

Ethical Hacking and Penetration Testing

Footprinting and Reconnaissance

LEARNING OBJECTIVES

01

Explain Footprinting Concepts

02

Demonstrate Footprinting through Search Engines

03

Demonstrate Footprinting through Internet Research Services

04

Demonstrate Footprinting through Social Networking Sites

05

Use Different Techniques for Whois Footprinting

06

Use Different Techniques for DNS Footprinting

07

Use Different Techniques for Network and Email Footprinting

08

Demonstrate Footprinting through Social Engineering

09

Automate Footprinting Tasks using Advanced Tools and AI

10

Explain Footprinting Countermeasures

LO#01: Explain Footprinting Concepts

Reconnaissance

Reconnaissance (also known as footprinting) refers to the preparatory phase where an attacker seeks to gather as much information as possible about a target of evaluation prior to launching an attack

Types of Reconnaissance

Passive

Gathering information about the target **without direct interaction**

It involves:

- Open-source Intelligence (OSINT) gathering
- Proprietary databases and paid services
- Sharing intelligence with partner organizations or industry groups

Active

Gathering information about the target **with direct interaction**

It involves:

- DNS interrogation
- Social engineering
- Network/port scanning
- User and service enumeration

Information Obtained in Footprinting



Organization information

- Employee details
- Telephone numbers
- Branch and location details
- Background of the organization
- Web technologies
- News articles, press releases, and related documents



Network information

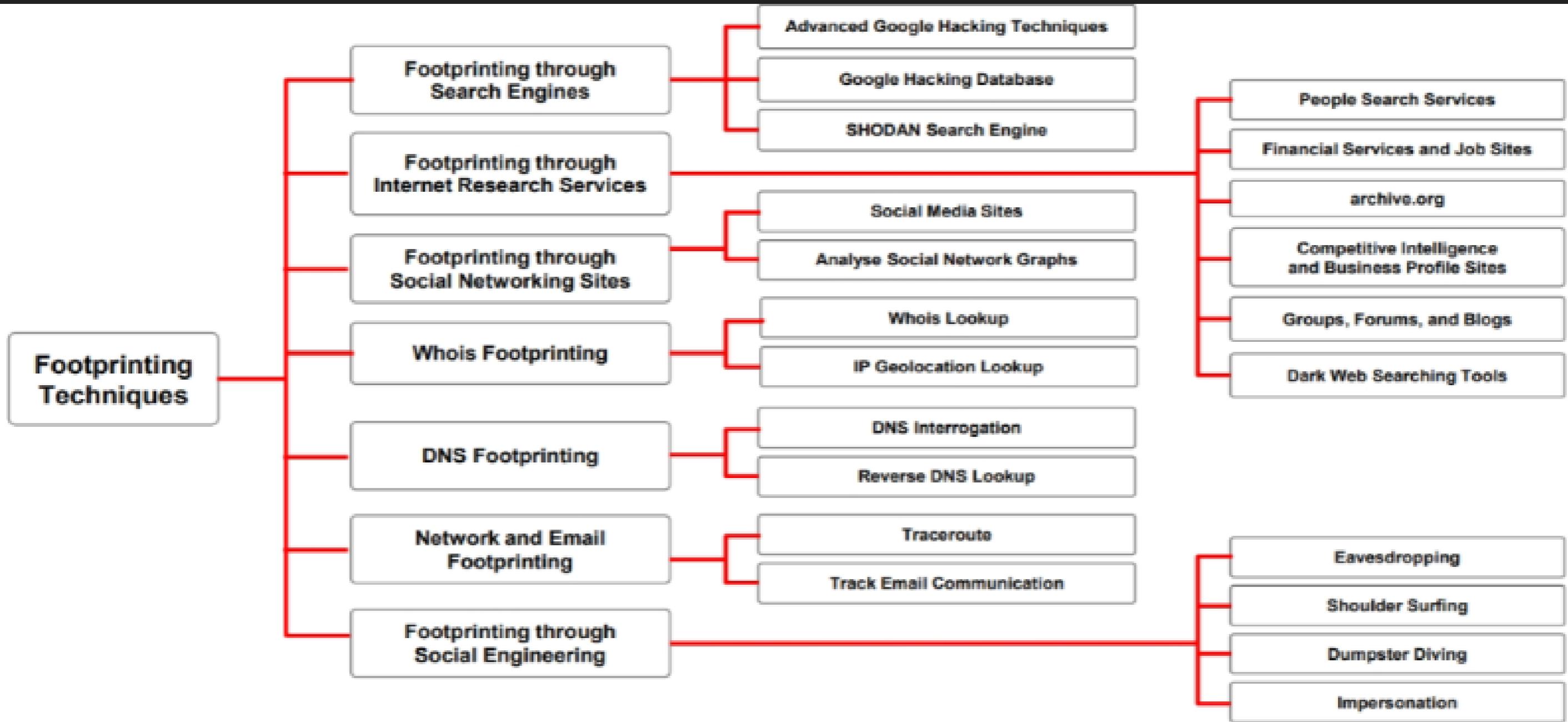
- Domain and sub-domains
- Network blocks
- Network topology, trusted routers, and firewalls
- IP addresses of the reachable systems
- Whois records
- DNS records



System information

- Web server OS
- Location of web servers
- Publicly available email addresses
- Usernames and passwords

Footprinting Methodology



LO#02: Demonstrate Footprinting through Search Engines

Footprinting through Search Engines

- Attackers use search engines to **extract information about a target**, such as employed technology platforms, employee details, login pages, and intranet portals, which help the attacker to perform social engineering and other types of advanced system attacks

- Major search engines:

Google

Bing

YAHOO!

Ask.com

Aol.

Baidu 百度



DuckDuckGo

- Attackers can use **advanced search operators** available with these search engines and create complex queries to find, filter, and sort specific information about the target

- Search engines are also used to find other sources of **publically accessible information resources**, e.g., you can type “top job portals” to find major job portals that provide critical information about the target organization

Footprinting Using Advanced Google Hacking Techniques

- Attackers use search engines to **extract information about a target**, such as employed technology platforms, employee details, login pages, and intranet portals, which help the attacker to perform social engineering and other types of advanced system attacks
- Google hacking refers to the use of advanced Google search operators for **creating complex search queries** to extract sensitive or **hidden** information that helps attackers find **vulnerable targets**

Popular Google advanced search operators

Search Operator	Purpose	Search Operator	Purpose
[cache:]	Displays the web pages stored in the Google cache	[allintitle:]	Restricts the results to those websites containing all the search keywords in the title
[link:]	Lists web pages that have links to the specified web page	[intitle:]	Restricts the results to documents containing the search keyword in the title
[related:]	Lists web pages that are similar to the specified web page	[allinurl:]	Restricts the results to those containing all the search keywords in the URL
[info:]	Presents some information that Google has about a particular web page	[inurl:]	Restricts the results to documents containing the search keyword in the URL
[site:]	Restricts the results to those websites in the given domain	[location:]	Finds information for a specific location

Footprinting Using Advanced Google Hacking Techniques with AI



- An attacker can also leverage **AI-powered ChatGPT** or other generative AI technology to perform this task by using an appropriate prompt such as:

"Use filetype search operator to obtain pdf files on the target website eccouncil.org and store the result in the recon1.txt file"

```
● ● ○ sgpt --chat footprint --shell "Use filetype search operator to obtain pdf files on the target website e
File Edit View Search Terminal Help
[root@parrot]~[~]
#sgpt --chat footprint --shell "Use filetype search operator to obtain
pdf files on the target website eccouncil.org and store the result in the
recon1.txt file"
lynx --dump "http://www.google.com/search?q=site:eccouncil.org,filetype:pdf"
| grep "http" | cut -d ":" -f2 | grep -o "http[%s]*" > recon1.txt
[E]xecute, [D]escribe, [A]bort: E
[root@parrot]~[~]
```

A screenshot of a terminal window titled "recon1.txt (~) - Pluma (as superuser)". The window shows a list of ten URLs, each ending in ".pdf", which were found using the specified search query. The URLs are:

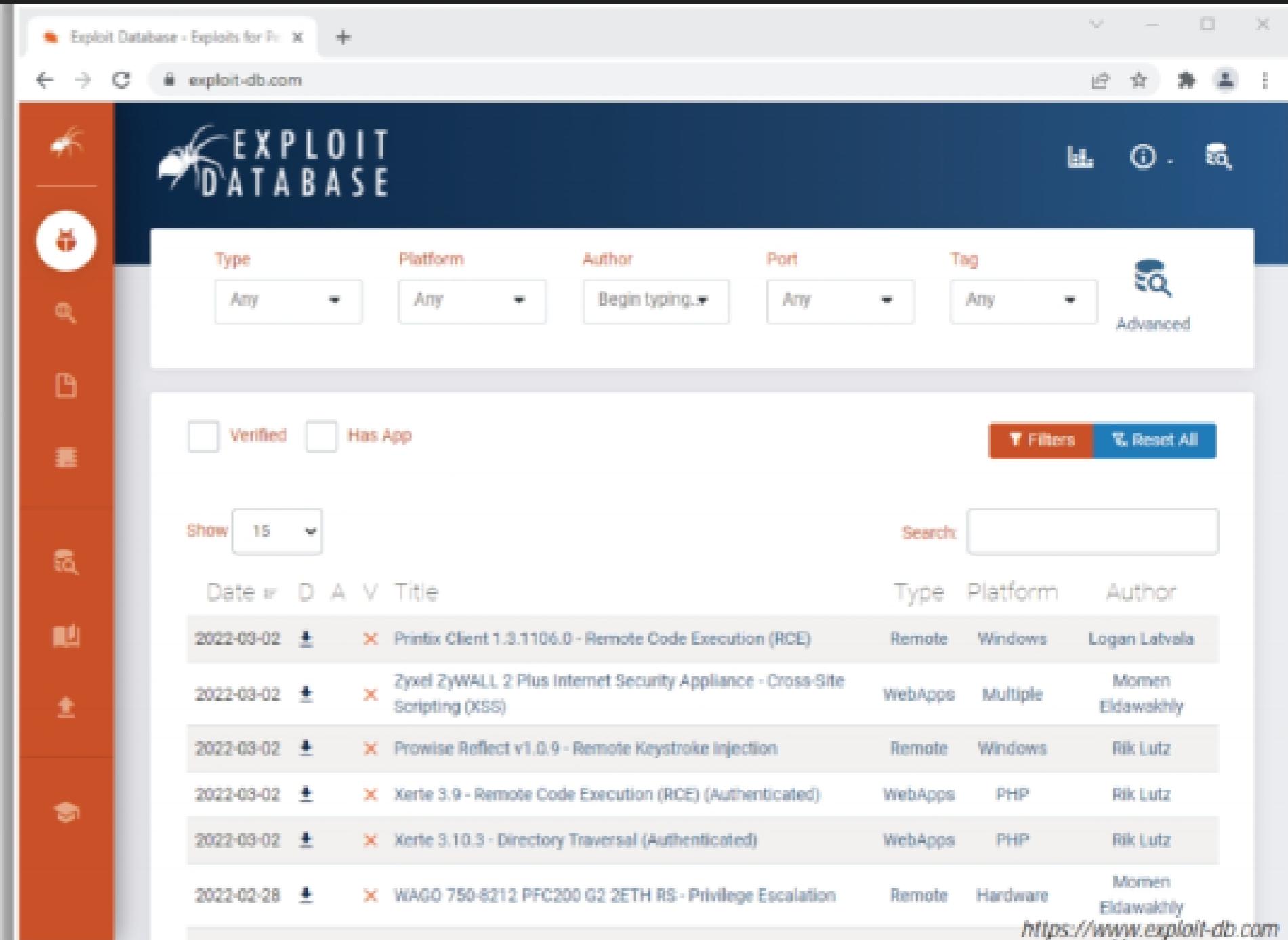
- 1 https://cert.eccouncil.org/images/doc/candidateagreement.pdf
- 2 https://aspen.eccouncil.org/Docs/Applications/ATC_Agreementv9.0.pdf
- 3 https://iclass.eccouncil.org/wp-content/uploads/2019/10/CSA-Essential-Concepts-Self-Study.pdf
- 4 https://aspen.eccouncil.org/Docs/UserGuides/AccessCourseware-UserGuide.pdf
- 5 https://aspen.eccouncil.org/Docs/UserGuides/CEHPractical-DashboardUserGuide.pdf
- 6 https://cert.eccouncil.org/images/doc/CEH-Handbook-v6.pdf
- 7 https://aspen.eccouncil.org/Docs/CISOMAG/CISOMAG-January2020-Preview.pdf
- 8 https://cert.eccouncil.org/images/doc/CEH-Handbook-v5.pdf
- 9 https://cert.eccouncil.org/images/doc/Appeal-Form-v2.pdf
- 10 https://cert.eccouncil.org/images/doc/CND-Handbook-v4.pdf

At the bottom of the terminal window, there are buttons for "Plain Text", "Tab Width: 4", "Ln 1, Col 1", and "INS".

Google Hacking Database

- The Google Hacking Database (GHDB) is an authoritative source for **querying the ever-widening reach of the Google search engine**
- Attackers use **Google dorks** in Google advanced search operators to extract sensitive information about their target, such as vulnerable servers, error messages, sensitive files, login pages, and websites

**EXPLOIT
DATABASE**



The screenshot shows the Exploit Database homepage. The top navigation bar includes links for Home, Exploits, Tools, and About. The main header features a red exploit icon and the text "EXPLOIT DATABASE". Below the header is a search bar with dropdown filters for Type (Any), Platform (Any), Author (Begin typing...), Port (Any), and Tag (Any). There are also "Filters" and "Reset All" buttons. The main content area displays a table of vulnerabilities with columns for Date, Title, Type, Platform, and Author. The table lists several recent findings:

Date	Title	Type	Platform	Author
2022-03-02	Printix Client 1.3.1106.0 - Remote Code Execution (RCE)	Remote	Windows	Logan Latvala
2022-03-02	Zyxel ZyWALL 2 Plus Internet Security Appliance - Cross-Site Scripting (XSS)	WebApps	Multiple	Momen Eldawakly
2022-03-02	Prowise Reflect v1.0.9 - Remote Keystroke Injection	Remote	Windows	Rik Lutz
2022-03-02	Xerte 3.9 - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	Rik Lutz
2022-03-02	Xerte 3.10.3 - Directory Traversal (Authenticated)	WebApps	PHP	Rik Lutz
2022-02-28	WAOO 750-8212 PFC200 G2 2ETH RS - Privilege Escalation	Remote	Hardware	Momen Eldawakly

At the bottom right, there is a link to the website: <https://www.exploit-db.com>.

VPN Footprinting through Google Hacking Database

Google Dork	Description
inurl:"/sslvpn_logon.shtml" intitle:"User Authentication" "WatchGuard Technologies"	Finds pages containing login portals
inurl:/sslvpn/Login/Login	Finds VPN login portals
site:vpn.*.*/ intitle:"login"	
intext:Please Login SSL VPN inurl:remote/login	Finds Fortinet VPN login pages
intext:FortiClient	
site:vpn.*.*/ intext:"login" intitle:"login"	Retrieves various VPN login pages
intitle:"index of" /etc/openvpn/	Retrieves juicy information and sensitive directories
"-----BEGIN OpenVPN Static key V1-----" ext:key	Finds OpenVPN static keys
intitle:"index of" "vpn-config.*"	Retrieves juicy information about the vpn-config file
Index of / *.ovpn	Finds OpenVPN configuration files, some certificates, and keys
inurl:"/vpn/tmindex.html" vpn	Finds Netscaler and Citrix Gateway VPN login portals
intitle:"SSL VPN Service" + intext:"Your system administrator provided the following information to help understand and remedy the security conditions:"	Finds Cisco ASA login web pages

Other Techniques for Footprinting through Search Engines

Footprinting Technique	Description	Information Gathered	Tools Used
Google Advanced Search	Provides the same precision as that achieved with advanced operators but without typing or remembering the operators	List of sites that may link back to the target organization's website	Google Advanced Search
Advanced Image Search			Google Advance Image Search
Reverse Image Search	Uses an image as a search query	Original source and details of images, such as photographs, profile pictures, and memes	Google Image Search, TinEye Reverse Image Search, and Yahoo Image Search
Video Search Engines	Search for video content related to the target	Hidden information such as time/date and thumbnails	YouTube Metadata, YouTube DataViewer, and EZGif
Meta Search Engines	Use other search engines (Google, Bing, Ask.com, etc.) to produce their own results from the Internet	Detailed information about the target, such as images, videos, blogs, and news articles, from different sources	Startpage and MetaGer
FTP Search Engines	Search for files located on FTP servers	Critical files and directories that reveal valuable information, such as business strategy, tax documents, and employees' personal records	NAPALM FTP Indexer and FreewareWeb FTP File Search
IoT Search Engines	Crawl the Internet for IoT devices that are publicly accessible	Manufacturer details, geographical location, IP address, hostname, and open ports of IoT devices	Shodan, Censys, and Thingful

Footprinting through SHODAN Search Engine

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Pricing & | **VPS** | |  | **Login**

TOTAL RESULTS
204,560

[View Report](#) | [Browse Images](#) | [View on Map](#)

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

TOP COUNTRIES



Country	Count
Italy	190,040
Taiwan	4,700
Germany	2,300
United States	1,170
South Africa	842
More...	...

TOP PORTS

Port	Count
2000	191,807
8000	2,809
8001	1,700
8002	1,370
8003	617
More...	...

TOP ORGANIZATIONS

Organization	Count
WIND TRE ...	137,590
WIND Telec ...	10,307
Wind Telecoms ...	7,801

151.48.235.161 | 2024-03-07T09:47:20Z | 2024-03-07T09:47:20Z

User-Agent: curl/7.67.0 libcurl/7.67.0 OpenSSL/1.1.1f zlib/1.2.11 libssl/1.1.1f libcurl/openssl-darwin

Host: curl/7.67.0 libcurl/7.67.0 OpenSSL/1.1.1f zlib/1.2.11 libssl/1.1.1f libcurl/openssl-darwin

Content-Type: ...

151.21.16.67 | 2024-03-07T09:47:20Z | 2024-03-07T09:47:20Z

User-Agent: curl/7.67.0 libcurl/7.67.0 OpenSSL/1.1.1f zlib/1.2.11 libssl/1.1.1f libcurl/openssl-darwin

Host: curl/7.67.0 libcurl/7.67.0 OpenSSL/1.1.1f zlib/1.2.11 libssl/1.1.1f libcurl/openssl-darwin

Content-Type: ...

37.101.203.236 | 2024-03-07T09:47:20Z | 2024-03-07T09:47:20Z

User-Agent: curl/7.67.0 libcurl/7.67.0 OpenSSL/1.1.1f zlib/1.2.11 libssl/1.1.1f libcurl/openssl-darwin

Host: curl/7.67.0 libcurl/7.67.0 OpenSSL/1.1.1f zlib/1.2.11 libssl/1.1.1f libcurl/openssl-darwin

Content-Type: ...

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Pricing & | **VPS** | |  | **Login**

TOTAL RESULTS
2,761,685

[View Report](#) | [Browse Images](#) | [View on Map](#)

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

TOP COUNTRIES



Country	Count
Japan	523,724
China	420,963
United States	372,254
Australia	237,826
Germany	156,287
More...	...

TOP PORTS

Port	Count
500	2,626,109
4500	61,944
443	20,694
1723	9,825
80	7,271
More...	...

TOP ORGANIZATIONS

Organization	Count
Telstra	162,252
Open Com ...	100,346
Telstra Inter ...	91,936
98.101.58.99	98,101.58.99
100.101.100.100	100.101.100.100
100.101.100.101	100.101.100.101
100.101.100.102	100.101.100.102

218.41.232.62 | 2024-03-07T09:47:20Z | 2024-03-07T09:47:20Z

User-Agent: curl/7.67.0 libcurl/7.67.0 OpenSSL/1.1.1f zlib/1.2.11 libssl/1.1.1f libcurl/openssl-darwin

Host: curl/7.67.0 libcurl/7.67.0 OpenSSL/1.1.1f zlib/1.2.11 libssl/1.1.1f libcurl/openssl-darwin

Content-Type: ...

178.32.89.193 | 2024-03-07T09:47:20Z | 2024-03-07T09:47:20Z

User-Agent: curl/7.67.0 libcurl/7.67.0 OpenSSL/1.1.1f zlib/1.2.11 libssl/1.1.1f libcurl/openssl-darwin

Host: curl/7.67.0 libcurl/7.67.0 OpenSSL/1.1.1f zlib/1.2.11 libssl/1.1.1f libcurl/openssl-darwin

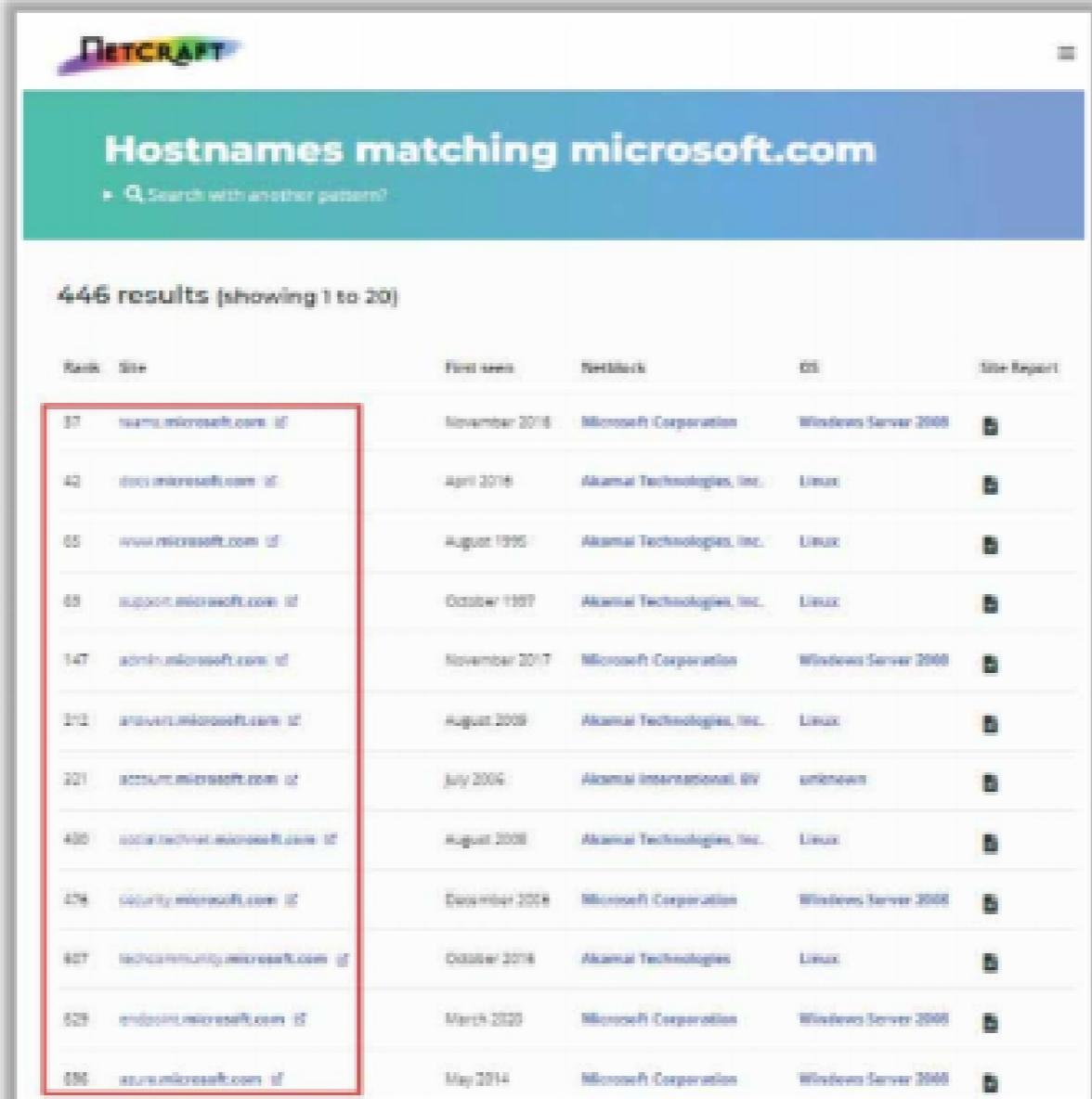
Content-Type: ...

