Module 02

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

Objective 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

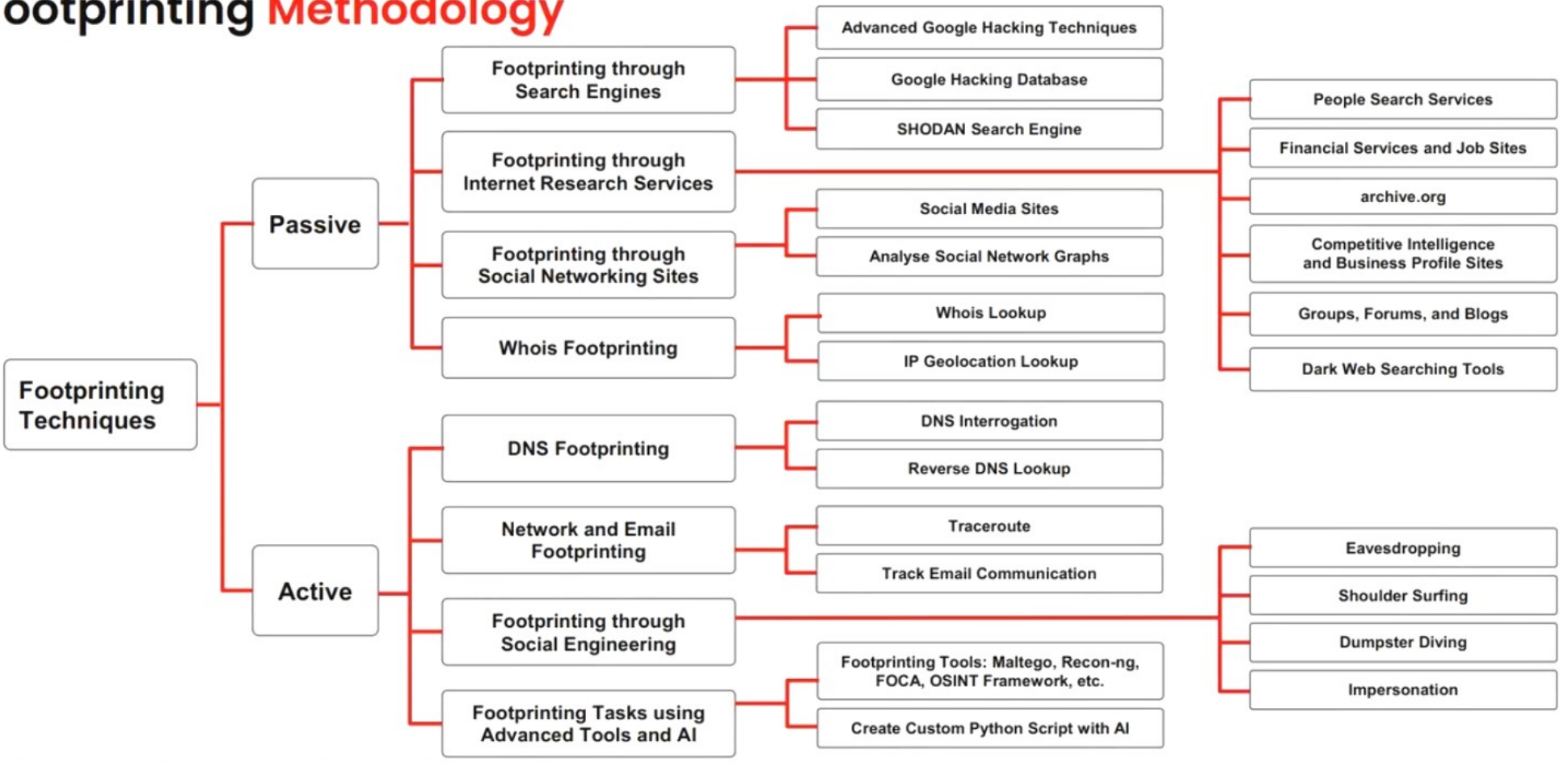
Network information

- 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



Objective 02

Demonstrate Footprinting through Search Engines

Passive Reconnaissance

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

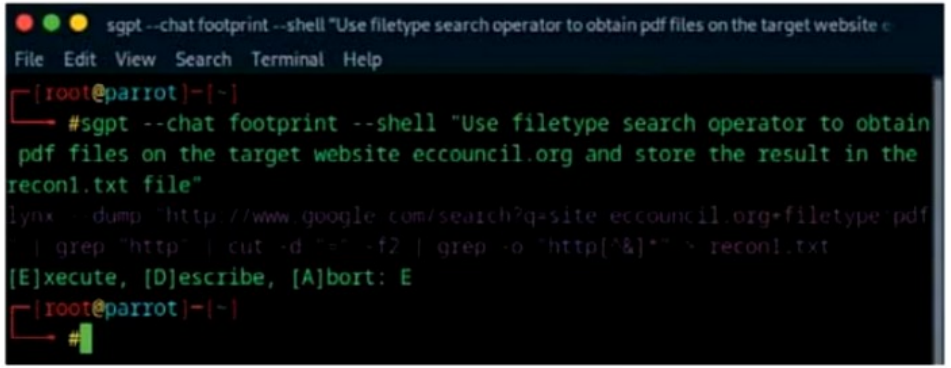
Search Operator	Purpose
[cache:]	Displays the web pages stored in the Google cache
[link:]	Lists web pages that have links to the specified web page
[related:]	Lists web pages that are similar to the specified web page
[info:]	Presents some information that Google has about a particular web page
[site:]	Restricts the results to those websites in the given domain

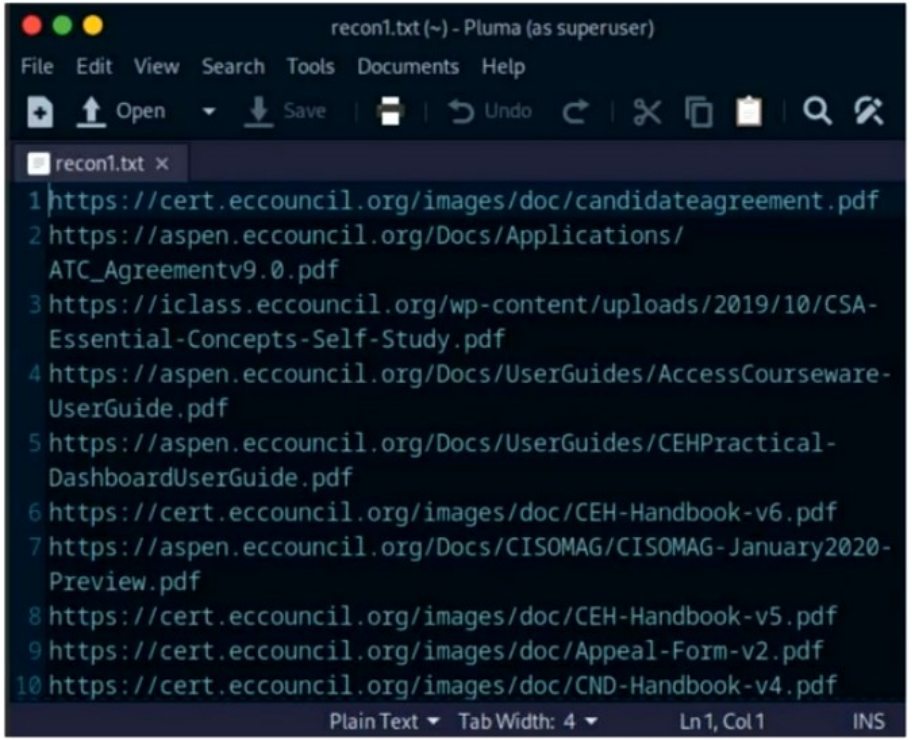
Search Operator	Purpose
[allintitle:]	Restricts the results to those websites containing all the search keywords in the title
[intitle:]	Restricts the results to documents containing the search keyword in the title
[allinurl:]	Restricts the results to those containing all the search keywords in the URL
[inurl:]	Restricts the results to documents containing the search keyword in the URL
[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:

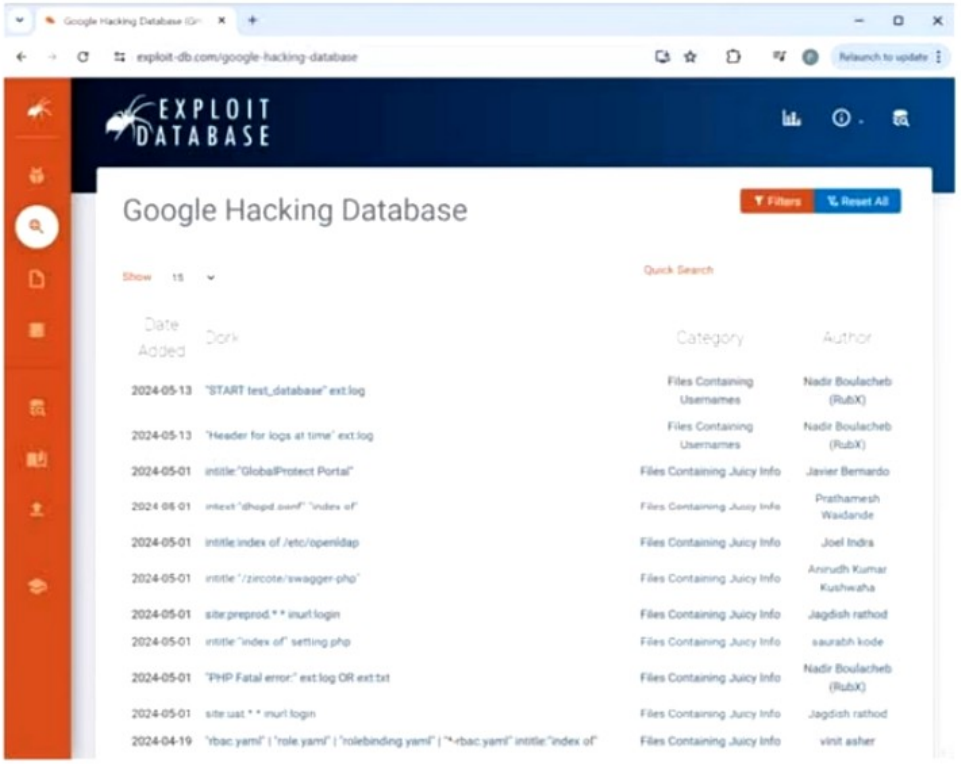
  "Use filetype search operator to obtain pdf files on the target website eccouncil.org and store the result in the recon1.txt file"





