A·P·U
ASIA PACIFIC UNIVERSITY
OF TECHNOLOGY & INNOVATION

Ethical Hacking and Incident Response
CT080-3-2 (Version VE1)
02: FOOTPRINTING & RECONNAISSANCE

TOPIC & STRUCTURE OF THE LESSON

- Footprinting Concepts
- Footprinting Methodology
- Footprinting Tools
- Footprinting Countermeasures

LEARNING OUTCOMES

At the end of this module, you will be able to:

- Describe footprinting concepts
- Perform footprinting through
  - Search engines and using advanced Google hacking techniques
  - Web services and social networking sites
  - Website footprinting and email footprinting
  - Whois, DNS, and network footprinting
  - Social engineering
- Use different footprinting tools
- Apply footprinting best practices

KEY TERMS YOU MUST BE ABLE TO USE

- Footprinting
- Whois Footprinting
- Social Engineering
- Traceroute
- Eavesdropping
- Shoulder surfing
- Dumpster diving

1. FOOTPRINTING CONCEPTS

1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting Tools
4. Footprinting Countermeasures

What is Footprinting?

Footprinting is the first step of any attack on information systems in which an attacker **collects information about a target network** to identify various ways to intrude into the system

Types of Footprinting

- **Passive Footprinting**
  - Gathering information about the target **without direct interaction**
- **Active Footprinting**
  - Gathering information about the target **with direct interaction**

Information Obtained in Footprinting

- **Organization information**
  - Employee details, telephone numbers, location, background of the organization, web technologies, etc.
- **Network information**
  - Domain and sub-domains, network blocks, IP addresses of the reachable systems, Whois record, DNS, etc.
- **System information**
  - OS and location of web servers, users and passwords, etc.

Objectives of Footprinting

- Knowledge of security posture
- Reduction of focus area
- Identifying vulnerabilities
- Drawing of network map

Objectives of Footprinting

Footprinting helps to:

1. **Know Security Posture**:
   - Gives the complete profile of the organization's security posture. Hackers can then analyze the report to identify loopholes in the security posture of the target organization and build a hacking plan accordingly.
2. **Reduce Focus Area**:
   - By using a combination of tools and techniques, attackers can take an unknown entity (for example, XYZ Organization) and reduce it to a specific range of domain names, network blocks, and individual IP addresses of systems directly connected to the Internet, as well as many other details pertaining to its security posture.
3. **Identify Vulnerabilities**:
   - A detailed footprint provides maximum information about the target organization. It allows the attacker to identify vulnerabilities in the target systems to select appropriate exploits. Attackers can build their own information database about the security weaknesses of the target organization. Such a database can then help in identifying the weakest link in the organization's security perimeter.
4. **Draw Network Map:**
   - To create diagrammatic representations of the target organization's network presence. Specifically, it allows attackers to draw a map or outline of the target organization's network infrastructure to know about the actual environment that they are going to break into. A network map will depict the attacker's understanding of the target's Internet footprint. These network diagrams can guide the attacker in performing an attack.

2. Footprinting Methodology

1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting Tools
4. Footprinting Countermeasures

Steps in Footprinting Methodology

1. Identify the Target
2. Passive Footprinting
3. Active Footprinting
4. Network Information Gathering
5. Social Engineering
6. Website Footprinting
7. DNS Footprinting
8. Compile & Report

🛠️ 1. Identify the Target

This is the initial step where you define the scope of your footprinting activity. The target can be:

- **Company or Organization** (for corporate reconnaissance)
- **IP Address or Network** (to identify services and ports)
- **Domain or Website** (to find vulnerabilities in web applications)
- **Individual or Person** (for social engineering or human factor attacks)

Tools used: **Google Dorks, Whois, Shodan, OSINT Framework, Maltego**

Activities: Identify the domain name, IP address, network range, and subnets of the target. Pinpoint the external-facing systems, like servers, routers, and firewalls. Identify public-facing services (like web servers, FTP, email servers, etc.).

🌐 2. Passive Footprinting

Passive footprinting involves collecting information without interacting directly with the target. This ensures stealth, as no requests are sent to the target's systems.

Techniques:

- **OSINT (Open-Source Intelligence)** – Use public databases, social media, and search engines.
- **DNS Enumeration** – Collect domain-related data (like subdomains, nameservers, and DNS records).
- **Social Media Recon** – Extract employee names, job titles, and emails from social platforms.
- **Public Repositories** – Look for exposed credentials, source code, or misconfigurations on GitHub, Pastebin, etc.
- **File Metadata Extraction** – Analyze metadata from company documents, PDFs, and media files.

Tools used: **OSINT Framework, Google Dorks, Maltego, Netcraft, FOCA, Shodan, Hunter.io**

🔍 3. Active Footprinting
📡 4. Network Info Gathering

Active footprinting involves interacting directly with the target. It's more likely to be detected by security monitoring tools but provides more detailed information.

Techniques:

- **Port Scanning** – Identify open ports and running services on the target system.
- **Network Scanning** – Map out the network topology, IP addresses, and connected devices.
- **Service Fingerprinting** – Identify the operating system, web server software, and versions.
- **Email Harvesting** – Extract email addresses from the target's website or external services.
- **Website Enumeration** – Discover subdomains, directories, and files exposed to the public.

Tools used: **Nmap, Masscan, Sublist3r, DNSDumpster, Burp Suite, OWASP ZAP, Nmap, Masscan, Shodan, IPinfo.io, Censys, Zenmap, Maltego, SpiderFoot**

🤝 5. Social Engineering

This step involves collecting **non-technical information** from people to gain access to sensitive systems. It focuses on manipulating employees, staff, or contractors to reveal confidential information.

Techniques:

- **Phishing Attacks** – Sending fake emails to employees to trick them into giving credentials.
- **Impersonation** – Calling or interacting with staff while pretending to be a company representative.
- **Dumpster Diving** – Searching for sensitive information (passwords, notes, etc.) in discarded files or trash.
- **Social Media Profiling** – Collecting personal data from LinkedIn, Facebook, or Instagram to identify employees' habits, behaviors, or potential security flaws.

Tools used: **Social-Engineer Toolkit (SET), Sherlock, Maltego, OSINT Framework, Have I Been Pwned**

🔐 6. Website Footprinting

This step focuses on web application reconnaissance. The objective is to discover vulnerabilities in web apps, including APIs, files, and misconfigured endpoints.

Techniques:

- **Website Enumeration** – Identify subdomains, directories, and hidden files.
- **Server Fingerprinting** – Identify the web server (e.g., Apache, Nginx) and its version.
- **Content Discovery** – Look for hidden files and directories using directory brute-forcing.
- **SSL/TLS Analysis** – Identify weaknesses in the encryption protocol or misconfigurations.

Tools used: **Burp Suite, OWASP ZAP, Wappalyzer, Nikto, Gobuster, Dirb, WhatWeb**

🔍 7. DNS Footprinting

The DNS (Domain Name System) provides valuable information about subdomains, mail servers, and IP mappings.

