

FOOTPRINTING

What is 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 interact 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 interact 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

```
(kali@dexter)-[~]
$ nslookup google.com
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.193.238
Name:   google.com
Address: 2404:6800:4009:829::200e
```

Whois is used for domain availability and ip search

```
(kali@dexter)-[~]
$ whois google.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-03-09T05:44:07Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

Reconnaissance

In cybersecurity reconnaissance is the part where we discover and collect 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 interact directly with the target and attempt to obtain information through techniques using automated scanning or manual testing and tools like ping and netcat. Active recon is faster and more accurate but also riskier because it creates more noise 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
hackerone.com
```

Shodan is use to find the leak ip address of websites

The screenshot shows the Shodan search engine interface. The search bar at the top contains the word "bugcrowd". Below the search bar, there are several sections of results:

- TOTAL RESULTS:** 7
- TOP PORTS:** A list of ports and their counts: 443 (2), 80 (1), 3883 (1), 2280 (1), 9002 (1).
- TOP ORGANIZATIONS:** A list of organizations and their counts: Amazon.com, Inc. (2), Google LLC (2), DigitalOcean, LLC (1), Hostinger International Limited (1), Microsoft Corporation (1).
- TOP PRODUCTS:** A list of products and their counts: Apache HTTP (1), Mosquitto (1), Remote Desktop Protocol (1), nginx (1).

The main results section displays three items:

- 44.230.182.207:** A new server with a connection code of 0. It lists various endpoints like `api.hackerone.com`, `docs.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`, and `hackerone.com`.
- 35.230.91.179:** A server with a connection code of 0. It lists various endpoints like `api.hackerone.com`, `docs.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`, and `hackerone.com`.
- 35.230.91.179:** A server with a connection code of 0. It lists various endpoints like `api.hackerone.com`, `docs.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`, and `hackerone.com`.

[illegible]

```
(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/v/report/v3?s=np5s4w5VvfJvm0v5wLsU5XtsRCFvJMNvYRBQ0KsQwy%2Bn36S91lneR6VsWfgW7l%2BLSmIT84GfOP1psPD%2BDHoCRJRbVcawRhM3f0gZLVBmDgDVGb2G5CwOKUw5lCA1rqEbZ56wRGskbQ%3D%3D"}],"group":"cf-nel","max_age":604800}
WfWgW7l%2BLSmIT84GfOP1psPD%2BDHoCRJRbVcawRhM3f0gZLVBmDgDVGb2G5CwOKUw5lCA1rqEbZ56wRGskbQ%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-G17xpJR8tSkrpFF7aordPZQlW2DltzULzCumsS8dMQjwDHEEnw9I7ZyLioOj/6tZStRBGTGgN6ceN6cMH8sz7etPGLw==" data-cf-beacon="{\"rayId\":\"6e91cbfb7aa48889\", \"version\":\"2021.12.0\", \"r\":\"1\", \"token\":\"5a2926a53a1b4147b5bd58b8a16537a4\", \"si\":100}\" crossorigin=\"anonymous\"}</script>
</body></html>
```