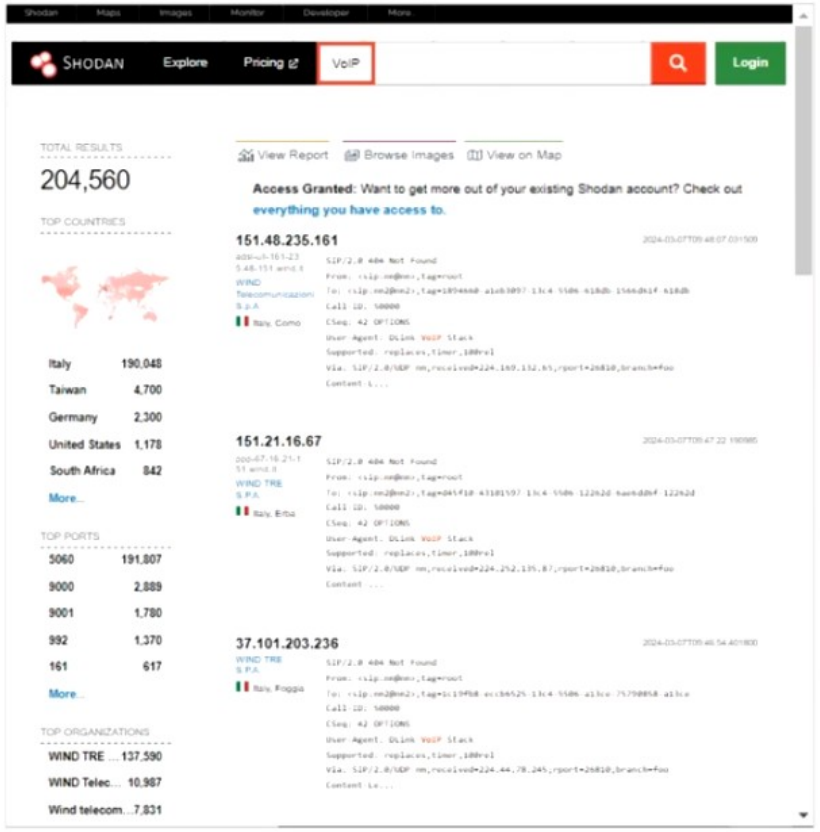
Google Hacking Database

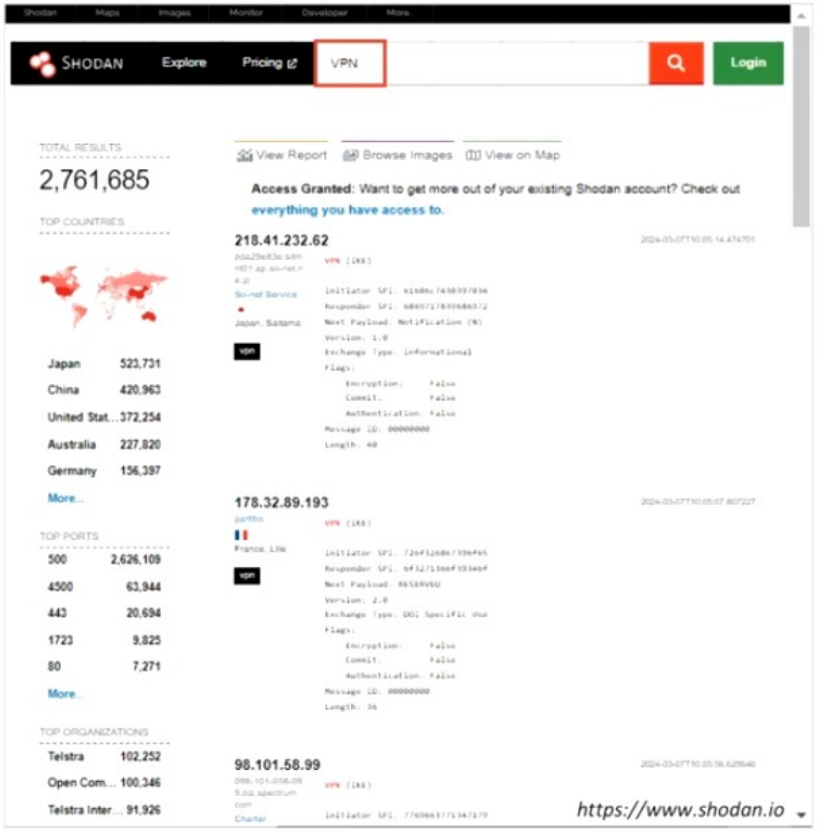
- The Google Hacking Database (GHDB) is an authoritative source for **querying the ever-widening reach of the Google search engine**
- Attackers use **Google dorks** in Google advanced search operators to extract sensitive information about their target, such as exposed files, directories, and devices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



https://www.exploit-db.com/google-hacking-database

Footprinting through SHODAN Search Engine





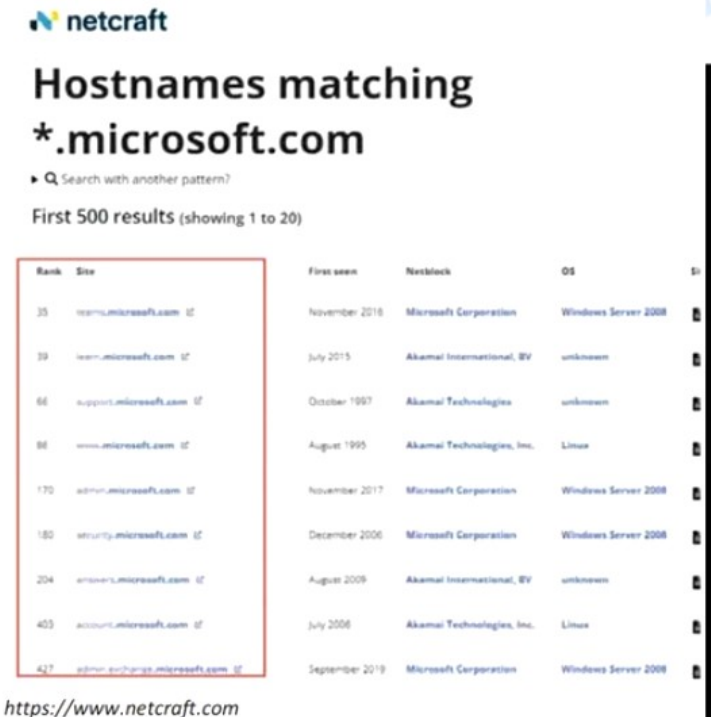
Objective 03

Demonstrate Footprinting through Internet Research Services

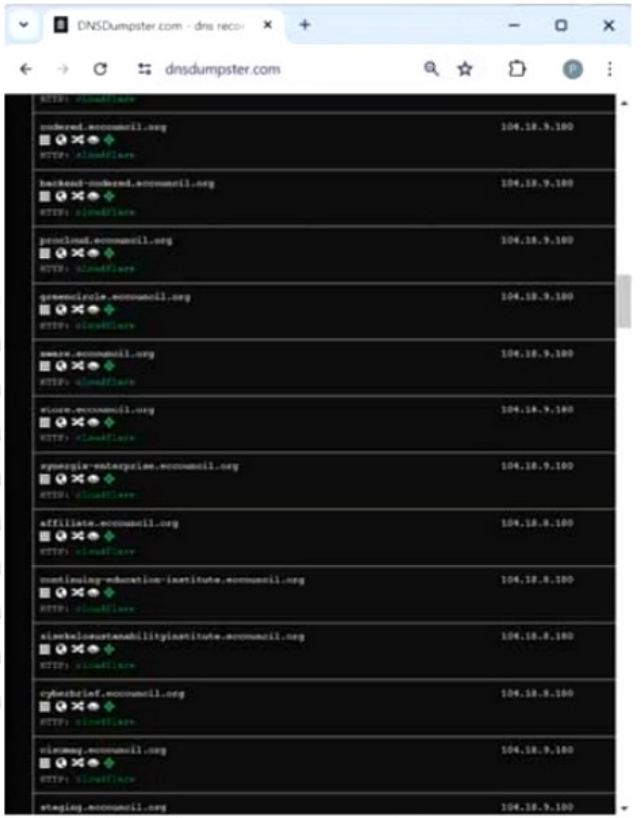
Passive Reconnaissance

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 **DNSdumpster** tool, which can discover hosts related to a domain



