
Passive Recon -

1. DNS Lookup Utility `host` Tool

```
whatis host
```

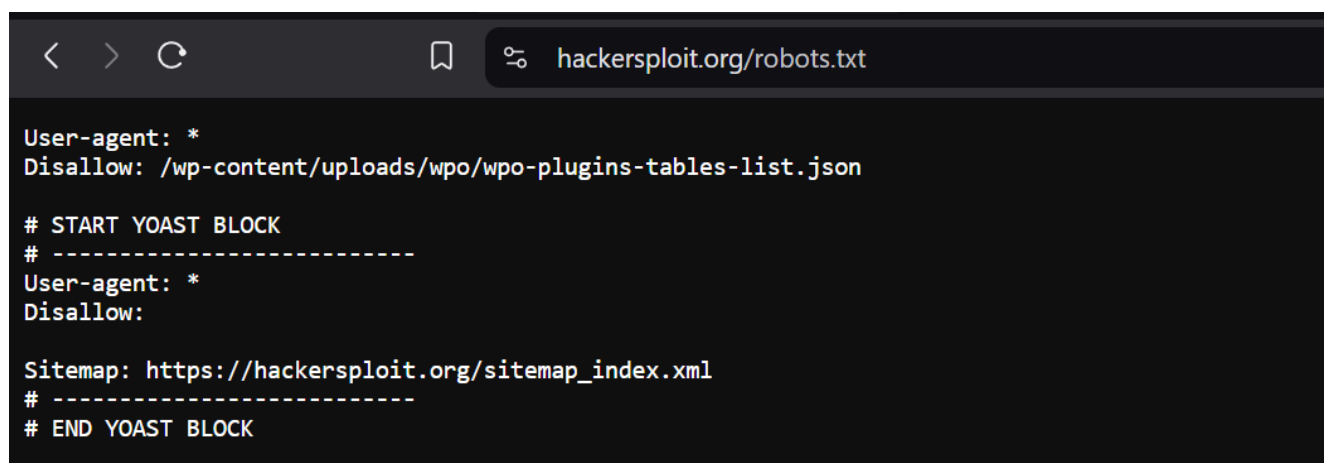
Tool used to find IP address to the domain name

```
host hackersploit.org
```

2. `robots.txt` & `sitemap.xml` file

this text file tells information about what endpoints are indexed or allowed for crawling by search engines like google, duck-duckGo, bing, etc.

- Crawling : Web crawling, also known as web spidering or web scraping, is a process where automated programs, called bots or spiders, systematically browse the internet to gather information from websites.



```
< > ↻ 📖 🌐 hackersploit.org/robots.txt

User-agent: *
Disallow: /wp-content/uploads/wpo/wpo-plugins-tables-list.json

# START YOAST BLOCK
# -----
User-agent: *
Disallow:

Sitemap: https://hackersploit.org/sitemap_index.xml
# -----
# END YOAST BLOCK
```

XML Sitemap

Generated by **Yoast SEO**, this is an XML Sitemap, meant for consumption by search engines.

You can find more information about XML sitemaps on sitemaps.org.

This XML Sitemap Index file contains 3 sitemaps.

Sitemap	Last Modified
https://hackersploit.org/post-sitemap.xml	2023-02-26 15:22 +00:00
https://hackersploit.org/page-sitemap.xml	2024-08-17 00:17 +00:00
https://hackersploit.org/category-sitemap.xml	2023-02-26 15:22 +00:00

