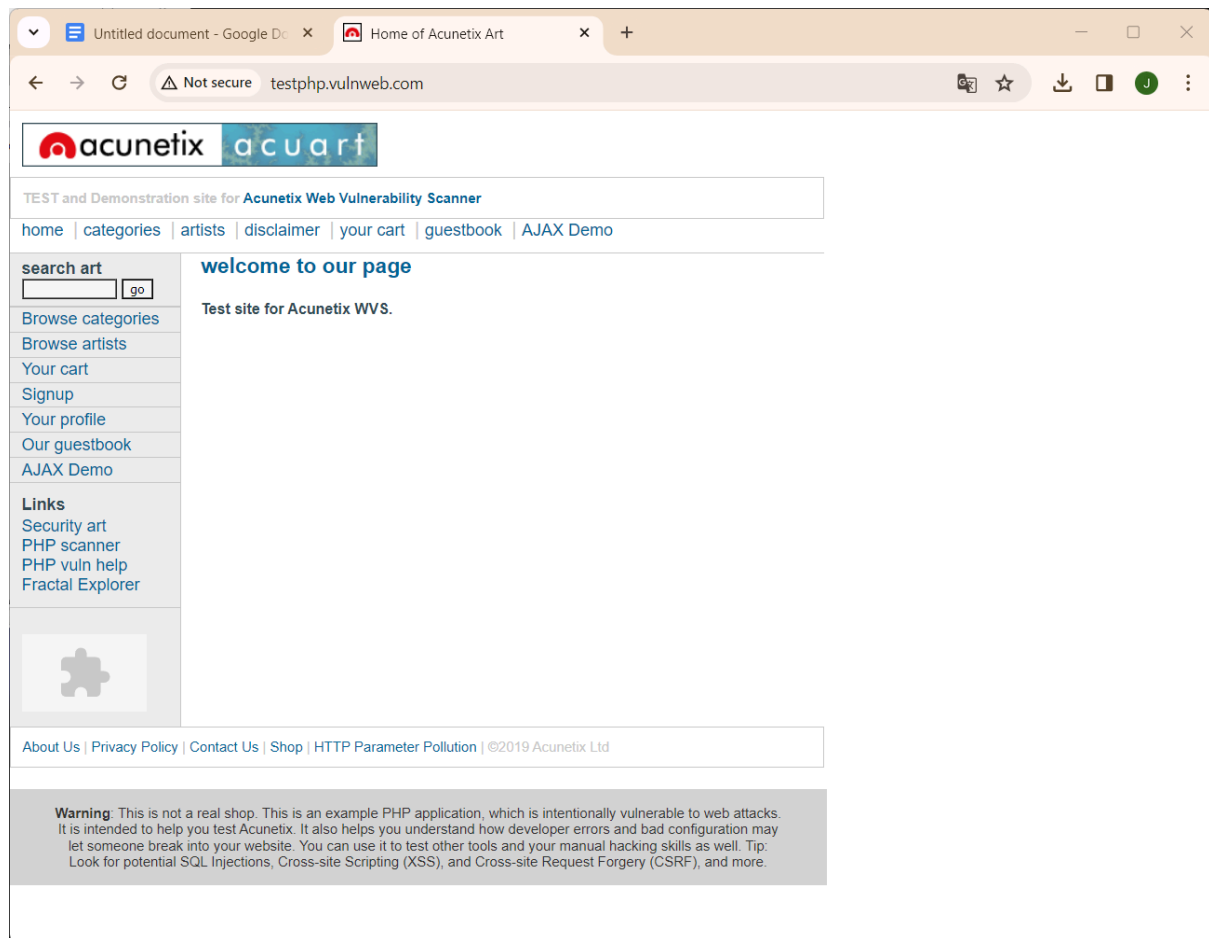
Footprinting is the process of gathering information about a target system or network to create a profile or "footprint" of its infrastructure, services, and security posture. This information can include details about the organisation's domain names, IP addresses, network topology, employee names, email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