Techniques:

- **Zone Transfer Attacks** – Extract complete DNS records from misconfigured DNS servers.
- **DNS Lookup** – Identify nameservers, MX records, CNAMEs, and TXT records.
- **Subdomain Enumeration** – Identify subdomains related to the target.

Tools used: **DNSDumpster, Fierce, Sublist3r, Nslookup, MXToolbox, Whois**

What is Zone Transfer attack?

A Zone Transfer Attack is a method used to gather information from a DNS (Domain Name System) server. This attack exploits the **DNS zone transfer (AXFR) mechanism**, which is designed to **synchronize DNS records** between **primary** and **secondary** DNS servers.

How Does Zone Transfer Work?

1. **DNS Servers Synchronize**: A primary DNS server (authoritative) maintains the original zone file. The secondary DNS server requests the latest copy of the zone file using an AXFR (Asynchronous Full Zone Transfer) request.
2. **Legitimate Use Case**: This synchronization ensures redundancy and availability, so if one server fails, the DNS records are still available from the secondary server.
3. **Exploitation**: An attacker mimics the behavior of a secondary DNS server and sends an AXFR request to the primary DNS. If the DNS server is misconfigured to allow transfers to unauthorized users, the attacker receives the entire DNS zone file.

📜 8. Information Compilation & Reporting

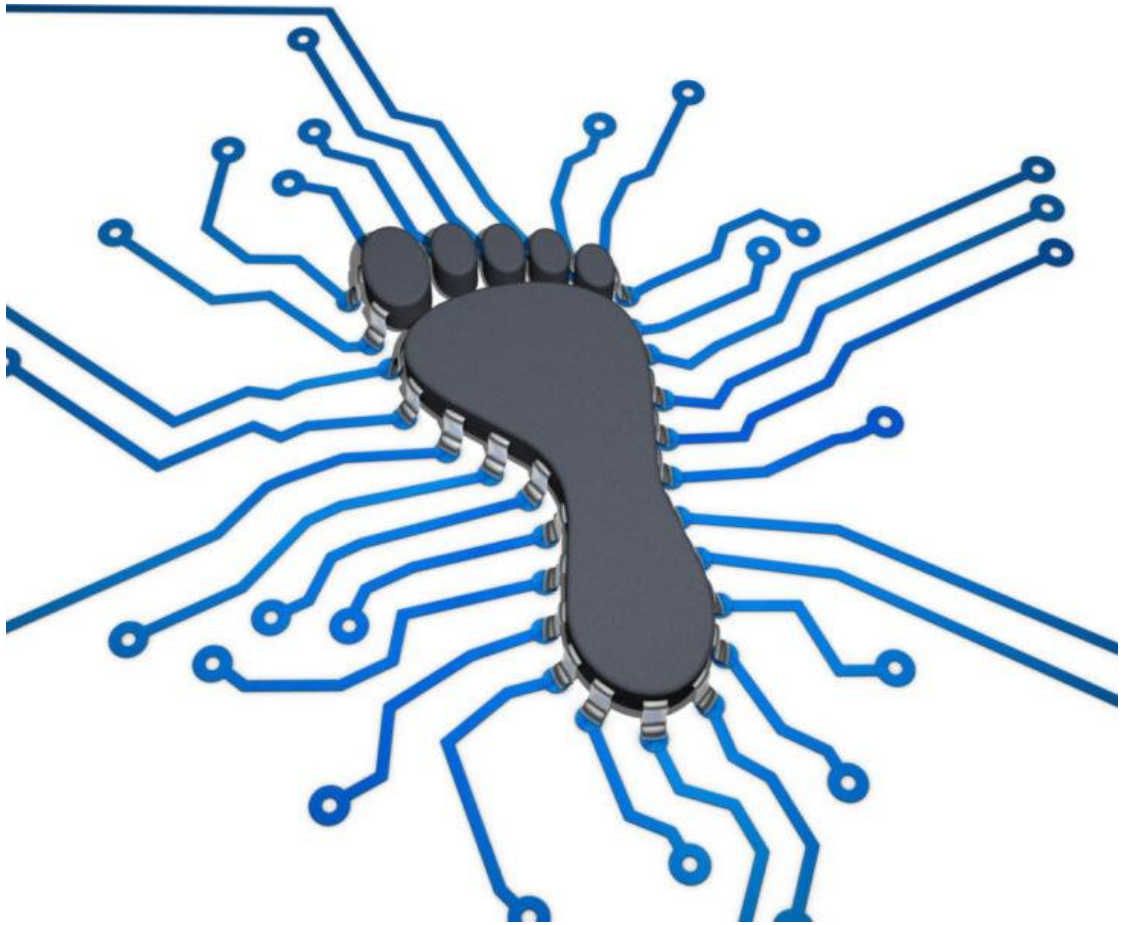
This is the final phase where all the collected information is organized and reported. The data collected can be used to plan penetration tests or attacks.

Key Deliverables:

- **Network Map** – IP addresses, devices, and system topology.
- **List of Subdomains** – Public subdomains and potential attack vectors.
- **Port and Service List** – Open ports and services running on them (like HTTP, SSH, FTP).
- **System Details** – OS version, web server details, CMS used, and software versions.
- **Employee Information** – List of employees, job titles, and email addresses.
- **Vulnerability List** – Known issues and exploits associated with the identified software.

🚀 Best Practices for Ethical Footprinting

1. **Set Clear Objectives** – Know what data is critical for your attack plan.
2. **Use Passive Techniques First** – This avoids detection by IDS/IPS systems.
3. **Document Everything** – Keep notes on tools, techniques, and findings.
4. **Be Legal and Ethical** – Obtain permissions before active scanning.Use
5. **Comprehensive Tools** – Combine tools like Nmap, OSINT, and Maltego.



FOOTPRINTING VIA SEARCH ENGINES

Footprinting via 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

Advanced search operators allows to create complex queries to find, filter, and sort specific information regarding the target. Search engines are also used to find other sources of publicly accessible information. For example, you can type "top job portals" to find major job portals that provide critical information about the target organization. As an ethical hacker, if you find any deleted pages/information about your company in SERPs or the search engine cache, you can request the search engine to remove the pages/information from its indexed cache.