- usage :

```
< URL > /robots.txt
```

```
< URL > /sitemap.xml
```

3. BuiltWith and Wapplayzer

chrome web store

Search extensions and themes

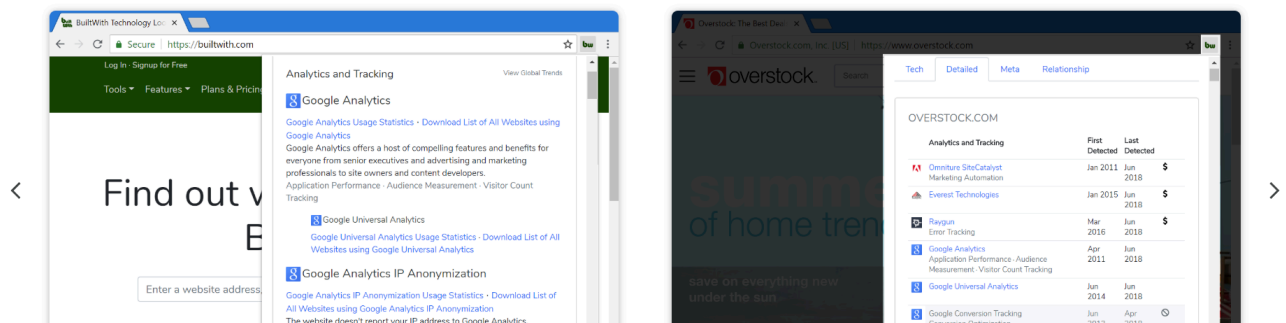
Discover Extensions Themes

bw BuiltWith Technology Profiler

Add to Brave

builtwith.com Featured 4.4★ (406 ratings) [Share](#)

Extension Developer Tools 300,000 users



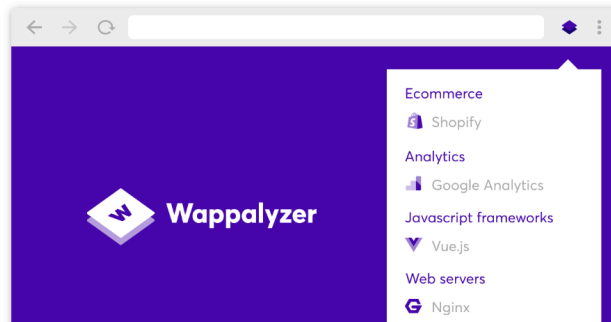


Wappalyzer - Technology profiler

Add to Brave

 wappalyzer.com Featured 4.6 ★ (1.9K ratings) Share

Extension	Developer Tools	3,000,000 users
-----------	-----------------	-----------------



4. Whatweb Tool

```
root@Mrwebsecure: /home/yash
(yash@Mrwebsecure)-[~]
$ sudo su
[sudo] password for yash:
root@Mrwebsecure:/home/yash#
root@Mrwebsecure:/home/yash# whatis whatweb
whatweb (1)          - Next generation Web scanner. Identify technologies use...
root@Mrwebsecure:/home/yash# whatweb

.### $$. .### $$$ $. .###$. .###$. .###$. .###$. .###$.
### $$. .### $$$ $. .###$. .###$. .###$. .###$. .###$.
$ $$. .### $$$ $. .###$$$ $. .###$$$ $. .###$$$ $. .###$$$ $.
$ $$. .### $$$ $. .###$$$ $. .###$$$ $. .###$$$ $. .###$$$ $.
$. .### $$$ $. .###$$$ $. .###$$$ $. .###$$$ $. .###$$$ $.
$:.$$. .### $$$ $. .###$$$ $. .###$$$ $. .###$$$ $. .###$$$
$;$$. .### $$$ $. .###$$$ $. .###$$$ $. .###$$$ $. .###$$$
##### ##### $$$ $$$ $$$ $$$ $$$ $$$ $$$ $$$ $$$
```

WhatWeb - Next generation web scanner version 0.5.5.
Developed by Andrew Horton (urbanadventurer) and Brendan Coles (bcoles)
Homepage: <https://www.morningstarsecurity.com/research/whatweb>

Usage: whatweb [options] <URLs>

<TARGETS>	Enter URLs, hostnames, IP addresses, filenames or IP ranges in CIDR, x.x.x-x, or x.x.x.x-x.x.x.x format.
--input-file=FILE, -i	Read targets from a file.
--aggression, -a=LEVEL 1. Stealthy	Set the aggression level. Default: 1. Makes one HTTP request per target and also follows redirects.
3. Aggressive	If a level 1 plugin is matched, additional requests will be made.
--list-plugins, -l	List all plugins.
--info-plugins, -I=[SEARCH]	List all plugins with detailed information. Optionally search with a keyword.
--verbose, -v	Verbose output includes plugin descriptions.