## Reconnaissance:

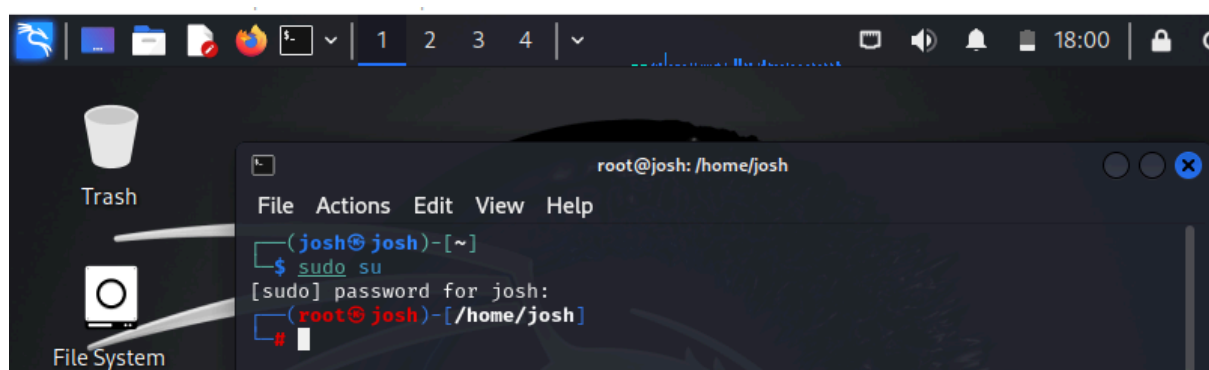
: Reconnaissance, also known as "recon," is the active process of scanning and probing a target system or network to gather additional information beyond what is available through passive footprinting. Reconnaissance activities typically involve techniques such as network scanning, port scanning, banner grabbing, and vulnerability scanning to identify potential points of entry or weaknesses in the target's defences. 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 and Reconnaissance is -