<https://www.shodan.io>

LO#03: Demonstrate Footprinting through Internet Research Services

Finding a Company's Top-Level Domains (TLDs) and Sub-domains

- Search for the target company's external URL in a search engine, such as **Google** and **Bing**
- Sub-domains **provide an insight** into different departments and business units in an organization
- You may find a company's sub-domains by **trial and error method** or using a service such as <https://www.netcraft.com>
- You can use the **Sublist3r** python script, which enumerates subdomains across multiple sources at once



NETCRAFT

Hostnames matching microsoft.com

446 results (showing 1 to 20)

Rank	Site	Last seen	Network	OS	Site Report
37	name.microsoft.com	11/2018	Microsoft Corporation	Windows Server 2008	
42	docs.microsoft.com	4/2018	Akamai Technologies, Inc.	Linux	
65	www.microsoft.com	8/1995	Akamai Technologies, Inc.	Linux	
69	support.microsoft.com	10/1997	Akamai Technologies, Inc.	Linux	
147	admin.microsoft.com	11/2017	Microsoft Corporation	Windows Server 2008	
212	anonsupport.microsoft.com	8/2008	Akamai Technologies, Inc.	Linux	
221	account.microsoft.com	7/2006	Akamai International, BV	unknown	
400	socialtechnet.microsoft.com	8/2008	Akamai Technologies, Inc.	Linux	
479	security.microsoft.com	12/2018	Microsoft Corporation	Windows Server 2008	
507	techcommunity.microsoft.com	10/2018	Akamai Technologies	Linux	
629	endpoint.microsoft.com	3/2020	Microsoft Corporation	Windows Server 2008	
630	azure.microsoft.com	5/2014	Microsoft Corporation	Windows Server 2008	

<https://www.netcraft.com>



Parrot Terminal

```
[attacker@parrot:~/Sublist3r]
$ python sublist3r.py -d google.com
```

Sublist3r

Coded By Ahmed Aboul-Ela - @abou131a

```
[+] Enumerating subdomains now for google.com
[-] Searching now in Baidu...
[-] Searching now in Yahoo...
[-] Searching now in Google...
[-] Searching now in Bing...
[-] Searching now in Ask...
[-] Searching now in Netcraft...
[-] Searching now in DNSdumpster...
[-] Searching now in VirusTotal...
[-] Searching now in ThreatCrowd...
[-] Searching now in SSL Certificates...
[-] Searching now in PassiveDNS...
[!] Error: VirusTotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 37962
www.google.com
1.google.com
alt1.google.com
alt.aspx.1.google.com
client.1.google.com
clients.1.google.com
gmail-smtp-inbound.1.google.com
disc-anycast.1.google.com
167.179.108.180.google.com
109-cache-blicnet.google.com
101-cache-blicnet.google.com
102-cache-blicnet.google.com
34.14.238.183.google.com
96.68.68.183.google.com
5.61.68.183.google.com
```

<https://github.com>

Finding a Company's Top-Level Domains (TLDs) and Sub-domains with AI

 SAAC
SOUTHERN AFRICAN ACADEMY OF COUNSELLING

An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using appropriate prompts such as

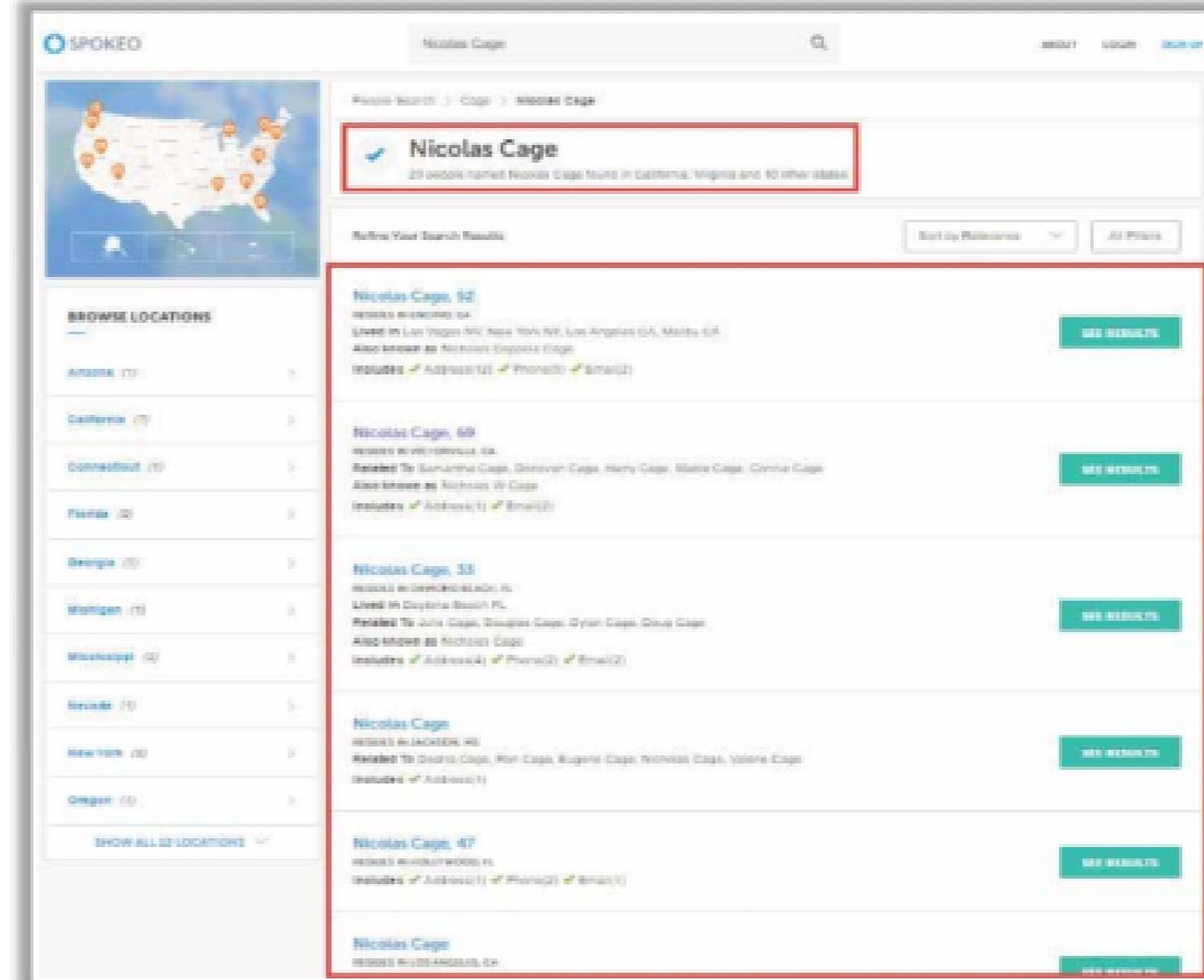
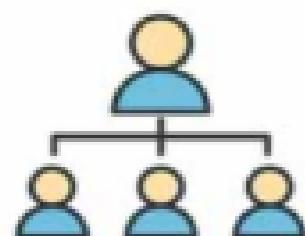
1. "Discover all the subdomains of 'google.com' using dig command"
 2. "Use Sublist3r to gather a list of subdomains of the target organization eccouncil"

```
sgpt --chat footprint --shell "Use Sublist3r to gather a list of subdomains of the target organization e"
File Edit View Search Terminal Help
[root@parrot] ~ [~]
[root@parrot] ~ [~]
#sgpt --chat footprint --shell "Use Sublist3r to gather a list of
subdomains of the target organization e
council"
sublist3r -d e
council.org -o e
council_subdomains.txt
[E]xecute, [D]escribe, [A]bort: E
```

```
green -> development, about how to make it go faster in a lot of different areas of the  
Web, like New, Recent, Trending, etc.  
  advertising, advertisement, account12.org  
  website, account12.org  
  new, advertisement, account12.org  
  search, advertisement, account12.org  
  user, account12.org  
  user, account12.org  
  affiliate, account12.org  
  advertiser, account12.org  
  organization, organization, account12.org  
  open, account12.org  
  open, open, account12.org  
  site, about12.org, strategies, account12.org  
  post12linksharing, account12.org  
  blog, account12.org  
  blogpost, account12.org  
  campaign, account12.org  
  campaign, account12.org  
  copyright, copyright, account12.org  
  publications, account12.org  
  user, account12.org  
  user, user, account12.org  
  writing, account12.org  
  checklist, account12.org  
  checklist, profile, account12.org
```

People Search on Social Networking Sites and People Search Services

- Social networking services, such as Facebook, Twitter, and LinkedIn, provide **useful information about the individual** that helps the attacker in performing social engineering and other attacks
- The people search can provide critical **information about a person or an organization**, including location, emails, websites, blogs, contacts, important dates, etc.
- People search online services, such as **Spokeo, Intelius, pipl, BeenVerified, Whitepages, and PeekYou**, provide people's names, addresses, contact details, date of birth, photographs, videos, profession, and so on



The screenshot shows the Spokeo search interface for the query "Nicolas Cage". The top navigation bar includes "People Search", "Cage", "Nicolas Cage", a search icon, and "SEARCH". Below the navigation is a map of the United States with orange dots representing search results across various states. A sidebar on the left lists "BROWSE LOCATIONS" for states like Arizona, California, Connecticut, Florida, Georgia, Michigan, Mississippi, Nevada, New York, and Oregon, each with a count of results (e.g., 111 for Arizona). The main search results are displayed in a grid. The first result is highlighted with a red border and labeled "Nicolas Cage" with a checkmark, indicating 23 results found in California, Virginia, and 10 other states. Other results include "Nicolas Cage, 52", "Nicolas Cage, 69", "Nicolas Cage, 53", "Nicolas Cage", "Nicolas Cage, 47", and "Nicolas Cage". Each result card provides basic information like name, location, and aliases, along with a "SEE RESULTS" button.

Gathering Information from LinkedIn

- Attackers use **theHarvester** tool to perform enumeration on LinkedIn and find employees of the target company along with their job titles
- Attackers can use this information to gather more information, such as **current location and educational qualifications**, and perform social engineering or other kinds of attacks

```
Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot] ~
$theHarvester -d microsoft -l 200 -b linkedin
=====
* [!] Target: microsoft
* [!] Searching 100 results.

Attackers search on LinkedIn
to obtain employee details
```

```
Parrot Terminal
File Edit View Search Terminal Help
[*] LinkedIn Users found: 106
-----
Ahmed Zayed
Akosua Boadi-Agyemang
Alex Simons
Amit Fulay
Andrey Cavalcanti - General Manager
Andrey Proskurin - Corporate Vice President of Engineering
Anthony Chu - Senior Program Manager
Betty Rhiger - Chief Technology Officer
Brooke Mikalachki - Business Applications Sales Executive
Charles Lamanna - Corporate Vice President
Charlie Bell
Chelsea Lee - Microsoft Technical Trainer
Cheri Chevalier
Chris Pratley - Corporate Vice President
Christine Guyot - Director Corporate Affairs
Cindy Davison - National Azure Director
Dan Kelcey - Datacenter Technician
David Beauchemin
David Kozera - Microsoft 365 for Education Country Lead
David Peterson
```

Obtains information about target employee name, job title, etc.

Harvesting Email Lists

- Gathering email addresses related to the target organization acts as an **important attack vector during the later phases of hacking**
- Attackers use automated tools such as **theHarvester** and **Email Spider** to collect publicly available email addresses of the target organization that helps them perform social engineering and brute-force attacks

Parrot Terminal

```
File Edit View Search Terminal Help
└─ $theHarvester -d microsoft.com -l 200 -b baidu
=====
* [!] Target: microsoft.com
* [!] Searching Baidu.
```

Parrot Terminal

```
File Edit View Search Terminal Help
[*] Searching Baidu.

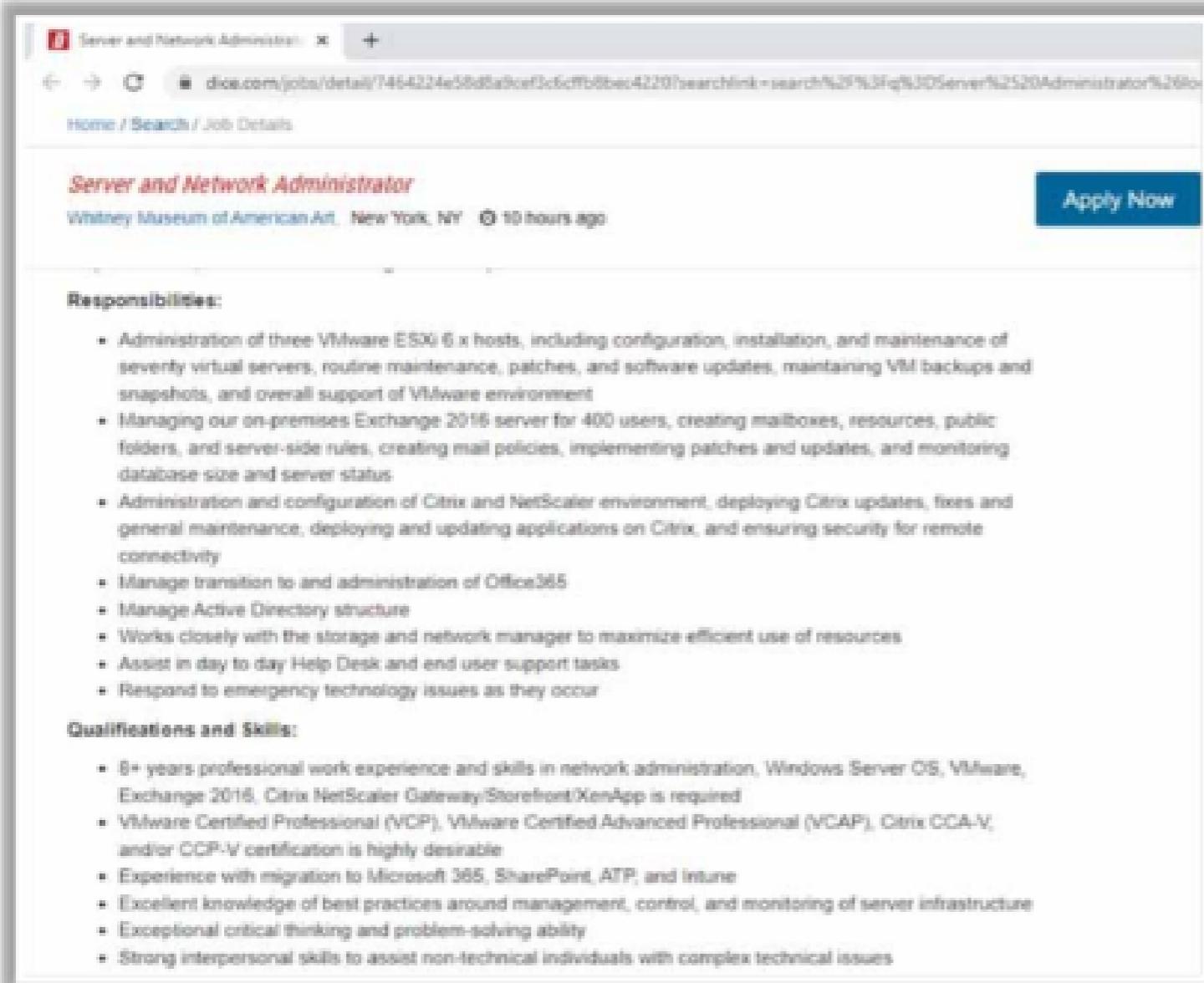
[*] No IPs found.

[*] Emails found: 1
-----
gloriac@microsoft.com

[*] Hosts found: 5
-----
apps.dev.microsoft.com:40.126.29.20, 40.126.29.21, 40.126.29.0, 40.126.2
0.2, 40.126.29.22, 40.126.29.23, 40.126.29.1
redeem.microsoft.com:23.219.127.195
signup.microsoft.com:13.107.246.41, 13.107.213.41
support.microsoft.com:23.193.120.116
www.microsoft.com:23.46.201.6
[attacker@parrot]-(~)
```

Footprinting through Job Sites

company's infrastructure details can be gathered from job postings



The screenshot shows a job listing for a "Server and Network Administrator" position at the Whitney Museum of American Art in New York. The listing includes:

- Responsibilities:**
 - Administration of three VMware ESXi 6.x hosts, including configuration, installation, and maintenance of seventy virtual servers, routine maintenance, patches, and software updates, maintaining VM backups and snapshots, and overall support of VMware environment.
 - Managing our on-premises Exchange 2016 server for 400 users, creating mailboxes, resources, public folders, and server-side rules, creating mail policies, implementing patches and updates, and monitoring database size and server status.
 - Administration and configuration of Citrix and NetScaler environment, deploying Citrix updates, fixes and general maintenance, deploying and updating applications on Citrix, and ensuring security for remote connectivity.
 - Manage transition to and administration of Office365.
 - Manage Active Directory structure.
 - Works closely with the storage and network manager to maximize efficient use of resources.
 - Assist in day to day Help Desk and end user support tasks.
 - Respond to emergency technology issues as they occur.
- Qualifications and Skills:**
 - 8+ years professional work experience and skills in network administration, Windows Server OS, VMware, Exchange 2016, Citrix NetScaler Gateway/Shorefront/XenApp is required
 - VMware Certified Professional (VCP), VMware Certified Advanced Professional (VCAP), Citrix CCA-V, and/or CCP-V certification is highly desirable
 - Experience with migration to Microsoft 365, SharePoint, ATP, and Intune
 - Excellent knowledge of best practices around management, control, and monitoring of server infrastructure
 - Exceptional critical thinking and problem-solving ability
 - Strong interpersonal skills to assist non-technical individuals with complex technical issues

Look for these:

- Job requirements
- Employees' profiles
- Hardware information
- Software information

- Attackers use the technical information obtained through job sites, such as Dice, LinkedIn, and Simply Hired, to **detect underlying vulnerabilities in the target IT infrastructure**



Deep and Dark Web Footprinting

Deep web

- It consists of web pages and contents that are **hidden and unindexed** and cannot be located using traditional web browsers and search engines
- It can be accessed by **search engines** like Tor Browser and The WWW Virtual Library

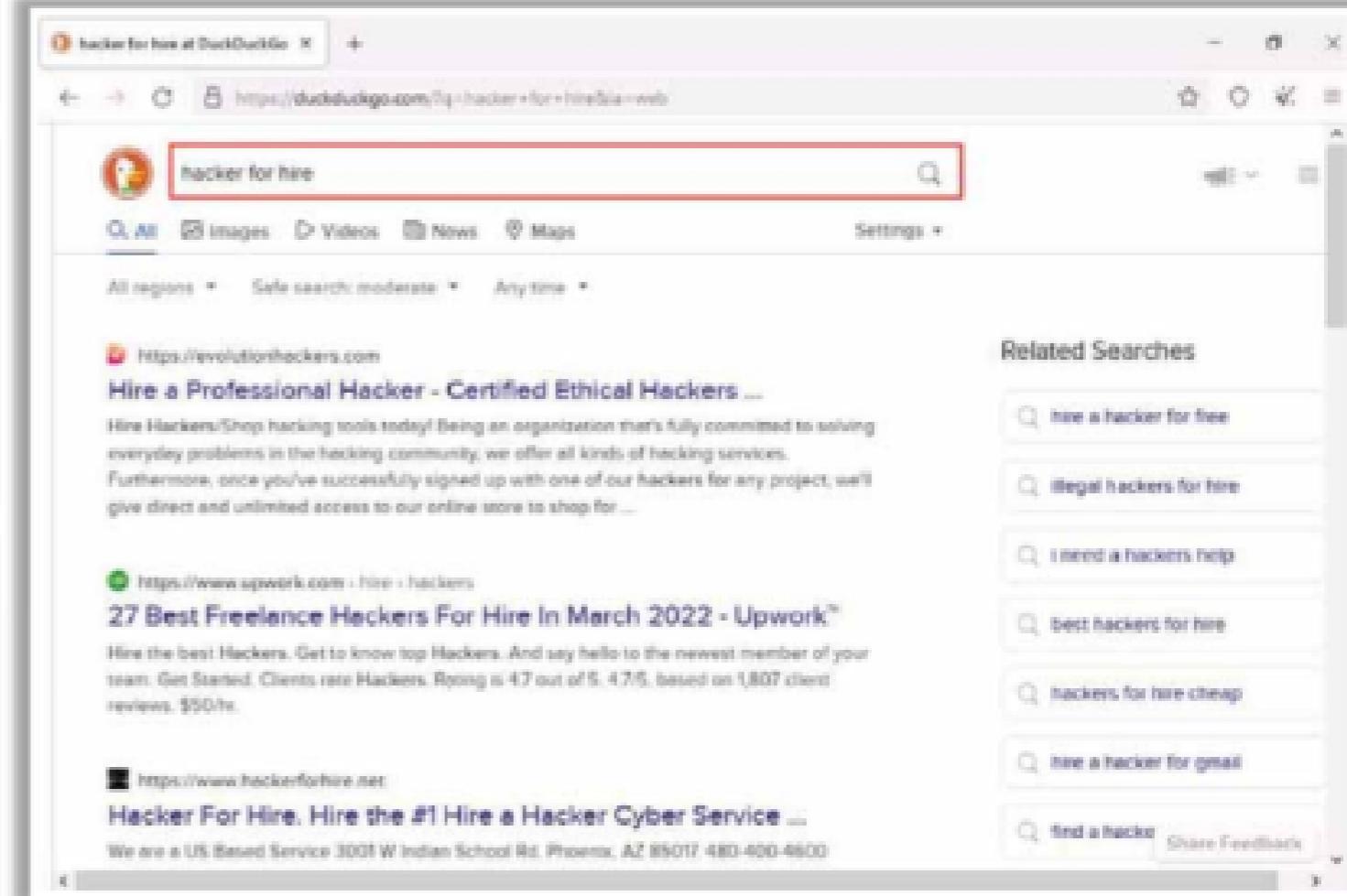
Dark web or Darknet

- It is the subset of the deep web that enables anyone to **navigate anonymously** without being traced
- It can be accessed by **browsers**, such as TOR Browser, Freenet, GNUnet, I2P, and Retroshare

- Attackers use deep and dark web searching tools, such as **Tor Browser** and **ExoneraTor**, to **gather confidential information about the target**, including credit card details, passport information, identification card details, medical records, social media accounts, Social Security Numbers (SSNs), etc.