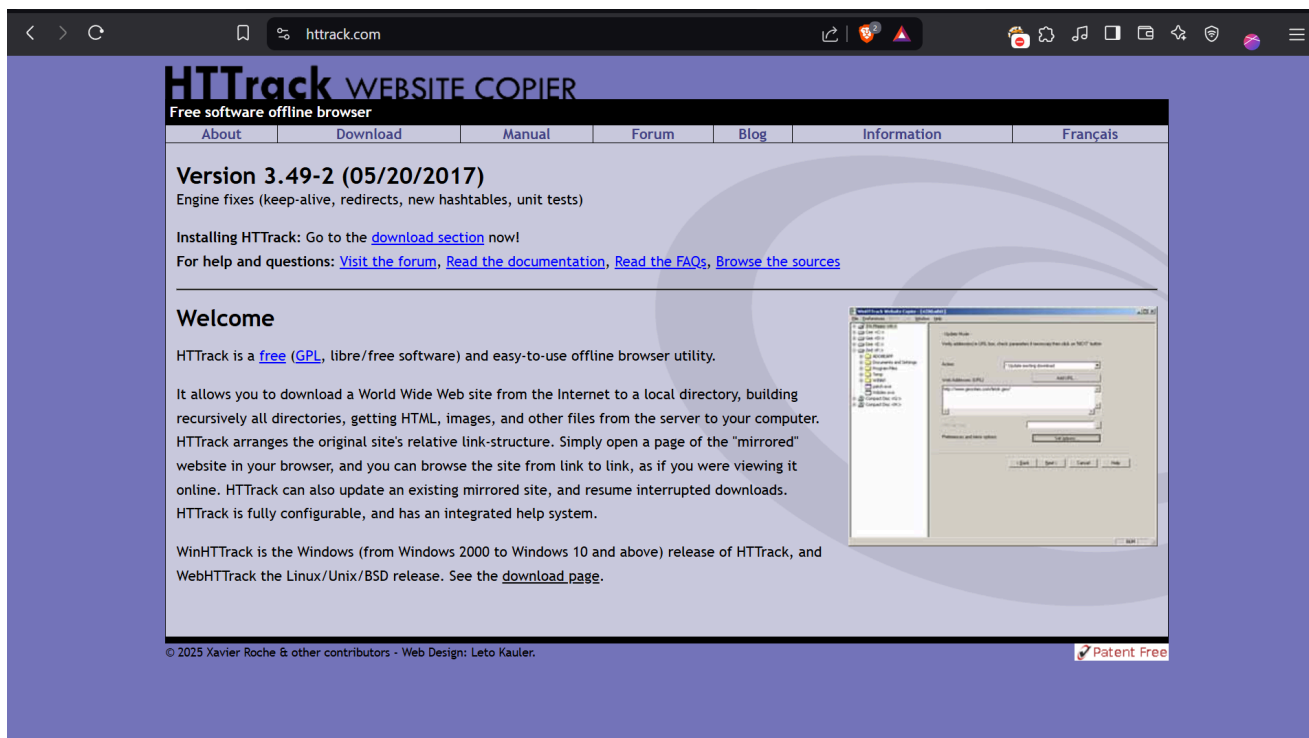
Note: This is the short usage help. For the complete usage help use -h or --help.

```
root@Mrwebsecure:/home/yash# S
```

- usage :