<http://testphp.vulnweb.com/>



### Step 1: open kali linux and change to root user to further process

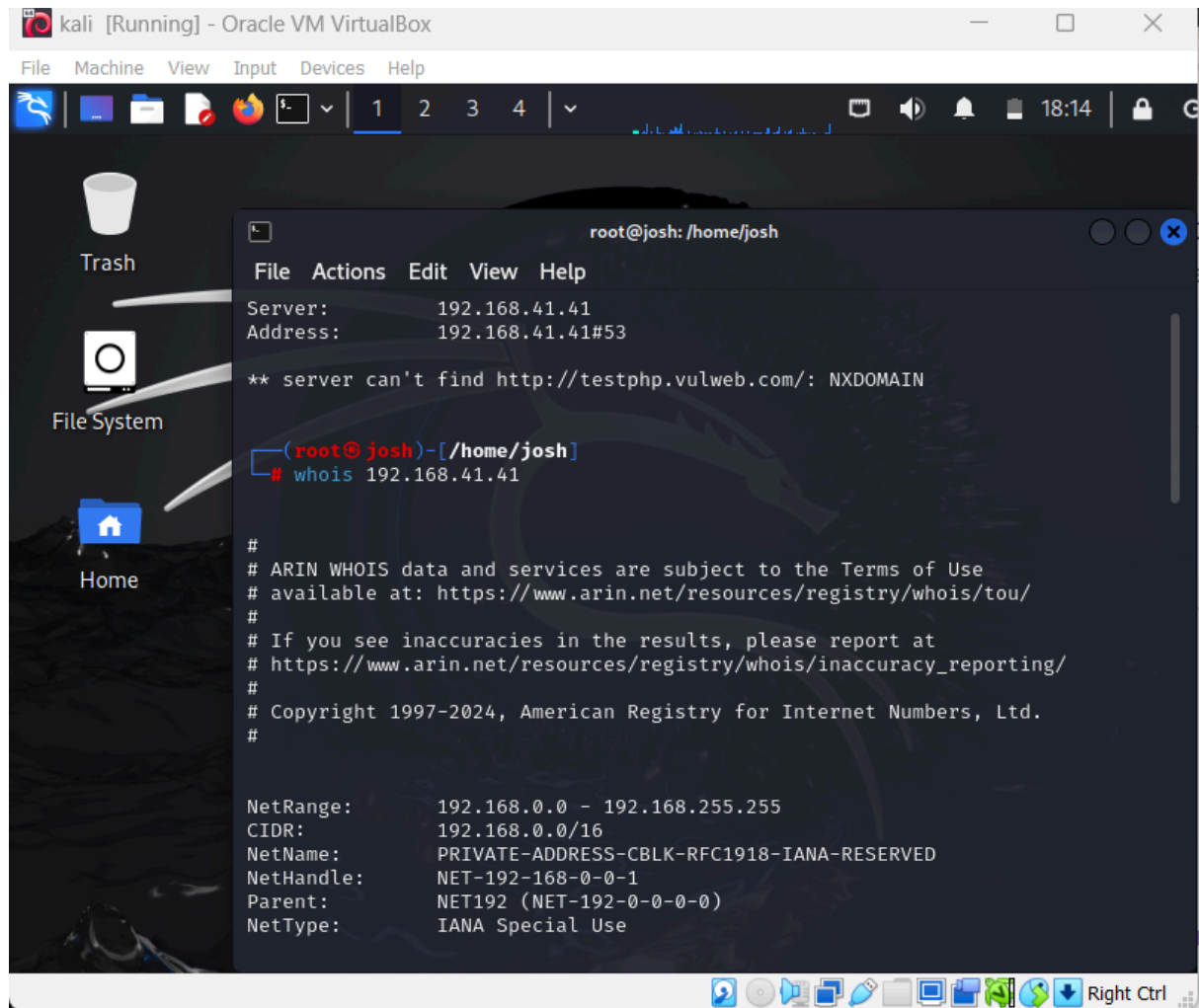


### Step 2: use nslookup on the panel



We got the server ip address as shown above

### Step 3: now use whois command



The screenshot shows a Kali Linux terminal window titled "root@josh: /home/josh". The terminal output displays the results of a 'whois' command for the IP address 192.168.41.41. The output includes the server and address information, a message about a failed HTTP request, and detailed WHOIS data from ARIN, including the net range, CIDR, net name, net handle, parent, and net type.