1. Footprinting Using Advanced Google Hacking Techniques

- 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

- **[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
- **[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

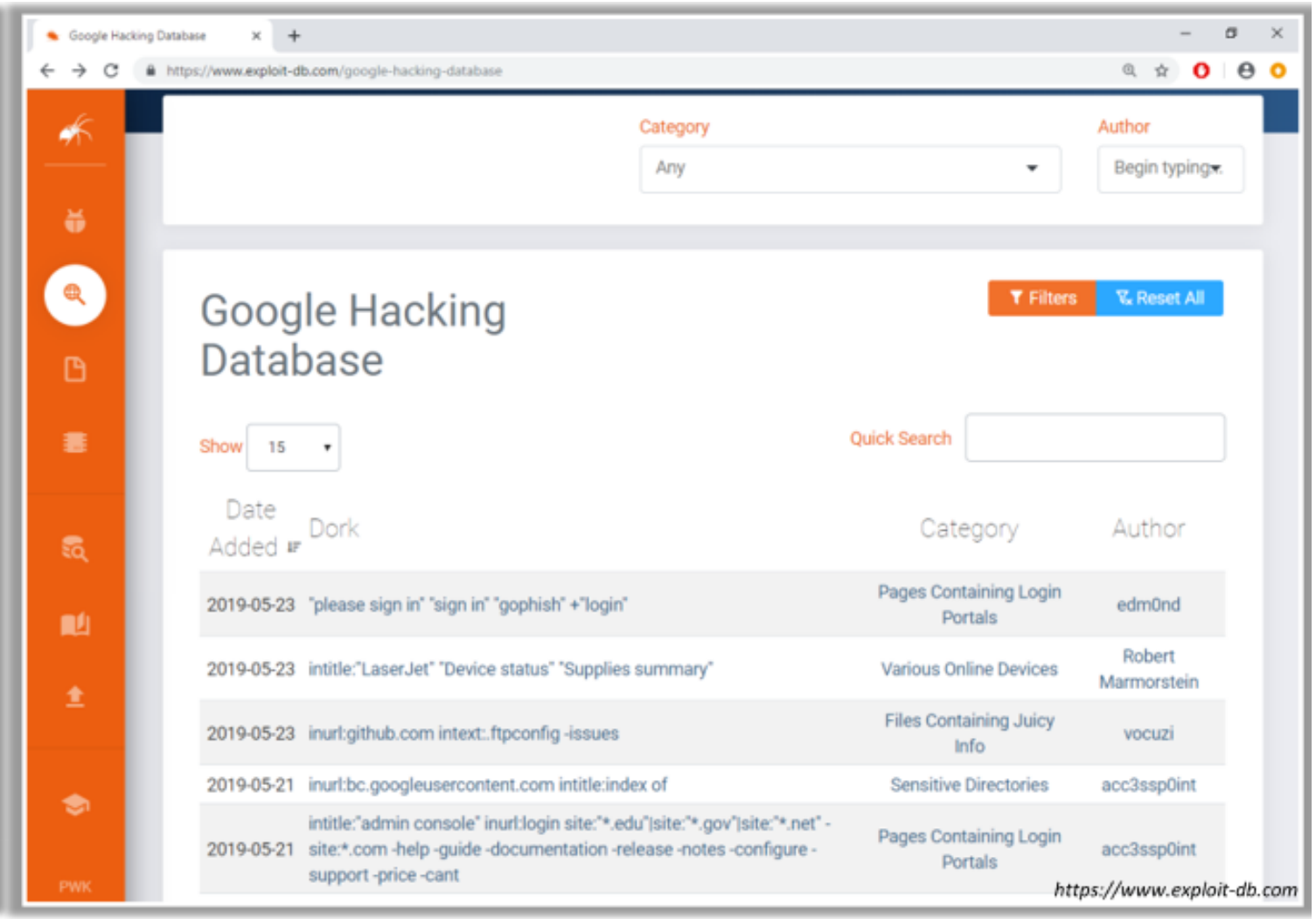
2. What can a Hacker do with Google Hacking?

- An attacker can create complex search engine queries to filter large amounts of search results to obtain information related to computer security.
- The attacker uses Google operators that help locate specific strings of text within the search results. Thus, the attacker can not only detect websites and web servers that are vulnerable to exploitation but also locate private, sensitive information about others, such as credit card numbers, social security numbers, passwords, and so on.
- Once a vulnerable site is identified, attackers try to launch various possible attacks, such as buffer overflow and SQL injection, which compromise information security.
- Examples of sensitive information on public servers that an attacker can extract with the help of Google Hacking Database (GHDB) queries include:
    1. Error messages that contain sensitive information
    2. Files containing passwords
    3. Sensitive directories
    4. Pages containing logon portals
    5. Pages containing network or vulnerability data, such as IDS, firewall logs, and configurations
    6. Advisories and server vulnerabilities
    7. Software version information
    8. Web application source code
    9. Connected IoT devices and their control panels, if unprotected
    10. Hidden web pages such as intranet and VPN services

3. 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



4. VoIP and VPN Footprinting through Google Hacking Database

Google search queries for VoIP footprinting

Google Dork	Description
intitle:"Login Page" intext:"Phone Adapter Configuration Utility"	Pages containing login portals
inurl:/voice/advanced/ intitle:Linksys SPA configuration	Finds the Linksys VoIP router configuration page
intitle:"D-Link VIP Router" "Welcome"	Pages containing D-Link login portals
intitle:asterisk.management.portal web-access	Look for the Asterisk management portal
intitle:"SPA504G Configuration"	Finds Cisco SPA504G Configuration Utility for IP phones
intitle:asterisk.management.portal web-access	Finds the Asterisk web management portal
inurl:8080 intitle:"login" intext:"UserLogin" "English"	VoIP login portals
intitle:"Sipura.SPA.Configuration" -.pdf	Finds configuration pages for online VoIP devices

Google search queries for VPN footprinting

Google Dork	Description
filetype:pcf "cisco" "GroupPwd"	Cisco VPN files with Group Passwords for remote access
"[main]" "enc_GroupPwd=" ext:txt	Finds Cisco VPN client passwords (encrypted but easily cracked!)
"Config" intitle:"Index of" intext:vpn	Directory with keys of VPN servers
inurl:/remote/login?lang=en	Finds FortiGate Firewall's SSL-VPN login portal
!Host=*.* intext:enc_UserPassword=* ext:pcf	Looks for profile configuration files (.pcf), which contain user VPN profiles
filetype:rcf inurl:vpn	Finds Sonicwall Global VPN Client files containing sensitive information and login
filetype:pcf vpn OR Group	Finds publicly accessible .pcf used by VPN clients

https://www.exploit-db.com

5. Other Techniques for Footprinting through Search Engines Gathering **

Gathering Information Using Google Advanced Search and Advanced Image Search

- Attackers can use Google Advanced Search and Advanced Image Search to achieve the same precision as that of using the advanced operators but **without typing or remembering the operators**
- Using Google's Advanced search option, attackers can **find sites that may link back to the target organization's website**

Gathering Information using Reverse Image Search

- Reverse image search **helps an attacker in tracking the original source and details of images**, such as photographs, profile pictures, and memes
- Attackers can use online tools such as Google Image Search, TinEye Reverse Image Search, and Yahoo Image Search to perform reverse image search

Gathering Information from Video Search Engines

- Video search engines such as YouTube, and Google Videos allow attackers to **search for a video content related to the target**
- Attackers can further analyze the video content to **gather hidden information** such as time/date and thumbnail of the video
- Using video analysis tools such as YouTube DataViewer, and EZGif, an attacker can **reverse and convert video** to text formats to extract critical information about the target

(cont.)