https://www.netcraft.com

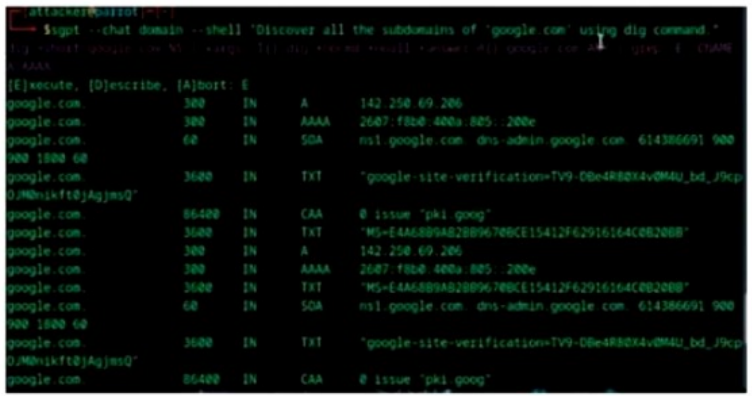


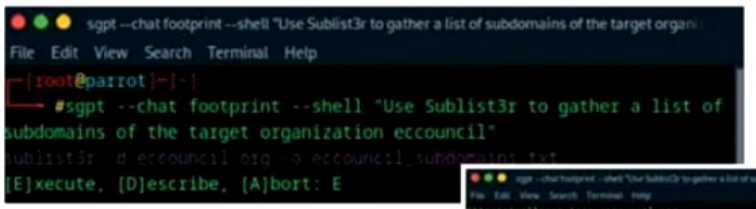
https://dnsdumpster.com

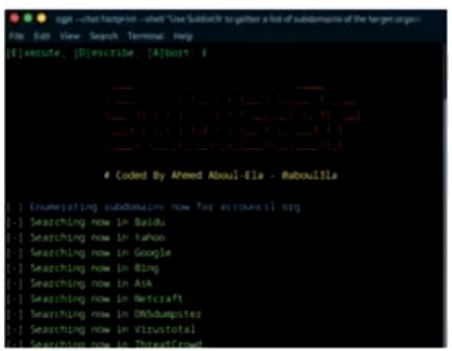
Finding a Company's Top-Level Domains (TLDs) and Sub-domains with AI

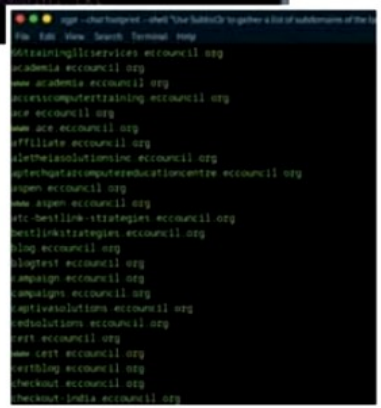
An attacker can also leverage **AI-powered ChatGPT** or other generative AI technology to perform this task by using appropriate prompts such as

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"***



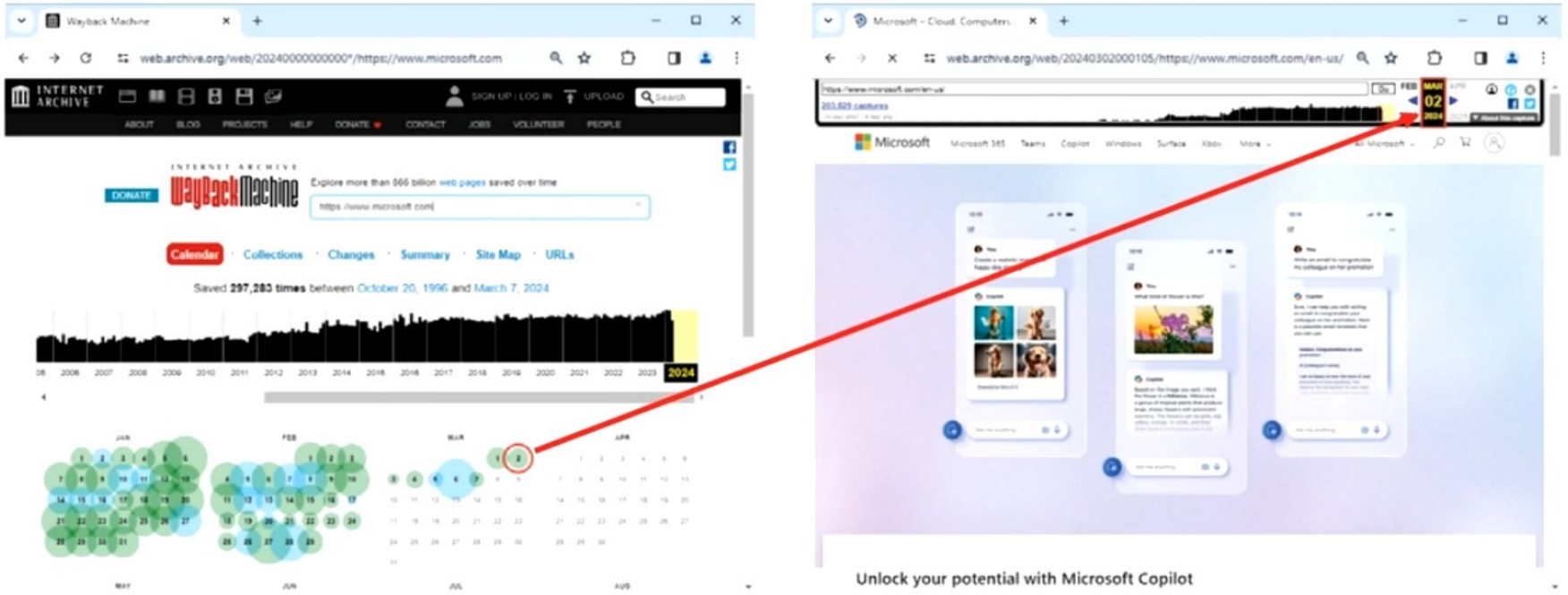






Extracting Website Information from https://archive.org

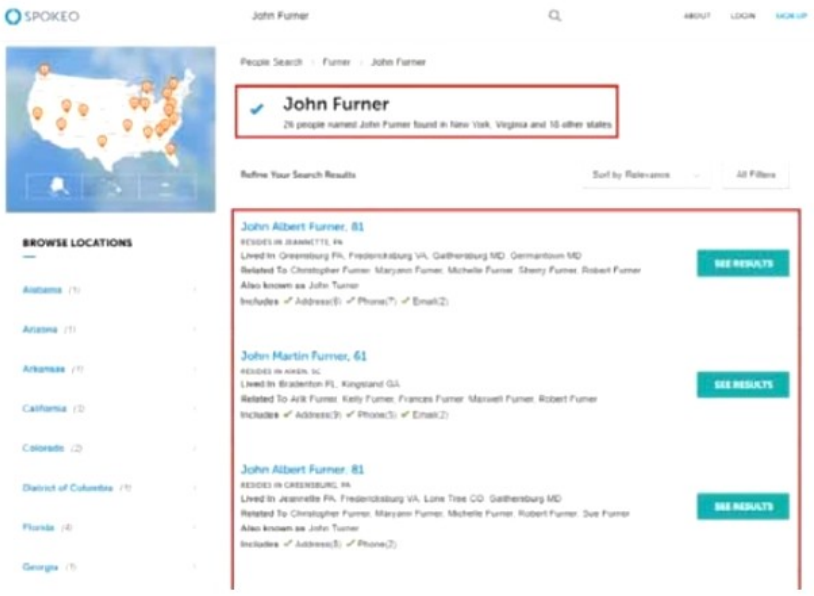
- Internet Archive's Wayback Machine allows one to visit **archived versions of websites**



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

Footprinting through People Search Services and Job Sites

- People search services, such as **Spokeo**, **Intelius**, and **pipl** can provide critical **information about a person or an organization**, including location, emails, websites, blogs, contacts, important dates, address, etc.



https://www.spokeo.com

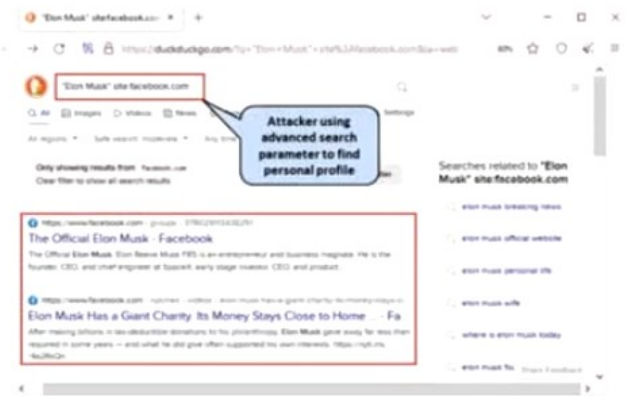
- Job sites such as Dice, LinkedIn, and Glassdoor can reveal details about a **company's infrastructure**, potentially aiding attackers in **identifying vulnerabilities within the target's IT environment**

https://www.glassdoor.com

Dark Web Footprinting

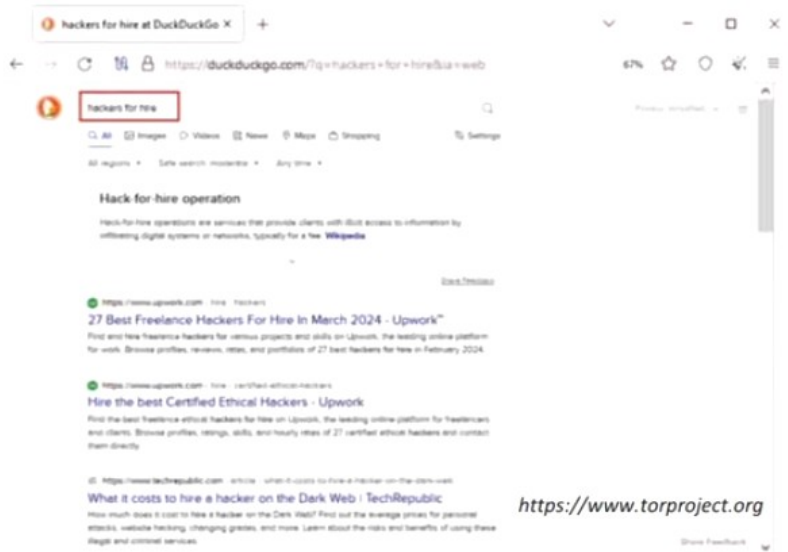
Dark web or Darknet

- The dark web or Darknet is a deeper layer of the online cyberspace, that enables anyone to **navigate anonymously without being traced**
- Attackers use dark web searching tools, such as **Tor Browser** and **ExoneraTor**, to **gather confidential information about the target**
- Attackers can also **use advanced search parameters to refine searches in the Dark Web** to find specific data