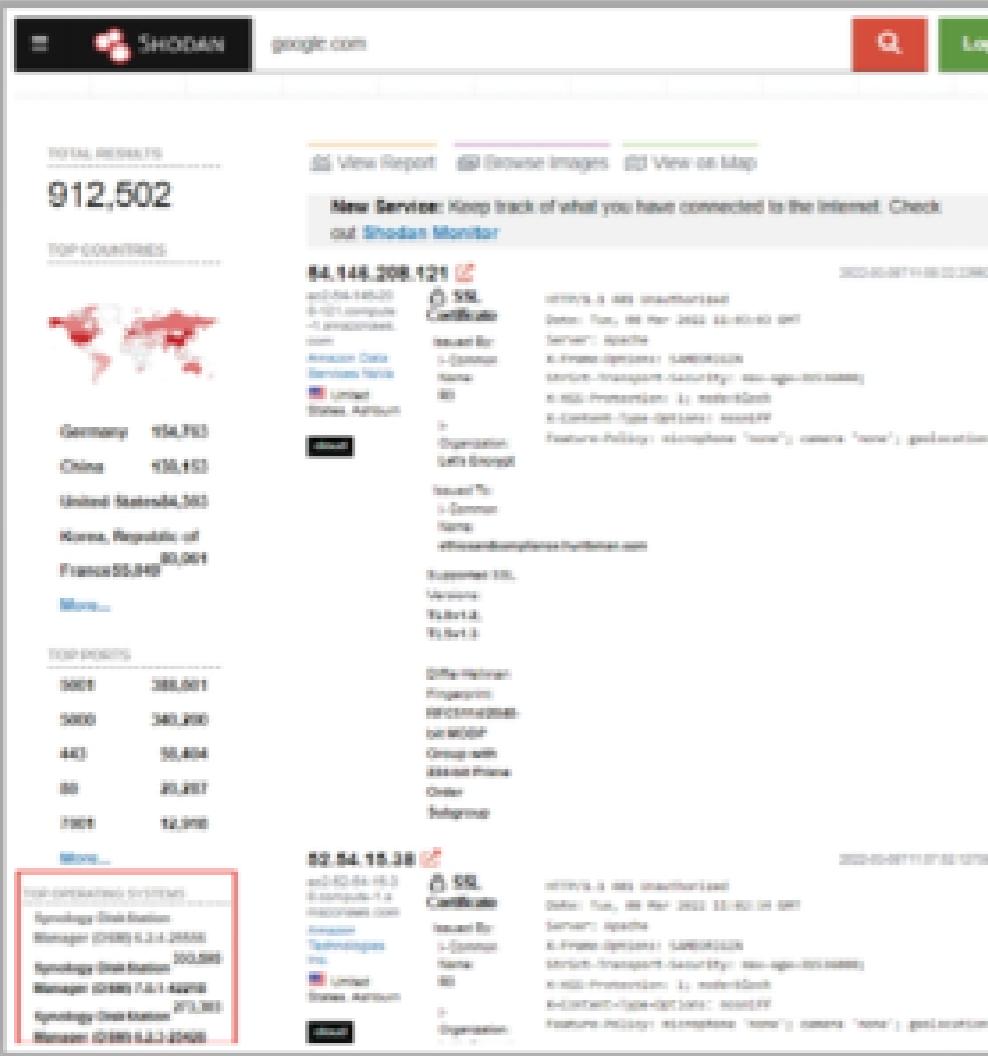
TOR Browser

It is used to access the deep and dark web where it acts as a **default VPN** for the user and bounces the network IP address through several servers before interacting with the web



Determining the Operating System

- SHODAN search engine lets you **find connected devices** (routers, servers, IoT, etc.) using a variety of filters

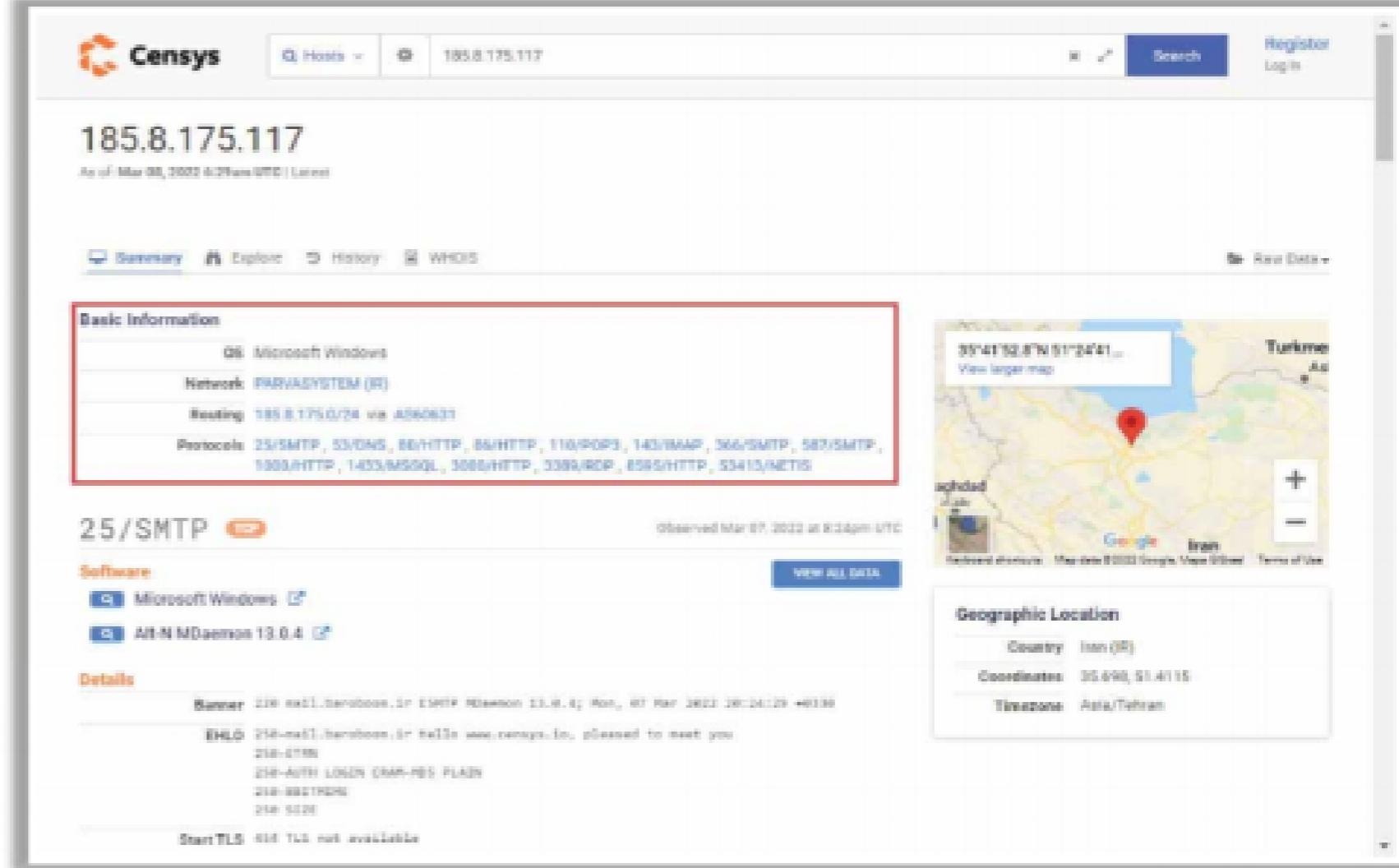


The screenshot shows the SHODAN search interface. At the top, there's a search bar with 'google.com' and a search button. Below the search bar, it says 'TOTAL: 912,502' and 'TOP COUNTRIES'. A world map shows red dots representing found devices. On the left, there's a sidebar with 'TOP SERVICES' and a table of services with their counts. The main area displays two device entries:

- 94.146.208.121**: An Apache server with SSL/TLS certificate information.
- 82.84.15.38**: An Apache server with SSL/TLS certificate information.

<https://www.shodan.io>

- Censys search engine provides a full view of every **server and device exposed** to the Internet



The screenshot shows the Censys search results for the IP address 185.8.175.117. The interface includes a search bar with '185.8.175.117', a 'Search' button, and 'Register Login' links. The main content area has tabs for 'Summary', 'Explore', 'History', and 'WHOIS'. The 'Summary' tab is active, showing basic information about the device:

- OS:** Microsoft Windows
- Network:** PARAVSYSTEM (B)
- Routing:** 185.8.175.0/24 via AF40631
- Protocols:** 25/SMTP, 53/DNS, 80/HTTP, 80/HTTPS, 110/POP3, 143/IMAP, 368/SMTP, 587/SMTP, 993/HTTP, 1433/MSSQL, 3389/RDP, 5555/HTTP, 55413/NETS

A red box highlights this information. To the right, there's a map showing the location in Turkey, with coordinates 39°41'52.8"N 31°24'41"E. Below the map, there's a 'Geographic Location' section with 'Country: Iran (B)', 'Coordinates: 35.490, 51.415', and 'Timezone: Asia/Tehran'. The 'Details' section shows a banner and ECHO responses.

<https://censys.io>

VoIP and VPN Footprinting through SHODAN

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN Explore Pricing of **VoIP** Q

TOTAL RESULTS
257,685

TOP COUNTRIES



Country	Count
Italy	245,224
Germany	3,829
Taiwan	2,110
United States	939
France	639
More...	

TOP PORTS

Port	Count
5000	206,623
592	2,766
5800	1,965
80	898
1800	858
More...	

TOP ORGANIZATIONS

Organization	Count
WIND TEL S.P.A.	132,624
WIND Telecommunications S.r.l.	76,723

View Report **View on Map**

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monit](#)

181.41.130.64

HTTP/1.1 404 Not Found
From: <alpinetech> To: <alpinetech>
Subject: <alpinetech>
Date: Sun, 25 Jul 2010 08:22:00 +0200
Content-Type: text/html
Content-Length: 100
User-Agent: DLink VoIP Stack
Supported: replace, timer, MTRR
Via: SIP/2.0/UDP my.receiver-220.127.106.30:port=20810;branch=from-ua
Content-Id: ...

181.34.253.246

HTTP/1.1 404 Not Found
From: <alpinetech> To: <alpinetech>
Subject: <alpinetech>
Date: Sun, 25 Jul 2010 08:22:00 +0200
Content-Type: text/html
Content-Length: 100
User-Agent: DLink VoIP Stack
Supported: replace, timer, MTRR
Via: SIP/2.0/UDP my.receiver-220.127.106.30:port=20810;branch=from-ua
Content-Id: ...

151.54.247.153

HTTP/1.1 404 Not Found
From: <alpinetech> To: <alpinetech>
Subject: <alpinetech>
Date: Sun, 25 Jul 2010 08:22:00 +0200
Content-Type: text/html
Content-Length: 100
User-Agent: DLink VoIP Stack
Supported: replace, timer, MTRR
Via: SIP/2.0/UDP my.receiver-220.127.106.30:port=20810;branch=from-ua
Content-Id: ...

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN Explore Pricing of **VPN** Q

TOTAL RESULTS
5,012,000

TOP COUNTRIES



Country	Count
United States	894,772
Japan	723,749
China	527,385
Australia	218,579
Germany	219,154
More...	

TOP PORTS

Port	Count
5000	3,211,173
139	315,958
4800	94,998
443	26,917
80	16,898
More...	

TOP ORGANIZATIONS

Organization	Count
Amazon Technologies Inc.	674,562
Open Computer Network	647,377
CHINAETT HENAN PROVINCIAL NETWORK	123,52,110,243

View Report **Browse Images** **View on Map**

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monit](#)

82.74.240.166

VPN (IKE SA/T1)
Initiator SPI: 3200000000000000
Responder SPI: 0000000000000000
Next Payload: Notification (0)
Version: 1.0
Exchange Type: Informational
Flags:
Encryption: False
Content: False
Authentication: False
Message ID: Reference
Length: 48

78.94.215.218

VPN (IKE)
Initiator SPI: 0000000000000000
Responder SPI: 0000000000000000
Next Payload: RESERVED
Version: 2.0
Exchange Type: IKE Specific User
Flags:
Encryption: False
Content: False
Authentication: False
Message ID: 00000000
Length: 20

<https://www.shodan.io>

Competitive Intelligence Gathering

- Competitive intelligence gathering is the process of **identifying, gathering, analyzing, verifying**, and using information about your competitors from resources, such as the Internet
- Competitive intelligence is **non-interfering** and **subtle in nature**



Sources of Competitive Intelligence

- | | |
|---|---|
| <p>1 Company websites and employment ads</p> <p>2 Search engines, Internet, and online database</p> <p>3 Press releases and annual reports</p> <p>4 Trade journals, conferences, and newspapers</p> <p>5 Patent and trademarks</p> | <p>6 Social engineering employees</p> <p>7 Product catalogs and retail outlets</p> <p>8 Analyst and regulatory reports</p> <p>9 Customer and vendor interviews</p> <p>10 Agents, distributors, and suppliers</p> |
|---|---|

Competitive Intelligence Gathering...

When Did this Company Begin? How Did it Develop?

Information Resource Sites

- EDGAR Database
<https://www.sec.gov/edgar.shtml>
- D & B Hoovers
<https://www.dnb.com>
- LexisNexis
<https://www.lexisnexis.com>
- Business Wire
<http://www.businesswire.com>

What Are the Company's Plans?

Information Resource Sites

- MarketWatch
<https://www.marketwatch.com>
- The Wall Street Transcript
<https://www.twst.com>
- Euromonitor
<https://www.euromonitor.com>
- Experian
<https://www.experian.com>

What Expert Opinions Say About the Company?

Information Resource Sites

- SEMRush
<https://www.semrush.com>
- ABI/INFORM Global
<https://www.proquest.com>
- SimilarWeb
<https://www.similarweb.com>
- SERanking
<https://seranking.com>

Other Techniques for Footprinting through Web Services

Footprinting Technique	Description	Information Gathered	Tools Used
Finding the Geographical Location of the Target	Obtain the physical location of the target	Entrances to buildings, security cameras, gates, places to hide, weak spots in perimeter fences, etc.	Google Earth, Google Maps, and Wikimapia
Gathering Information from Financial Services	Search for financial data such as stock quotes and charts, financial news, and portfolios	Market value of a company's shares, company profile, and competitor details	Google Finance, MSN Money, and Yahoo! Finance
Gathering Information from Business Profile Sites	Retrieve business information of companies located in a particular region	Location, addresses, contact information, and employee database of the target organization	opencorporates, Crunchbase, and corporationwiki
Monitoring Targets Using Alerts	Obtain up-to-date information of the target, usually via email or SMS	Mentions of the organization's name, member names, website, or any of its people or projects	Google Alerts, Twitter Alerts, and Giga Alerts
Tracking the Online Reputation of the Target	Monitor a company's reputation on the Internet	Search engine ranking information, email notifications when a company is mentioned online, and social news about the company	Mention, ReviewPush, and Reputology
Gathering Information from Groups, Forums, and Blogs	Join the target organization's employee groups, where they share personal and company information	Public network information, system information, and personal information	Google Groups and Yahoo! Groups
Gathering Information from NNTP Usenet Newsgroups	Retrieve messages on various subjects and topics that are submitted by users over the Internet	Operating systems, software, web servers, etc. used by the target organization	Newshosting, Eweka, and Supernews
Gathering Information from Public Source-Code Repositories	Identify information about the developers and technologies used	Configuration files, private SSH and SSL keys, source-code files, dynamic libraries, and software tools developed by contributors	Recon-ng

LO#04: Demonstrate Footprinting through Social Networking Sites

Collecting Information through Social Engineering on Social Networking Sites

- Attackers use **social engineering tricks** to gather sensitive information from social networking websites
- Attackers create a **fake profile** and then use the false identity to lure employees into revealing their sensitive information
- Attackers collect information about the employees' **interests** and tricks them into revealing more information

What Users Do	What Attacker Gets	What Organizations Do	What Attacker Gets
Maintain profile	Contact info, location, etc.	User surveys	Business strategies
Connect to friends, chat	Friends list, friends' info, etc.	Promote products	Product profile
Share photos and videos	Identity of family members, interests, etc.	User support	Social engineering
Play games, join groups	Interests	Recruitment	Platform/technology
Create events	Activities	Background check to hire employees	Type of business

General Resources for Locating Information from Social Media Sites

- Attackers track social media sites using BuzzSumo, Google Trend, Hashatit, etc. to **discover most shared content** using hashtags or keywords, track accounts and URLs, email addresses, etc.

- Attackers use this information to perform **phishing, social engineering**, and other types of attacks

BuzzSumo

BuzzSumo's advanced social search engine **finds the most shared content** for a topic, author or a domain

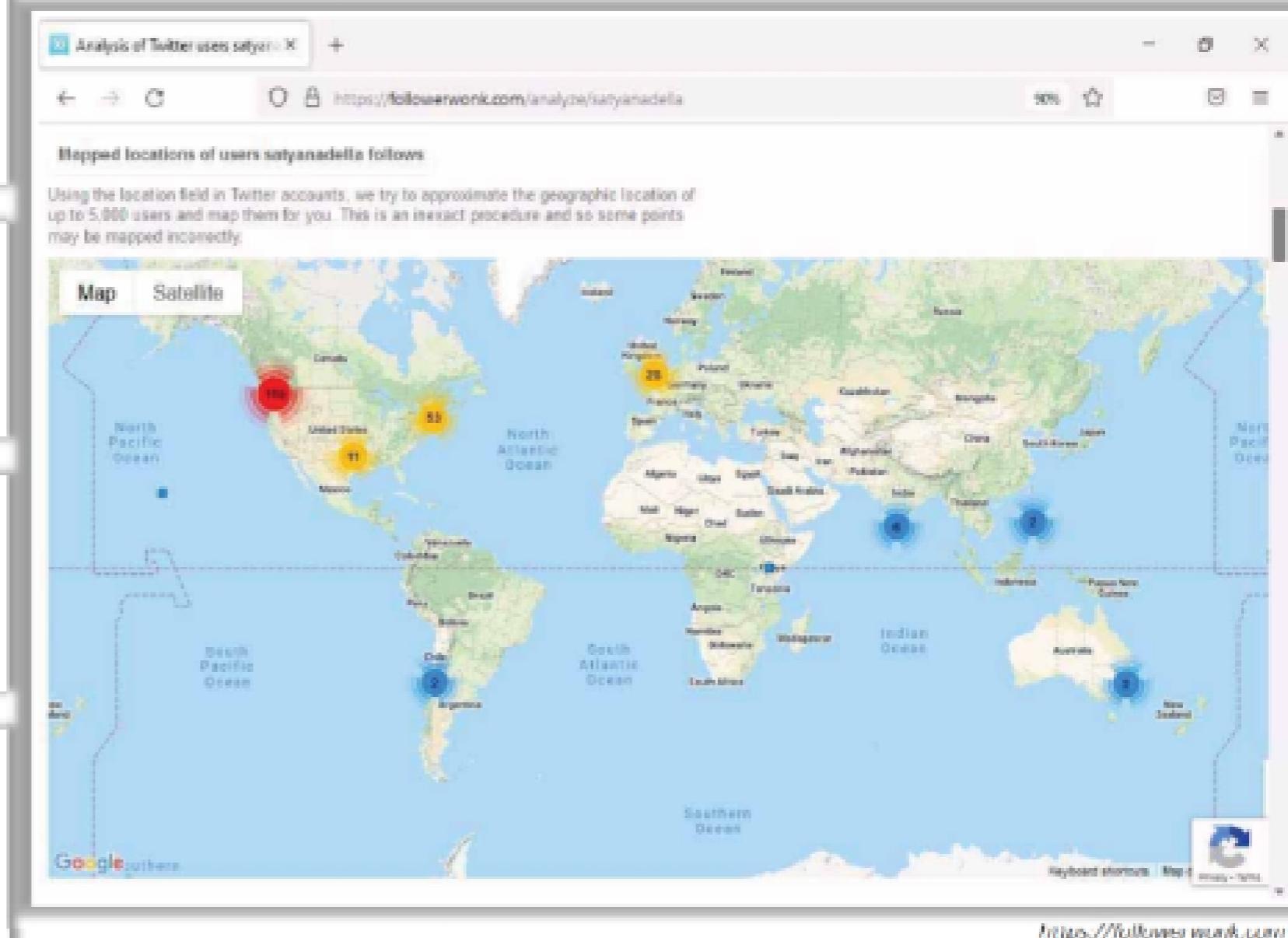
The screenshot shows the BuzzSumo Content Analyzer interface. At the top, there's a navigation bar with tabs for Home, Discover, Content, Influencers, Monitoring & Alerts, and Projects. The Content tab is selected, and the sub-tab 'Content Analyzer' is also selected. Below the navigation is a search bar with the query 'www.microsoft.com'. To the right of the search bar are buttons for 'SAVE SEARCH' and 'CREATE ALERT'. Underneath the search bar, there's a note about using the OR operator for more relevant results. Below this, there's a section for filtering results by date, location, language, and publisher. The main content area displays a list of three articles from Microsoft, each with engagement metrics represented by colored circles. The first article is 'Download SwiftKey Smart Keyboard and be more productive | SwiftKey' by Microsoft SwiftKey, posted on Feb 18, 2023. The second is 'One-to-One Devices and Learning | A Step-by-step guide' by microsoft.com, posted on Feb 12, 2023. The third is 'Microsoft Whitepaper - Guide for universities: How digitization can enable more sustainability' by microsoft.com, posted on Feb 23, 2023. The columns for engagement metrics include Facebook Engagement, Twitter Shares, Pinterest Shares, Reddit Engagements, Number of Links, Engagement Score, and Total Engagement. The 'Total Engagement' column is highlighted with a red border. At the bottom right of the interface is a blue 'EXPORT' button.