Gathering Information from Meta Search Engines

- Meta search engines use other search engines (Google, Bing, Ask.com, etc.) to produce their own results from the Internet
- Attackers use meta search engines such as Startpage and MetaGer to **gather more detailed information about the target**, such as images, videos, blogs, and news articles, from different sources

Gathering Information from FTP Search Engines

- FTP search engines are used to search for files located on the FTP servers
- Attackers use FTP search engines, such as NAPALM FTP Indexer and Global FTP Search Engine, to **retrieve critical files and directories about the target** that reveal valuable information, such as business strategy, tax documents, and employee's personal records

Gathering Information from IoT Search Engines

- IoT search engines crawl the Internet for IoT devices that are publicly accessible
- Attackers use IoT search engines, such as Shodan, Censys, and Thingful, to **gather information about the target IoT devices**, such as manufacturer details, geographical location, IP address, hostname, and open ports

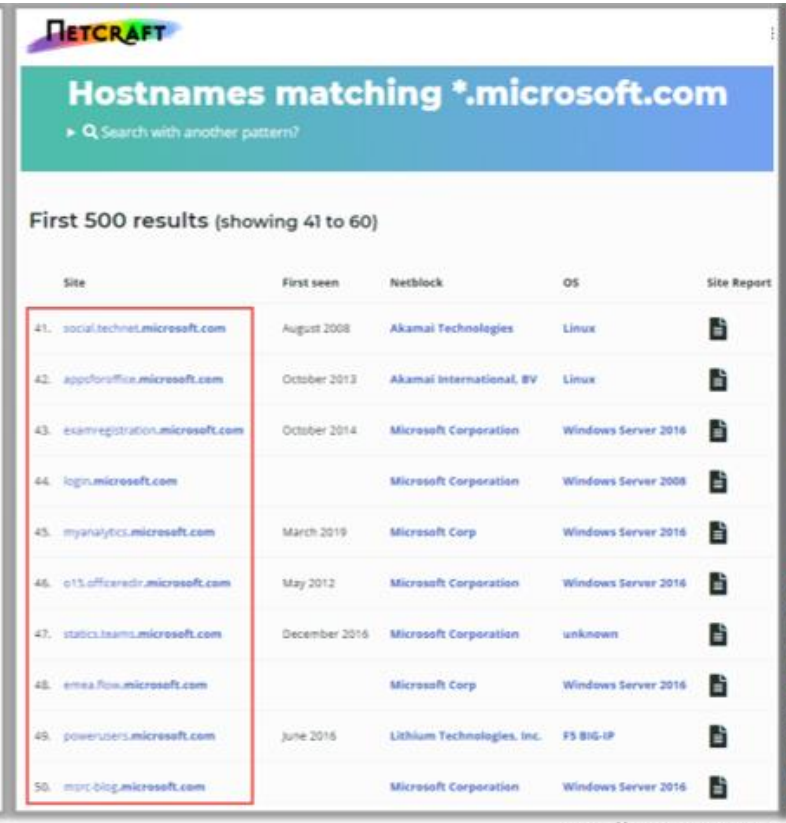
FOOTPRINTING VIA WEB SERVICES

Footprinting through Web Services

- **Internet archives** may also provide sensitive information that has been removed from the World Wide Web (WWW).
- **Social networking sites, people search services, alerting services, financial services**, and **job sites** provide information about a target such as infrastructure details, physical location, and employee details.
- **Groups, forums**, and **blogs** can help attackers in gathering sensitive information about a target, such as public network information, system information, and personal information.
- Useful information:
  - Company's top-level domains, sub-domains, and geographical location,
  - Performing people search on social networking sites
  - Using people search services,
  - Gathering information from job sites, financial services, third-party data repositories,
  - Performing deep and dark web footprinting,
  - Determining the operating system VOIP
- Using this information, an attacker may build a **hacking strategy** to break into the target organization's network and carry out other types of advanced system attacks.

