

Task-7

SELECT A WEBSITE DO FOOTPRINTING AND RECONNAISSANCE LIKE COLLECT INFORMATION ABOUT WEBSITE USING NSLOOKUP OSINT FRAMEWORK

The website choosen is <http://testfire.net/> . Wensite and tools used to collect information.

1.<https://www.nslookup.io/domains/testfire.net/dns-records/> (ns lookup)

2.<https://osintframework.com/> (osint framework)

3.nmap

Footprinting using nmap:-

```
niraianbu@localhost: ~  
(niraianbu@localhost)-[~]  
$ nmap testfire.net  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-07 12:55 IST  
Nmap scan report for testfire.net (65.61.137.117)  
Host is up (0.27s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp    open  https  
8080/tcp   open  http-proxy  
8443/tcp   closed https-alt  
  
Nmap done: 1 IP address (1 host up) scanned in 20.81 seconds  
  
(niraianbu@localhost)-[~]  
$
```

1. Port 80/tcp: This is the HTTP port, commonly used for serving web pages over the standard HTTP protocol. It suggests that a web server is running on this port, and you can access web content hosted on this server by opening a web browser and navigating to the IP address or domain name.

2. Port 443/tcp: This is the HTTPS port, used for secure web communication over the HTTPS protocol. Similar to port 80, it indicates the presence of a web server that offers secure browsing capabilities.
3. Port 8080/tcp: This is typically associated with an HTTP proxy server. An HTTP proxy server can be used to forward web requests from clients to other servers while providing various functions like caching, filtering, or anonymizing. It might be used for load balancing or filtering web traffic.
4. Port 8443/tcp: This port is closed, meaning there is no active service listening on it. Port 8443 is often associated with HTTPS services running on an alternative port. The fact that it's closed suggests that there might not be a service configured to listen on this port.

DNS records for **testfire.net**

Cloudflare Google DNS OpenDNS Authoritative Local DNS ▾



The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
> 65.61.137.117	24h

AAAA records

No AAAA records found.

CNAME record

No CNAME record found.

TXT records

SPF record

This record is valid for 30m.

Pass if the email sender's IP is in the MX records (with CIDR /24 for IPv4) of testfire.net.

mx/24

Or else, mark the email as fail.

-all

By Nslookup.io

DNS for Developers

Never be confused
about DNS again.

NS records

Name server	Revalidate in
usc3.akam.net.	24h
ns1-206.akam.net.	24h
ns1-99.akam.net.	24h
eur5.akam.net.	24h
usw2.akam.net.	24h
usc2.akam.net.	24h
eur2.akam.net.	24h
asia3.akam.net.	24h

MX records

No mail servers found.

Other records

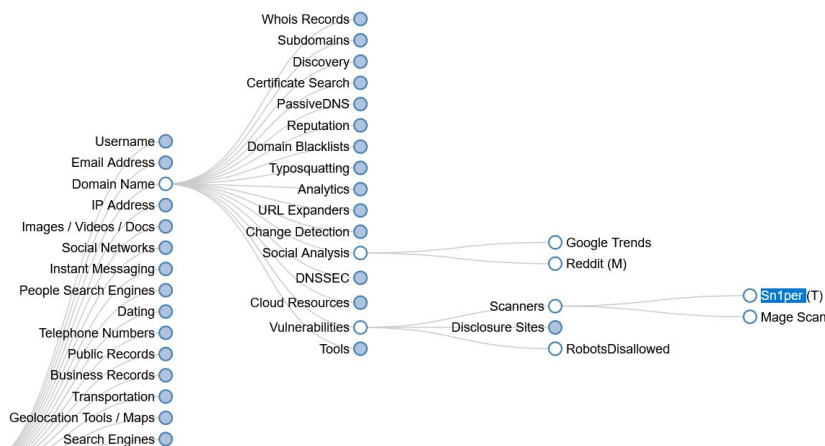
SOA


SOA data	Revalidate in
Start of authority	asia3.akam.net. 24h
Email	hostmaster@akamai.com
Serial	1366025607
Refresh	12h
Retry	2h
Expire	168h
Negative cache TTL	24h

Onsit frame work:

OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork, for more information: [Google Hacking](#)
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the itself must be edited manually




 **Sn1per** Public

Watch 328

master 1 branch 53 tags

Go to file Add file Code

 **1N3 Delete bin/inurlbr.php**

✓ d51dece last week 🕒 593 commits

bin	Delete bin/inurlbr.php	last week
conf	Merge pull request #422 from benemohamed/master	3 months ago
loot	Delete nmap-10.0.0.1.xml	7 years ago
modes	Merge pull request #422 from benemohamed/master	3 months ago
pro	Sn1per by @sn1persecurity - https://sn1persecurity.com	2 years ago
templates	Sn1per by @sn1persecurity - https://sn1persecurity.com	10 months ago
wordlists	Sn1per by @sn1persecurity - https://sn1persecurity.com	2 years ago