Conducting Location Search on Social Media Sites

- Conducting location search on social media sites, such as Twitter, Instagram, and Facebook, helps attackers in **detecting the geolocation of the target**
- Attackers use online tools, such as **Followerwonk**, **Hootsuite**, and **Meltwater**, to search for both geotagged and non-geotagged information about the target on social media sites
- Attackers use this information to perform various **social engineering and non-technical attacks**

Followerwonk

Followerwonk helps to explore and grow one's social graph by digging deeper into Twitter analytics

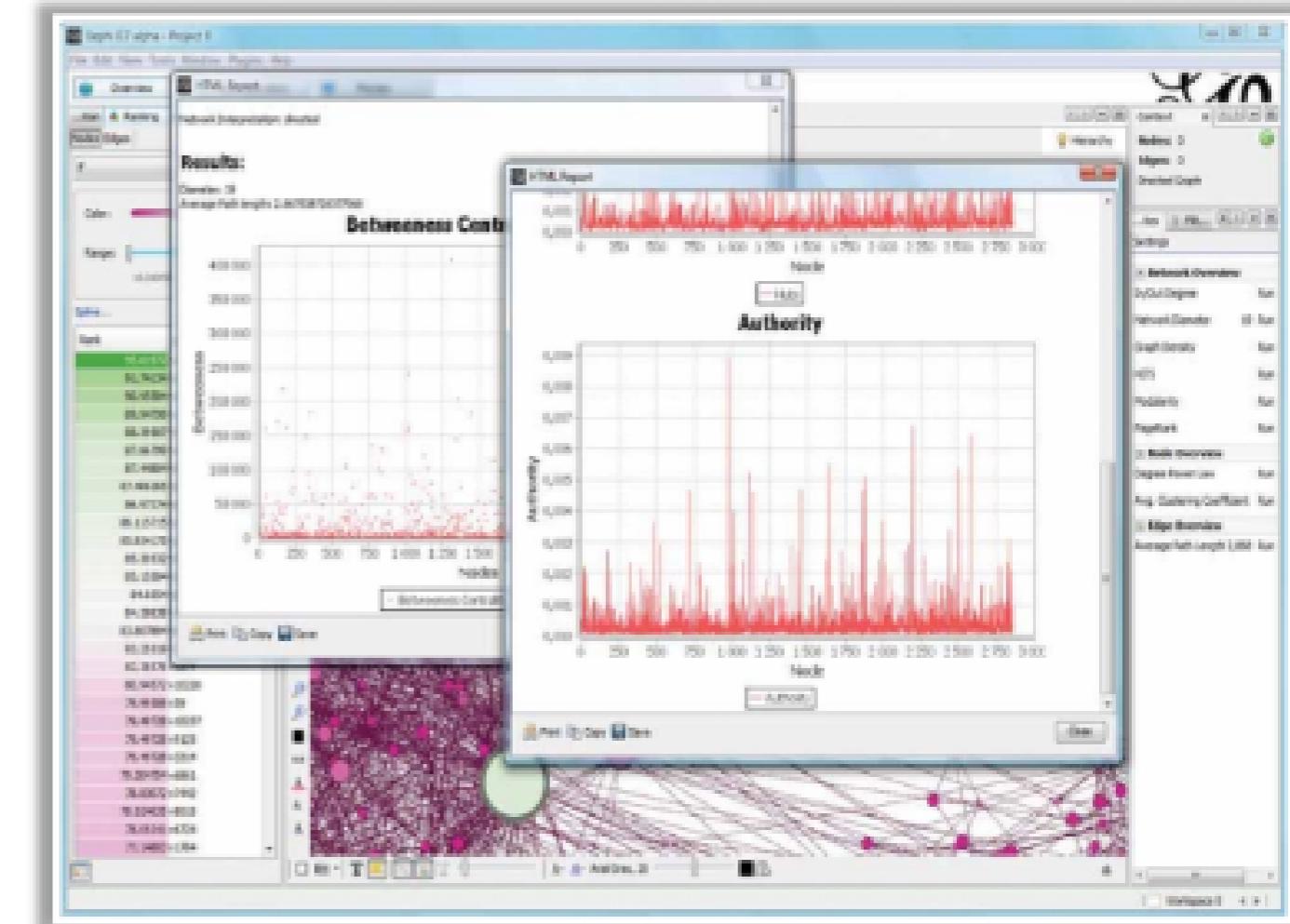


Constructing and Analyzing Social Network Graphs

- The construction of social network graphs involves representing various **connections** and **relationships between people** in the form of graphs to analyze and extract valuable information from various social networking connections

- Using graphical analysis, attackers can identify how a **group of users** communicate, what **information they share**, and their personal and professional interests

- Attackers use tools such as **Gephi**, **SocNetV**, and **NodeXL** to construct and analyze social networks and obtain critical information about the target organization/users



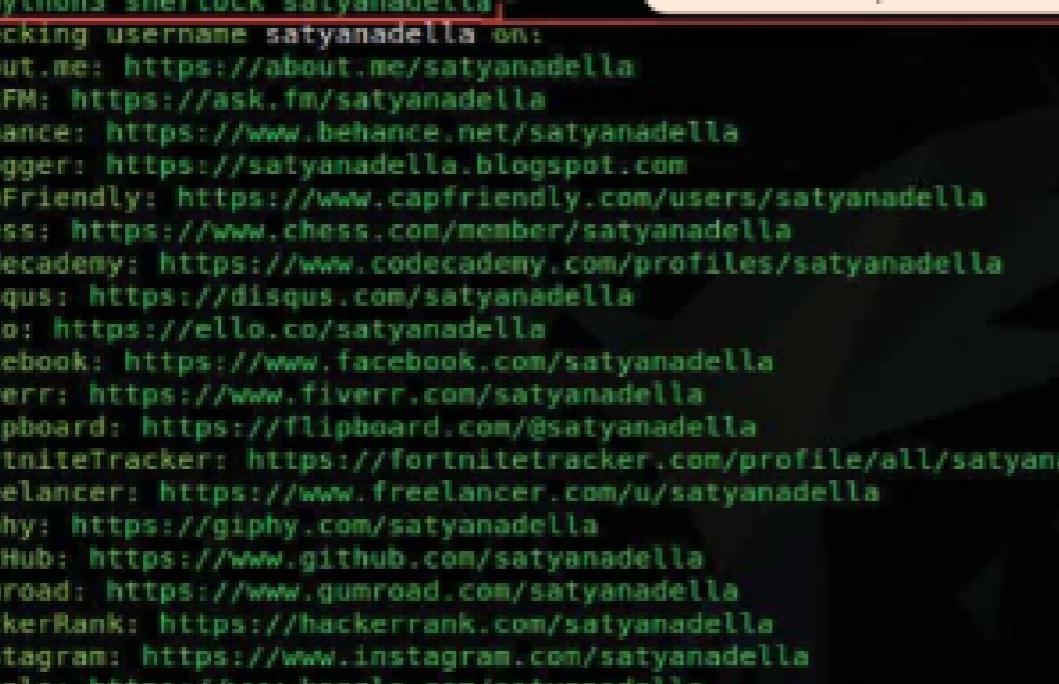
<https://gephi.org>



Tools for Footprinting through Social Networking Sites

Sherlock

Sherlock tool is used to **search a vast number of social networking sites** for a target username

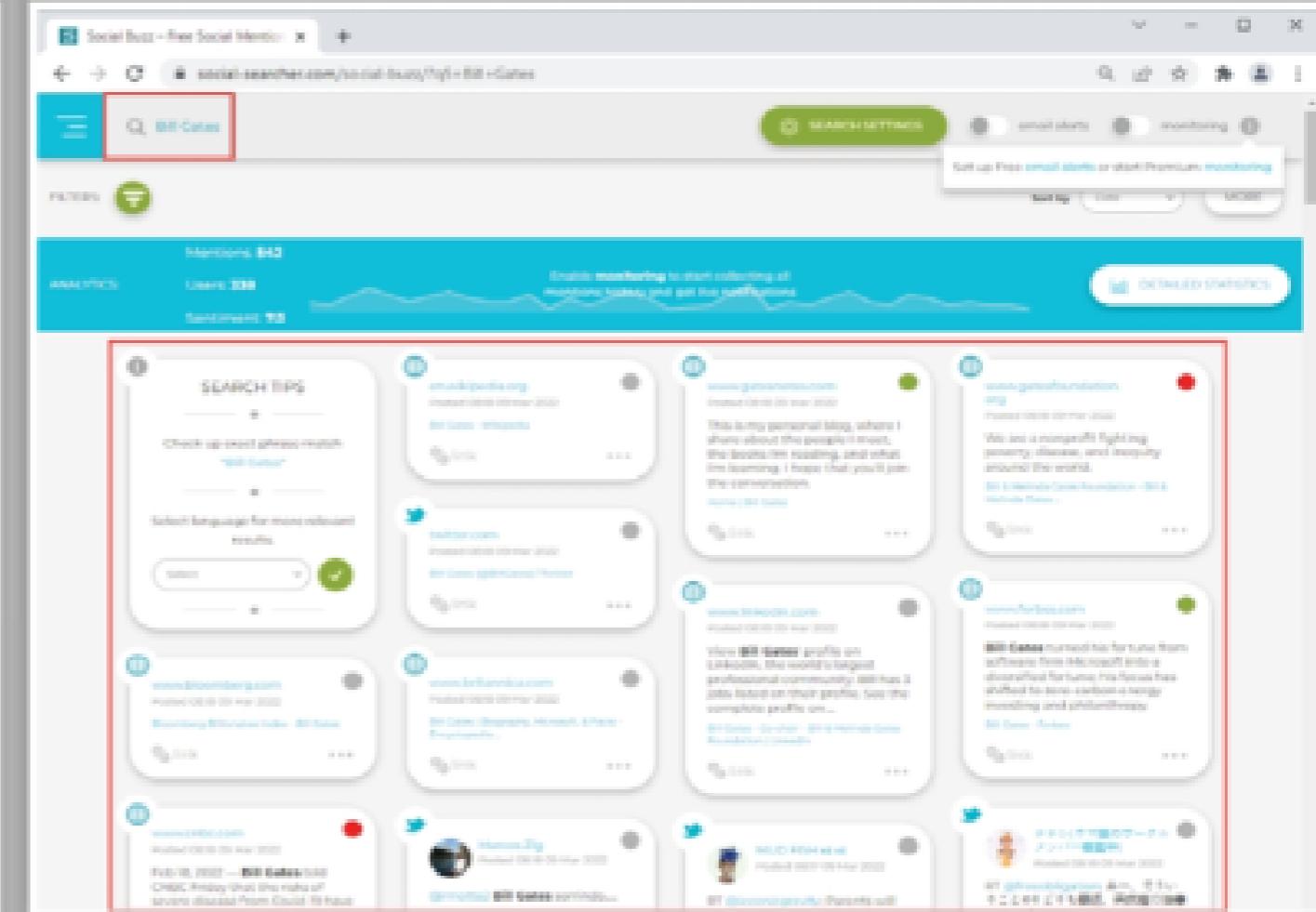


File Edit View Search Terminal Help

```
[*] [root@parrot] [-/sherlock]
[*] #python3 sherlock satyanadella
[*] Checking username satyanadella on:
[*] About.me: https://about.me/satyanadella
[*] AskFM: https://ask.fm/satyanadella
[*] Behance: https://www.behance.net/satyanadella
[*] Blogger: https://satyanadella.blogspot.com
[*] CapFriendly: https://www.capfriendly.com/users/satyanadella
[*] Chess: https://www.chess.com/member/satyanadella
[*] Codecademy: https://www.codecademy.com/profiles/satyanadella
[*] Disqus: https://disqus.com/satyanadella
[*] Ello: https://ello.co/satyanadella
[*] Facebook: https://www.facebook.com/satyanadella
[*] Fiverr: https://www.fiverr.com/satyanadella
[*] Flipboard: https://flipboard.com/@satyanadella
[*] FortniteTracker: https://fortnitetracker.com/profile/all/satyanadella
[*] Freelancer: https://www.freelancer.com/u/satyanadella
[*] Giphy: https://giphy.com/satyanadella
[*] GitHub: https://www.github.com/satyanadella
[*] Gumroad: https://www.gumroad.com/satyanadella
[*] HackerRank: https://hackerrank.com/satyanadella
[*] Instagram: https://www.instagram.com/satyanadella
[*] Kaggle: https://www.kaggle.com/satyanadella
[*] LeetCode: https://leetcode.com/satyanadella
[*] Lichess: https://lichess.org/@/satyanadella
[*] Lolchess: https://lolchess.qq/profile/na/satyanadella
```

Social Searcher

Social Searcher allows you to **search for content** in social networks in real-time and provides deep analytics data



LO#05: Use Different Techniques for Website Footprinting

Website Footprinting

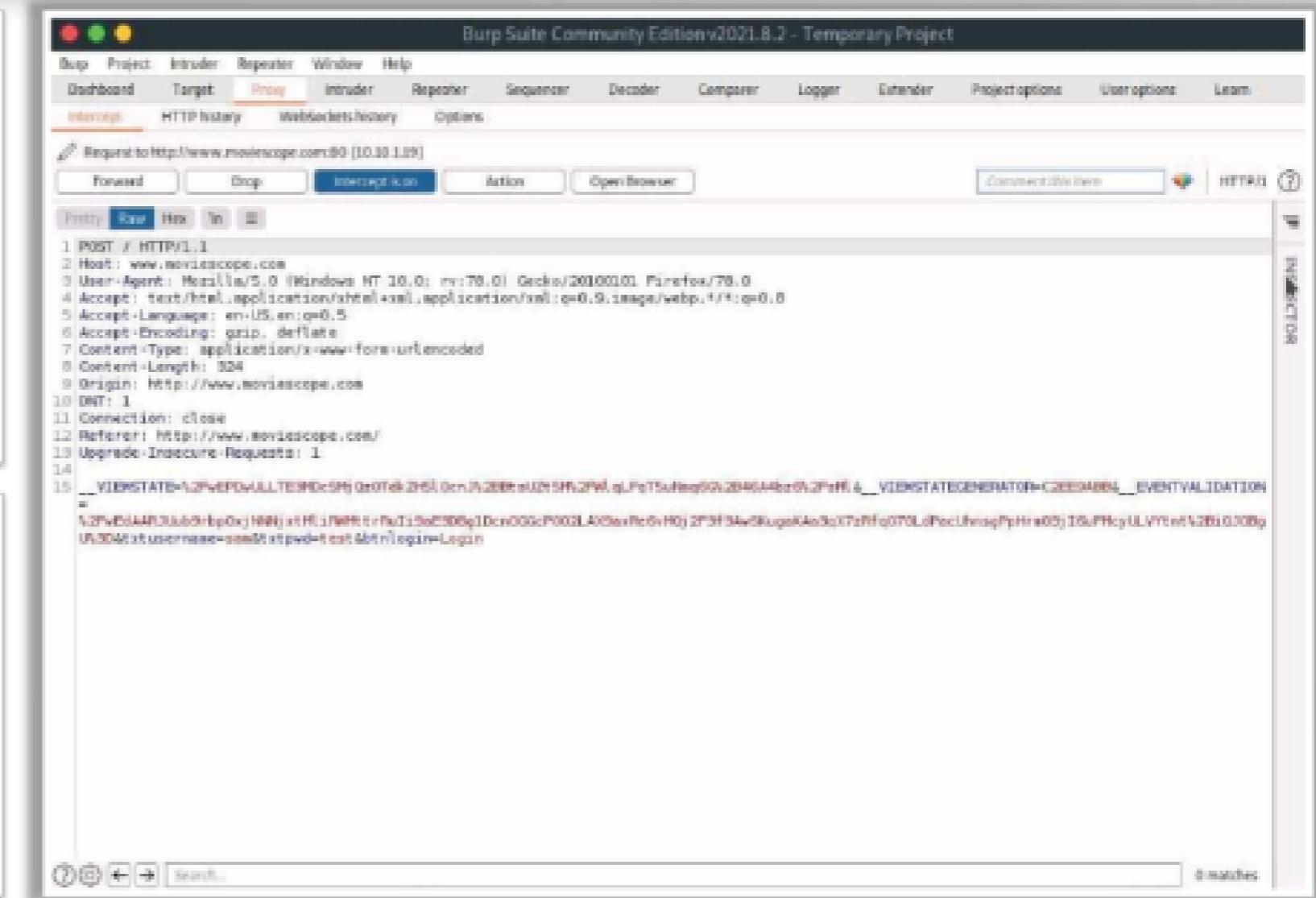
- Website footprinting refers to the **monitoring and analysis of the target organization's website** for information

Browsing the target website may provide the following information:

- Software used and its version
- Operating system used and its scripting platform
- Sub-directories and parameters
- Filename, path, database field name, or query
- Technologies used
- Contact and CMS details

Attackers use **Burp Suite**, **Zaproxy**, **Wappalyzer**, **CentralOps**, **Website Informer**, etc. to view headers that provide the following information:

- Connection status and content-type
- Accept-Ranges and Last-Modified
- X-Powered-By information
- Web server in use and its version



Website Footprinting

Examining the HTML source code may provide

- Comments present in the source code
 - Contact details of the web developer or admin
 - File system structure and script type

```
1<!DOCTYPE html>
2<html lang="en-in" dir="ltr">
3  <head data-info="(quot;)quot;1.0.0000.35724quot;,quot;quot;c1a57395-aed9-4de7-ad64-17cc2a13efafquot;,
4    <meta charset="UTF-8" />
5
6  <meta http-equiv="X-UA-Compatible" content="IE=Edge" />
7  <meta name="viewport" content="width=device-width, initial-scale=1" />
8  <title>Microsoft - Cloud, Computers, Apps & Gaming</title>
9
10 <meta name="twitter:image" content="http://img-prod-cms-rt-microsoft-com.akamaihd.net/cms/api/am/
11 <meta property="og:image" content="http://img-prod-cms-rt-microsoft-com.akamaihd.net/cms/api/am/
12 <meta name="twitter:url" content="https://www.microsoft.com/en-in" />
13 <meta property="og:url" content="https://www.microsoft.com/en-in" />
14 <meta name="twitter:title" content="Microsoft - Cloud, Computers, Apps & Gaming" />
15 <meta property="og:title" content="Microsoft - Cloud, Computers, Apps & Gaming" />
16 <meta name="twitter:description" content="Explore Microsoft products and services for your home or
17 <meta property="og:description" content="Explore Microsoft products and services for your home or
18 <meta name="twitter:card" content="summary" />
19 <meta property="og:type" content="website" />
20
21
22
23
24
25
26
27
28
29 <link rel="dns-prefetch" href="https://assets.onestore.ms" />
30 <link rel="preconnect" href="https://assets.onestore.ms" />
31 <link rel="dns-prefetch" href="https://web.vortex-data.microsoft.com" />
32 <link rel="preconnect" href="https://web.vortex-data.microsoft.com" />
33 <link rel="dns-prefetch" href="https://mem.gfx.ms" />
34 <link rel="preconnect" href="https://mem.gfx.ms" />
35 <link rel="dns-prefetch" href="https://img-prod-cms-rt-microsoft-com.akamaihd.net" />
36 <link rel="preconnect" href="https://img-prod-cms-rt-microsoft-com.akamaihd.net" />
37 <link rel="dns-prefetch" href="https://microsoftwindows.112.2a7.net" />
38 <link rel="preconnect" href="https://microsoftwindows.112.2a7.net" />
```

Examining cookies may provide

- Software in use and its behavior
 - Scripting platforms used

All sites		Search
Sort by	Most visited	▼
Total storage used by sites: 65.8 KB		Clear all data
 google.com	4.0 KB · 5 cookies	▲ ■
 www.google.com	4.0 KB · 1 cookie	▲ ■
 oga.google.com	1 cookie	▲ ■
 microsoft.com	6.3 KB · 47 cookies	▲ ■
 2ssslr - http	0 B · 1 cookie	▲ ■
 adnxa.com - http	0 B · 2 cookies	▲ ■
 adsrvr.org - http		▲ ■

Website Footprinting using Web Spiders

- Web spiders, such as **Web Data Extractor** and **ParseHub**, perform automated searches on the target website and collect specified information, such as **employee names** and **email addresses**
- Attackers use the collected information to perform **footprinting** and **social engineering attacks**

User-Directed Spidering

- Attackers use **standard web browsers** to walk through the target website functionalities
- The incoming and outgoing **traffic of the target website is monitored** and analyzed by tools that include features of both a web spider and an intercepting proxy
- Attackers use tools such as **Burp Suite** and **WebScarab** to perform user-directed spidering