TOR Browser

It is used to access the 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



https://www.torproject.org

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

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

Other Techniques for Footprinting through Internet Research 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, X 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 LinkedIn Groups
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

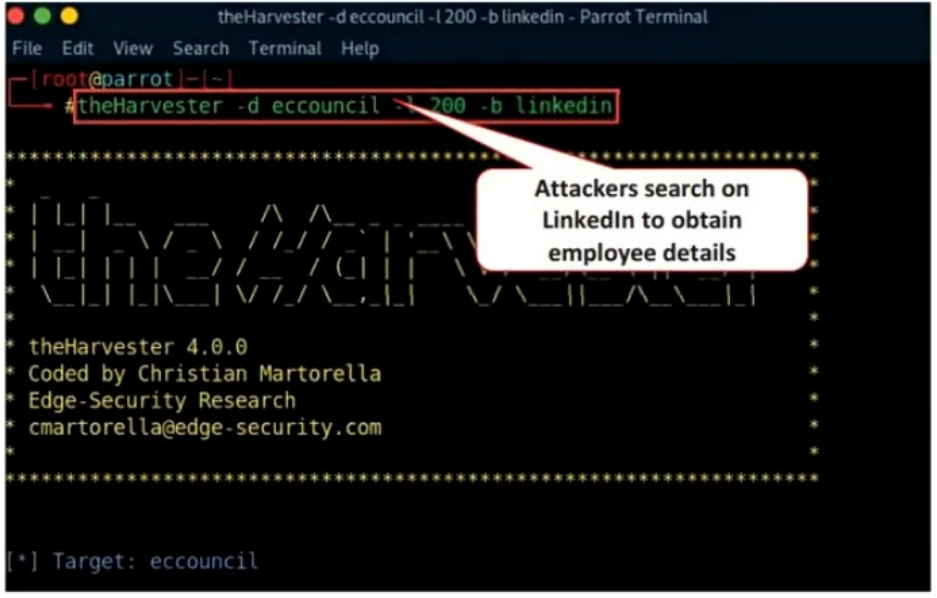
Objective 04

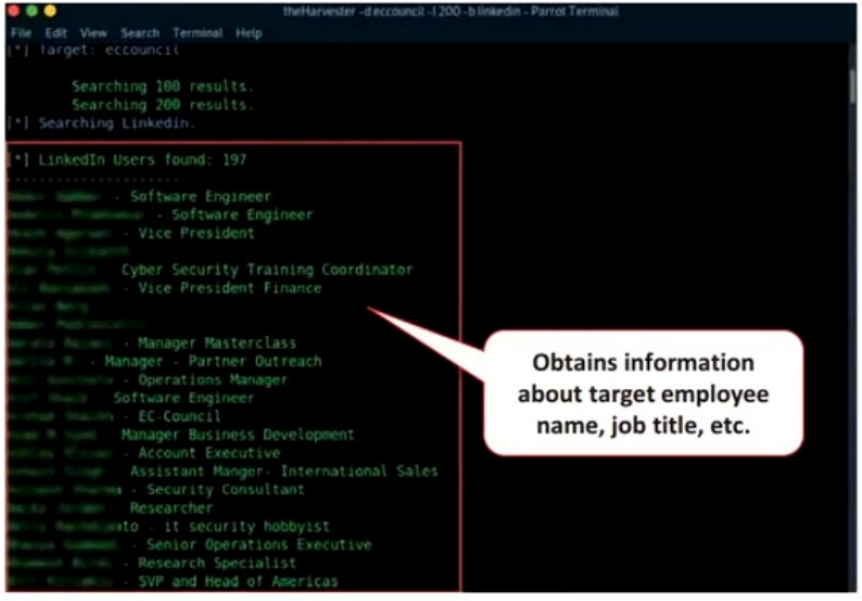
Demonstrate Footprinting through Social Networking Sites

Passive Reconnaissance

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





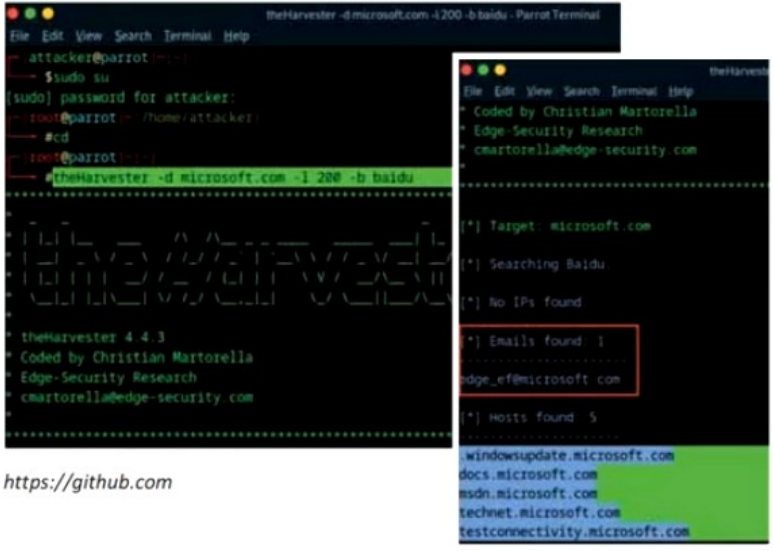
https://github.com

Harvesting Email Lists with AI

- 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

- 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 theHarvester to gather email accounts associated with microsoft.com, limiting results to 200, and leveraging 'baidu' as a data source"