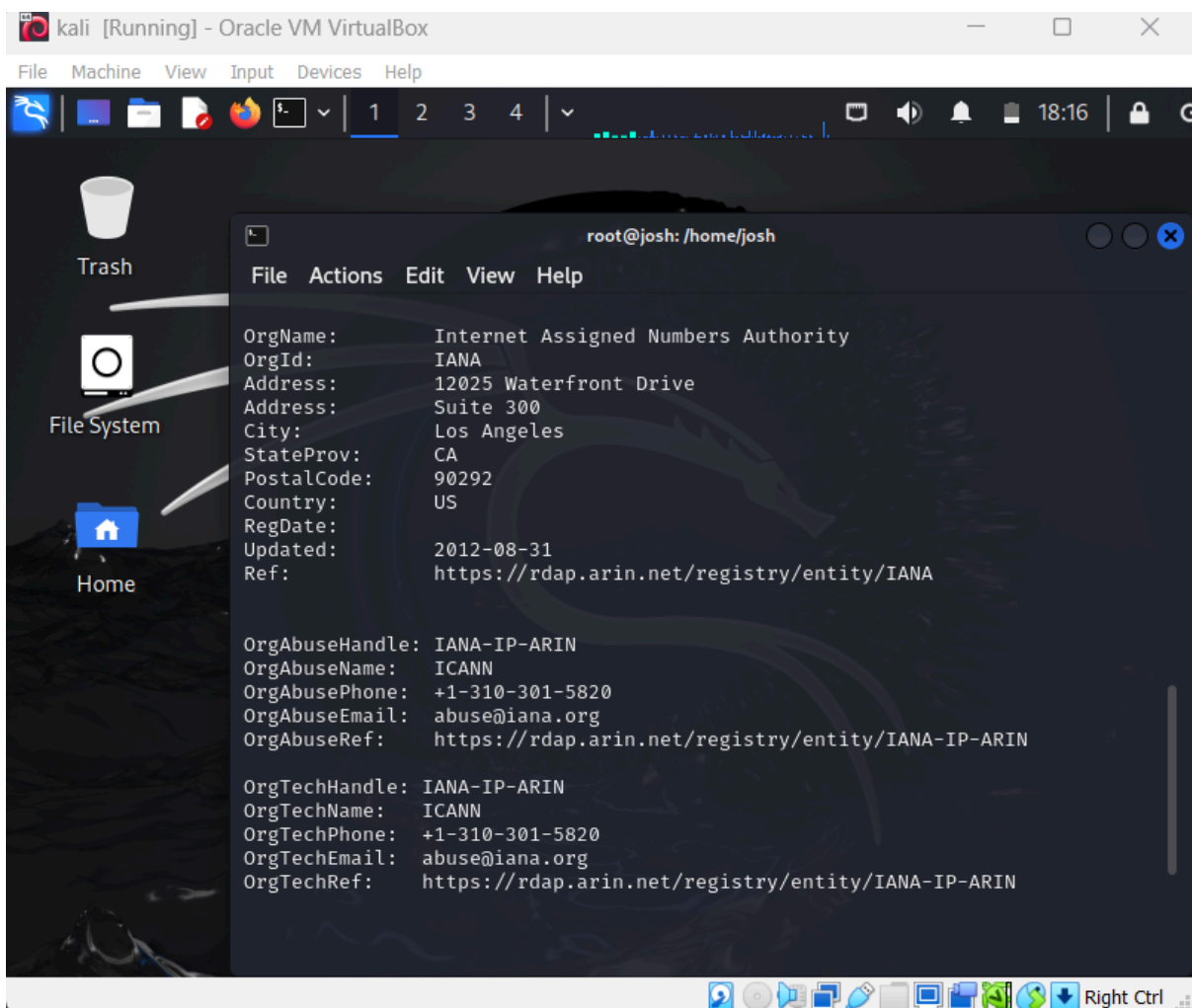
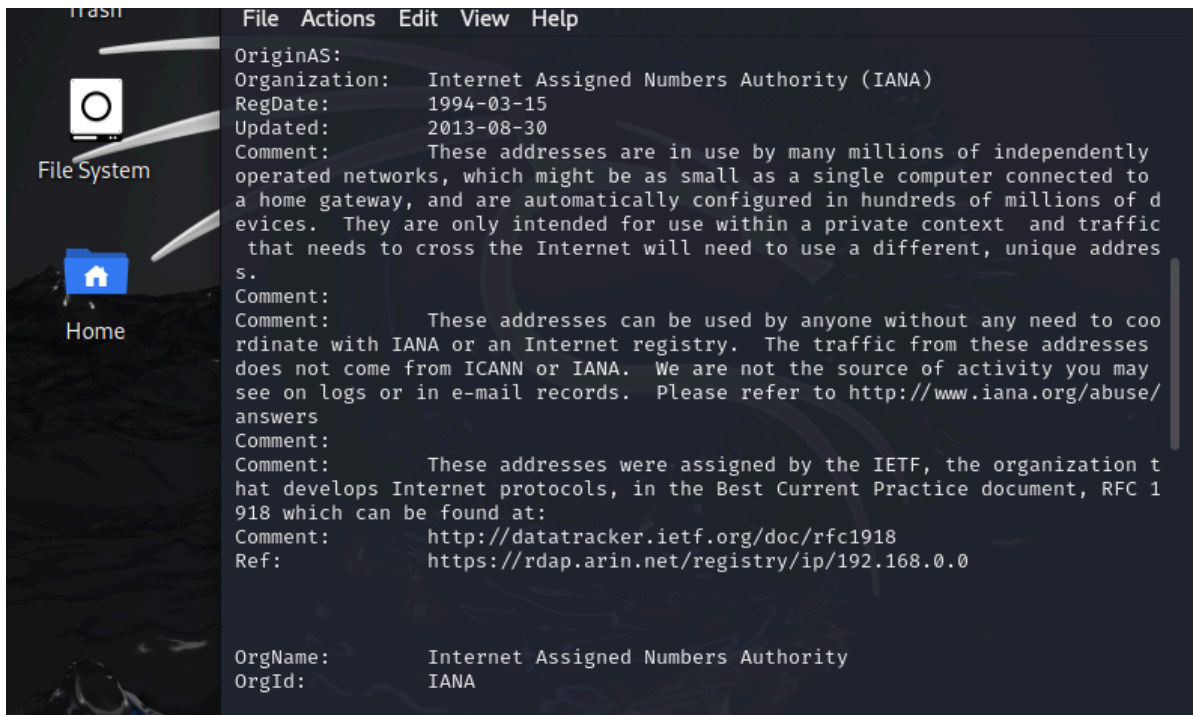
```
File Actions Edit View Help
Server:      192.168.41.41
Address:     192.168.41.41#53

