FOOTPRINTING

What if footprinting ?

We know footprinting refers to one of the pre attack phase. Also its performed before doing the actual attack. And footprinting is the first step To perform hacking on any organization's. During this phase a hacker can collect various information about the target.

- Domain name
- Ip addresses
- Namespaces
- Employ information
- Phone numbers
- E-mails
- Job information

It can help hackers find many opportunities to penetrate the target's network. For finding some information hackers have various tool and technologies

Some of the tools used for footprinting

- Nmap
- Whois
- Nessus
- Superscan

NMAP

Download nmap from its own side it is available for both windows and linux. It will do ping sweeps, os identifications, port scan and much more things.

Whois

A whois command is used for search the general public database for information of few specific domain, like the registration date , expiration date, current registrar etc. whenever you run the command the request is sent to general public whois database and they will show you result.

Nessus

Once you discover the list of open ports. Next step is begin searching the vulnerability within the server. One in all the efficient tool for vulnerability scan is nessus. But one bad thing is the nessus is not free tool.

Superscan

Download Super Scan from its new area and introduce it. SuperScan permits you to examine an assortment of data handling addresses and do TCP port filtering. It will really take a look at all ports, or those you pick. it's an outrageously speedy and integral asset.

Types of Footprinting

There are two types of footprinting

Active - in this process the attacker gather the data with the use of tools like ping sweep traceroute. In this the attacker directly intract with the target.active footprinting trigger the IDS.
Passive - in this process the attacker gather the data from browsing and social media of the target. In this the attacker is not directly intract with the target.passive footprinting not trigger the IDS

Some examples of ways to perform active footprinting

- Performing traceroute analysis
- Gathering information through email tracking
- Performing whois lookup
- Extracting DNS information

Some example of ways to perform passive footprinting

- Browsing the target's website
- Monitoring target using alert services
-
- Visiting social media profiles of employees
- Collecting information through social engineering on social network sites

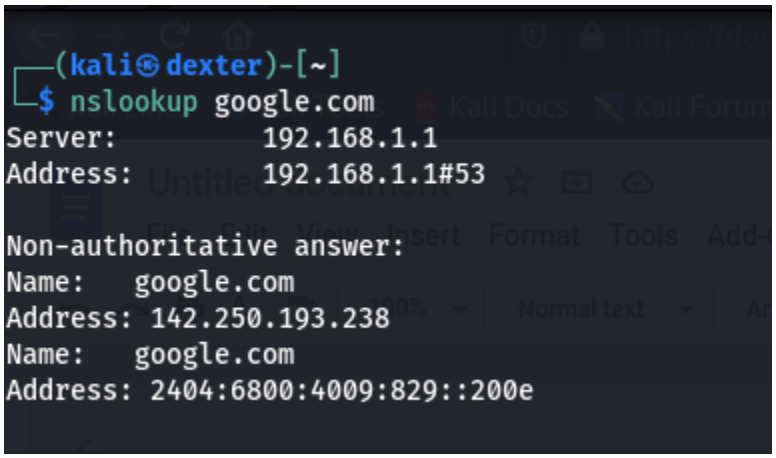
Methodologies of footprinting (manual)

Nmap is used for open port scanning

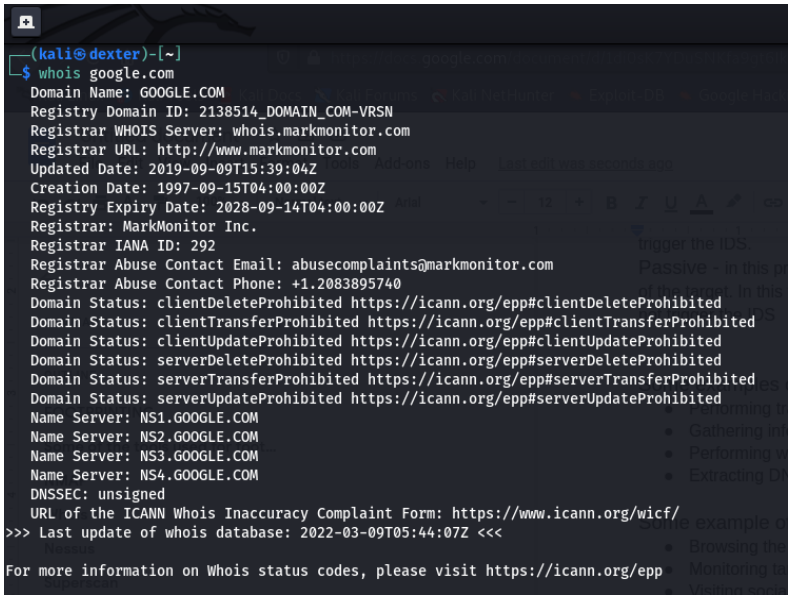
```
┌──(kali㉿dexter)-[~]
└─$ nmap google.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-09 11:18 IST
Nmap scan report for google.com (142.250.193.238)
Host is up (0.059s latency).
Other addresses for google.com (not scanned): 2404:6800:4002:81d::200e
rDNS record for 142.250.193.238: del11s18-in-f14.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 7.77 seconds
```

Nslookup is used for finding DNS records



Whois is used for domain availability and ip search



Reconnaissance

In cybersecurity reconnaissance is the part where we discovering and collecting information about the system. This method is often used for ethical hacking or penetration testing.

How reconnaissance works

Reconnaissance generally follows seven steps

- Collecting initial information
- Determine the network range
- Identify active machines
- Find access point and active ports
- Fingerprint the operating system
- Discover service on ports
- Map the network

Using these steps an hacker can gain the following information about the network

- File permission
- Running network services
- Os platform
- Trust relationship
- User account information

There are two types of reconnaissance - active and passive

Active - in this hacker intract directly with the target and attempt to obtain information through technics using automate scanning or manual testing and tool like ping and netcat. Active recon is faster and more accurate but also riskier because it creates more nois and chances of detection.