1. 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

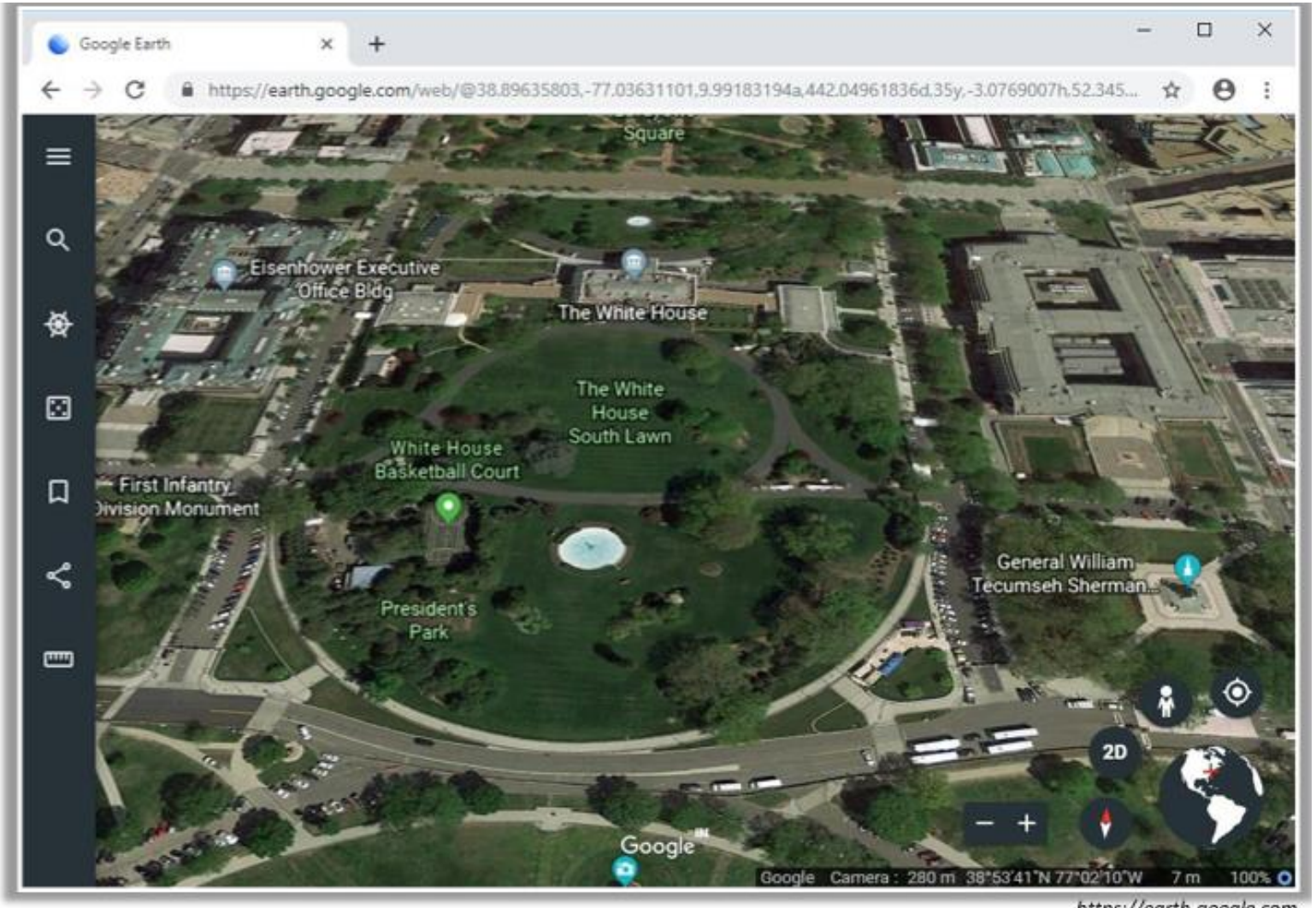


https://www.netcraft.com

https://github.com

2. Finding the Geographical Location of the Target

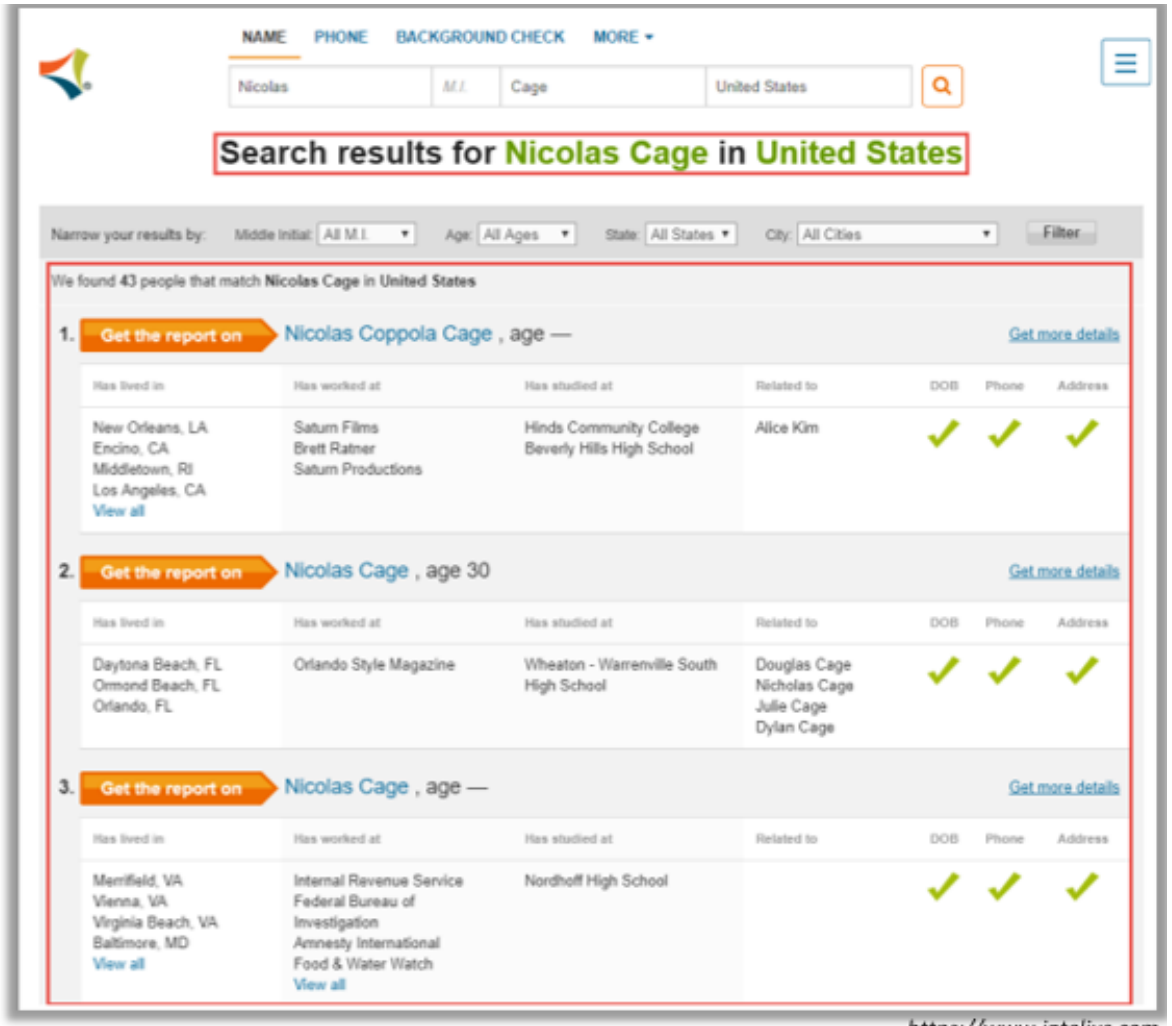
- Attackers use tools, such as **Google Earth**, **Google Maps**, and **Wikimapia**, to obtain the physical location of the target, which helps them to perform social engineering and other non-technical attacks
- These tools help attackers to find or locate entrances to buildings, security cameras, gates, places to hide, weak spots in perimeter fences, etc.



https://earth.google.com

3. People Search on Social Networking Sites and People Search Services

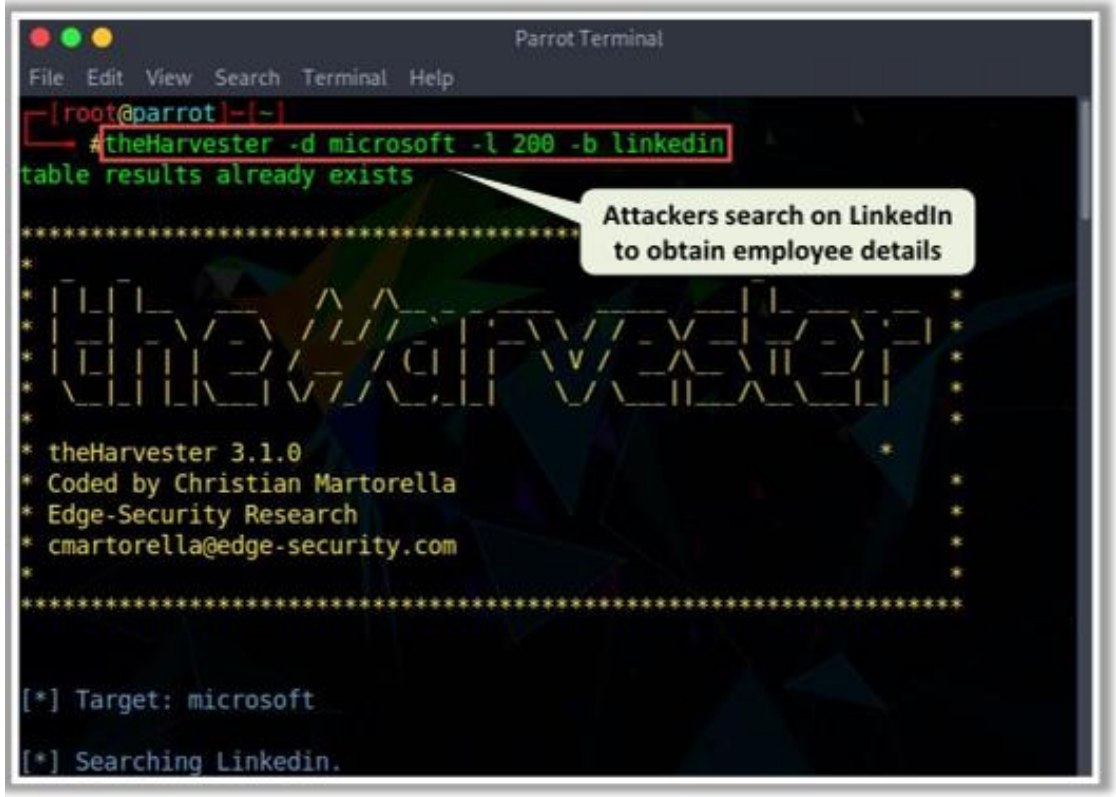
- Social networking services, such as Facebook, Twitter, and LinkedIn, provide **useful information about the individual** that helps the attacker in performing social engineering and other attacks
- The people search can provide critical **information about a person or an organization**, including location,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