Web Data Extractor

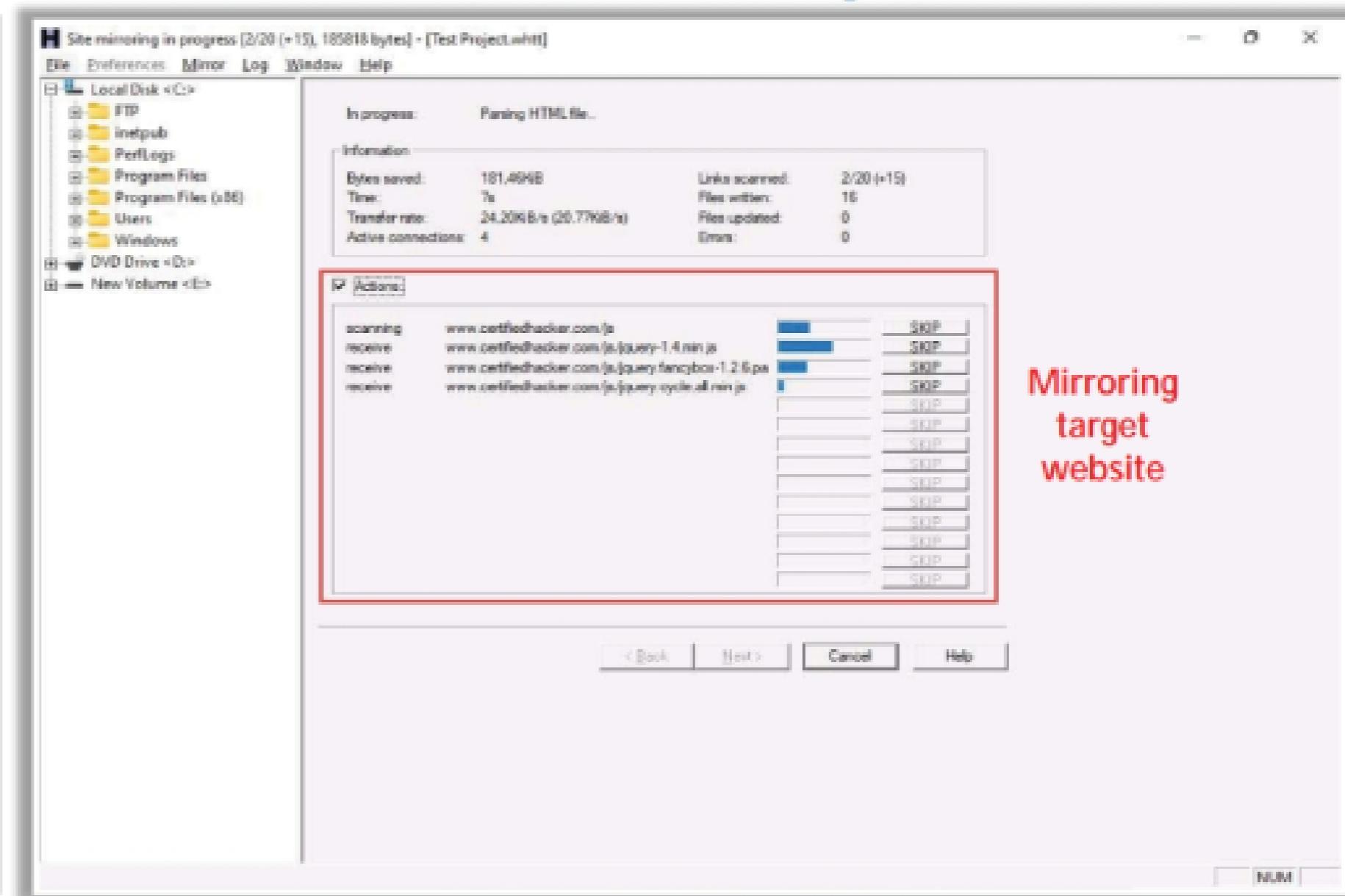
URL	Title	Keywords	Description	Mod.	Domain	Page size	Pages crawled	Key
http://www.footech.com/Online%20Booking/Online%20Booking.html	Online Booking - Hotel Info	booking hotel info Online Booking	http://www.footech.com	29496	2/10/2011			
http://www.footech.com/Online%20Booking/Online%20Booking%20Review	Booking - Hotel,Info Online Booking	booking hotel info Online Booking	http://www.footech.com	5603	2/10/2011			
http://www.footech.com/About%20Us/about%20footech	About footech			5307	2/10/2011			
http://www.footech.com/Find%20a%20Hotel%20Near%20Me	Find a Hotel Near Me			5464	2/10/2011			
http://www.footech.com/Find%20a%20Hotel%20Near%20Me%20Near%20Me	Find a Hotel Near Me Near Me			8571	2/10/2011			
http://www.footech.com/Find%20a%20Hotel%20Near%20Me%20Near%20Me%20Near%20Me	Find a Hotel Near Me Near Me Near Me			10049	2/10/2011			
http://www.footech.com/Real%20Estate%20Professional%20Real%20Estate%20Service%20Professional%20Real%20Estate%20Service	Professional Real Estate Service Real Estate, real estate Professional Real Estate Service	Professional Real Estate Service Real Estate, real estate	http://www.footech.com	3683	2/10/2011			
http://www.footech.com/Real%20Estate%20Professional%20Real%20Estate%20Service%20Professional%20Real%20Estate%20Service	Professional Real Estate Service Real Estate, real estate Professional Real Estate Service	Professional Real Estate Service Real Estate, real estate	http://www.footech.com	4362	2/10/2011			
http://www.footech.com/Real%20Estate%20Professional%20Real%20Estate%20Service%20Professional%20Real%20Estate%20Service	Professional Real Estate Service Real Estate, real estate Professional Real Estate Service	Professional Real Estate Service Real Estate, real estate	http://www.footech.com	6767	2/10/2011			
http://www.footech.com/Real%20Estate%20Professional%20Real%20Estate%20Service%20Professional%20Real%20Estate%20Service	Professional Real Estate Service Real Estate, real estate Professional Real Estate Service	Professional Real Estate Service Real Estate, real estate	http://www.footech.com	8799	2/10/2011			
http://www.footech.com/Recipes/about%20Your%20Company	About us		Some keywords that is about description of your company	http://www.footech.com	5702	2/10/2011		
http://www.footech.com/Recipes/apple	Your company - Recipe detail		Some keywords that is about description of your company	http://www.footech.com	1047	2/10/2011		
http://www.footech.com/Recipes/cheese	Your company - Recipe detail		Some keywords that is about description of your company	http://www.footech.com	10001	2/10/2011		
http://www.footech.com/Recipes/cheese	Your company - Recipe detail		Some keywords that is about description of your company	http://www.footech.com	9994	2/10/2011		
http://www.footech.com/Recipes/cheese	Your company - Recipe detail		Some keywords that is about description of your company	http://www.footech.com	9629	2/10/2011		
http://www.footech.com/Recipes/contact%20Your%20Company	Contact us		Some keywords that is about description of your company	http://www.footech.com	8620	2/10/2011		
http://www.footech.com/Recipes/peach	Your company - Recipe detail		Some keywords that is about description of your company	http://www.footech.com	9355	2/10/2011		
http://www.footech.com/Recipes/peach	Your company - Recipe detail		Some keywords that is about description of your company	http://www.footech.com	8397	2/10/2011		
http://www.footech.com/Recipes/peach%20menu	Your company - Menu		Some keywords that is about description of your company	http://www.footech.com	7909	2/10/2011		
http://www.footech.com/Recipes/peach%20menu	Your company - Recipe		Some keywords that is about description of your company	http://www.footech.com	12716	2/10/2011		
http://www.footech.com/Recipes/peach%20menu	Your company - Recipe detail		Some keywords that is about description of your company	http://www.footech.com	8962	2/10/2011		
http://www.footech.com/Recipes/peach%20menu	Your company - Recipe detail		Some keywords that is about description of your company	http://www.footech.com	10804	2/10/2011		
http://www.footech.com/Recipes/peach%20menu	Your company - Recipe category		Some keywords that is about description of your company	http://www.footech.com	11584	2/10/2011		
http://www.footech.com/Recipes/peach%20menu	Your company - Recipes category		Some keywords that is about description of your company	http://www.footech.com	12451	2/10/2011		
http://www.footech.com/Social%20Media%20Units	- Together is Better (created by Parallelogram, or phrase A brief description of this website)		Some keywords that is about description of this website	http://www.footech.com	13074	2/10/2011		
http://www.footech.com/Social%20Media%20Units	- Together is Better (created by Parallelogram, or phrase A brief description of this website)		Some keywords that is about description of this website	http://www.footech.com	16239	2/10/2011		
http://www.footech.com/Social%20Media%20Units	- Together is Better (created by Parallelogram, or phrase A brief description of this website)		Some keywords that is about description of this website	http://www.footech.com	12443	2/10/2011		
http://www.footech.com/Social%20Media%20Units				1489	2/10/2011			
http://www.footech.com/Social%20Media%20Units				16239	2/10/2011			
http://www.footech.com/Taste%20Wise				8227	2/10/2011			
http://www.footech.com/Taste%20Wise				8583	2/10/2011			
http://www.footech.com/Taste%20Wise				2903	2/10/2011			
http://www.footech.com/Taste%20Wise				5002	2/10/2011			

Mirroring Entire Website

- Mirroring an entire website onto a local system enables an attacker to browse website offline; it also assists in finding **directory structure** and other valuable information from the mirrored copy without sending multiple requests to web server
- Web mirroring tools, such as HTTrack Web Site Copier, and Cyotek WebCopy, allow you to **download a website to a local directory**, recursively building all directories, HTML, images, flash, videos, and other files from the server to your computer



HTTrack Web Site Copier



The screenshot shows the HTTrack Web Site Copier application window. The title bar reads "HTTrack Web Site Copier" and the main window title is "Site mirroring in progress [2/20 (+1), 185818 bytes] - [Test Project.htm]". The menu bar includes File, Preferences, Mirror, Log, Window, and Help. A tree view on the left shows the local disk structure under "Local Disk <C:>". The main area displays a progress table with the following data:

In progress	Parsing HTML file...
Bytes saved:	181,463B
Time:	7s
Transfer rate:	24,208 B/s (2.77KB/s)
Active connections:	4
Links scanned:	2/20 (+1)
File written:	16
File updated:	0
Errors:	0

A red box highlights the "Actions" section, which lists the status of various files being downloaded:

scanning	www.certifedchecker.com/ja	SOP
receive	www.certifedchecker.com/ja/jquery-1.4.min.js	SOP
receive	www.certifedchecker.com/ja/jquery.fancybox-1.2.6.js	SOP
receive	www.certifedchecker.com/ja/jquery.cycle.all.min.js	SOP
		SOP

At the bottom of the window are buttons for Back, Next, Cancel, and Help.

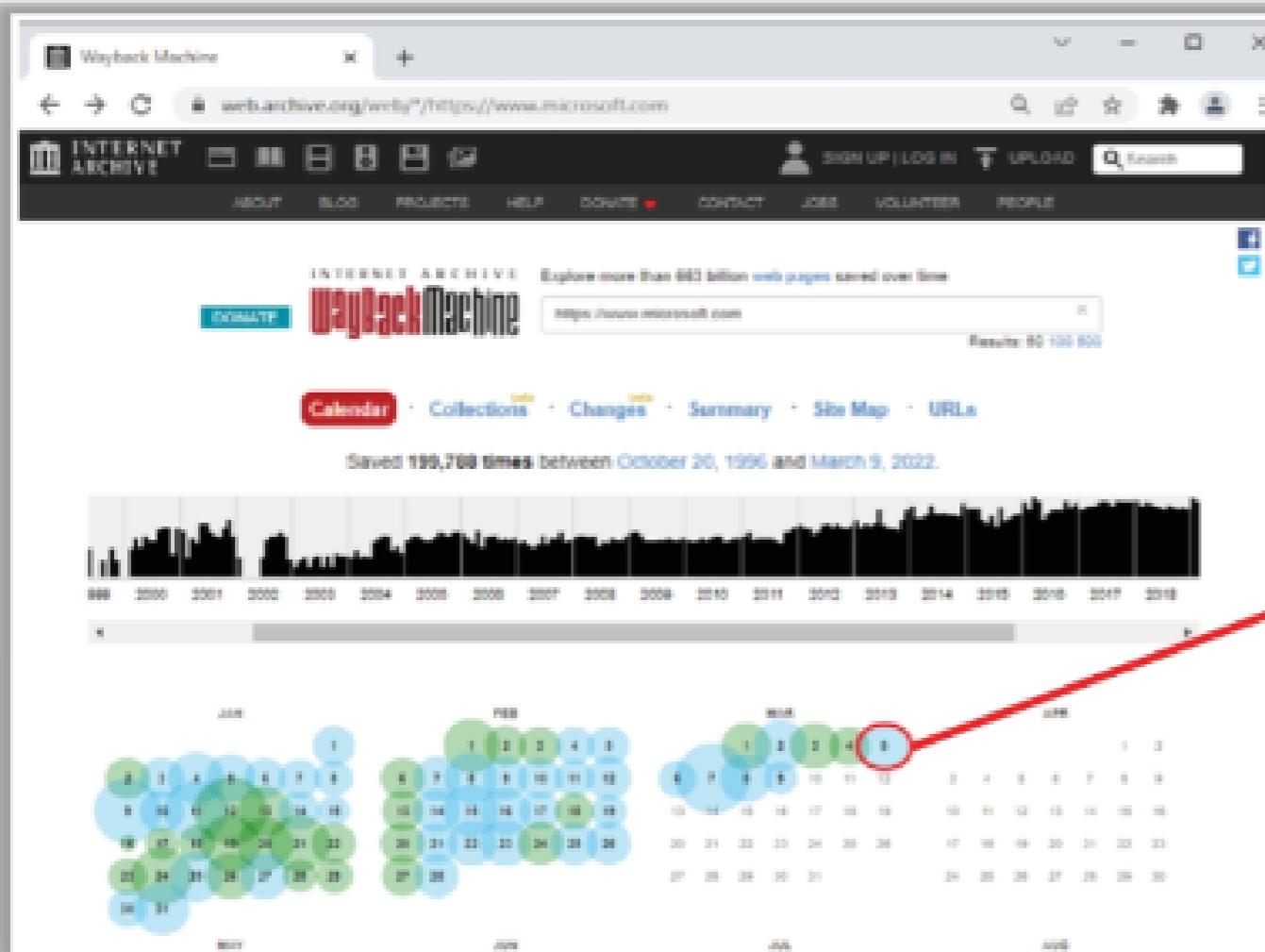
Mirroring target website

NUM

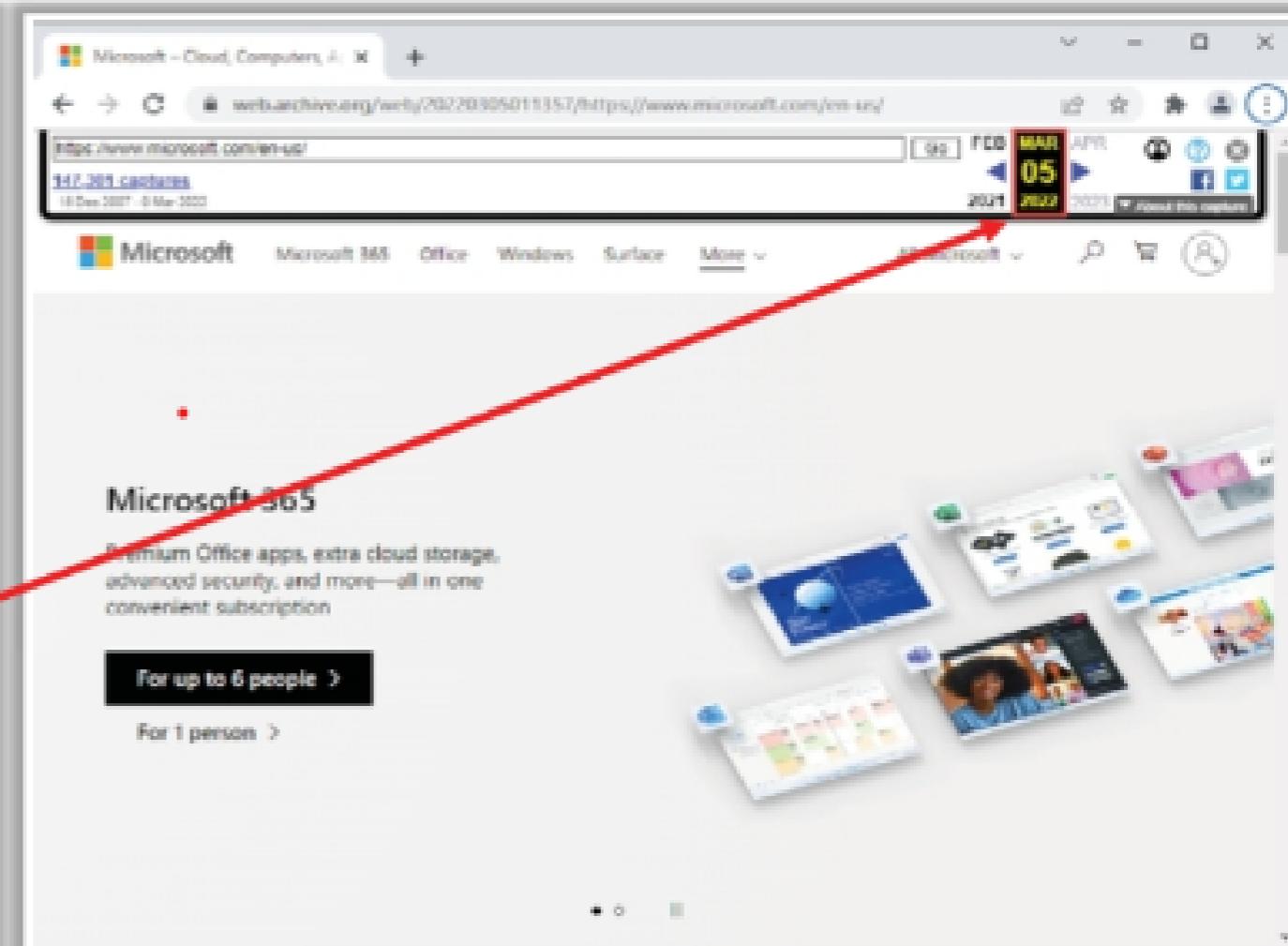
<https://www.httrack.com>

Extracting Website Information from https://archive.org

- Internet Archive's Wayback Machine allows one to visit **archived versions of websites**



The screenshot shows the Wayback Machine interface. At the top, there's a search bar with the URL "webarchive.org/web/https://www.microsoft.com". Below it is the Internet Archive logo and a navigation menu with links like "ABOUT", "BLOG", "PROJECTS", "HELP", "DONATE", "CONTACT", "JOBS", "VOLUNTEER", and "PEOPLE". A "Wayback Machine" button is highlighted in blue. The main content area features a timeline visualization with a grid of colored circles representing different archived versions of the Microsoft website. A red circle highlights a specific point on the timeline, which corresponds to the date "MAR 05 2022" shown in the browser's address bar.



The screenshot shows the Microsoft website as it appeared on March 5, 2022. The URL in the address bar is "https://www.microsoft.com/en-us/" and the timestamp is "147,381 captures 14 Dec 2007 - 5 Mar 2022". The Microsoft homepage is displayed, featuring the Microsoft logo, navigation links for "Microsoft 365", "Office", "Windows", "Surface", and "More". A prominent "Microsoft 365" section is shown with the text "Premium Office apps, extra cloud storage, advanced security, and more—all in one convenient subscription". Buttons for "For up to 6 people" and "For 1 person" are visible. To the right, there are images of various Microsoft products like Surface tablets and phones.

- Attackers can use tools such as **Photon** to retrieve archived URLs of the target website from archive.org

Other Techniques for Website Footprinting

Footprinting Technique	Description	Information Gathered	Tools Used
Extracting Website Links	Analyze the target website to determine its internal and external links	Linked images, scripts, iframes, and URLs of the target website	Octoparse, Netpeak Spider, and Link Extractor
Gathering the Wordlist from the Target Website	Gather the wordlist available on the target website to brute-force the email addresses gathered through search engines, social networking sites, web spidering, etc.	List of words from the target website	CeWL
Extracting Metadata of Public Documents	Useful information may reside on the target website in the form of pdf documents, Microsoft Word files, etc.	Title of the page, description, keywords, creation/modification date and time of the content, and usernames and e-mail addresses of employees of the target organization	ExifTool, Web Data Extractor, and Metagoofil
Monitoring Web Pages for Updates and Changes	Detect changes or updates in the target website	Changes to the login pages, password-protected pages, software version and driver updates, and images	WebSite-Watcher, Visual Ping, and Follow That Page
Searching for Contact Information, Email Addresses, and Telephone Numbers from Company Website	Search the target company's website to gather crucial information about the company	Contact details, location, partner information, news, and links to other sites	Target website
Searching for Web Pages Posting Patterns and Revision Numbers	Search for copyright notices and revision numbers on the web	Copyright symbol, year of creation, name of the author, and a rights statement	Web search
Monitoring Website Traffic of the Target Company	Collect information about the target's customer base	Total visitors, page views, bounce rate, live visitor map, site ranking, and customer locations	Web-Stat, Rank Tracker, and TeamViewer

Deep and Dark Web Footprinting

Deep web

- It consists of web pages and contents that are **hidden and unindexed** and cannot be located using traditional web browsers and search engines
- It can be accessed by **search engines** like Tor Browser and The WWW Virtual Library

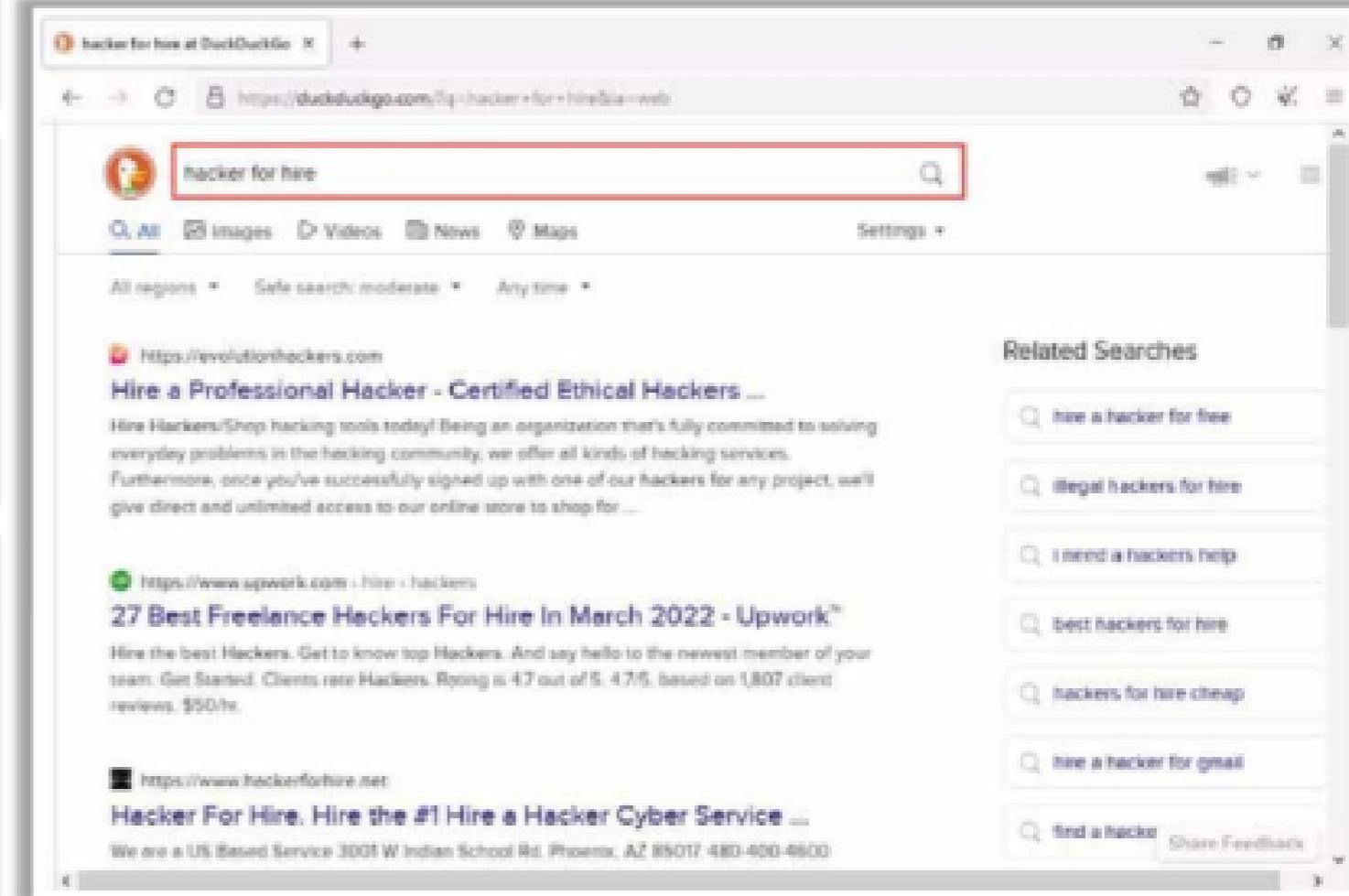
Dark web or Darknet

- It is the subset of the deep web that enables anyone to **navigate anonymously** without being traced
- It can be accessed by **browsers**, such as TOR Browser, Freenet, GNUnet, I2P, and Retroshare

- Attackers use deep and dark web searching tools, such as **Tor Browser** and **ExoneraTor**, to **gather confidential information about the target**, including credit card details, passport information, identification card details, medical records, social media accounts, Social Security Numbers (SSNs), etc.