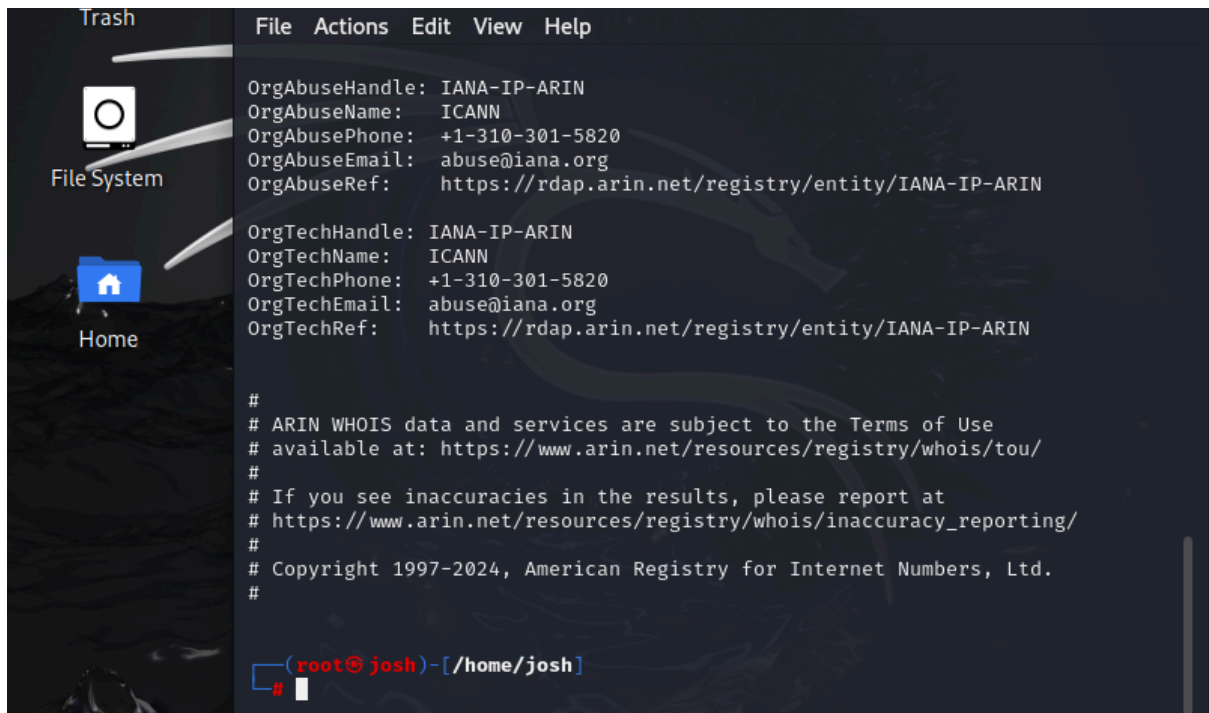
** server can't find http://testphp.vulweb.com/: NXDOMAIN

(root@josh)-[/home/josh]
# whois 192.168.41.41

#
# 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
```



