Assignment 1

Name :moin pasha

College:Dr.Lankapalli Bullayya College
Regd.No : 721128805566

Date :16/02/2024

Footprinting:

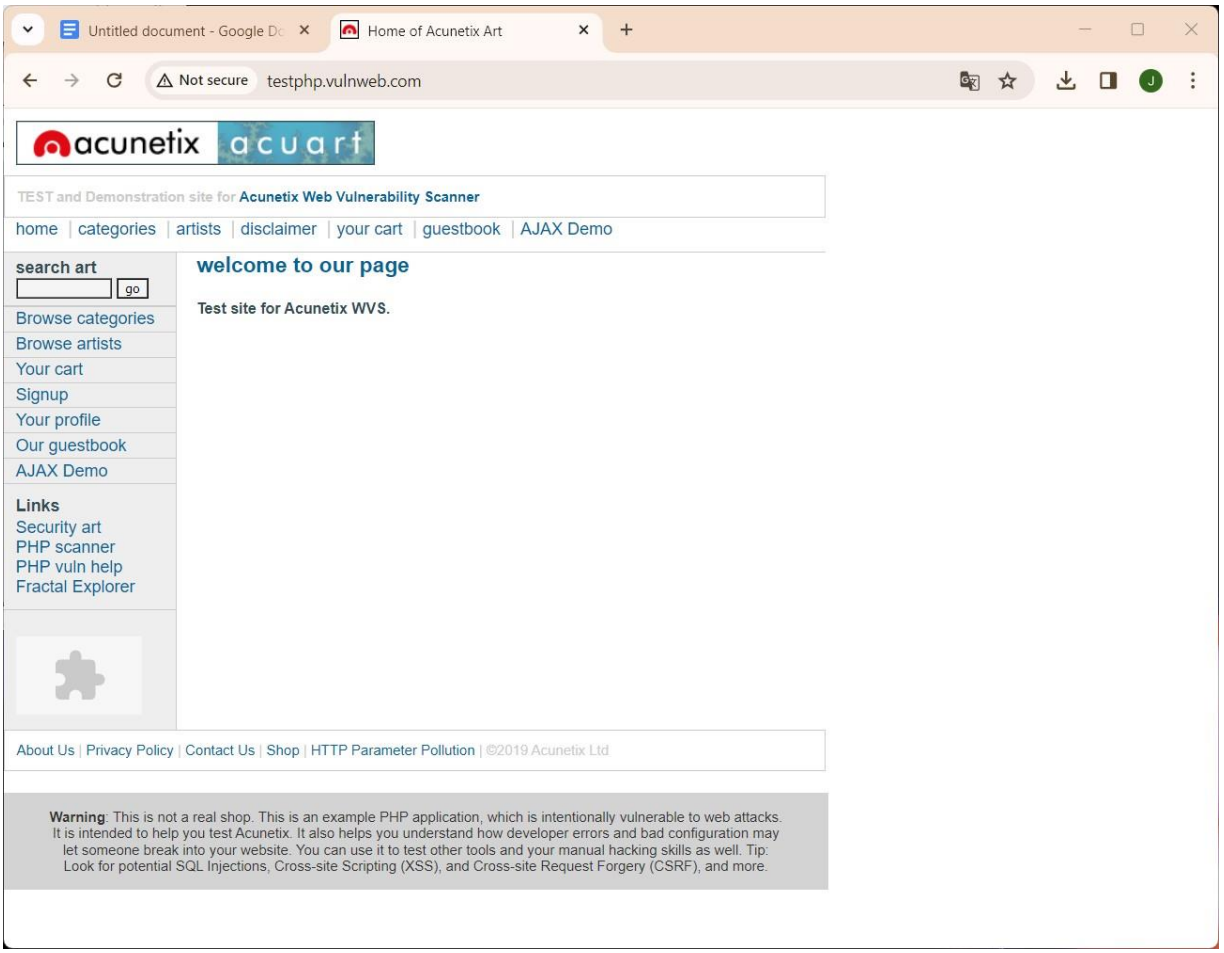
Footprinting is the process of gathering information about a target system or network to create a profile or "footprint" of its infrastructure, services, and security posture. This information can include details about the organisation's domain names, IP addresses, network topology, employee names, email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

Reconnaissance:

