

BHAVANI SIVA CHARAN CHITTI

721128805293

Dr.L.B.Degree And Pg College

What is Footprinting ?

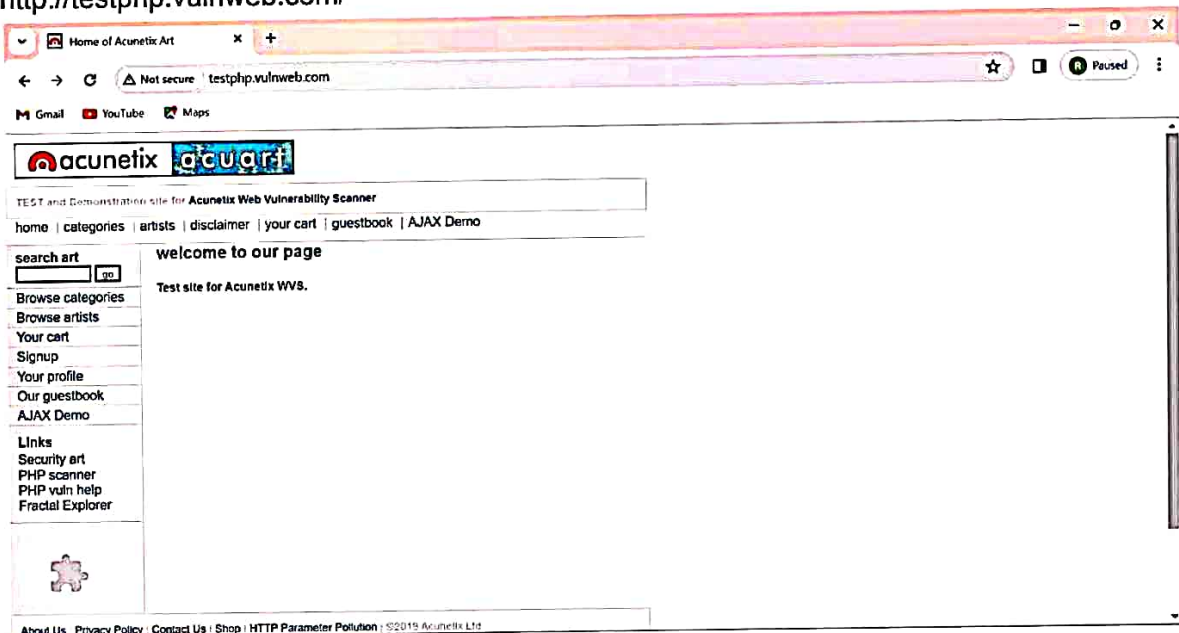
Footprinting is one of the most convenient ways for hackers to collect information about targets such as computer systems, devices, and networks. Using this method, hackers can unravel information on open ports of the target system, services running, and remote access probabilities

What is Reconnaissance?

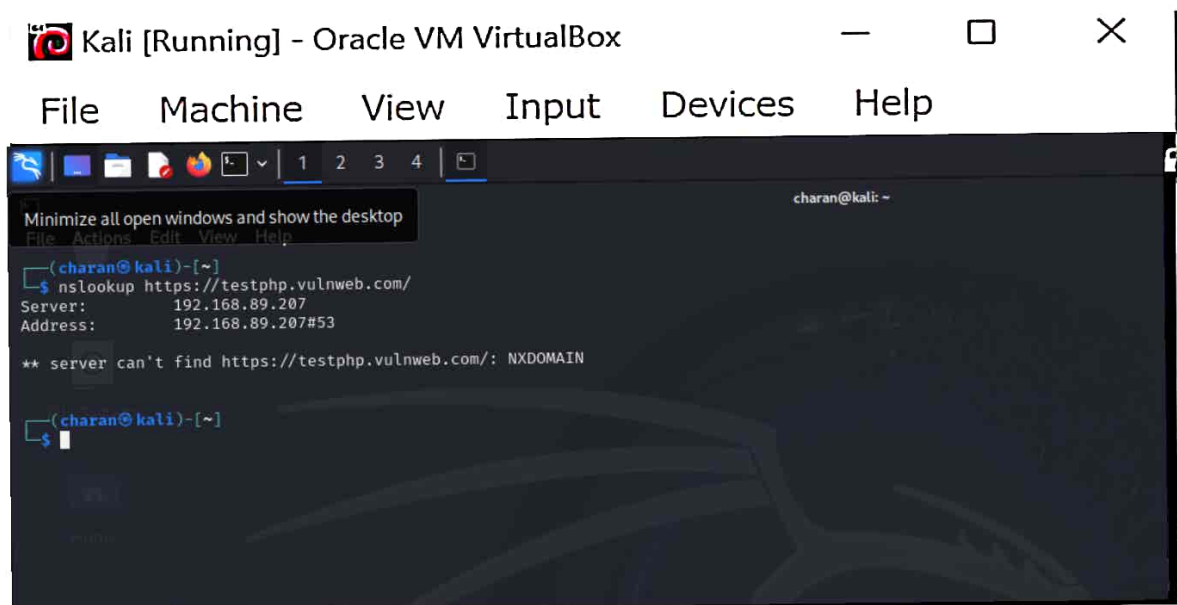
Reconnaissance's most common form involves scanning networks looking for vulnerabilities - such as email messages, websites, social media sites, messaging applications and a company's internal network looking for access to systems and computers running outdated software or security systems