TOR Browser

It is used to access the deep and dark web where it acts as a **default VPN** for the user and bounces the network IP address through several servers before interacting with the web



LO#06: Use Different Techniques for Email Footprinting

Tracking Email Communications

- Email tracking is used to **monitor the delivery of emails** to an intended recipient
 - Attackers track emails to **gather information about a target recipient**, such as IP addresses, geolocation, browser and OS details, to build a hacking strategy and perform social engineering and other attacks



Collecting Information from Email Header

Email Tracking Tools

- Email tracking tools, such as eMailTrackerPro, Infoga, Mailtrack, and PoliteMail, allow an attacker to **track an email and extract information**, such as sender identity, mail server, sender's IP address, and location
- eMailTrackerPro analyzes email headers and reveals information, such as **sender's geographical location** and IP address

Parrot Terminal

```

File Edit View Search Terminal Help
-[x]-[attacker@parrot]-[-/Infoga]
-- $python infoga.py --domain microsoft.com --source all --breach -v 2
--report ../microsoft.txt

=====
[ Infoga - Email OSINT
[ MoMo (m4ll0k) Outaadi
[ https://github.com/m4ll0k

=====
[*] Searching "microsoft.com" in Ask...
[!] Found 0 emails in Ask
[*] Searching "microsoft.com" in Baidu...
[!] Found 4 emails in Baidu
[*] Searching "microsoft.com" in Bing...
[!] Found 8 emails in Bing
[*] Searching "microsoft.com" in DogPile...
[!] Found 0 emails in Dogpile
[*] Searching "microsoft.com" in Exalead...
[*] Searching "microsoft.com" in Google...
[!] Found 1 emails in Google
[*] Searching "microsoft.com" in PGP...
[!] Found 0 emails in PGP
[*] Searching "microsoft.com" in Yahoo...
[!] Found 1 emails in Yahoo
  
```

eMailTrackerPro v7.0.0 Advanced Edition. Trial day 1 of 15

File Help

My Trace Reports Trace Headers Trace Address Email Accounts Settings Options

The trace is complete, the information found is displayed on the right.

Email Summary

From: [REDACTED].com
 To: [REDACTED].gmail.com
 Date: 09/01/2014 -0500 (UTC)
 Subject: Please verify your SecurityHealth account
 to action [America]

Missed recipient: [REDACTED] (possibly spam)
 Abuse Address: abuse@exalead.com
 Abuse Reporting: To automatically generate an email abuse report: click here.
 From IP: [REDACTED]
 Header Analysis:
 A time stamp claimed to be added by a server along the email route is not valid. This is a mistake by the spammer that means a header in this email is fake.

System Information:

- There is no SMTP server running on this system. (the port is closed)

Network Where

Domain Where

Email Header

Hop	Hop IP	Hop Name	Location
1	[REDACTED]		
2	[REDACTED]		
3	[REDACTED]		
4	[REDACTED]	[Europe]	
5	[REDACTED]	[America]	
6	[REDACTED]	telk30-6.sx21.spfH.atis.cognitivsys.PL.USA	
7	[REDACTED]	bs2020.cc22.mw01.atis.cognitivsys.PL.USA	
8	[REDACTED]	bs2027.cc22.mw03.atis.cognitivsys.PL.USA	
9	[REDACTED]	level3.mw03.atis.cognitivsys.com.Miami.PL.USA	

You are on day 1 of a 15 day trial. To make a license click here or for purchase information click here.

LO#07: Use Different Techniques for Whois Footprinting

Whois Lookup

Whois databases are maintained by **Regional Internet Registries** and contain **personal information of domain owners**

Whois query returns

- Domain name details
- Contact details of domain owners
- Domain name servers
- NetRange
- When a domain was created
- Expiry records
- Last updated record

Information obtained from Whois database assists an attacker to

- Gather personal information that assists in social engineering
- Create a map of the target organization's network
- Obtain internal details of the target network



Regional Internet Registries (RIRs)



Whois Lookup

Whois Record for CertifiedHacker.com

Domain Profile

Registrant: PERFECT PRIVACY, LLC

Registrant Country: US

Registrar: Network Solutions, LLC

IANA ID: 2

URL: <http://networksolutions.com>

Whois Server: whois.networksolutions.com

domain.operations@web.com

(P) 18777228662

Registrar Status: clientTransferProhibited

Dates: 7,164 days old

Created on 2002-07-29

Expires on 2022-07-29

Updated on 2021-08-22

Name Servers: NS1.BLUEHOST.COM (has 2,681,575 domains)

NS2.BLUEHOST.COM (has 2,681,575 domains)

Tech Contact: PERFECT PRIVACY, LLC

5335 Gate Parkway care of Network Solutions PO Box 459,
Jacksonville, FL, 32256, US

kq9t994x73e@networksolutionsprivateregistration.com

(P) 15707088622

IP Address: 162.241.216.11 - 1,745 other sites hosted on this server

IP Location:  - Utah - Provo - Unified Layer

ASN:  AS26337 OH51, US (registered Oct 09, 2013)

Domain Status: Registered And Active Website

IP History: 13 changes on 13 unique IP addresses over 16 years

Registrar History: 3 registrars with 2 drops

Hosting History: 6 changes on 4 unique name servers over 19 years
<http://whois.domaintools.com>

SmartWhois - Evaluation Version

File Query Edit View Settings Help

IP, host or domain: Query

certifiedhacker.com

 certifiedhacker.com

 162.241.216.11

 PERFECT PRIVACY, LLC
5335 Gate Parkway care of Network Solutions PO Box 459
Jacksonville
FL
32256
United States
Phone: +1.5707088622
kq9t994x73e@networksolutionsprivateregistration.com

 PERFECT PRIVACY, LLC
5335 Gate Parkway care of Network Solutions PO Box 459
Jacksonville
FL
32256
United States
Phone: +1.5707088622
kq9t994x73e@networksolutionsprivateregistration.com

 PERFECT PRIVACY, LLC
5335 Gate Parkway care of Network Solutions PO Box 459
Jacksonville
FL
32256
United States
Phone: +1.5707088622
kq9t994x73e@networksolutionsprivateregistration.com

 NS1.BLUEHOST.COM
NS2.BLUEHOST.COM

Done <https://www.tamos.com>

certifiedhacker.com - Source

Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 00049374_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: <http://networksolutions.com>
Updated Date: 2021-08-22T00:51:43Z
Creation Date: 2002-07-29T00:32:08Z
Registrar Registration Expiration Date: 2022-07-29T00:52:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 1
Reseller:
Domain Status: clientTransferProhibited
<https://icann.org/epp/clientTransferProhibited>
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of
network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.5707088622
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email:
kq9t994x73e@networksolutionsprivateregistration.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
Admin Organization:
Admin Street: 5335 Gate Parkway care of Network
Solutions PO Box 459
Admin City:
Admin State/Province:
Admin Postal Code:
Admin Country:
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email:
kq9t994x73e@networksolutionsprivateregistration.com

Close

Finding IP Geolocation Information

- IP geolocation helps to identify information, such as country, region/state, city, ZIP/postal code, time zone, **connection speed, ISP (hosting company)**, domain name, IDD country code, area code, mobile carrier, and elevation

- **IP geolocation lookup tools**, such as **IP2Location** and **IP Location Finder**, help to collect IP geolocation information about the target, which in turn helps attackers in **launching social engineering attacks**, such as spamming and phishing



IP2Location

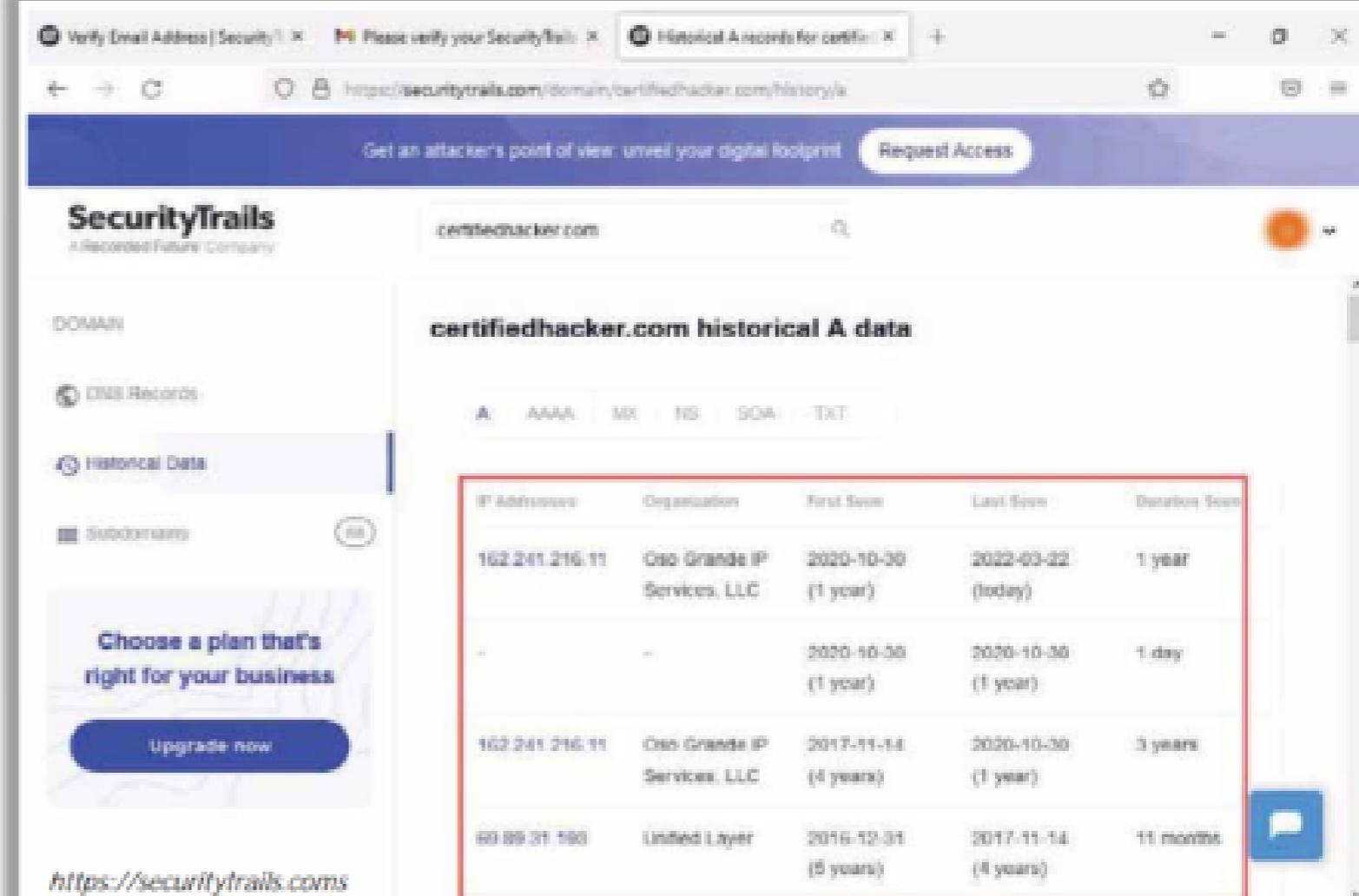
<input checked="" type="checkbox"/> IP Address	207.46.232.182
<input checked="" type="checkbox"/> Country	Singapore [SG] ⓘ
<input type="checkbox"/> Region	Singapore
<input type="checkbox"/> City	Singapore
<input type="checkbox"/> Coordinates of City	1.289670, 103.850070 (1°17'23"N 103°51'0"E)
<input type="checkbox"/> ISP	Microsoft Corporation
<input type="checkbox"/> Local Time	10 Mar, 2022 07:54 PM (UTC +08:00)
<input type="checkbox"/> Domain	microsoft.com
<input type="checkbox"/> Net Speed	(COMP) Company/T1
<input type="checkbox"/> IDD & Area Code	(65) 06
<input type="checkbox"/> ZIP Code	179431
<input type="checkbox"/> Weather Station	Singapore (SNX0006)

LO#08: Use Different Techniques for DNS Footprinting

Extracting DNS Information

- DNS records provide important information about the **location and types of servers**
- Attackers can gather DNS information to **determine key hosts in the network** and can perform social engineering attacks

- Attackers query DNS servers using DNS interrogation tools, such as SecurityTrails, NSLOOKUP, and DNS Records, to **retrieve the record structure** that contains information about the target DNS



The screenshot shows a web browser window with three tabs open:

- Verify Email Address | SecurityTrails
- Please verify your SecurityTrails account
- Historical A records for certifiedhacker.com

The main content area is titled "certifiedhacker.com historical A data". It displays a table of historical A records:

IP Address	Organization	First Seen	Last Seen	Duration
162.241.216.11	Oso Grande IP Services, LLC	2020-10-30 (1 year)	2022-03-22 (today)	1 year
-	-	2020-10-30 (1 year)	2020-10-30 (1 year)	1 day
162.241.216.11	Oso Grande IP Services, LLC	2017-11-14 (4 years)	2020-10-30 (1 year)	3 years
69.89.31.193	United Layer	2016-12-01 (5 years)	2017-11-14 (8 years)	11 months

At the bottom left, there is a call-to-action button: "Choose a plan that's right for your business" with a "Upgrade now" button.

The URL in the address bar is <https://securitytrails.com/>.

Reverse DNS Lookup

- Attackers perform a reverse DNS lookup on IP ranges in an attempt to **locate a DNS PTR record** for those IP addresses
- Attackers use various tools, such as **DNSRecon** and **Reverse Lookup** to perform the reverse DNS lookup on the target host

MX TOOLBOX

Pricing Tools Delivery Center Monitoring

SuperTool MX Lookup Blocklists DMARC Diagnostics Email Health DNS Lookup

SuperTool Beta7

162.241.216.11 Reverse Lookup +

ptr:162.241.216.11 Find Problems

Type	IP Address	Domain Name	TTL
TypePTR	IP Address 162.241.216.11 One Grande IP Services, LLC (AS28937)	Domain Name box5331.bluehost.com	TTL 24 hrs

	Test	Result
Status	✓ NameDNS Record Published	Response DNS Record found

smtp diag blacklist subnet tool dns propagation

Reported by ns1.unifiedlayer.com on 3/10/2022 at 7:22:21 AM (UTC -6). Just for you. Transcript

Parrot Terminal

```

File Edit View Search Terminal Help
[attacker@parrot:~]-
└── Sod dnsrecon
  └── [attacker@parrot:~/dnsrecon]
    └── $ ./dnsrecon.py -r 162.241.216.0-162.241.216.255
      [*] Performing Reverse Lookup from 162.241.216.0 to 162.241.216.255
      [*] PTR 162.241.216.3.unifiedlayer.com 162.241.216.3
      [*] PTR 162.241.216.1.unifiedlayer.com 162.241.216.1
      [*] PTR 162.241.216.2.unifiedlayer.com 162.241.216.2
      [*] PTR 162.241.216.4.unifiedlayer.com 162.241.216.4
      [*] PTR 162.241.216.5.unifiedlayer.com 162.241.216.5
      [*] PTR 162.241.216.6.unifiedlayer.com 162.241.216.6
      [*] PTR 162.241.216.7.unifiedlayer.com 162.241.216.7
      [*] PTR 162.241.216.8.unifiedlayer.com 162.241.216.8
      [*] PTR 162.241.216.9.unifiedlayer.com 162.241.216.9
      [*] PTR 162.241.216.10.unifiedlayer.com 162.241.216.10
      [*] PTR box5331.bluehost.com 162.241.216.11
      [*] PTR 162.241.216.12.unifiedlayer.com 162.241.216.12
      [*] PTR box5334.bluehost.com 162.241.216.14
      [*] PTR 162.241.216.13.unifiedlayer.com 162.241.216.13
      [*] PTR 162.241.216.15.unifiedlayer.com 162.241.216.15
      [*] PTR 162.241.216.16.unifiedlayer.com 162.241.216.16
      [*] PTR box5348.bluehost.com 162.241.216.17
      [*] PTR 162.241.216.19.unifiedlayer.com 162.241.216.19
      [*] PTR 162.241.216.18.unifiedlayer.com 162.241.216.18
      [*] PTR box5358.bluehost.com 162.241.216.20
      [*] PTR 162.241.216.21.unifiedlayer.com 162.241.216.21
      [*] PTR 162.241.216.22.unifiedlayer.com 162.241.216.22
      [*] PTR 162.241.216.24.unifiedlayer.com 162.241.216.24
      [*] PTR box5353.bluehost.com 162.241.216.23
      [*] PTR box5354.bluehost.com 162.241.216.26
  
```

Menu Parrot Terminal

LO#09: Use Different Techniques for Network Footprinting

Locate the Network Range

- Network range information assists attackers in creating a **map of the target network**
- One can find the **range of IP addresses** using **ARIN whois database search tool**
- One can also find the range of IP addresses and the subnet mask used by the target organization from **Regional Internet Registry (RIR)**



Network: NET-207-46-0-0-1

Source Registry	ARIN
Net Range	207.46.0.0 - 207.46.255.255
CIDR	207.46.0.0/16
Name	MICROSOFT-GLOBAL-NET
Handle	NET-207-46-0-0-1
Parent	NET-207-0-0-0-0
Net Type	DIRECT ALLOCATION
Origin AS	not provided
Registration	Mon, 31 Mar 1997 05:00:00 GMT (Mon Mar 31 1997 local time)
Last Changed	Wed, 15 Dec 2021 01:29:40 GMT (Wed Dec 15 2021 local time)
Self	https://index.arin.net/registry/ip/207.46.0.0
Alternate	https://whois.arin.net/rest/net/NET-207-46-0-0-1
Port 43 Whois	whois.arin.net

Related Entities → 1 Entity

Source Registry	ARIN	Network Whois Record
Kind	Org	Queried
Full Name	Microsoft Corporation	search.arin.net with
Handle	MSFT	"207.46.232.182"
Address	One Microsoft Way Redmond WA 98052 United States	
Roles	Registrant	
Registration	Fri, 10 Jul 1998 04:00:00 GMT (Fri Jul 10 1998 local time)	
Last Changed	Wed, 13 Oct 2021 21:39:04 GMT (Thu Oct 14 2021 local time)	
Comments	To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other illicit or illegal material through a Microsoft online service, please submit reports to: https://rcpt.microsoft.com .	

Traceroute

- Traceroute programs work on the concept of **ICMP protocol** and **use the TTL field in the header of ICMP packets** to discover the routers on the path to a target host

ICMP Traceroute

Administrator: Command Prompt

Microsoft Windows [Version 10.0.22000.469]
 © Microsoft Corporation. All rights reserved.

```
C:\Windows\system32 tracert 216.239.36.10
```

Tracing route to null.google.com [216.239.36.10]
 over a maximum of 30 hops:

1	1 ms	<1 ms	<1 ms	10.10.1.2
2	2 ms	2 ms	3 ms	172.18.0.1
3	1 ms	1 ms	1 ms	192.168.100.6
4	1 ms	1 ms	2 ms	103.152.3.225
5	3 ms	2 ms	2 ms	38.140.226.249
6	2 ms	4 ms	3 ms	te0-3-1-5.rer21.tpa01.atlas.cogentco.com [154.24.32.129]
7	9 ms	10 ms	9 ms	be2320.ccr22.mia01.atlas.cogentco.com [154.54.5.85]
8	9 ms	9 ms	8 ms	be3401.ccr21.mia03.atlas.cogentco.com [154.54.47.38]
9	17 ms	9 ms	8 ms	tata.mia03.atlas.cogentco.com [154.54.9.46]
10	8 ms	9 ms	8 ms	72.14.215.97
11	9 ms	8 ms	9 ms	108.170.253.3
12	10 ms	11 ms	10 ms	216.239.54.71
13	33 ms	32 ms	32 ms	142.250.226.24
14	32 ms	31 ms	30 ms	216.239.49.47
15	30 ms	30 ms	30 ms	142.250.56.231

TCP Traceroute

Parrot Terminal

```
-[x]-[attacker@parrot]-[~]
└─$ sudo tcptraceroute www.google.com
[sudo] password for attacker:
Running:
traceroute -T -0 info www.google.com
traceroute to www.google.com (142.250.217.196), 30 hops max, 60 byte packets
 1  10.10.1.2 (10.10.1.2)  3.499 ms  5.598 ms  9.187 ms
 2  172.18.0.1 (172.18.0.1)  12.137 ms  13.499 ms  14.918 ms
 3  192.168.100.6 (192.168.100.6)  17.382 ms  19.869 ms  20.324 ms
 4  103.152.3.225 (103.152.3.225)  21.434 ms  22.263 ms  23.227 ms
 5  38.140.226.249 (38.140.226.249)  24.835 ms  25.957 ms  27.143 ms
```

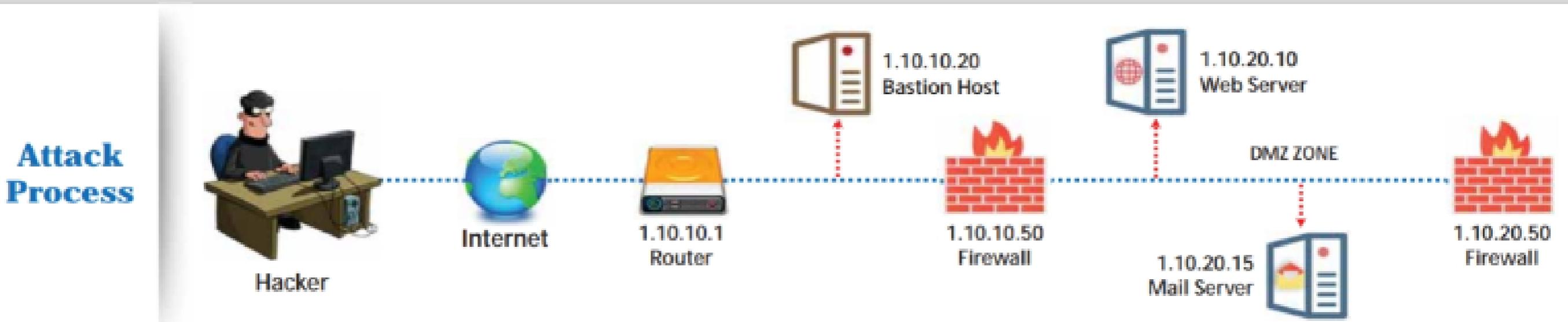
UDP Traceroute

Parrot Terminal

```
-[x]-[attacker@parrot]-[~]
└─$ traceroute www.google.com
traceroute to www.google.com (142.250.217.196), 30 hops max, 60 byte packets
 1  10.10.1.2 (10.10.1.2)  1.178 ms  1.442 ms  1.314 ms
 2  172.18.0.1 (172.18.0.1)  1.353 ms  1.723 ms  1.937 ms
 3  192.168.100.6 (192.168.100.6)  2.654 ms  2.605 ms  3.037 ms
 4  103.152.3.225 (103.152.3.225)  3.645 ms  3.925 ms  4.367 ms
 5  38.140.226.249 (38.140.226.249)  4.846 ms  5.799 ms  6.881 ms
 6  te0-3-1-5.rer21.tpa01.atlas.cogentco.com (154.24.32.129)  7.208 ms  4.270 ms
 7  be2320.ccr22.mia01.atlas.cogentco.com (154.54.5.81)  9.099 ms
 8  be3401.ccr21.tpa01.atlas.cogentco.com (154.54.5.181)  9.099 ms
 9  tata.mia03.atlas.cogentco.com (154.54.9.46)  9.099 ms
 10  72.14.215.97  9.099 ms
 11  108.170.253.3  9.099 ms
 12  216.239.54.71  9.099 ms
 13  142.250.226.24  9.099 ms
 14  216.239.49.47  9.099 ms
 15  142.250.56.231  9.099 ms
```