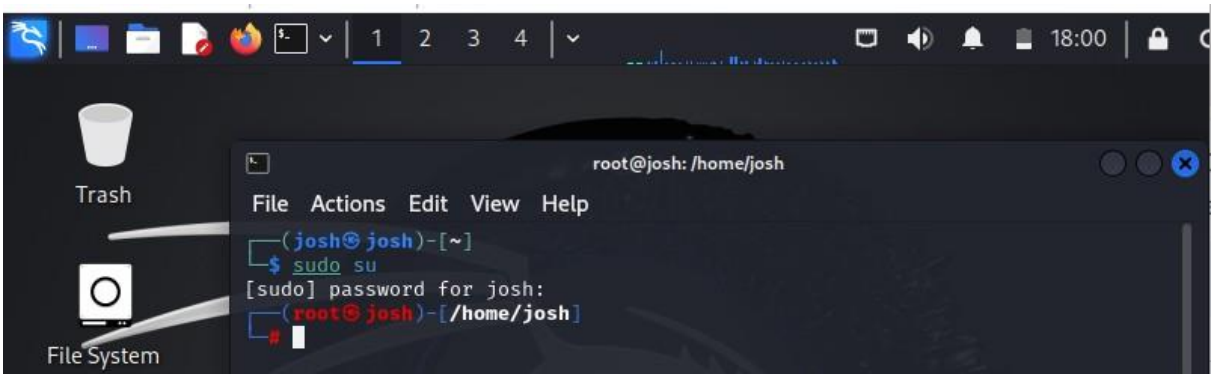
: Reconnaissance, also known as "recon," is the active process of scanning and probing a target system or network to gather additional information beyond what is available through passive footprinting. Reconnaissance activities typically involve techniques such as network scanning, port scanning, banner 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/



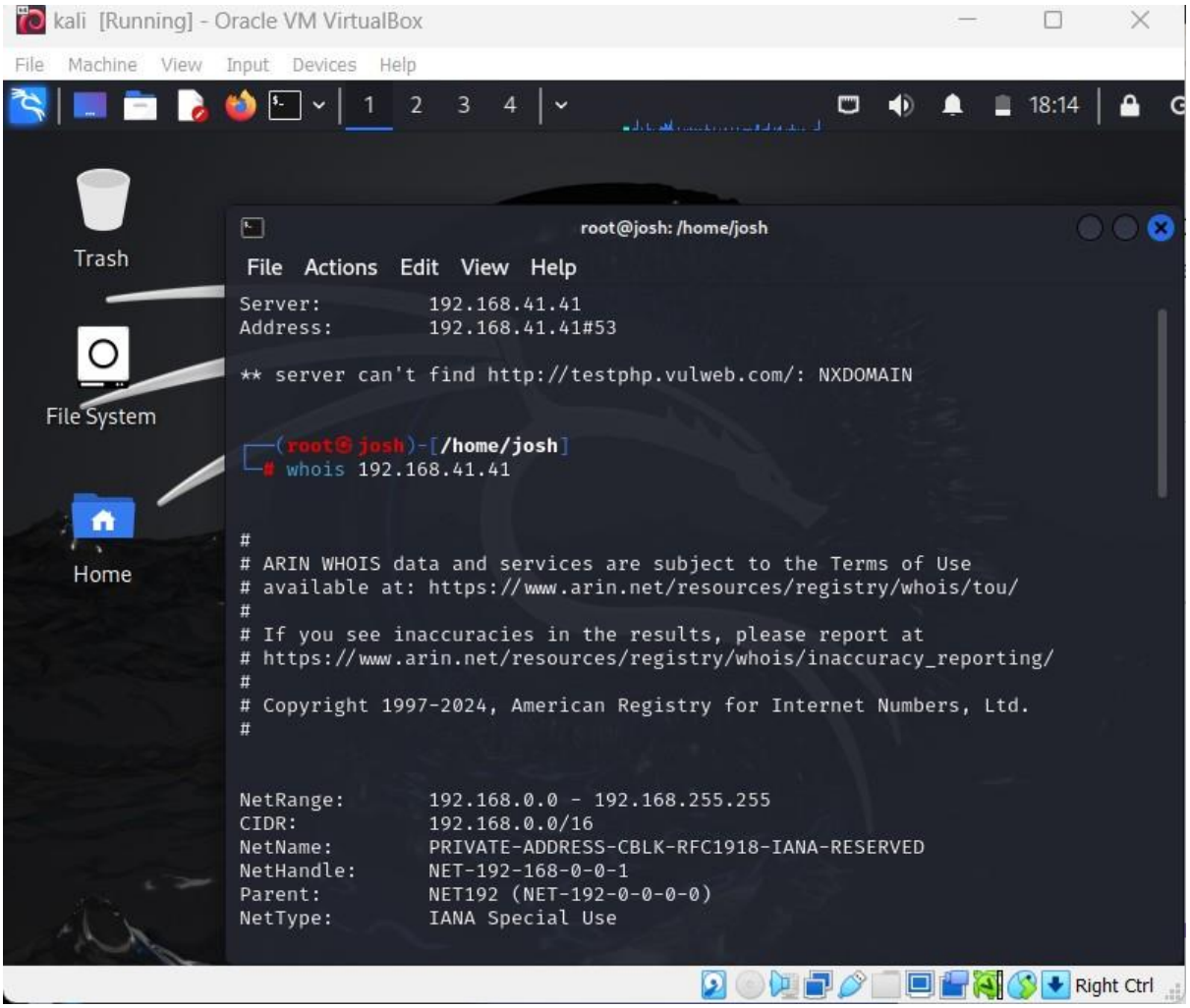
Step 1:open kali linux and change to root user to further process