The Website to Perform Footprinting and Reconnaissance is -

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



Step 1: open kali linux and change to root user to perform the task and use nslookup on the target for it



We got the server IP as shown above

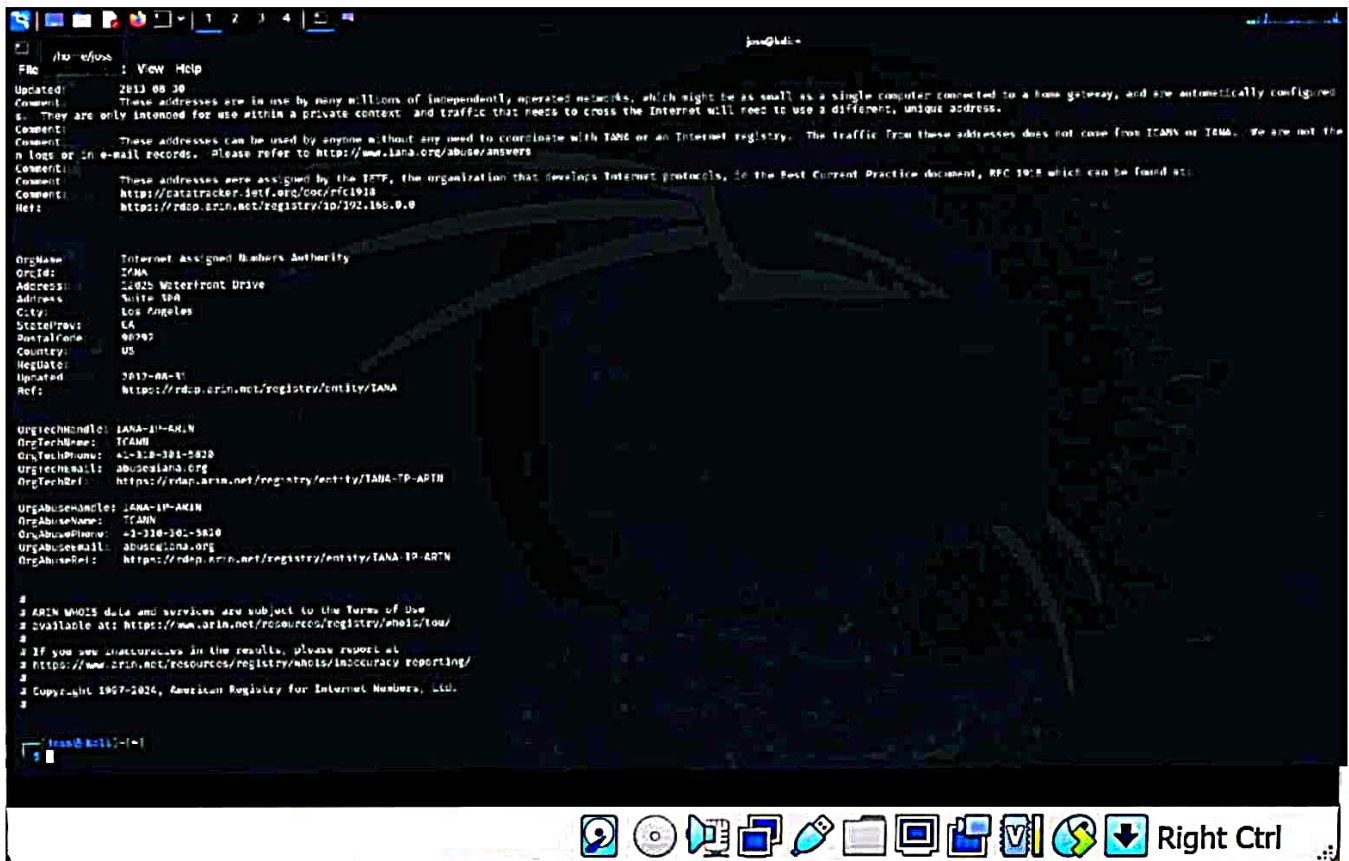
Step 2: now use whois command to gather information for needs

```
charan@kali: ~  
File Actions Edit View Help  
charan@kali: ~  
$ whois 192.168.0.0  
  
# 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)  
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 small as a single computer connected to a home gateway  
re automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross the Internet  
to use a different, unique address.  
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 IANA 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: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best 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  
Address: 12025 Waterfront Drive  
Address: Suite 300  
City: Los Angeles  
StateProv: CA  
PostalCode: 90292  
Country: US  
RegDate: 1994-03-15  
Updated: 2012-08-31  
Ref: https://rdap.arin.net/registry/entity/IANA
```

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
charan@kali: ~  
File Actions Edit View Help  
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 IANA 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: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best 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  
Address: 12025 Waterfront Drive  
Address: Suite 300  
City: Los Angeles  
StateProv: CA  
PostalCode: 90292  
Country: US  
RegDate: 1994-03-15  
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.
```



We have gathered enough info.

Step 3: Now let us use nmap command to find vulnerabilities

```

(charan@kali)-[~]
$ nmap 192.168.89.207
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 20:07 IST
Nmap scan report for 192.168.89.207
Host is up (0.0091s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds

```

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.