

# ASSIGNMENT -1

BATTU JHANSI

721128805494

Dr.L.B.Degree And pg college

## 1. What is Footprinting ?

### Footprinting

refers to the technique used for gathering information about computer systems and the entities they belong to. It's a crucial step in understanding the security posture of a target system. Here are some key points about footprinting:

1. **Purpose:**  
Footprinting provides valuable insights that can be used by both ethical hackers and malicious actors. It helps them understand the target system's vulnerabilities and weaknesses.
2. **Types of Footprinting:**
  - **Active Footprinting:** Involves direct interaction with the target machine. The attacker actively probes the system to gather information.
  - **Passive Footprinting:** Collects information remotely, without directly engaging with the target. This includes data from public sources and historical records.

## 2. What is Reconnaissance?

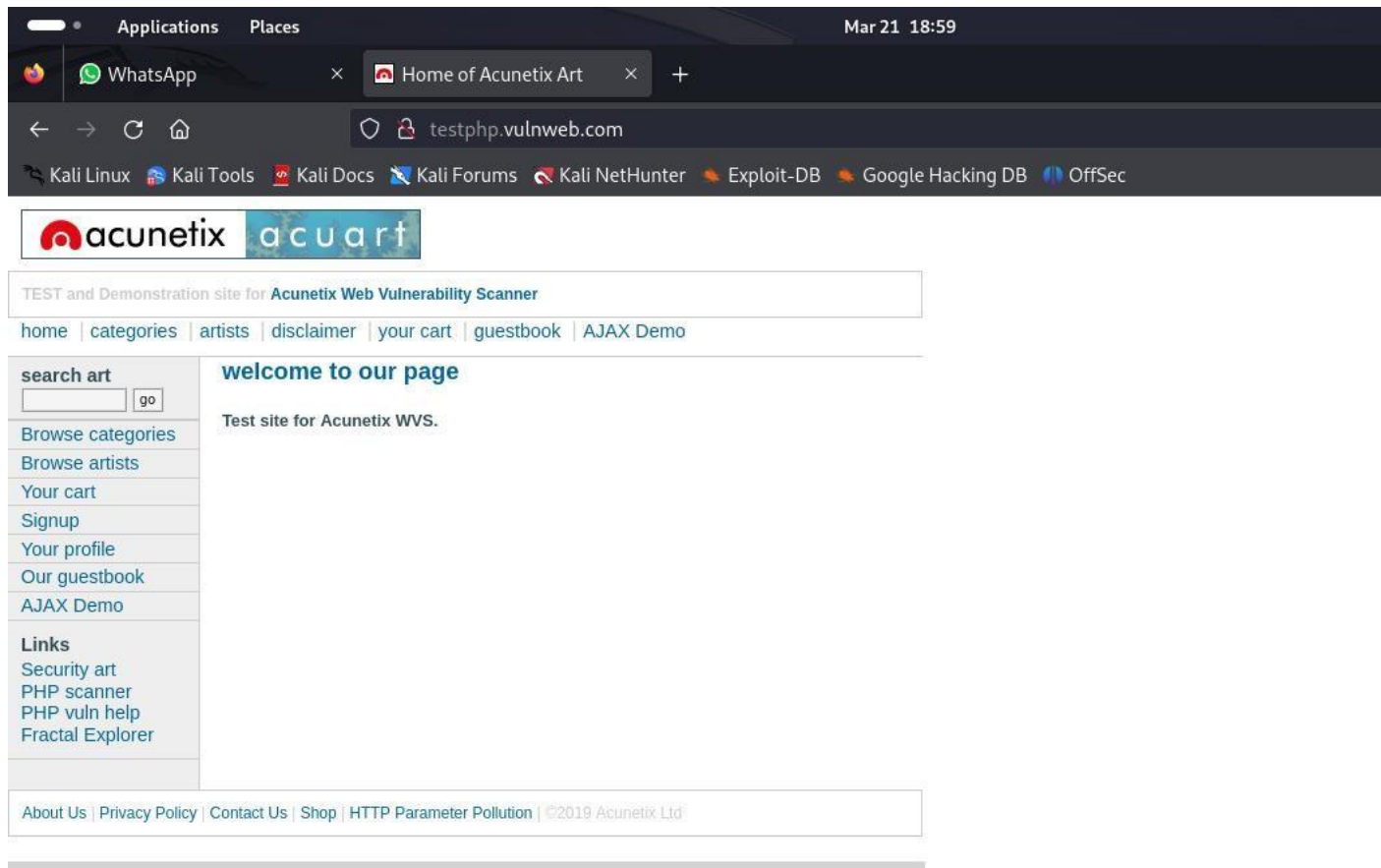
**Reconnaissance** in the realm of cybersecurity is akin to the initial fact-finding mission before a cyber attack. It involves systematically surveying or scanning systems, networks, or web applications to gather critical information about potential vulnerabilities that can be exploited