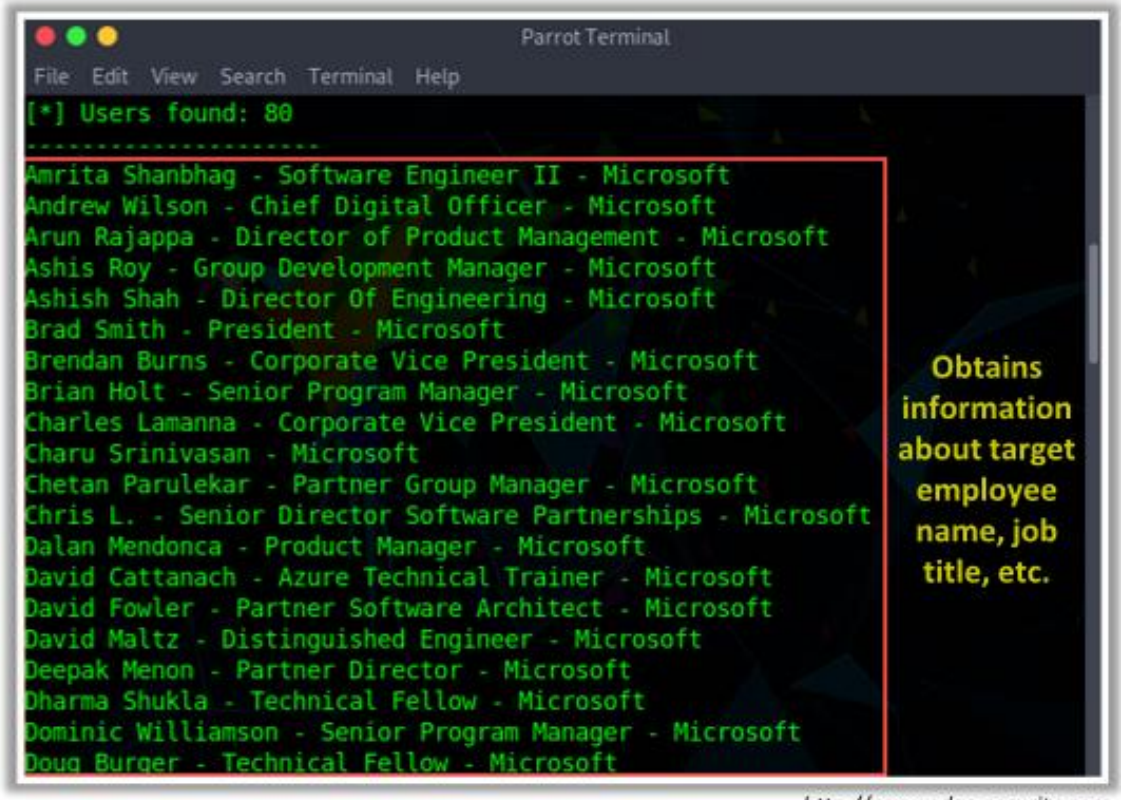


https://www.intelius.com

4. 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

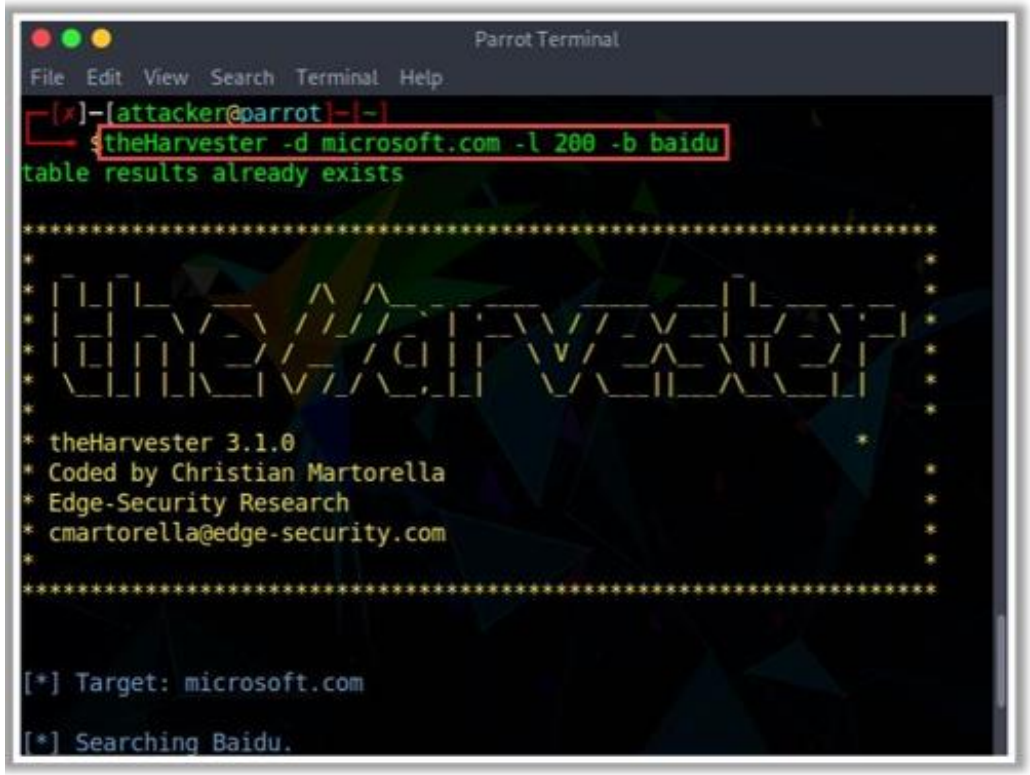


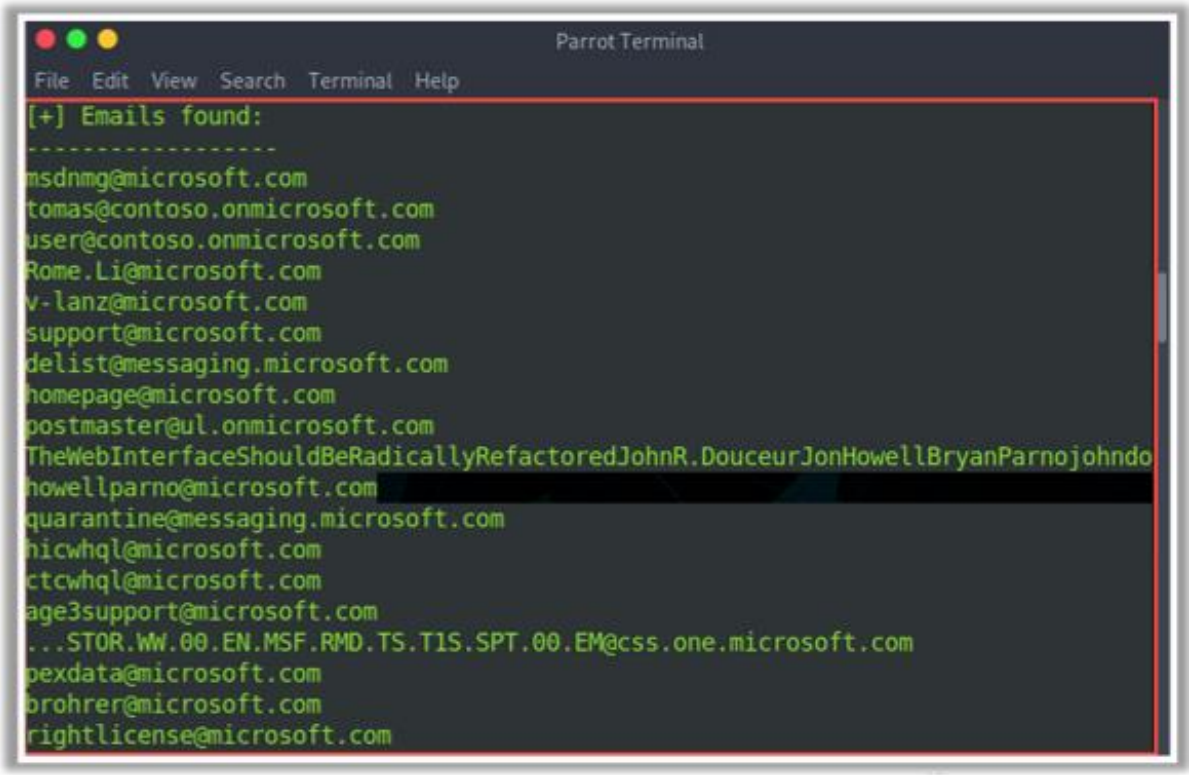


http://www.edge-security.com

5. Harvesting Email Lists

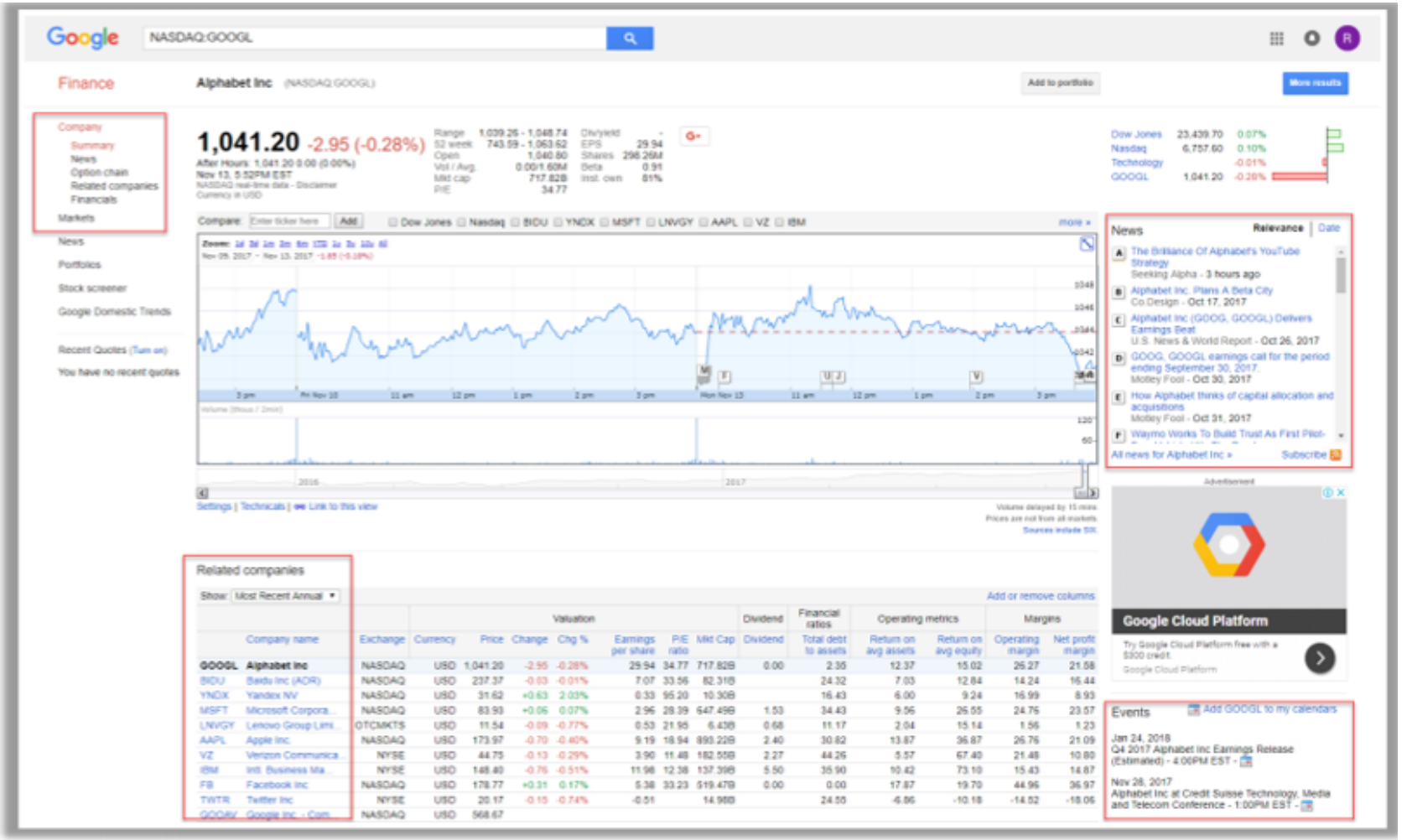
- Gathering email addresses related to the target organization acts as an **important attack vector during the later phases of hacking**
- Attackers use automated tools such as **theHarvester** and **Email Spider** to collect publicly available email addresses of the target organization that helps them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