https://github.com

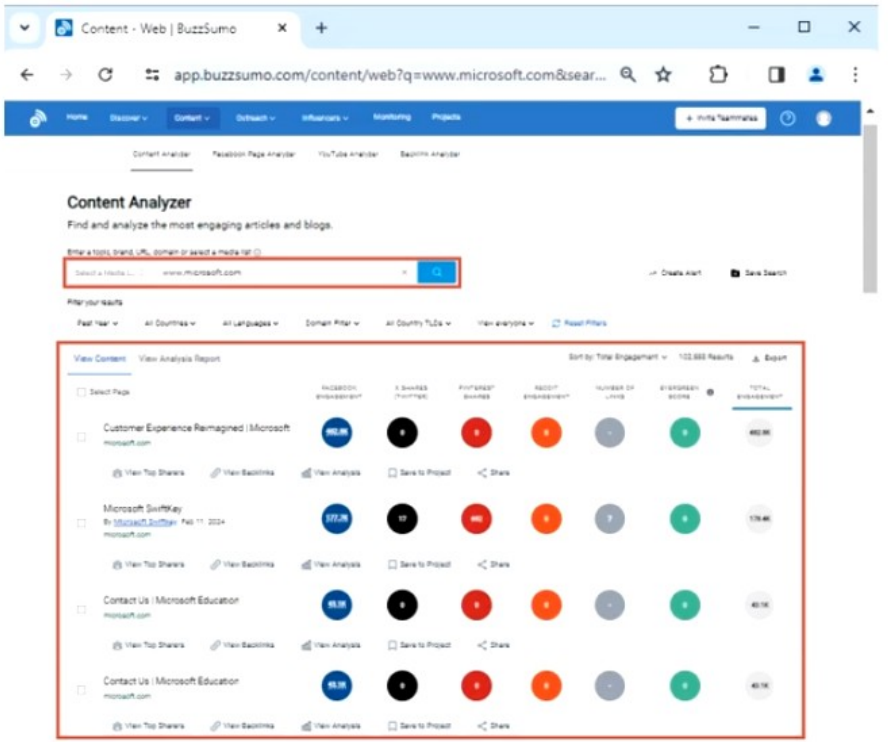
Analyzing Target Social Media Presence

- 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

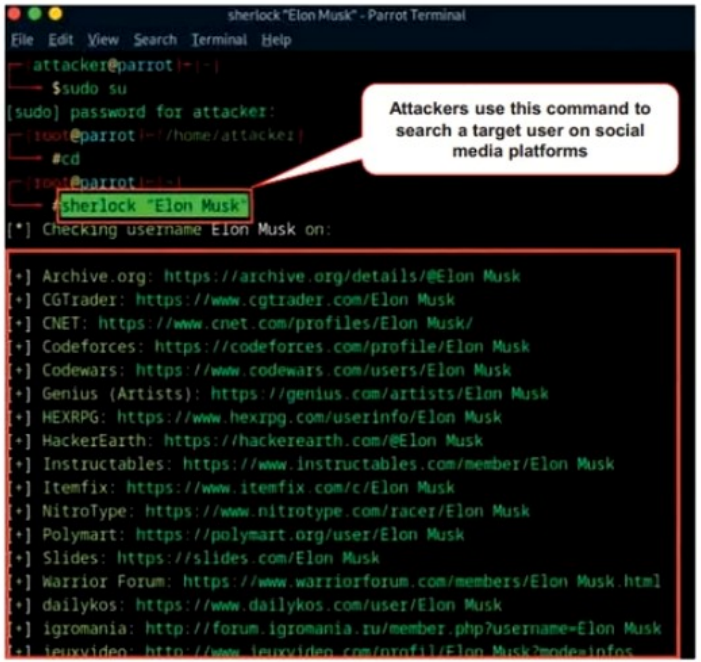


https://buzzsumo.com

Tools for Footprinting through Social Networking Sites

Sherlock

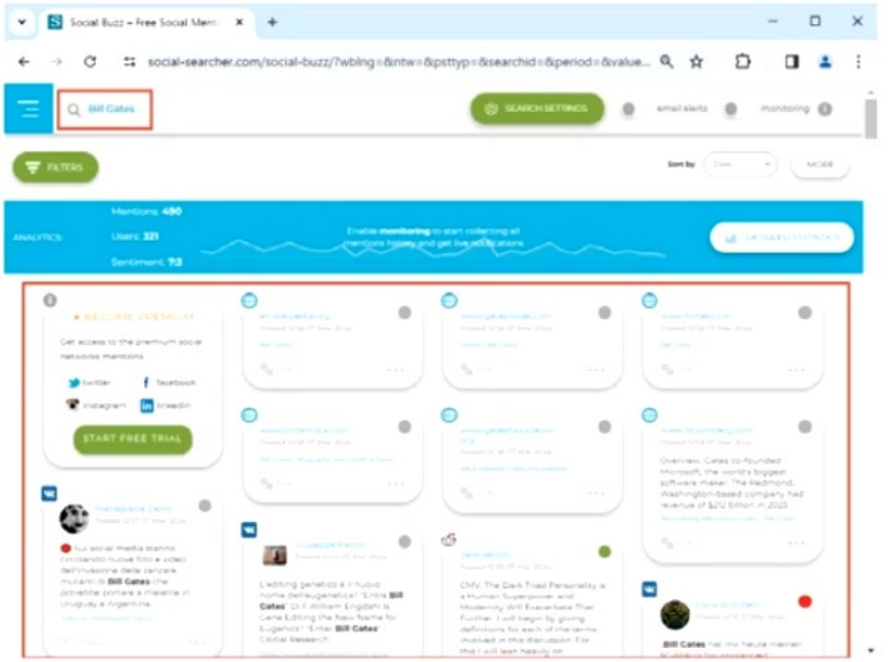
Sherlock tool is used to **search a vast number of social networking sites** for a target username



https://github.com

Social Searcher

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

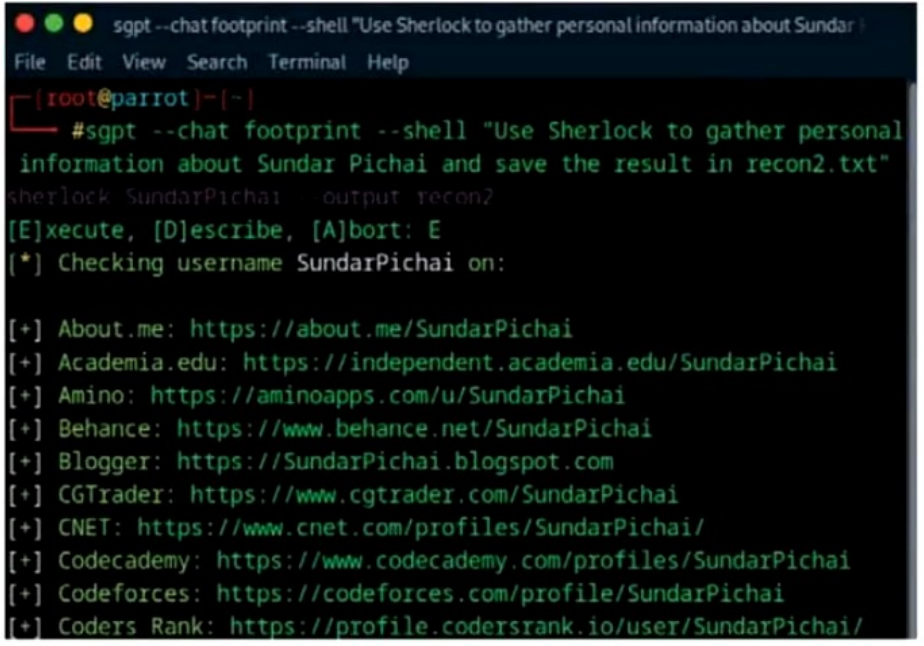


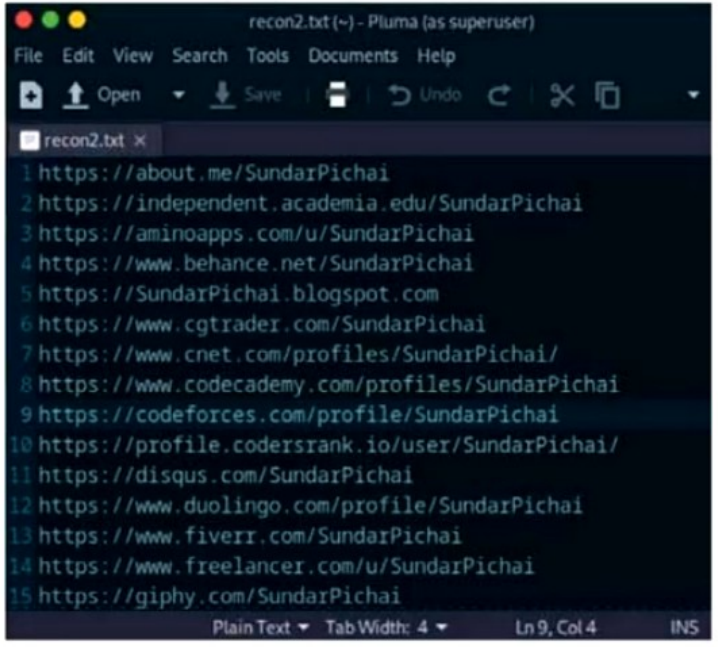
https://www.social-searcher.com

Footprinting through Social Networking Sites 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 Sherlock to gather personal information about Sundar Pichai and save the result in recon2.txt"





Objective 05

Use Different Techniques for Whois Footprinting

Passive Reconnaissance

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)

ARIN
American Registry for Internet Numbers

AFRINIC

RIPE NCC

lacnic

APNIC

Whois Lookup (Cont'd)

Whois Record for CertifiedHacker.com

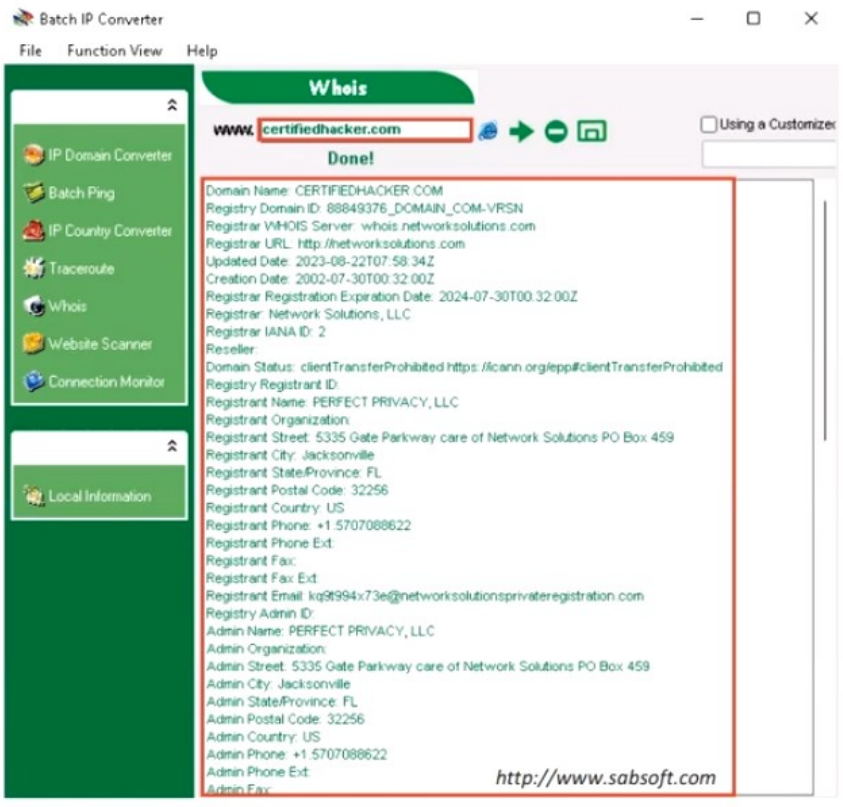
Domain Profile

Registrar	Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com domain.operations@web.com (p) +1.8777228662
Registrar Status	clientTransferProhibited
Dates	7,897 days old Created on 2002-07-30 Expires on 2024-07-30 Updated on 2023-08-22
Name Servers	NS1.BLUEHOST.COM (has 2,349,716 domains) NS2.BLUEHOST.COM (has 2,349,716 domains)
IP Address	162.241.216.11 - 1,299 other sites hosted on this server
IP Location	Utah - Provo - Unified Layer
ASN	AS46606 UNIFIEDLAYER-AS-1, US (registered Oct 24, 2008)
Domain Status	Registered And No Website
IP History	13 changes on 13 unique IP addresses over 10 years
Registrar History	3 registrars with 3 drops
Hosting History	6 changes on 4 unique name servers over 21 years

Whois Record (last updated on 2024-03-13)

```
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2023-08-22T07:58:54Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date: 2024-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
```