Passive - in this hacker gather information without directly interact with the target, using tools such as wireshark and shodan and methods such as OSfingerprint to gain information.

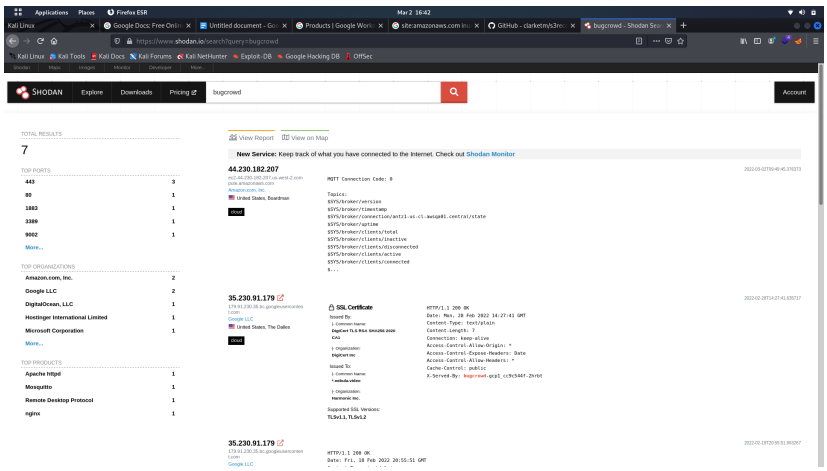
Some tools for reconnaissance

- Assetfinder
- Shodan
- Lazyrecon
- Nmap
- Httpx

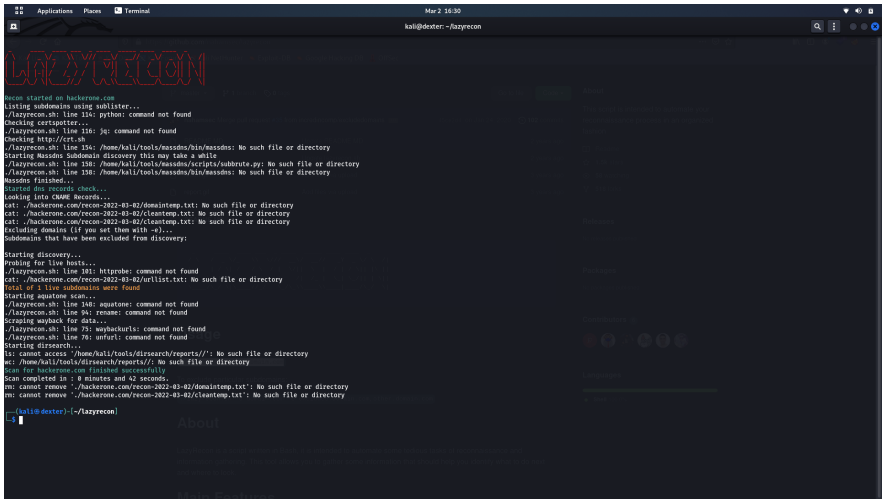
Assetfinder is use to find the subdomains of the websites

```
┌──(kali㉿dexter)-[~]
└─$ assetfinder hackerone.com
mta-sts.managed.hackerone.com
mta-sts.forwarding.hackerone.com
api.hackerone.com
docs.hackerone.com
a.ns.hackerone.com
b.ns.hackerone.com
mta-sts.hackerone.com
support.hackerone.com
www.hackerone.com
ns.hackerone.com
1.ns.hackerone.com
api.hackerone.com
hackerone.com
www.hackerone.com
gslink.hackerone.com
events.hackerone.com
hackerone.com
www.hackerone.com
api.hackerone.com
www.hackerone.com
hackerone.com
```

Shodan is use to find the leak ip address of websites



Lazyrecon is automate tool for reconnaissance



Httpx is fast and multi-purpose HTTP toolkit allow to run multiple probers using retryablehttp library, it is designed to maintain the result reliability with increased threads.

```
┌──(kali㉿dexter)-[~]
└─$ httpx https://www.itperfection.com
HTTP/1.1 403 Forbidden
Date: Wed, 09 Mar 2022 06:36:32 GMT
Content-Type: text/html; charset=iso-8859-1
Transfer-Encoding: chunked
Connection: keep-alive
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=np5s4w5VvfJvm0v5wLsU5XtsRCFvJMNpYRBQ0KsQWy%2Bn36S91lnER6VsWfgW7l%2Bl5mIT84GfOP1psPD%2BDHoCRJrBvCawRhM3fogZLVBmDgDvGB2G5CwOKUw5lCA1rqEbz56wRGskbQ%3D%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 6e91cbfb7aa48889-LHR
Content-Encoding: br
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<p>Additionally, a 403 Forbidden
error was encountered while trying to use an ErrorDocument to handle the request.</p>
<script defer src="https://static.cloudflareinsights.com/beacon.min.js/v652eace1692a40cfa3763df669d7439c1639079717194"
integrity="sha512-Gi7xpJR8tSkrpF7aordPZQlW2DLtzUlZcumS8dMQjwDHEnw9I7ZLyiOj/6tZStRBGtGgN6ceN6cMH8z7etPGlw=="
data-cf-beacon='{"rayId":"6e91cbfb7aa48889","version":"2021.12.0","r":1,"token":"5a2926a53a1b4147b5bd58b8a16537a4","si":100}'
crossorigin="anonymous"></script>
</body></html>
```