Traceroute Analysis

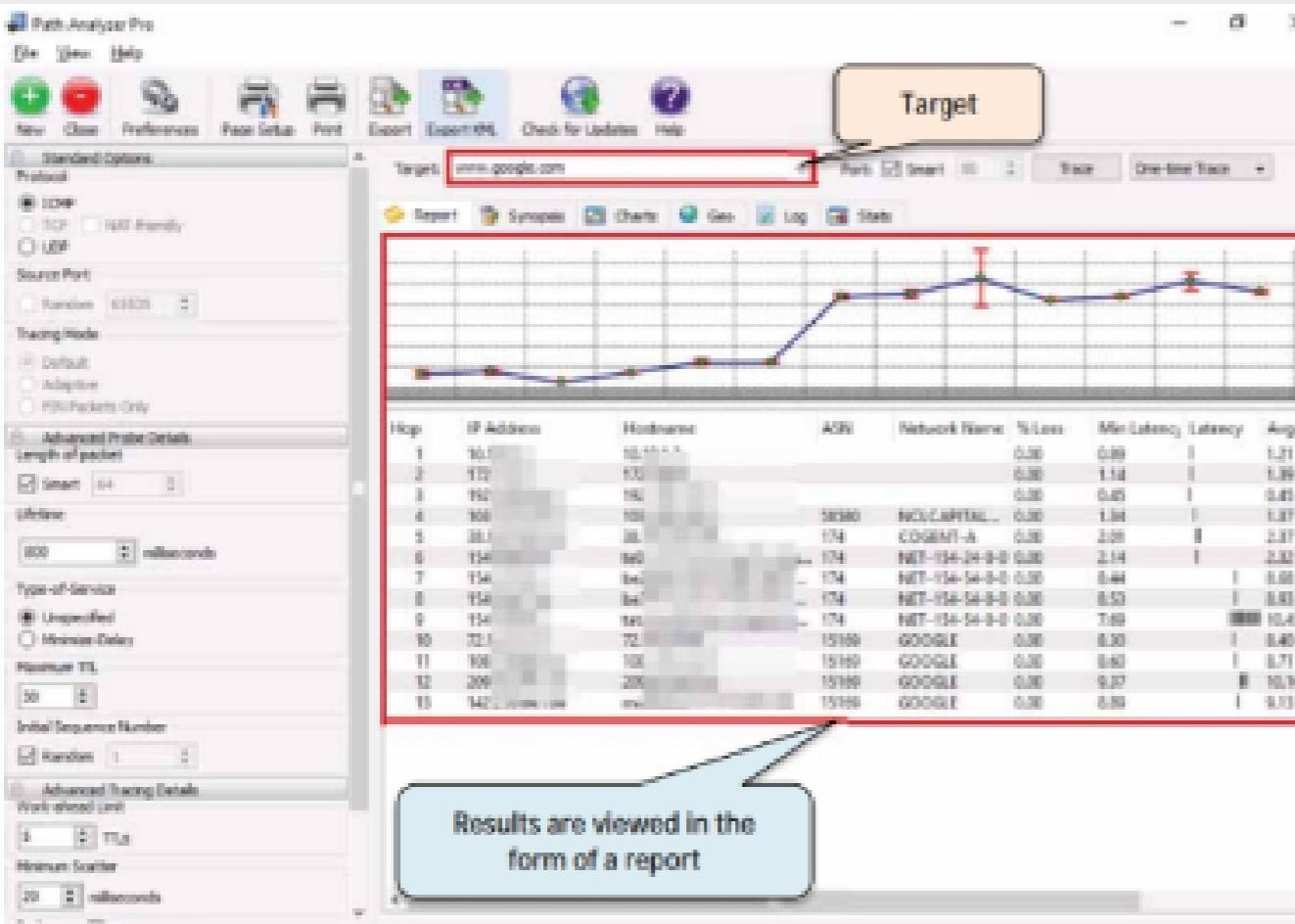
- Attackers execute traceroute to find the **IP addresses of intermediate devices** such as routers and firewalls present between a source and its destination
- For example, after running several **traceroutes**, an attacker might obtain the following information:
 - traceroute 1.10.10.20, second to last hop is 1.10.10.1
 - traceroute 1.10.20.10, third to last hop is 1.10.10.1
 - traceroute 1.10.20.10, second to last hop is 1.10.10.50
 - traceroute 1.10.20.15, third to last hop is 1.10.10.1
 - traceroute 1.10.20.15, second to last hop is 1.10.10.50
- By compiling this information, attackers can identify the intermediate devices or hosts in the path to the target network



Traceroute Tools

Path Analyzer Pro

It **delivers network route tracing** with performance tests, DNS, Whois, and network resolution to investigate network issues

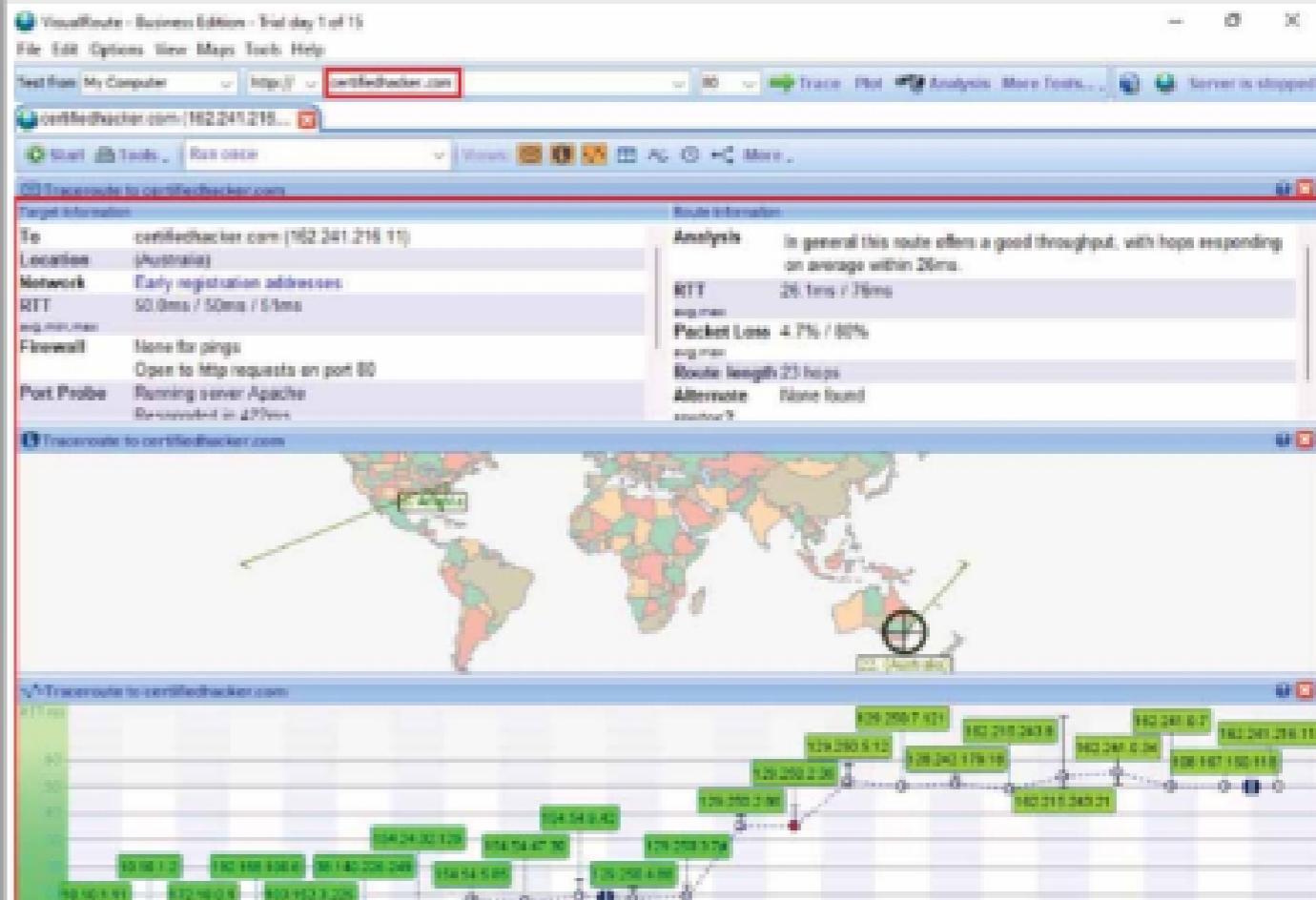


The screenshot shows the Path Analyzer Pro application window. At the top, there's a toolbar with icons for New, Open, Preferences, Export, Check for Location, and Help. Below the toolbar, the target URL is set to "www.google.com". The main interface features a chart showing the path to the target, followed by a detailed table of traceroute results. A callout box points to the table with the text: "Results are viewed in the form of a report".

Hop	IP Address	Hostname	AS#	Network Name	% Loss	Min Latency	Latency	Avg Lat
1	10.0.0.1	10.0.0.1			0.00	0.00	1	1.21
2	172	172			0.00	1.14	1	1.29
3	192	192			0.00	0.45	1	0.45
4	80	80	5000	INCLCAPITAL...	0.00	1.04	1	1.07
5	20	20	174	CLOUDFLARE-A	0.00	2.05	1	2.17
6	174	174	NET-174-24-0-0	0.00	2.14	1	2.22	
7	174	174	NET-174-24-0-0	0.00	0.44	1	0.44	
8	174	174	NET-174-24-0-0	0.00	0.53	1	0.53	
9	174	174	NET-174-24-0-0	0.00	7.09	1	10.45	
10	22	22	15199	GOOGLE	0.00	1.00	1	1.00
11	108	108	15199	GOOGLE	0.00	0.60	1	0.71
12	209	209	15199	GOOGLE	0.00	0.07	1	0.10
13	142.209.108.209		15199	GOOGLE	0.00	0.09	1	0.10

VisualRoute

It is a traceroute and network diagnostic tool that **identifies the geographical location of routers, servers, and other IP devices**



The screenshot shows the VisualRoute application window. At the top, the target URL is set to "http://certifiedchecker.com". The interface includes a toolbar with various tools like Start, Stop, Tools, Run traceroute, and More... Below the toolbar, there are sections for Target Information and Route Information. A world map shows the path taken to the target. A callout box points to the bottom section with the text: "Results are viewed in the form of a report".

Target Information:

- To: certifiedchecker.com (162.241.216.11)
- Location: (Australia)
- Network: Early registration addresses
- RTT: 50.0ms / 50ms / 5ms
- Port Probe: None for pings
Open to http requests on port 80
Running server Apache
Response code 200ms
- Analysis: In general this route offers a good throughput, with hops responding on average within 20ms.

Route Information:

- RTT: 26.1ms / 78ms
- Loss: 4.7% / 80%
- Packet Loss: 4.7% / 80%
- Route Length: 23 hops
- Alternate: None found

LO#10: Demonstrate Footprinting through Social Engineering

Footprinting through Social Engineering

- Social engineering is an art of exploiting human behaviour to **extract confidential information**
- Social engineers depend on the fact that **people are unaware** of their valuable information and are careless about protecting it



Social engineers attempt to gather

- Credit card details and social security number
- Usernames and passwords
- Security products in use
- Operating systems and software versions
- Network layout information
- IP addresses and names of servers



Social engineering techniques include

- Eavesdropping
- Shoulder surfing
- Dumpster diving
- Impersonation



Collecting Information Using Eavesdropping, Shoulder Surfing, Dumpster Diving, and Impersonation

Eavesdropping

- Unauthorized listening of conversations or reading of messages
- It is the interception of any form of communication, such as audio, video, or text



Shoulder Surfing

- Secretly observing the target to gather critical information, such as passwords, personal identification number, account numbers, and credit card information



Dumpster Diving

- Looking for treasure in someone else's trash
- It involves the collection of phone bills, contact information, financial information, operations-related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.



Impersonation

- Pretending to be a legitimate or authorized person and using the phone or other communication medium to mislead targets and trick them into revealing information

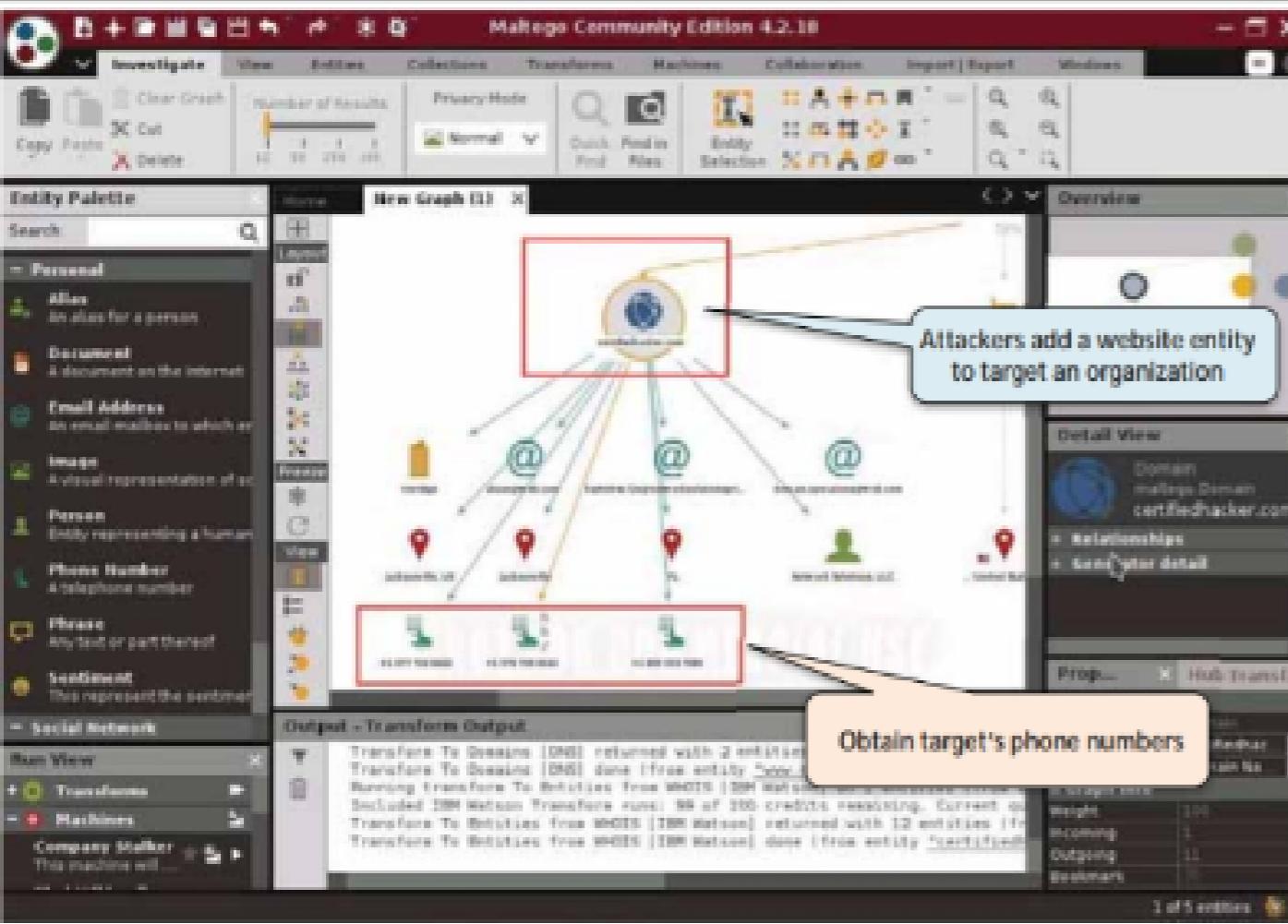


LO#11: Use Various Footprinting Tools

Footprinting Tools: Maltego and Recon-ng

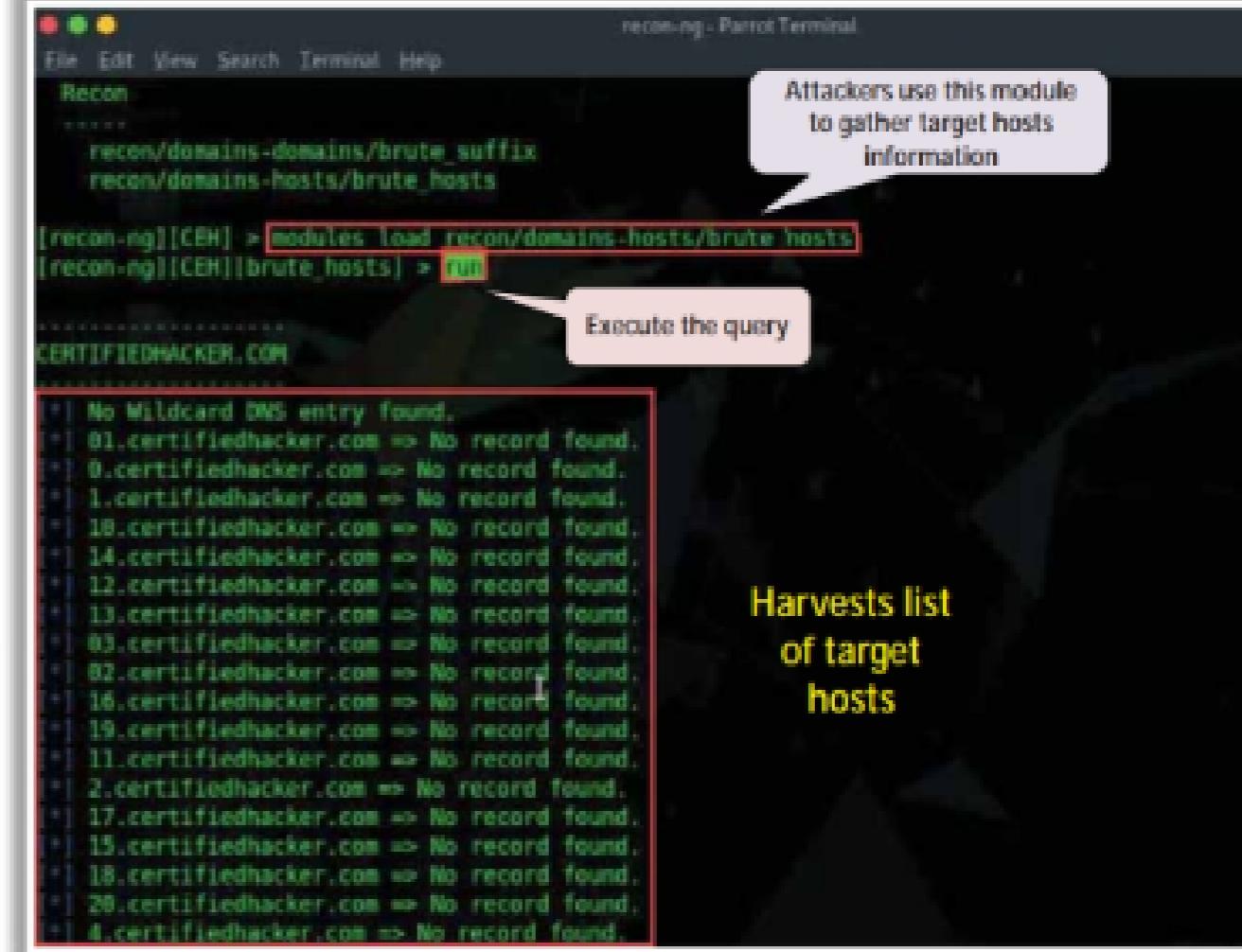
Maltego

Maltego can be used to determine the **relationships and real world links** between people, groups of people, organizations, websites, Internet infrastructure, documents, etc.



Recon-ng

Recon-ng is a **Web Reconnaissance framework** with independent modules and database interaction, which provides an environment in which open source, web-based reconnaissance can be conducted

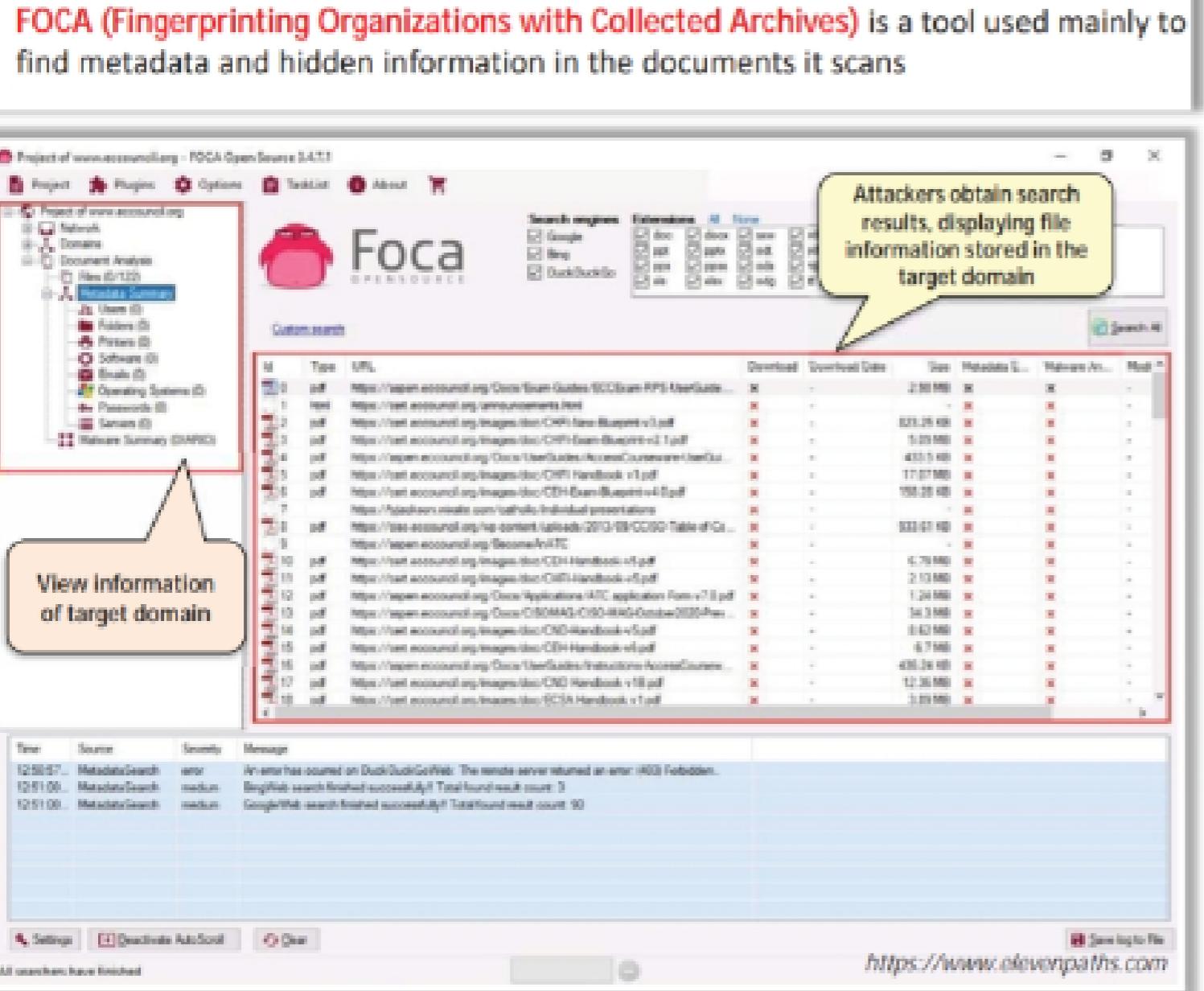


The screenshot shows the Recon module in Recon-ng. A speech bubble says: "Attackers use this module to gather target hosts information". Another bubble says: "Execute the query". The terminal output shows the command: [recon-ng](CEH) > modules load recon/domains-hosts/brute_hosts [recon-ng](CEH)(brute_hosts) > run. The results section displays a list of harvested host entries, each showing a domain name and a status message: "No Wildcard DNS entry found." followed by a list of subdomains from 01 to 40.certifiedhacker.com.