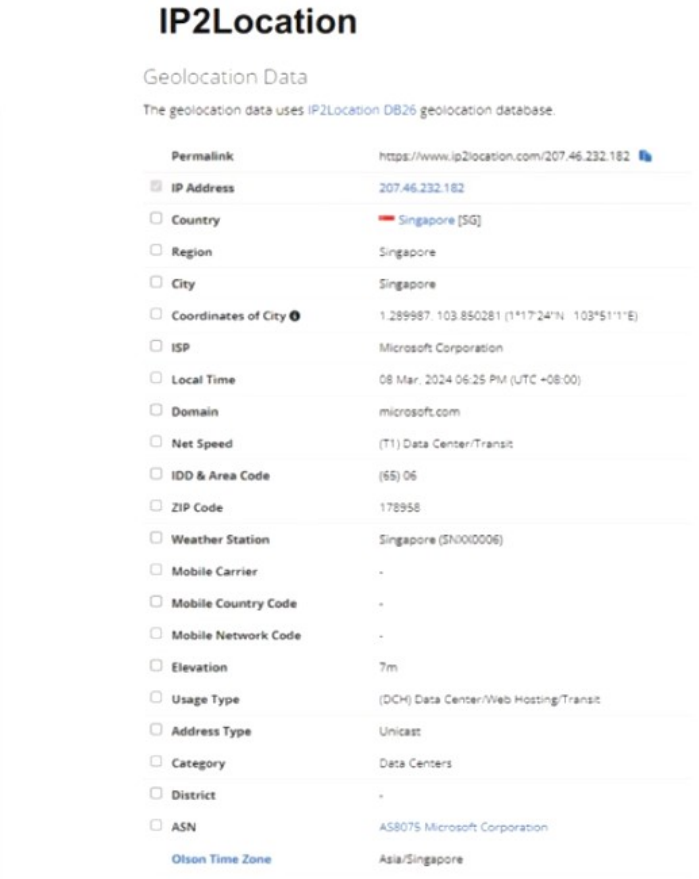
http://whois.domaintools.com



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



https://www.ip2location.com

Objective 06

Use Different Techniques for DNS Footprinting

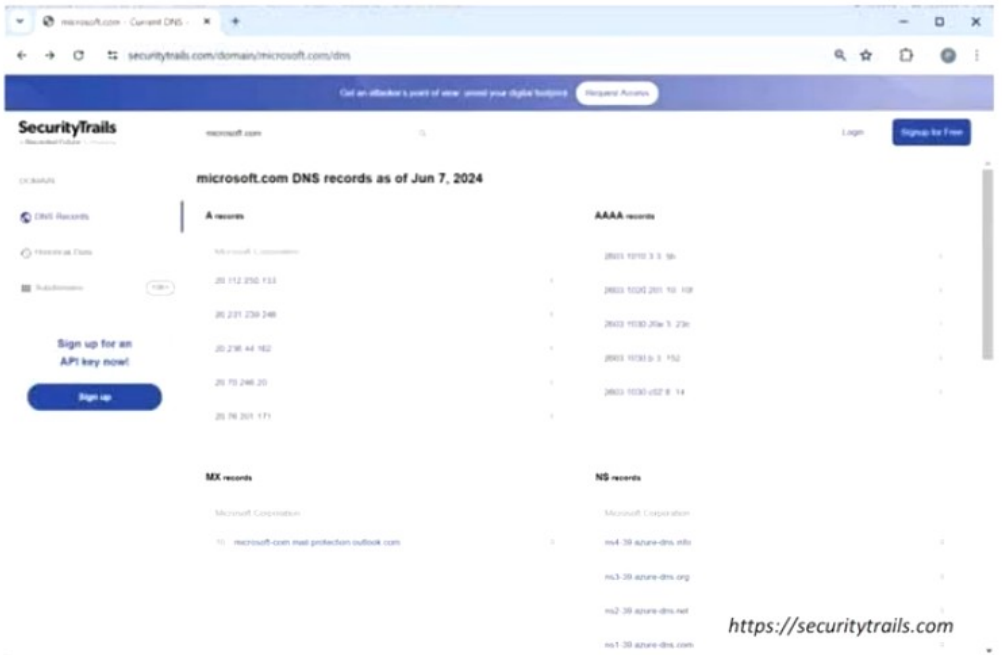
Active Reconnaissance

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

Record Type	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for a domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

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



DNS Lookup 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

"Install and use DNSRecon to perform DNS enumeration on the target domain www.certifiedhacker.com"

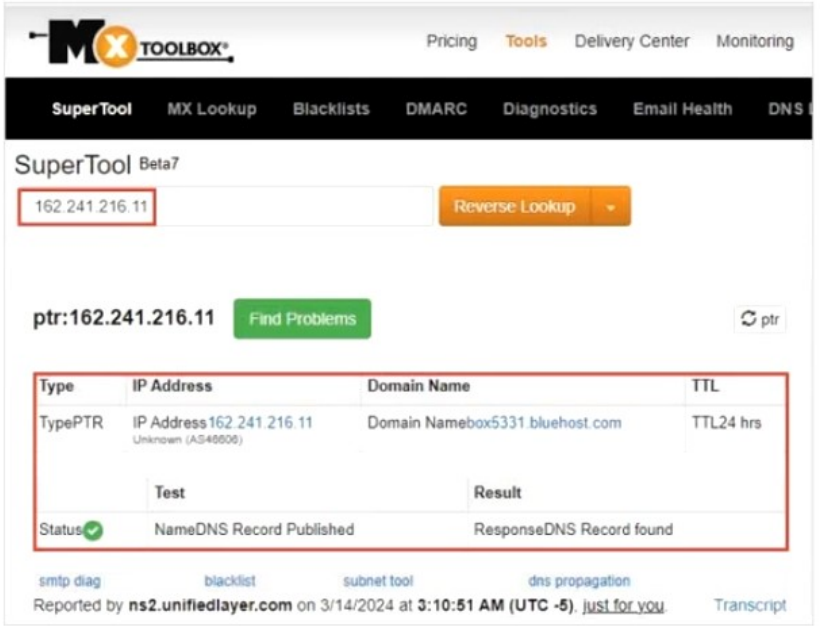
```
┌──[root@parrot]─[/home/attacker]
└─── #sgpt --chat domain --shell "Install and use DNSRecon to perform DNS enumeration on the target
domain www.certifiedhacker.com."
sudo apt-get update && sudo apt-get install -y dnsrecon && dnsrecon -d certifiedhacker.com -t std
[E]xecute, [D]escribe, [A]bort: E
Hit:1 https://deb.parrot.sh/parrot lory InRelease
Hit:2 https://deb.parrot.sh/direct/parrot lory-security InRelease
Hit:3 https://deb.parrot.sh/parrot lory-backports InRelease
Reading package lists... Done
```

```
[*] std: Performing General Enumeration against: certifiedhacker.com...
[-] DNSSEC is not configured for certifiedhacker.com
[*]     SOA ns1.bluehost.com 162.159.24.80
[*]     NS ns1.bluehost.com 162.159.24.80
[*]     Bind Version for 162.159.24.80 "2024.2.2"
[*]     NS ns2.bluehost.com 162.159.25.175
[*]     Bind Version for 162.159.25.175 "2024.2.2"
[*]     MX mail.certifiedhacker.com 162.241.216.11
[*]     A certifiedhacker.com 162.241.216.11
[*]     TXT certifiedhacker.com v=spf1 a mx ptr include:bluehost.com ?all
```

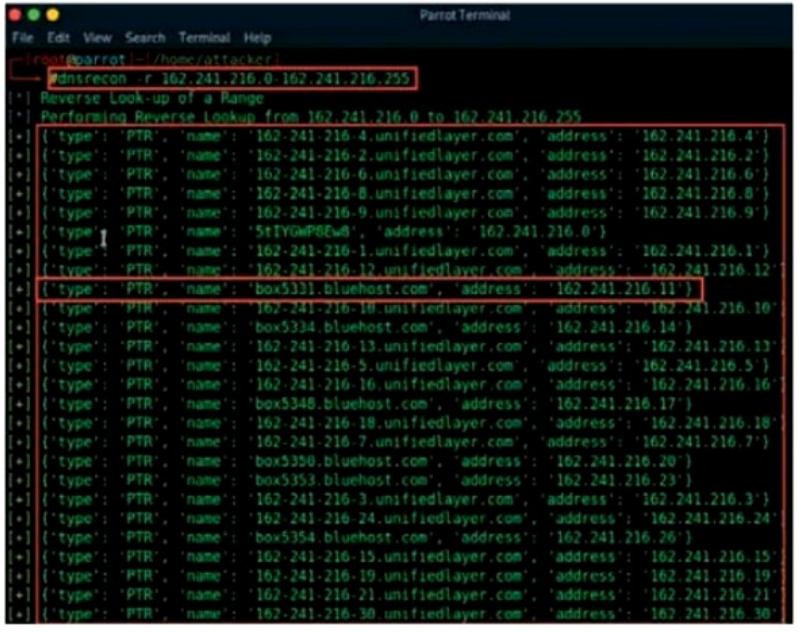
```
[*] Enumerating SRV Records
[+]     SRV _caldav._tcp.certifiedhacker.com box5331.bluehost.com 162.241.216.11 2079
[+]     SRV _caldavs._tcp.certifiedhacker.com box5331.bluehost.com 162.241.216.11 2080
[+]     SRV _carddavs._tcp.certifiedhacker.com box5331.bluehost.com 162.241.216.11 2080
[+]     SRV _carddav._tcp.certifiedhacker.com box5331.bluehost.com 162.241.216.11 2079
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 52.96.166.72 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 52.96.121.24 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 52.96.164.200 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 52.96.165.8 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 52.96.121.56 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 52.96.223.56 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 40.97.205.8 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 52.96.113.232 443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 2603:1036:308:2820::8
443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 2603:1036:308:282d::8
443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 2603:1036:308:282e::8
443
[+]     SRV _autodiscover._tcp.certifiedhacker.com autodiscover.bluehost.com 2603:1036:308:282a::8
443
[+] 16 Records Found
```

