BHAVANI SIVA CHARAN CHITTI

721128805293

Dr.L.B.Degree And Pg College

What is Footprinting ?

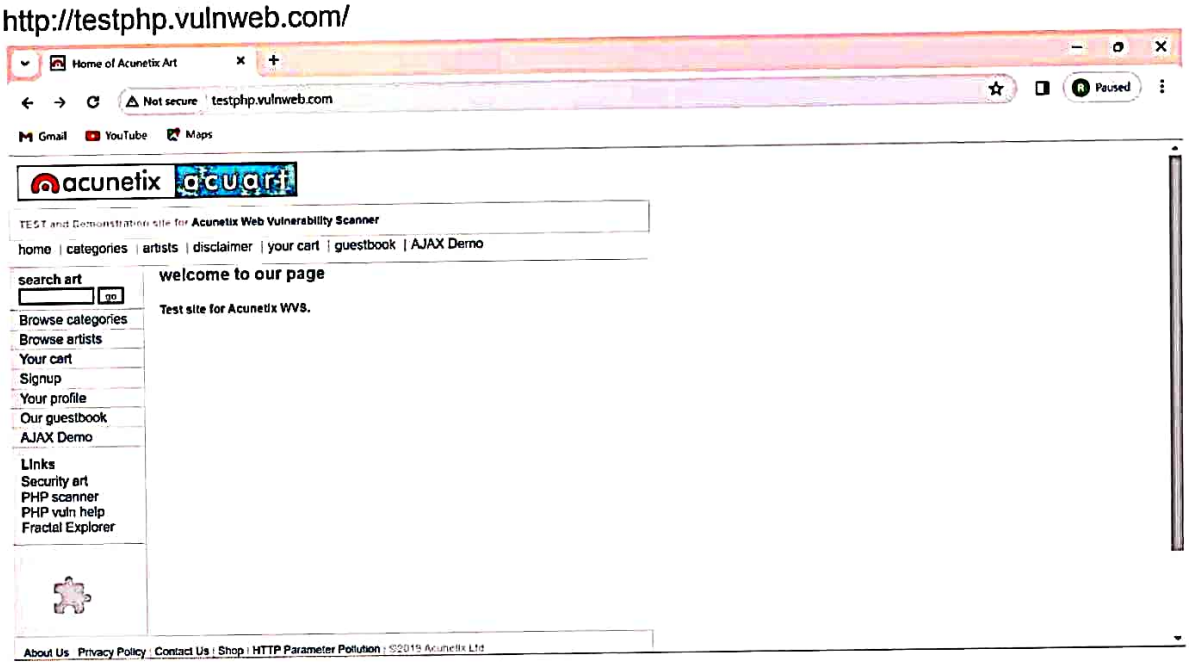
Footprinting is one of the most convenient ways for hackers to collect information about targets such as computer systems, devices, and networks. Using this method, hackers can unravel information on open ports of the target system, services running, and remote access probabilities

What is Reconnaissance?

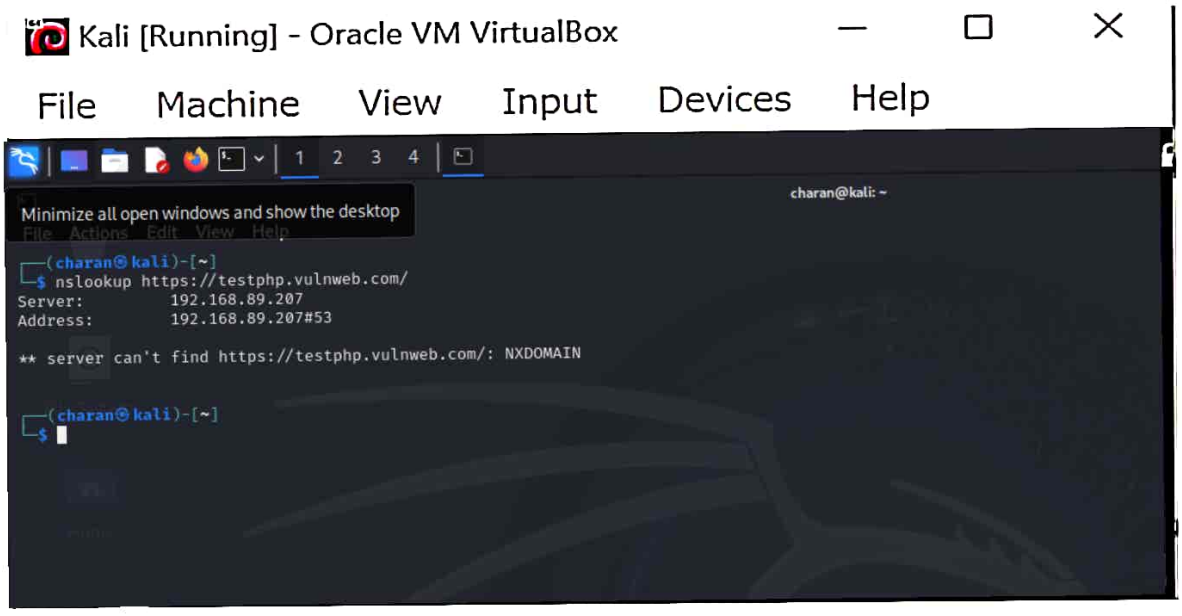
Reconnaissance's most common form involves scanning networks looking for vulnerabilities - such as email messages, websites, social media sites, messaging applications and a company's internal network looking for access to systems and computers running outdated software or security systems