A terminal window with a dark background. On the left, there is a sidebar with icons for 'Trash' and 'File System', and a 'Home' button. The main area shows the output of a WHOIS command. The output lists organizational details for IANA-IP-ARIN, including abuse and technical contact information. It also includes a disclaimer about the terms of use and a copyright notice for the American Registry for Internet Numbers, Ltd. The prompt at the bottom indicates the user is root on a machine named josh, in the directory /home/josh.

```
File Actions Edit View Help

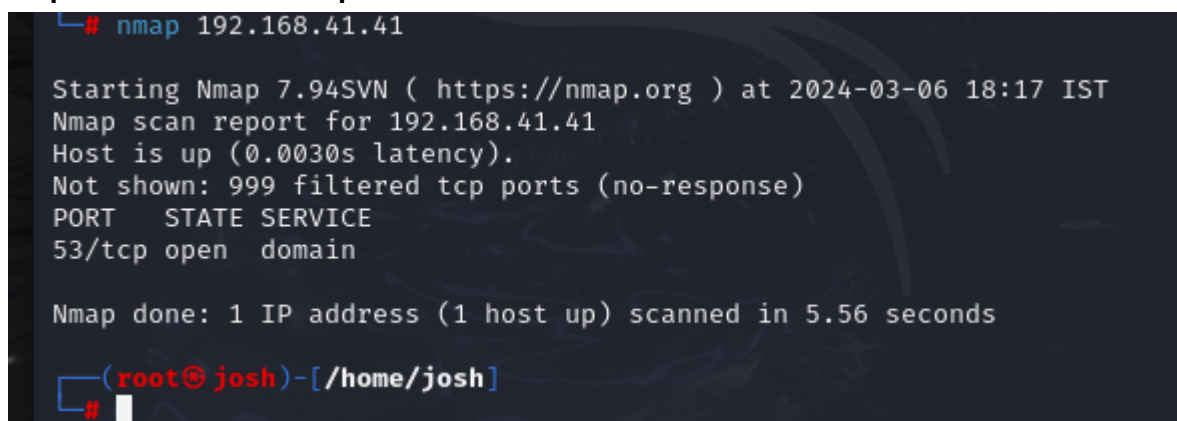
OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName: ICANN
OrgAbusePhone: +1-310-301-5820
OrgAbuseEmail: abuse@iana.org
OrgAbuseRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN

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

#
# 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@josh)-[/home/josh]
```

#### Step 4: now let use nmap command

A terminal window showing the output of an nmap scan. The command 'nmap 192.168.41.41' has been executed. The output shows that the host is up and that port 53/tcp is open and running the 'domain' service. The scan was completed in 5.56 seconds. The prompt at the bottom indicates the user is root on a machine named josh, in the directory /home/josh.

```
# nmap 192.168.41.41

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-06 18:17 IST
Nmap scan report for 192.168.41.41
Host is up (0.0030s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 5.56 seconds

(root@josh)-[/home/josh]
```

#### 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.

**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 source port equal to 53 UDP packets may be sent by passing the remote firewall, and attacker could inject UDP packets, in spite of the presence of a firewall.