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



https://mxtoolbox.com



https://github.com

Objective 07

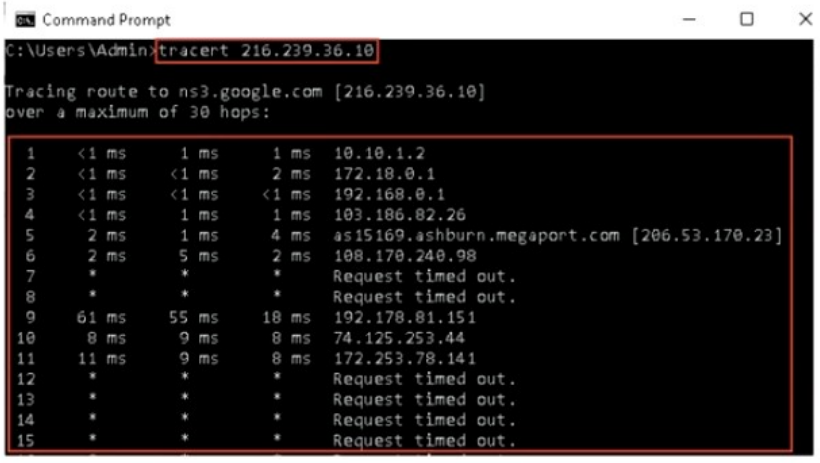
Use Different Techniques for Network and Email Footprinting

Active Reconnaissance

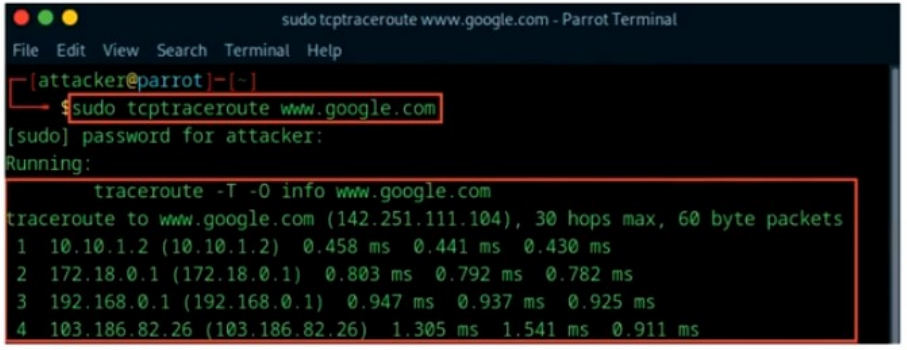
Traceroute

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

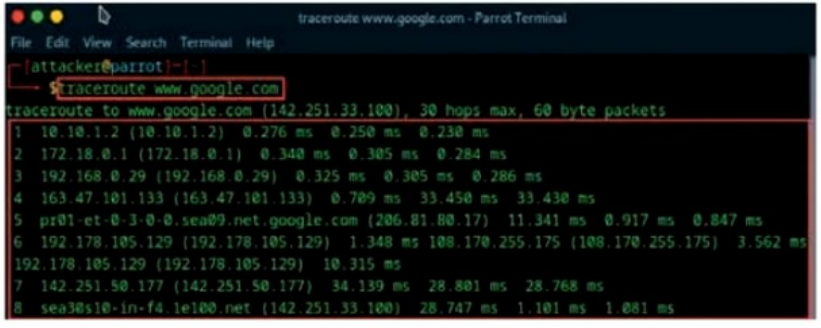
ICMP Traceroute



TCP Traceroute



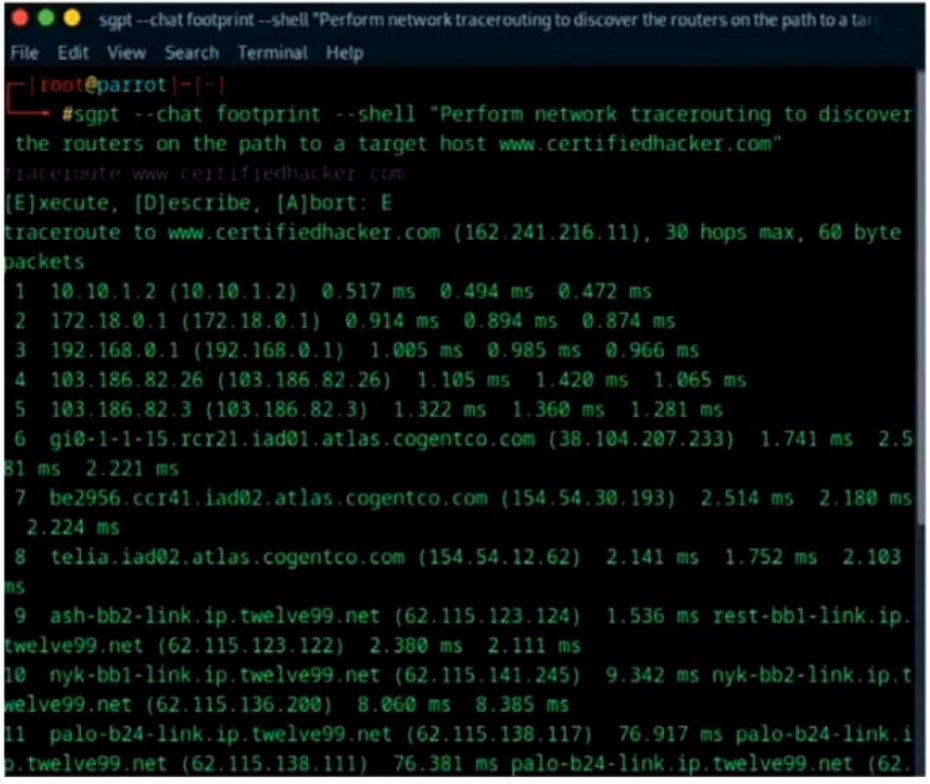
UDP Traceroute



Traceroute with AI

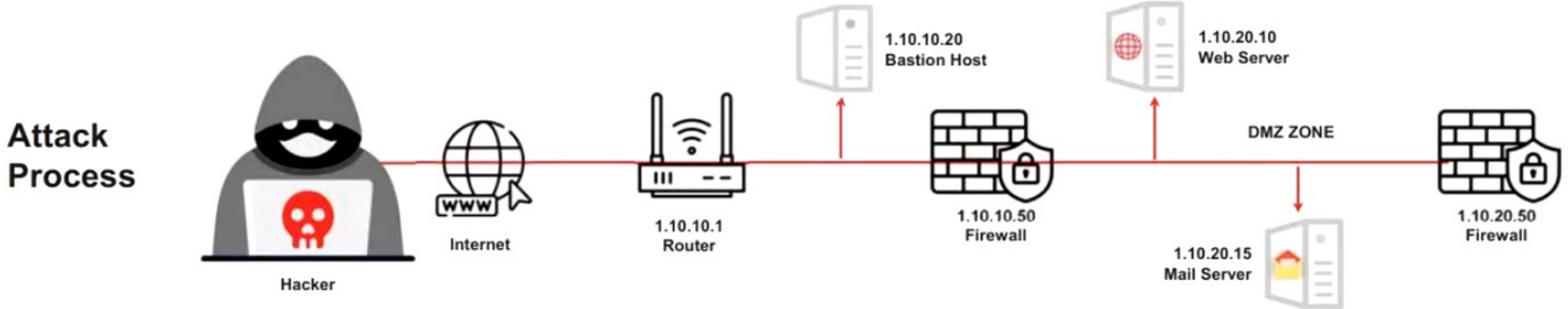
- An attacker can also leverage **AI-powered ChatGPT** or other generative AI technology to perform this task by using an appropriate prompt such as

"Perform network tracerouting to discover the routers on the path to a target host www.certifiedhacker.com"



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



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

Objective 08

Demonstrate Footprinting through Social Engineering

Active Reconnaissance

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 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
Maintain profile	Contact info, location, etc.
Connect to friends, chat	Friends list, friends' info, etc.
Share photos and videos	Identity of family members, interests, etc.
Play games, join groups	Interests
Create events	Activities

What Organizations Do	What Attacker Gets
User surveys	Business strategies
Promote products	Product profile
User support	Social engineering
Recruitment	Platform/technology
Background check to hire employees	Type of business

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

Objective 09

Automate Footprinting Tasks using Advanced Tools and AI

Active Reconnaissance

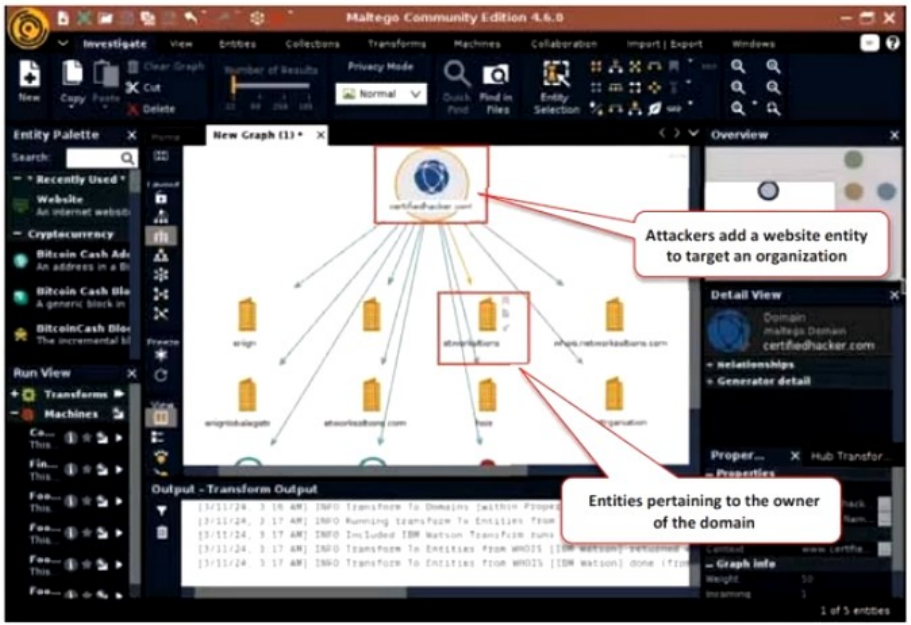
Footprinting Tools: Maltego and Recon-ng