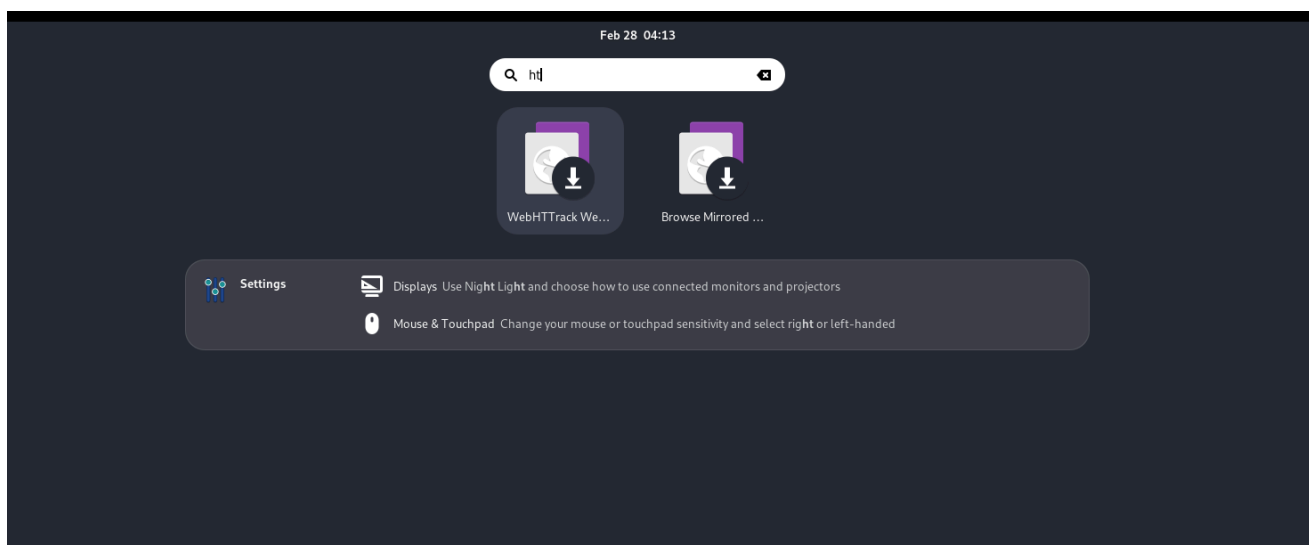
whatweb hackersploit.org

5. To Download entire website httrack tool.

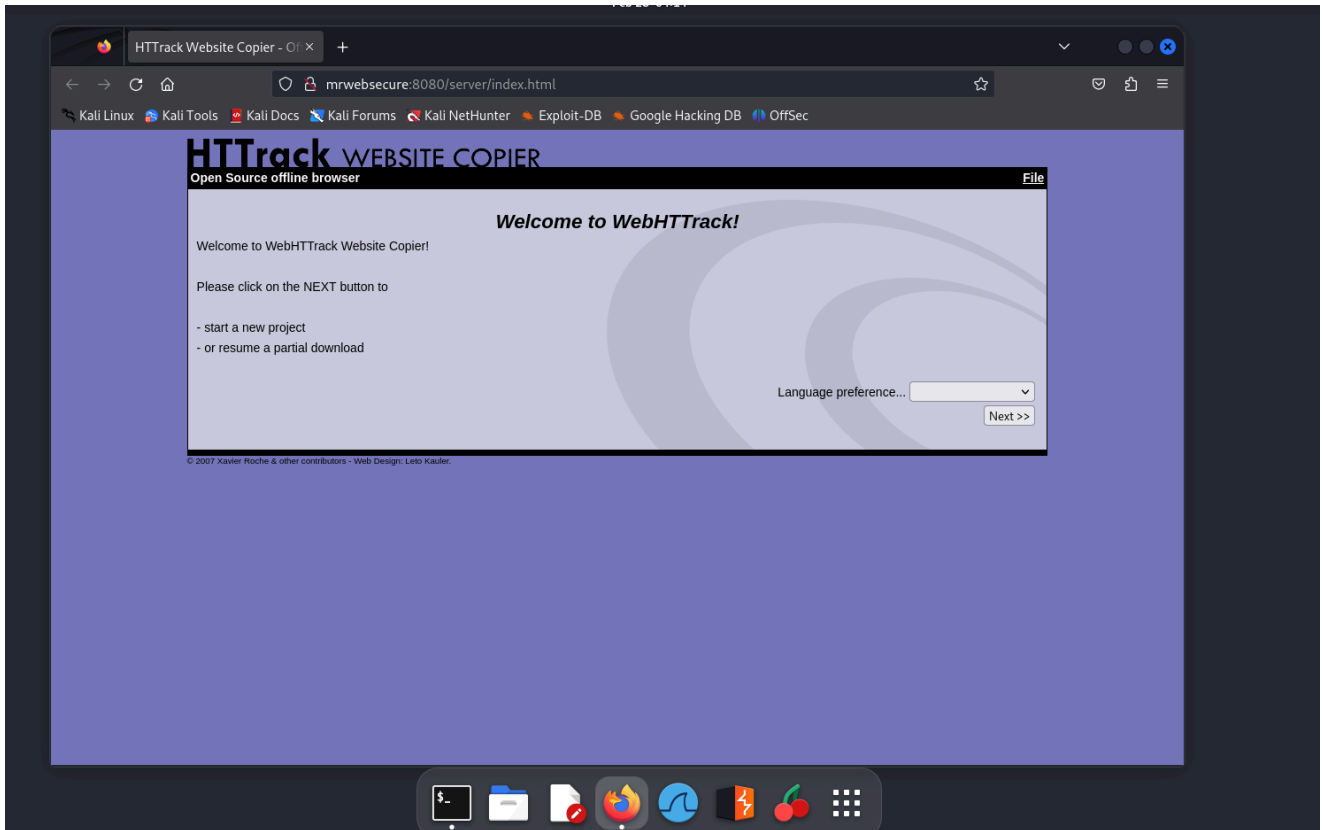


To install this tool in kali linux

apt install webhttrack



we can use to this tool to download all information about the webstite



6. Whois Tool for gathering information about the website

- GUI - <https://who.is/>

```
whois hackersploit.org
```

Target : <https://digi.ninja/projects/zonetransferme.php>

```
whois dnszonetransfer.me
```