Here are some key points about **cybersecurity reconnaissance**:

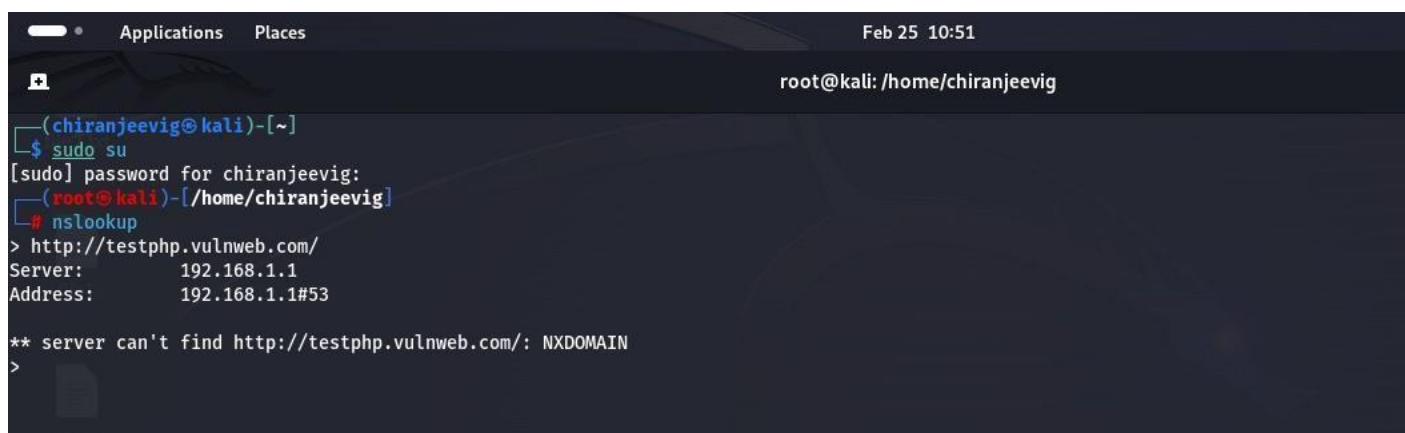
1. **Purpose and Importance:**
  - **Preliminary Phase:** Reconnaissance serves as the **first step** in the cyber attack process.
  - **Information Gathering:** It aims to collect data about the target system, including its infrastructure, configuration, and potential weaknesses.
  - **Strategic Advantage:** Comprehensive reconnaissance enables threat actors to build a precise understanding or profile of their targets, which they can later exploit.

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

Step2: Now use whois command to gather information for needs

```
Applications Places Mar 21 19:15
root@kali: /home/chiranjeevig

(root@kali)-[/home/chiranjeevig]
# whois 192.168.55.60

#
# 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:
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
, and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context
ernet 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 traf
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
```

+

```
Applications Places Mar 21 19:16
root@kali: /home/chiranjeevig

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.ia
Comment:
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current
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:
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
```

```
Applications  Places  Mar 21 19:16
root@kali: /home/chiranjeevig

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/you become, the more you are able to hear"
#
# 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/chiranjeevig]
```

We have gathered enough info

Step 3: Now let use nmap command to find vulnererabilities

```
(root@kali)-[/home/chiranjeevig]
# nmap 192.168.55.60
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-21 19:17 IST
Note: Host seems down. If it is really up, but blocking our ping probes
Nmap done: 1 IP address (0 hosts up) scanned in 4.93 seconds
```

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 flow to inject UDP packets to the remote hosts, in spite of the presence of 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.