Maltego

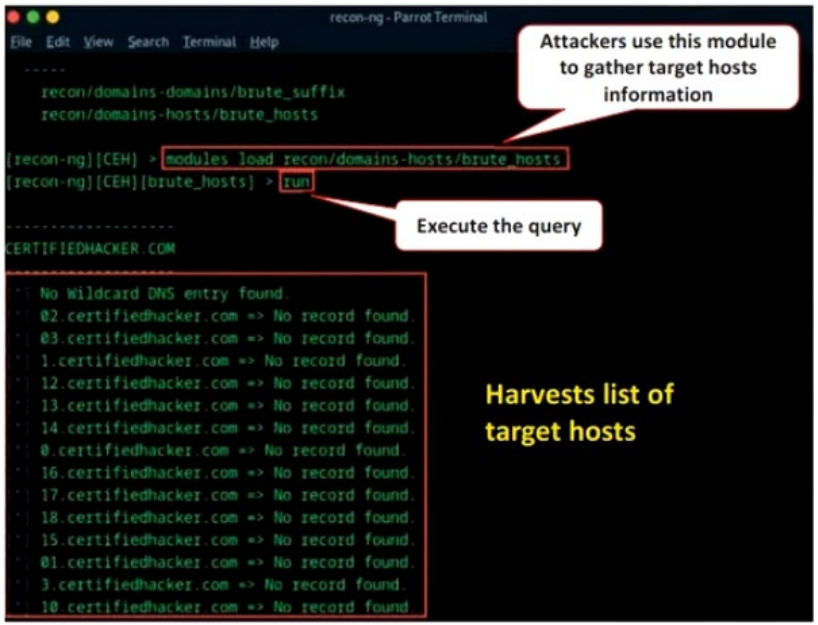
Maltego can be used to determine the **relationships and real world links** between people, groups of people, organizations, websites, Internet infrastructure, documents, etc.

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



https://www.maltego.com



https://github.com

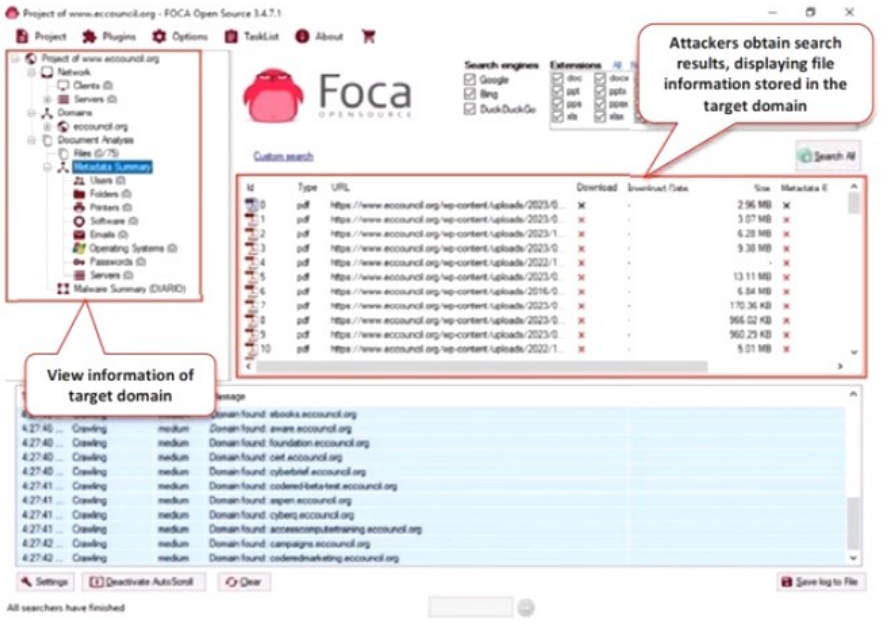
Footprinting Tools: FOCA and subfinder

FOCA

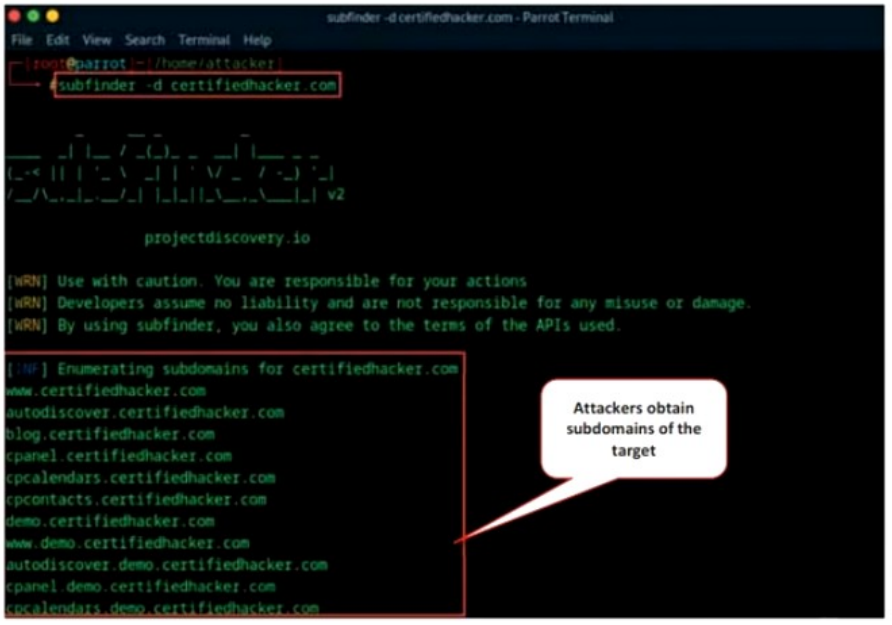
FOCA (Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents it scans

subfinder

subfinder is a **subdomain discovery** tool that helps attackers find valid subdomains for websites



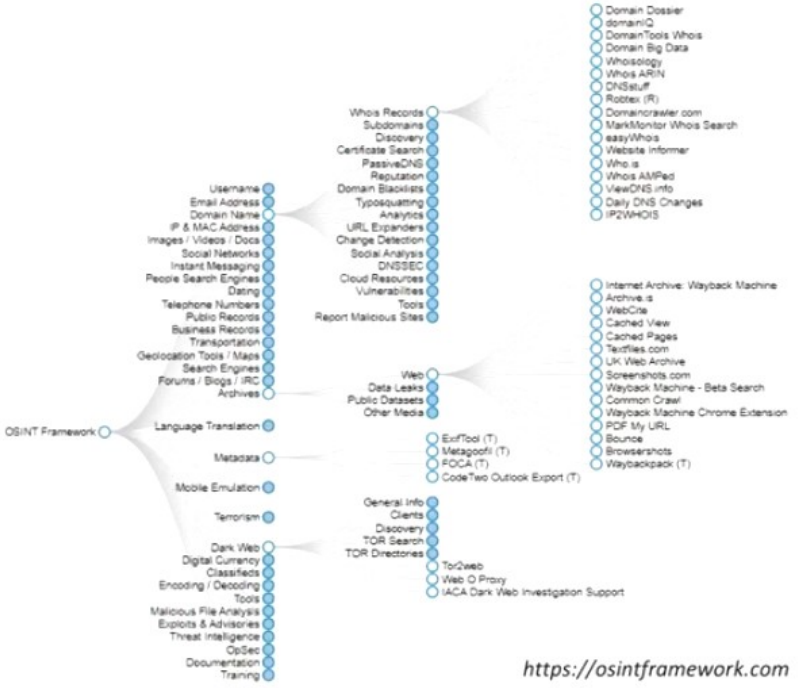
https://www.elevenpaths.com



https://github.com

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



https://osintframework.com

Other Tools:

Sudomy	BillCipher	whatweb	Raccoon	Recon-Dog	Web Check	OSINT.SH
https://github.com	*https://github.com*	*https://github.com*	*https://github.com*	*https://github.com*	*https://web-check.xyz*	*https://osint.sh*

AI-Powered OSINT Tools

Taranis AI

- Taranis AI is an advanced open source intelligence (OSINT) tool that leverages artificial intelligence to **gather, analyze, and interpret publicly available data**
- It assist ethical hackers in **identifying potential security threats, vulnerabilities**, and other relevant information from a **wide array of sources on the internet**

OSS Insight

- OSS Insight uses AI to **provide in-depth insights into the GitHub ecosystem**, analyzing over 5 billion GitHub events
- It offers powerful tools for understanding and navigating the open-source world, from comprehensive repository analytics to developer productivity insights

Other Tools:

DorkGPT	DorkGenius	Google Word Sniper	Cylect.io	ChatPDF
https://dorkgpt.com	*https://dorkgenius.com*	*https://googlewordsniper.eu*	*https://cylect.io*	*https://chatpdf.com*

Create and Run Custom Python Script to Automate Footprinting Tasks with AI

- An attacker can also leverage AI-powered ChatGPT or other generative AI technology to **automate various footprinting tasks** by **creating a custom Python script that will run automatically** and fetch the desired result. They can use appropriate prompts to create custom scripts, such as the one below:

  "Develop a Python script which will accept domain name www.microsoft.com as input and execute a series of website footprinting commands, including DNS lookups, WHOIS records retrieval, email enumeration, and more, to gather information about the target domain"

Objective 10

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 (Cont'd)

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

Module Summary

- In this module, we have discussed the following:
  - Footprinting concepts and the objectives of footprinting
  - Various footprinting techniques, such as footprinting through search engines, footprinting through Internet search services, and footprinting through social networking sites
  - Whois, DNS, and email footprinting
  - Network footprinting and footprinting through social engineering
  - Some important footprinting tools
  - How organizations can defend against footprinting and reconnaissance activities
- In the next module, we will discuss in detail how attackers, ethical hackers, and pen testers perform network scanning to collect information about a target of evaluation before an attack or audit