Gathers Information about websites -

- Register
- Mail's
- IANA ID
- Addresses

```
root@Mrwebsecure:/home/yash# whois hackersploit.org
Domain Name: hackersploit.org
Registry Domain ID: 77f8fe62a425487cbefef4bf7e27d2ec-LROR
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2025-01-07T14:38:39Z
Creation Date: 2018-04-05T11:27:07Z
Registry Expiry Date: 2026-04-05T11:27:07Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Capital Region
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IS
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin,
or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
```

7. Netcraft Website

- link : <https://www.netcraft.com/>

What's that site running?

Discover the web technologies and internet infrastructure powering any site.

hackersploit.org

ANALYZE

Background

Site title	HackerSploit Blog - Free Red Team & Penetration Testing Training	Date first seen	June 2018
Site rank	30480	Primary language	English
Description	HackerSploit is the leading provider of free Infosec and cybersecurity training. Our goal is to make cybersecurity training more effective and accessible to students and professionals. We achieve this by providing essential training on how to attack and defend systems with virtual labs and real-world scenarios. We offer individual and corporate training packages in Penetration Testing & Red Team Operations, Web application penetration testing, and cybersecurity awareness training.		

Site	http://hackersploit.org	Domain	hackersploit.org
Netblock Owner	Cloudflare, Inc.	Nameserver	dee.ns.cloudflare.com
Hosting company	Cloudflare	Domain registrar	pir.org
Hosting country	US	Nameserver organisation	whois.cloudflare.com

Privacy service provided by Withheld for Privacy ehf. REDACTED FOR PRIVACY

Network

8. DNSrecon tool

- Link : https://www.kali.org/tools/dnsrecon/

```
root@Mrwebsecure:/home/yash# dnsrecon
usage: dnsrecon [-h] [-d DOMAIN] [-n NS_SERVER] [-r RANGE] [-D DICTIONARY] [-f] [-a] [-s] [-b] [-y] [-k] [-w] [-z] [--threads THREADS] [--lifetime LIFETIME]
               [--tcp] [--db DB] [-x XML] [-c CSV] [-j JSON] [--iw] [--disable_check_recursion] [--disable_check_bindversion] [-V] [-v] [-t TYPE]
```

dnsrecon -d hackersploit.org

dnsrecon -d zonetransfer.me

dnsrecon -d zonetransfer.me -t axfr

Record	Description	Pentesting Use
A	Domain → IPv4	Find target's IP
AAAA	Domain → IPv6	IPv6 recon
CNAME	Alias for a domain	Detect hidden infrastructure
MX	Mail servers	Email spoofing, phishing
TXT	Text data (SPF, DKIM, DMARC)	Check email security flaws
NS	Name servers	Identify DNS infrastructure
SOA	Domain admin info	Find internal details
PTR	Reverse DNS (IP → Domain)	Identify hosts from IPs

Record	Description	Pentesting Use
SRV	Service & port info	Expose running services
CAA	SSL/TLS certificate policy	Check for misconfigurations

9. Sublist3r Tool

tool designed to enumerate subdomains of websites

Link : <https://github.com/about3la/Sublist3r>

```
apt install sublist3r
```

```
sublist3r -d hackersploit.org
```

```
sublist3r -d hackersploit.org -e yahoo,google
```

```
sublist3r -d ine.com
```

Short Form	Long Form	Description
-d	--domain	Domain name to enumerate subdomains of
-b	--bruteforce	Enable the subbrute bruteforce module
-p	--ports	Scan the found subdomains against specific tcp ports
-v	--verbose	Enable the verbose mode and display results in realtime
-t	--threads	Number of threads to use for subbrute bruteforce
-e	--engines	Specify a comma-separated list of search engines
-o	--output	Save the results to text file
-h	--help	show the help message and exit

10. Google Dorks

- `site:`


```
site:tesla.com  
site:*.tesla.com  
site:tesla.com employees
```

- `inurl:`

```
site:tesla.com inurl:admin  
site:*.tesla.com inurl:admin  
site:tesla.com inurl:forum
```

