



SRI SANKANRAS DEGREE COLLEGE KURNOOL

Shaik Reena Tasleem

Long term internship

Footprinting and Reconnaissance

FOOT PRINTING AND KEY POINTS

- Footprinting in the context of cybersecurity refers to gathering information about a target system or network to identify potential vulnerabilities and assess the security posture. Here are the key points:
- **Passive Footprinting:** This involves collecting information without directly interacting with the target system or network. This could include gathering data from public sources such as social media, company websites, search engines, and public databases.
- **Active Footprinting:** Involves directly interacting with the target system or network to gather information. This could include port scanning, network mapping, and reconnaissance to identify active hosts, services, and potential vulnerabilities.
- **Open Source Intelligence (OSINT):** Utilizing publicly available information to gather intelligence about the target. This includes information from websites, social media, online forums, job postings, press releases, and other public sources.
- **Tools and Techniques:** Various tools and techniques are used in footprinting, such as WHOIS lookup, DNS interrogation, network scanning tools like Nmap, web scraping tools, social engineering, and dumpster diving (physically going through trash for sensitive information).
- **Enumeration:** This involves extracting additional information about the target network, such as user accounts, shares, services, and system configurations. Enumeration is typically performed after initial information gathering and can involve techniques like querying DNS records, SNMP enumeration, and querying network services.
- **Ethical Considerations:** Footprinting should be conducted ethically and legally, adhering to all relevant laws and regulations. Unauthorized access to systems or networks is illegal and unethical.
- **Risk Assessment:** The information gathered during footprinting is used to assess the security posture of the target system or network. This includes identifying potential vulnerabilities, entry points, and areas of weakness that could be exploited by attackers.
- **Footprinting as a Phase in Penetration Testing:** Footprinting is often the initial phase in penetration testing or ethical hacking engagement. It provides the foundation for subsequent phases such as scanning, exploitation, and post-exploitation.
- By understanding the key points of footprinting, organizations can better protect their systems and networks by identifying and addressing potential security risks before they can be exploited by malicious actors.



RECONNAISSANCE AND KEY POINTS

- Reconnaissance, often called recon, is the initial phase of the hacking process where information is gathered about a target system or network. Here are the key points:
- **Purpose:** The primary goal of reconnaissance is to gather as much information as possible about the target to understand its structure, potential vulnerabilities, and the best approach for an attack.
- **Passive Reconnaissance:** Involves collecting information without directly interacting with the target system or network. This includes gathering data from public sources like social media, company websites, search engines, and public databases.
- **Active Reconnaissance:** Involves directly interacting with the target system or network to gather information. This could include port scanning, network mapping, and reconnaissance to identify active hosts, services, and potential vulnerabilities.
- **Open Source Intelligence (OSINT):** A significant part of reconnaissance involves utilizing publicly available information to gather intelligence about the target. This includes information from websites, social media, online forums, job postings, press releases, and other public sources.
- **Tools and Techniques:** Various tools and techniques are used in reconnaissance, such as WHOIS lookup, DNS interrogation, network scanning tools like Nmap, web scraping tools, social engineering, and dumpster diving (physically going through trash for sensitive information).
- **Information Gathering:** Reconnaissance involves gathering information about the target's infrastructure, including IP addresses, domain names, network topology, email addresses, employee names and roles, software versions, and potential entry

DOMAIN NAME "TESTPHP" LOOKUP SERVICE

http:testphp.vulnweb.com

Monitor This

⌂ http

Server Type	Status	ContentType
nginx/1.19.0	200 OK	text/html; charset=UTF-8

	Test	Result
✓	HTTP Connect	200 OK
✓	HTTP Filter	
✓	HTTP Delay Check	Success - response in 68 ms

dns lookup

smtp diag

blacklist

Reported by mxtoolbox.com on 2/24/2024 at 11:44:27 PM just for you

Transcript

http:testphp.vulnweb.com

⌂ http

Server Type	Status	ContentType
nginx/1.19.0	200 OK	text/html; charset=UTF-8

	Test	Result
✓	HTTP Connect	200 OK
✓	HTTP Filter	
✓	HTTP Delay Check	Success - response in 144 ms

dns lookup

smtp diag

blacklist

Reported by mxtoolbox.com on 2/24/2024 at 11:44:24 PM just for you

Transcript



DOMAIN SPECIFIED WEB SITE PARTICULAR SERVICE

ABOUT THE SUPERTOOL!

All of your MX record, DNS, blacklist and SMTP diagnostics in one integrated tool. Input a **domain name** or **IP Address** or **Host Name**. Links in the results will guide you to other relevant tools and information. And you'll have a chronological history of your results.