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

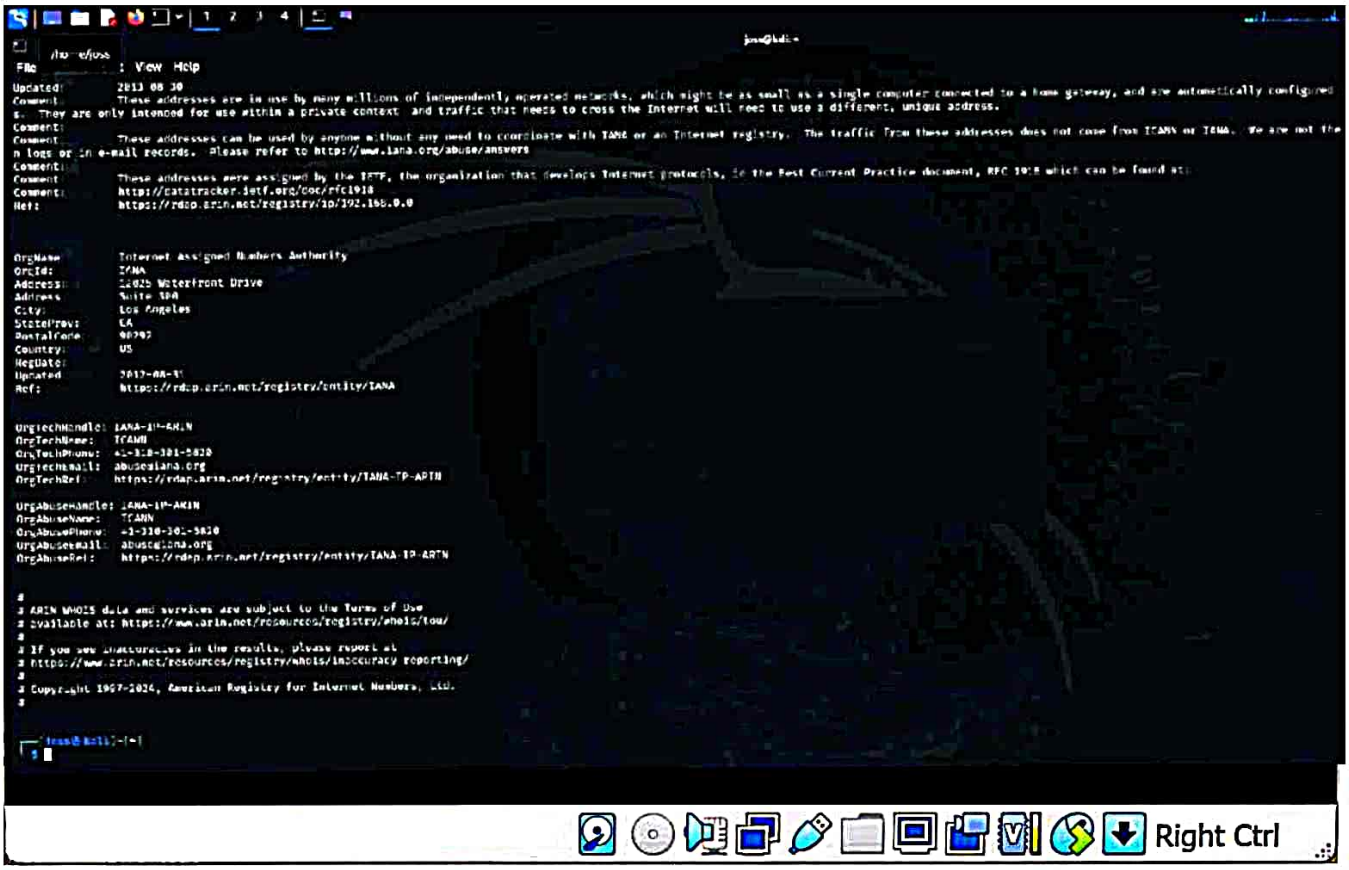


We got the server IP as shown above

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

Kali [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



We have gathered enough info.

Step 3:Now let 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.