Step 2: use nslookup on the panel

We got the server ip address as shown above

Step 3:now use whois command



File Actions Edit View Help

```
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 small as a single computer connected to
a home gateway, and are automatically configured in hundreds of millions of d
evices.  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 addres
s.
Comment:
Comment:        These addresses can be used by anyone without any need to coo
rdinate 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 on 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 t
hat develops Internet protocols, in the Best Current Practice document, RFC 1
918 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

1 2 3 4 18:16

root@josh: /home/josh

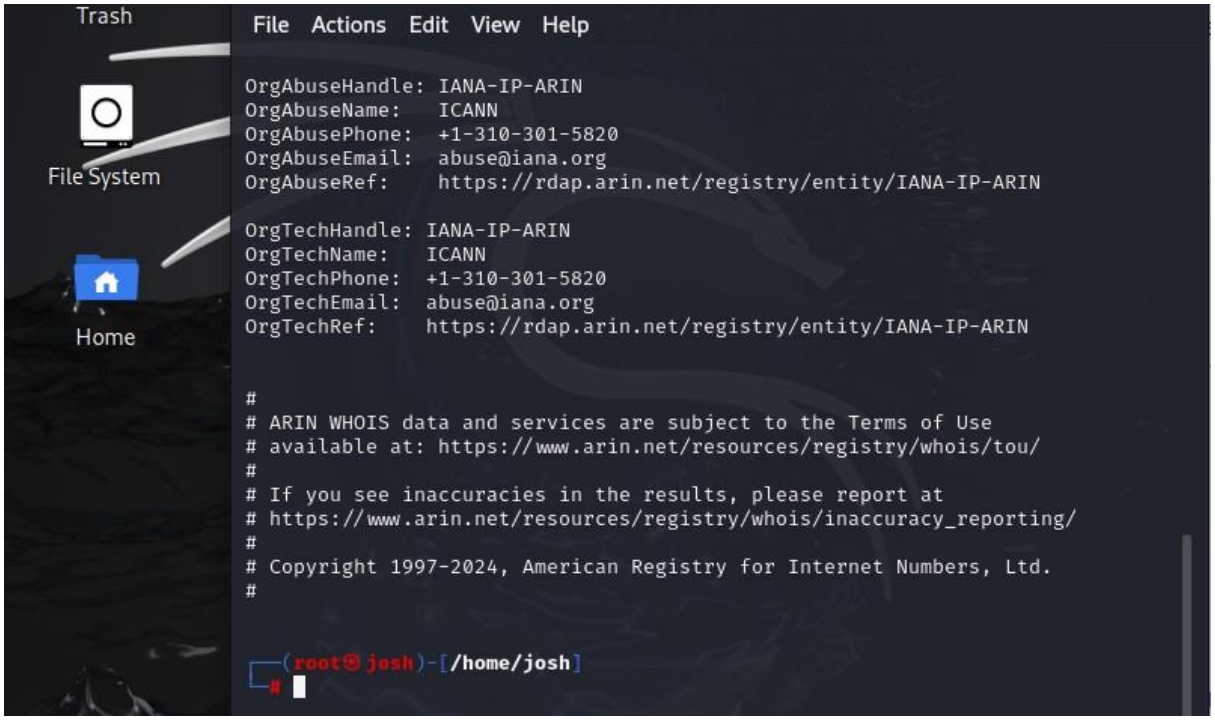
File Actions Edit View Help

```
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


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
```

Right Ctrl



Step 4: now let use nmap command

We have a open port 53

PORT 53: The standard port for DNS is port 53. DNS client applications use the DNSprotocol to query and request information from DNS servers, and the server returnsthe 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.