Harvests list
of target
hosts

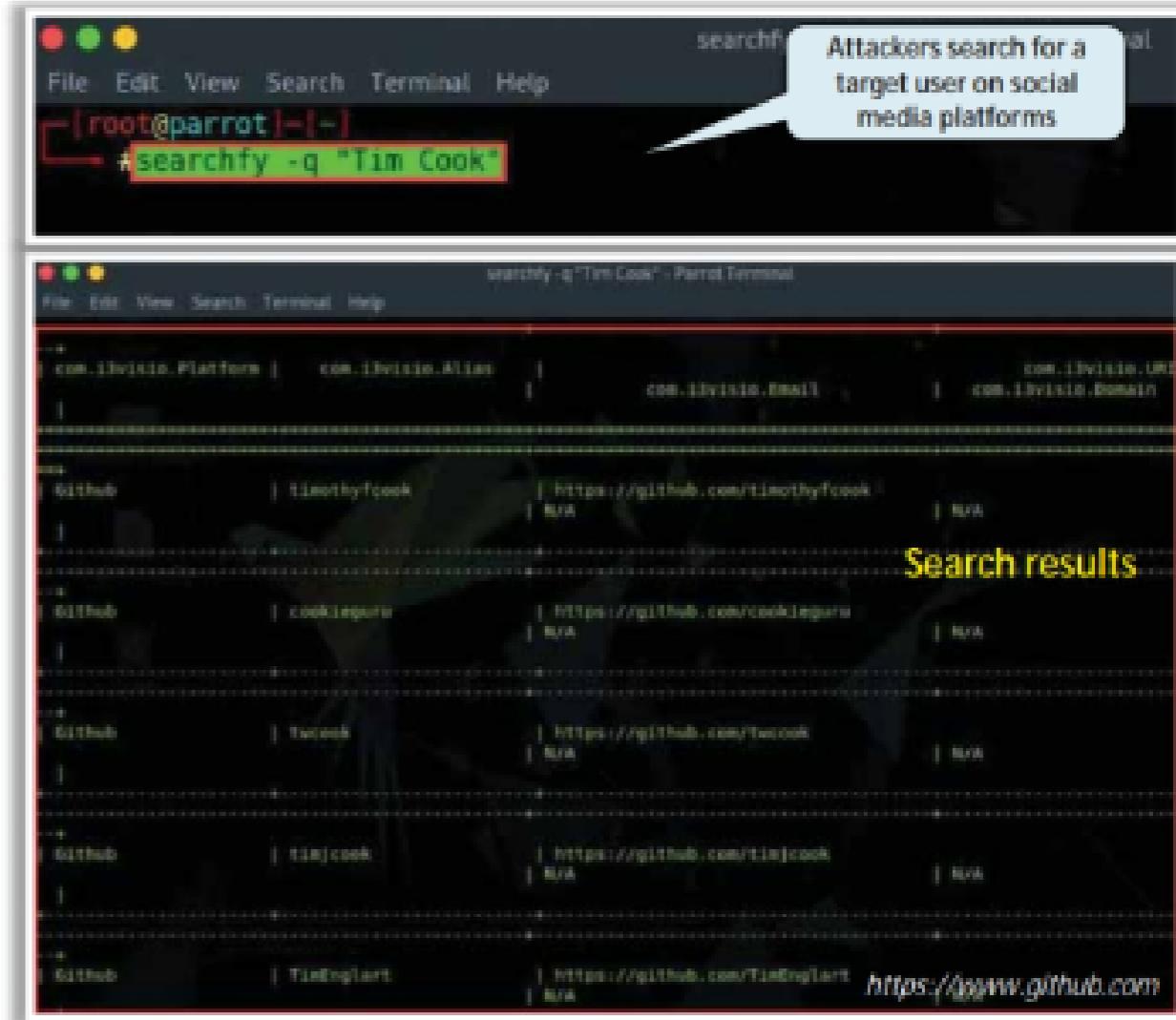
Footprinting Tools: FOCA and OSRFramework

FOCA (Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents it scans



The screenshot shows the FOCA Open Source 2.4.7.1 interface. On the left, there's a sidebar with a red border containing a navigation tree for the target domain `www.accounting.org`. The tree includes sections like Network, Domains, Document Analysis, and File (PDF). A yellow callout box points to this sidebar with the text "View Information of target domain". The main window has tabs for "Search engines", "Extensions", and "File". The "File" tab is selected, showing a table of scanned files with columns for Type, URL, Downloaded, Download Date, Size, Headers, Metadata, and MD5. A yellow callout box points to this table with the text "Attackers obtain search results, displaying file information stored in the target domain". At the bottom, a log table shows search progress: "MetadataSearch" was successful on DuckDuckGoWeb, BingWeb, and GoogleWeb. A yellow callout box points to the log table with the text "An error has occurred on DuckDuckGoWeb: The remote server returned an error: 403 Forbidden". The URL <https://www.elevenpaths.com> is at the bottom right.

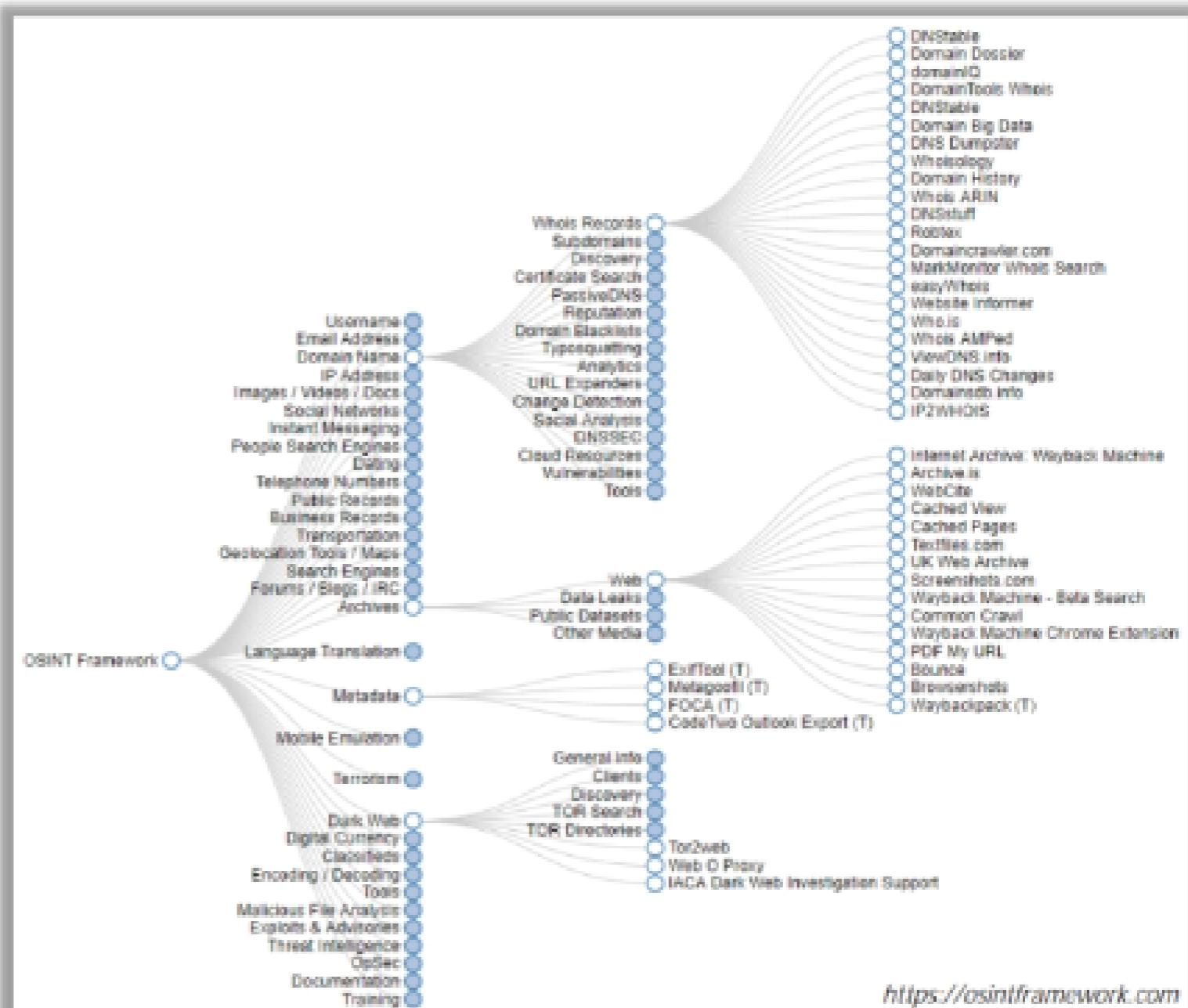
OSRFramework includes applications related to username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction, etc.



The screenshot shows the OSRFramework interface running on a Parrot Linux system. The terminal window shows the command `searchfy -q "Tim Cook"` being run. A yellow callout box points to the terminal with the text "Attackers search for a target user on social media platforms". Below the terminal, several browser windows are open, each showing search results for "Tim Cook" on different platforms: GitHub, LinkedIn, Stack Overflow, and Google. A yellow callout box points to one of the browser tabs with the text "Search results". The URL <https://www.github.com> is at the bottom right.

Footprinting Tools: OSINT Framework

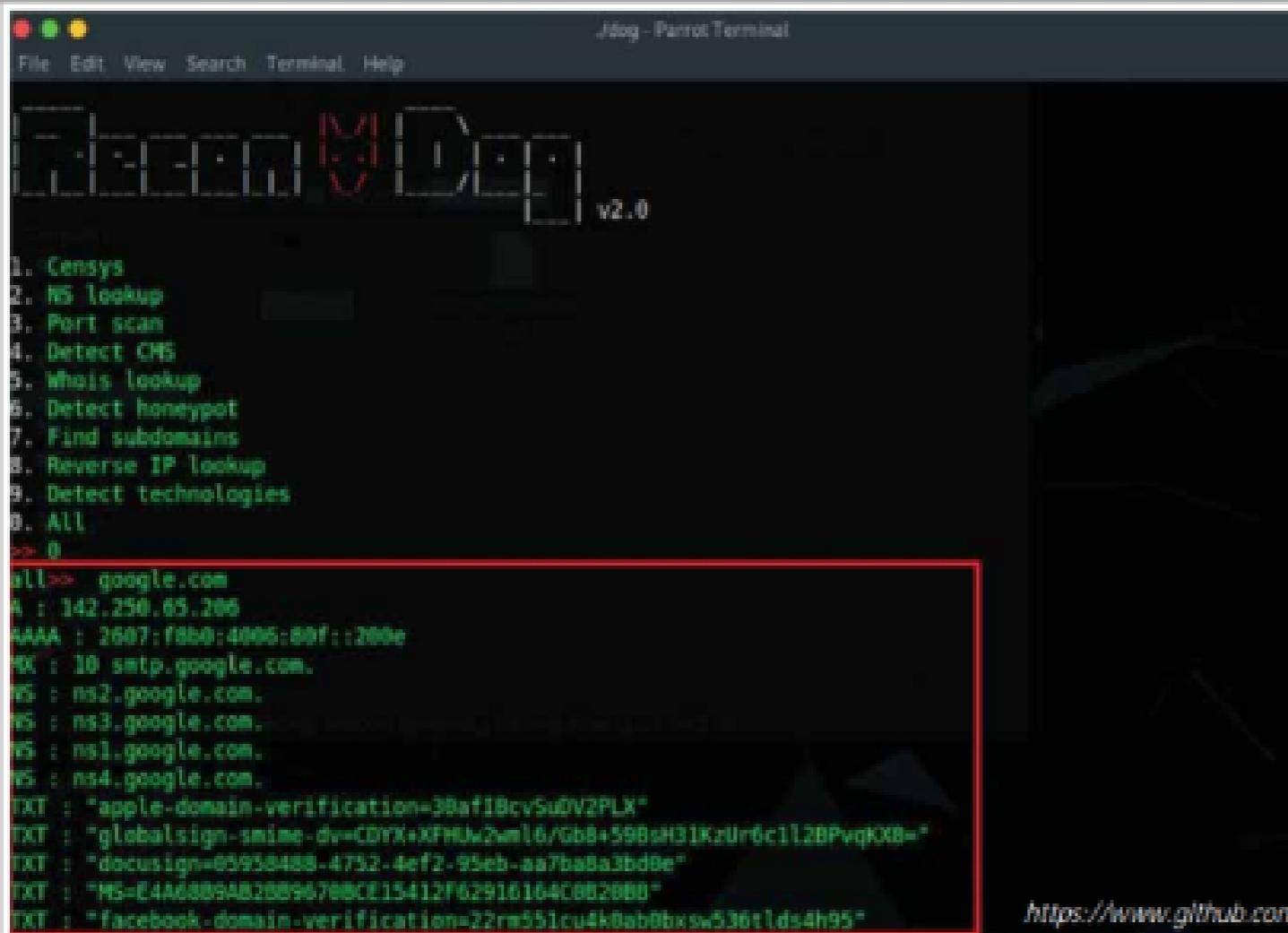
- OSINT Framework is an **open source intelligence gathering framework** that is focused on gathering information from free tools or resources
- It provides a simple web interface that lists various OSINT tools arranged by categories and is shown as **OSINT tree structure** on the web interface
- Tools listed includes the following indicators:
 - (T) - Indicates a link to a tool that must be installed and run locally
 - (D) - Google Dork
 - (R) - Requires registration
 - (M) - Indicates a URL that contains the search term and the URL itself must be edited manually



Footprinting Tools: Recon-Dog and BillCipher

Recon-Dog

- Recon-Dog is an **all-in-one tool** for information gathering needs, which uses APIs to collect information about the target system



Jdog - Parrot Terminal

```

File Edit View Search Terminal Help
[REDACTED] v2.0
1. Censys
2. NS lookup
3. Port scan
4. Detect CMS
5. Whois lookup
6. Detect honeypot
7. Find subdomains
8. Reverse IP lookup
9. Detect technologies
0. All
>> 0
all>> google.com
A : 142.250.65.206
AAAA : 2607:fabb:4000:80f::206
MX : 10 smtp.google.com.
NS : ns2.google.com.
NS : ns3.google.com.
NS : ns1.google.com.
NS : ns4.google.com.
TXT : "apple-domain-verification=39af18cvSu0V2PLX"
TXT : "globalsign-smime-dv=CDYXxXFHw2wml6/Gb8+598wH3KzUr6c1128PvkX8="
TXT : "docusign-ssime-dv=CDYXxXFHw2wml6/Gb8+598wH3KzUr6c1128PvkX8="
TXT : "MS=E4Ae889AB2B996788C115412F629161640882880"
TXT : "facebook-domain-verification=22rw551ou4k8ab0bxsw536t1ds4h95"

```

<https://www.github.com>

BillCipher

- BillCipher is an information gathering tool for a **website or IP address**



python3 billcipher.py - Parrot Terminal

```

# # # # #
***** 2.1
Information Gathering tool for a Website or IP address

Are you want to collect information of website or IP address? [website/IP]: website
Enter the website address: www.certifiedhacker.com

1) DNS Lookup          13) Host DNS Finder
2) Whois Lookup         14) Reserve IP Lookup
3) GeoIP Lookup         15) Email Gathering (use Infoga)
4) Subnet Lookup        16) Subdomain listing (use Sublist3r)
5) Port Scanner         17) Find Admin login site (use Breacher)
6) Page Links           18) Check and Bypass CloudFlare (use HttCloud)
7) Zone Transfer        19) Website Copier (use httrack)
8) HTTP Header          20) Host Info Scanner (use WhatWeb)
9) Host Finder          21) About BillCipher
10) IP-Locator          22) Fuck Out Of Here (Exit)
11) Find Shared DNS Servers
12) Get Robots.txt

what information would you like to collect? (1-20): 1
A : 162.241.216.11
MX : 0 mail.certifiedhacker.com.
NS : ns2.bluehost.com.
NS : ns1.bluehost.com.
TXT : "y=spfl a mx ptr include:bluehost.com ?all"
CNAME : certifiedhacker.com.
SOA : ns1.bluehost.com. dnsadmin.box5331.bluehost.com. 2018011203 80400 7200 3600000 300

Do you want to continue? [Yes/No]: Yes

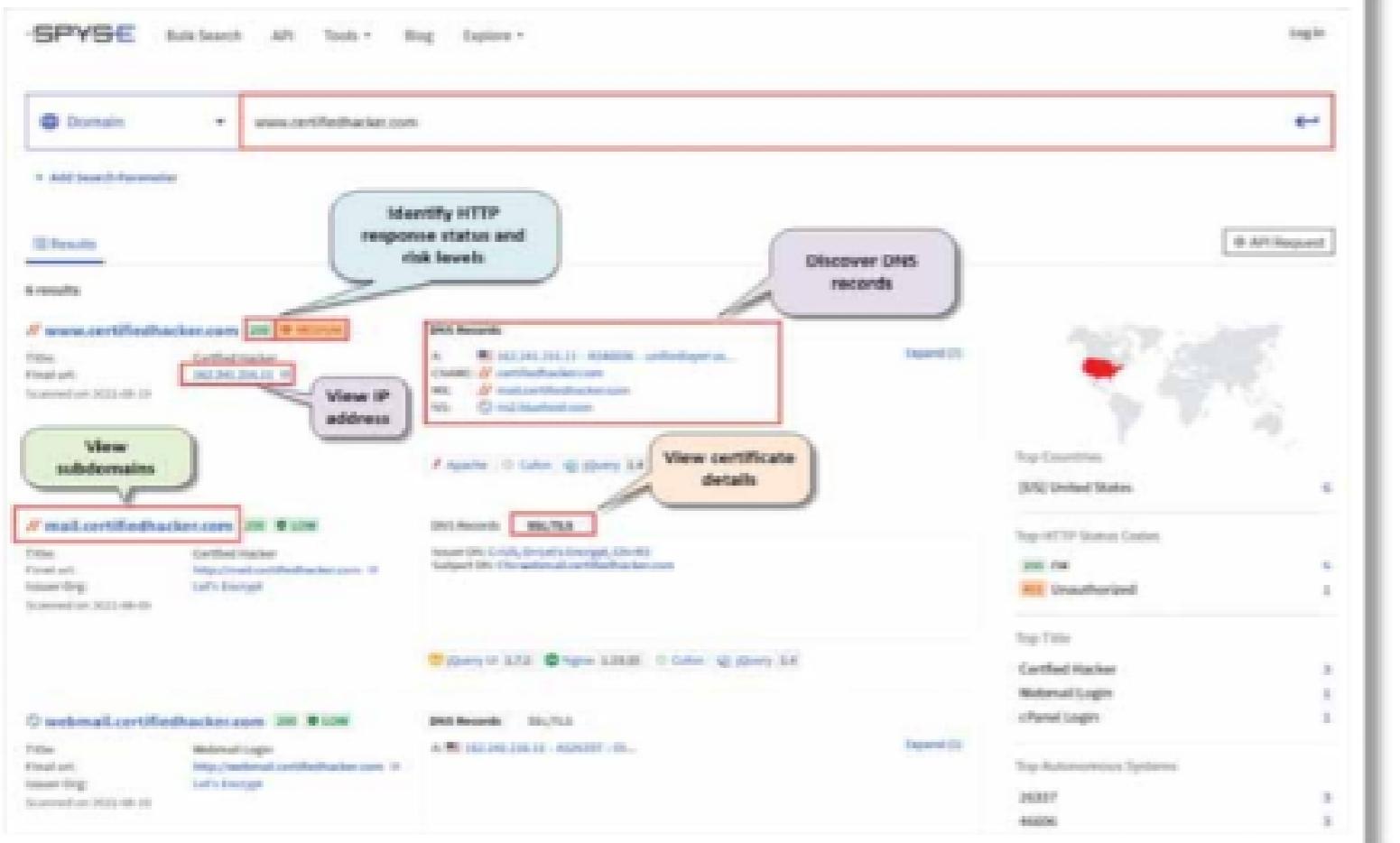
```

<https://github.com>

Footprinting Tools...

Spyse

Attackers can use different **parameters** available in this tool to identify information such as **subdomains**, **certificates**, and **vulnerabilities risk scores**



The screenshot shows the Spyse web interface with the URL www.certifethacker.com entered in the search bar. The results page displays several subdomains and their details:

- www.certifethacker.com**: IP address 192.168.200.11, status 200 OK, last seen 2023-08-01. Options: View IP address, View certificate details.
- mail.certifethacker.com**: IP address 192.168.200.10, status 200 OK, last seen 2023-08-01. Options: View subdomains.
- semail.certifethacker.com**: IP address 192.168.200.10, status 200 OK, last seen 2023-08-01. Options: View subdomains.
- www2.certifethacker.com**: IP address 192.168.200.10, status 200 OK, last seen 2023-08-01. Options: View subdomains.

On the right side, there are summary statistics and a world map:

- Top Countries**: United States (95%)
- Top HTTP Status Codes**: 200 (OK) 94%, 404 (Not Found) 5%
- Top Titles**: Certified Hacker, Material Usage, cPanel Usage
- Top Autonomous Systems**: 192.168.200.0/24, 192.168.0.0/24



Grecon

<https://github.com>



theHarvester

<http://www.edge-security.com>



Th3Inspector

<https://github.com>



Raccoon

<https://github.com>



Orb

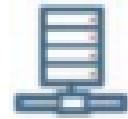
<https://github.com>

LO#12: Explain Footprinting Countermeasures

Footprinting Countermeasures



Restrict the employees' access to social networking sites from the organization's network



Configure web servers to avoid information leakage



Educate employees to use pseudonyms on blogs, groups, and forums



Do not reveal critical information in press releases, annual reports, product catalogues, etc.



Limit the amount of information published on a website or the Internet



Use footprinting techniques to discover and remove any sensitive information that is publicly available



Prevent search engines from caching a web page and use anonymous registration services

Footprinting Countermeasures...

- 1 Develop and enforce security policies to regulate the information that employees can reveal to third parties
- 2 Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers
- 3 Disable directory listings in the web servers
- 4 Conduct security awareness training periodically to educate employees about various social engineering tricks and risks
- 5 Opt for privacy services on a Whois Lookup database
- 6 Avoid domain-level cross-linking for critical assets
- 7 Encrypt and password-protect sensitive information
- 8 Place critical documents, such as business plans and proprietary documents offline to prevent exploitation
- 9 Train employees to thwart social engineering techniques and attacks
- 10 Sanitize the details provided to Internet registrars to hide the direct contact details of the organization
- 11 Disable the geo-tagging functionality on cameras to prevent geolocation tracking
- 12 Avoid revealing one's location or travel plans on social networking sites
- 13 Turn off geolocation access on all mobile devices when not required
- 14 Ensure that no critical information is displayed on notice boards or walls



DIGITAL
UNIVERSITY
KERALA

Curating a responsible digital world