If you already know exactly what you want, you can force a particular test or lookup. Try some of these examples:

(e.g. "blacklist: 127.0.0.2" will do a blacklist lookup)

Command	Explanation
blacklist:	Check IP or host for reputation
smtp:	Test mail server SMTP (port 25)
mx:	DNS MX records for domain
a:	DNS A record IP address for host name
spf:	Check SPF records on a domain
txt:	Check TXT records on a domain
ptr:	DNS PTR record for host name
cname:	DNS canonical host name to IP address
whois:	Get domain registration information
arin:	Get IP address block information
soa:	Get Start of Authority record for a domain
tcp:	Verify an IP Address allows tcp connections
http:	Verify a URL allows http connections
https:	Verify a URL allows secure http connections
ping:	Perform a standard ICMP ping
trace:	Perform a standard ICMP trace route
dns:	Check your DNS Servers for possible problems New!



SHODAN DNS WE CAN USE WEB SITE

SHODAN

Explore

Pricing

https://www.ibm.com/in-en

Q

Login

TOTAL RESULTS

6

TOP COUNTRIES

United States

5

Germany

1

TOP PORTS

3001

5

21

1

TOP ORGANIZATIONS

SoftLayer Technologies Inc.

4

NetActuate, Inc

1

SoftLayer Technologies, Inc.

1

View Report

View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to.](#)

52.118.148.191

bf 94.7634 ip4 static sl-reverse.com

SoftLayer Technologies Inc.

United States, Dallas

HTTP/1.1 200 OK

X-Powered-By: Express

content-type: text/html; charset=utf-8

x-dispatcher: prod-publish-e

x-headers: publish

x-content-type-options: nosniff

last-modified: Mon, 19 Feb 2024 18:26:09 GMT

x-frame-options: SAMEORIGIN

cf-cache-status: DYNAMIC

server: cloudflare

cf-ray: 857d8d5a...

2024-02-19T11:05:00.885518

160.240.71.133

85.47.4096 ip4 static sl-reverse.com

SoftLayer Technologies Inc.

United States, Dallas

HTTP/1.1 200 OK

X-Powered-By: Express

content-type: text/html; charset=utf-8

x-dispatcher: prod-east-publish-1

x-headers: publish

x-content-type-options: nosniff

last-modified: Sun, 18 Feb 2024 13:42:18 GMT

x-frame-options: SAMEORIGIN

cf-cache-status: DYNAMIC

server: cloudflare

cf-ray: 857...

2024-02-18T16:11:44.255270

149.81.14.244

14.0e.5105 ip4 static sl-reverse.com

SoftLayer Technologies, Inc.

Germany, Frankfurt am Main

HTTP/1.1 200 OK

X-Powered-By: Express

content-type: text/html; charset=utf-8

x-dispatcher: prod-east-publish-1

x-headers: publish

x-content-type-options: nosniff

last-modified: Thu, 15 Feb 2024 14:56:13 GMT

x-frame-options: SAMEORIGIN

cf-cache-status: DYNAMIC

cf-ray: 857...


2024-02-18T07:18:44.620467

IBM AND WEBSITE WITH IP ADDRESS

52.118.148.59 

3b.94.7634.ip4.static.sl-reverse.com

[SoftLayer Technologies Inc.](#)


 United States, Dallas

```
HTTP/1.1 200 OK
X-Powered-By: Express
content-type: text/html; charset=utf-8
x-dispatcher: prod-publish-0
x-vhost: publish
x-content-type-options: nosniff
last-modified: Thu, 15 Feb 2024 20:59:51 GMT
x-frame-options: SAMEORIGIN
cf-cache-status: DYNAMIC
server: cloudflare
cf-ray: 8560a4af...
```

52.116.129.25 

19.81.7434.ip4.static.sl-reverse.com

[SoftLayer Technologies Inc.](#)


 United States, Dallas

```
HTTP/1.1 200 OK
X-Powered-By: Express
content-type: text/html; charset=utf-8
x-dispatcher: prod-publish-0
x-vhost: publish
x-content-type-options: nosniff
last-modified: Wed, 14 Feb 2024 00:46:05 GMT
x-frame-options: SAMEORIGIN
cf-cache-status: DYNAMIC
server: cloudflare
cf-ray: 85515e63...
```

104.225.8.135

dts-iad3.dtssoftware.com

[NetActuate, Inc](#)

 United States, Ashburn

```
220-
220- | _ \  / |  / | / _ \ | _ \  / \ | _ \ |
220- | | | | \  \  \  \ | | | |  / \ / \ | | | |
220- | | | |  ) |  ) | | | |  | | \ ...
```