- `filetype:`

```
site:tesla.com filetype:pdf
```

- `intitle:index of`

```
intitle:index of
```

- `cache:`

```
cache:tesla.com
```

- `inurl:`

```
inurl:auth_user_file.txt  
inurl:password.txt  
inurl:wp-config.bak
```

```
site:gov.* "index of" *.csv  
site:gov.* "index of" *.csv passwords
```

11. Waybackmachine Web Archive

Link : <https://web.archive.org/>

12. theHarvester Tool

link : <https://github.com/laramies/theHarvester>

```
sudo apt install theharvester
```

```
theHarvester -d tesla.com
```

```
theHarvester -d tesla.com -b google,linkedin
```

```
theHarvester -d tesla.com -b all
```

13. Leak Password Databases

Link : <https://haveibeenpwned.com/>

14. Wafw00f Tool

link : <https://github.com/EnableSecurity/wafw00f>

```
wafw00f tesla.com
```

```
wafw00f zonetransfer.me
```

```
wafw00f https://hackertube.net -a
```

15. Email & Username OSINT

- Link : <https://phonebook.cz/>
 - Link : <https://dehashed.com/>
 - Link : <https://whatsmyname.app/>
-

16. Information gathering website

- Link : <https://centralops.net/>
 - Link : <https://dnslytics.com/>
 - Link : <https://www.virustotal.com/>
 - Link : <https://viewdns.info/>
 - Link : <https://crt.sh/>
-

17. Shodan

- Link : <https://www.shodan.io/>

city:

```
city:Mumbai rdp
```

```
city:mumbai remote desktop
```

18. Image OSINT

- Link : <https://pimeyes.com/en>
-

19. subfinder tool

```
subfinder -d tesla.com
```

20. Amass Tool

```
amass enum -d tesla.com
```

Active Recon -

1. DNS Zone Transfer

- DNS : Domain Name Server is an protocol used to resolve IP address, hostname to its IP addresses
- DNS Intorogation can provide information like IP address to particular server and records of Nameserver or Mail servers
- DNS Records :

Record	Description	Pentesting Use
A	Domain → IPv4	Find target's IP
AAAA	Domain → IPv6	IPv6 recon
CNAME	Alias for a domain	Detect hidden infrastructure
MX	Mail servers	Email spoofing, phishing
TXT	Text data (SPF, DKIM, DMARC)	Check email security flaws
NS	Name servers	Identify DNS infrastructure
SOA	Domain admin info	Find internal details
PTR	Reverse DNS (IP → Domain)	Identify hosts from IPs
SRV	Service & port info	Expose running services
CAA	SSL/TLS certificate policy	Check for misconfigurations

- DNS ZONE TRANSFER ATTACK -->

1. DNS server admins may wants to copy or transfer zone files from one DNS Server to another. This process is known as zone transfer.
2. If it is left misconfigured, this functionality can be abused by attackers to copy the zone file from primary DNS server to another DNS Server.
3. DNS zone transfer can provide penetration tester view of an organization's network layout
4. Internal Network address can be found on an Organizations DNS Servers.

```
dnsenum zonetransfer.me
```

```
dig axfr @nsztml1.digi.ninja zonetransfer.me
```

```
fierce -dns zonetransfer.me
```

2. arping tool

```
arping 192.168.1.1 -c 3
```

3. netdiscover Tool

```
netdiscover -p
```

- wireshark --> arp.proto.type

```
netdiscover -i eth0 -r 192.168.1.0/24
```

4. Nmap Network Scanner

- wireshark - ip.addr==target

1. Host Discovery -sn : Tells Nmap not to do port scan after Host discovery.

```
nmap -sn 192.168.10.0/24
```

2. Port Scanning

```
nmap 192.168.10.15
```

3. Ping Probes Blocking -Pn : Tells not to ping device directly scan for ports.

```
nmap -Pn 192.168.10.15
```

- p : For particular specific ports (ex. -p 80,445)
- p- : Scan for all TCP and UDP ports
- p1-1000 : Specific Port Range Scanning
- F : Fast Scan which Scans main 100 ports

- sU : For UDP Scan
 - v : Verbose Output and gives display while scanning
 - sV : Service Version Scans
 - O : Scan for Guessing the Operating System
 - sC : Script Scan
 - T4 : Ranges from 1 to 5 defines the Speed of Scan
 - oN : Output in .txt format
 - oX : Output in .xml format
 - PE : performs the ICMP ECHO ping scan.
 - PP : performs the ICMP timestamp ping scan.
-