6. Gathering Information from Financial Services

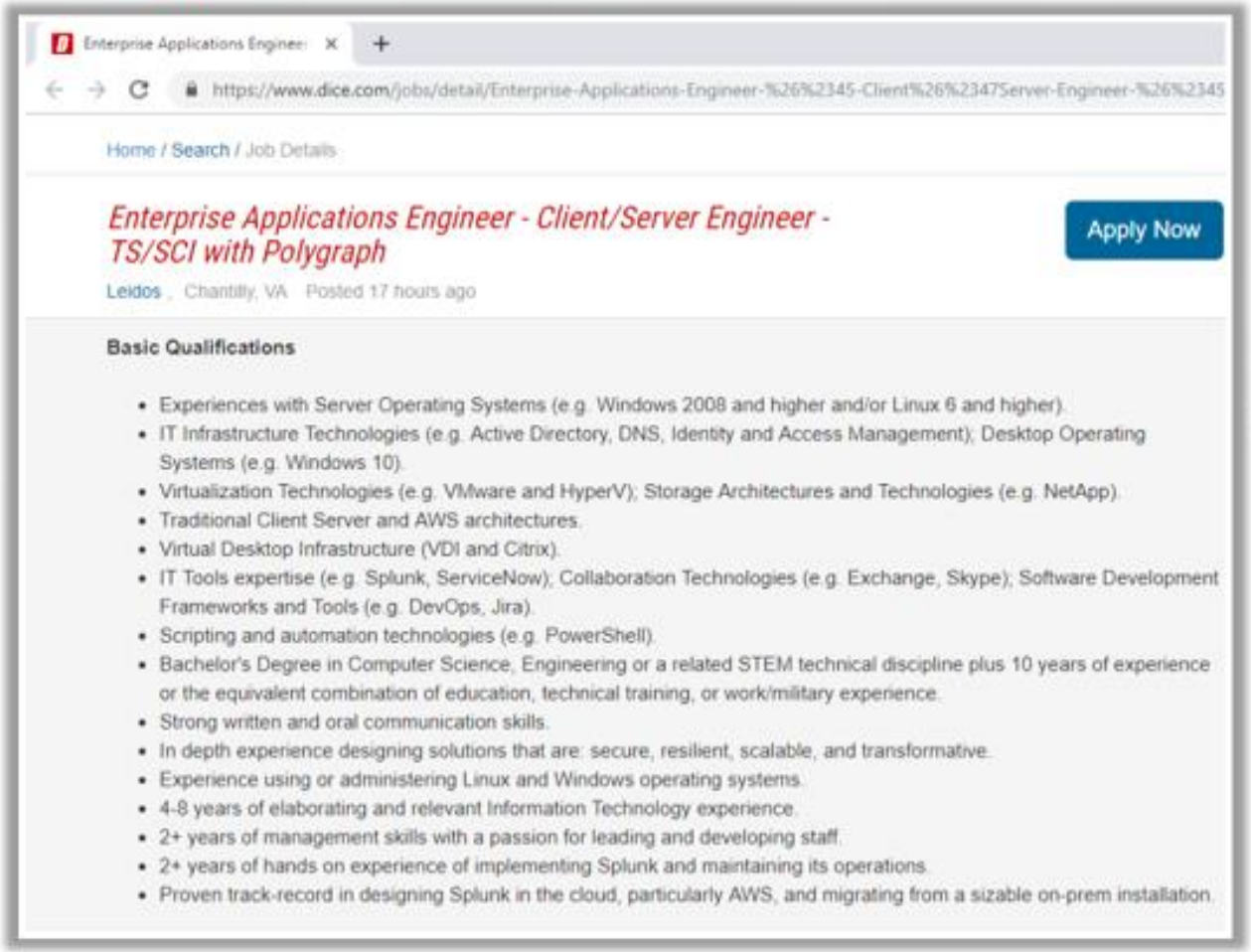
- Financial services, such as Google Finance, MSN Money, and Yahoo! Finance, provide useful information about the target company, such as the **market value of a company's shares**, **company profile**, and **competitor details**
- Attackers can use this information to perform service flooding, brute-force, or phishing attacks



https://www.google.com/finance

7. Footprinting through Job Sites

A **company's infrastructure details** can be gathered from job postings



https://www.dice.com

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**

8. 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

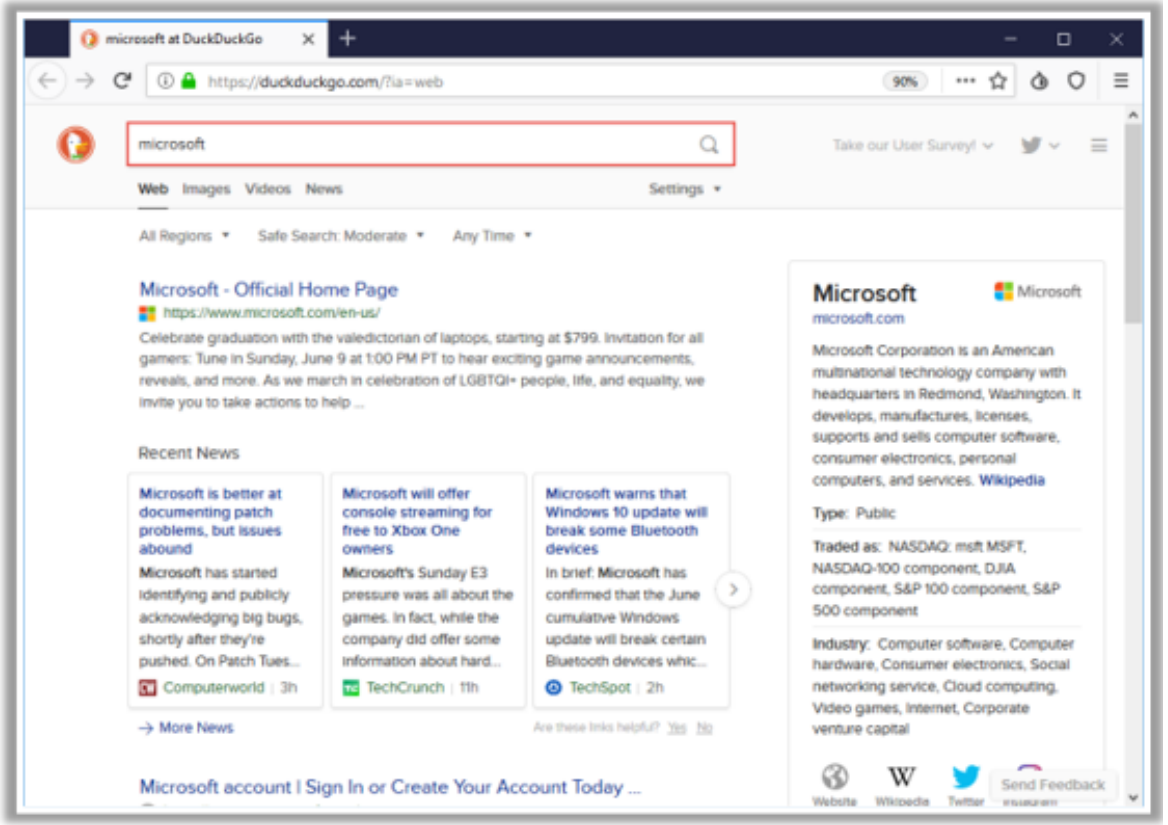
Dark web or Darknet

- 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

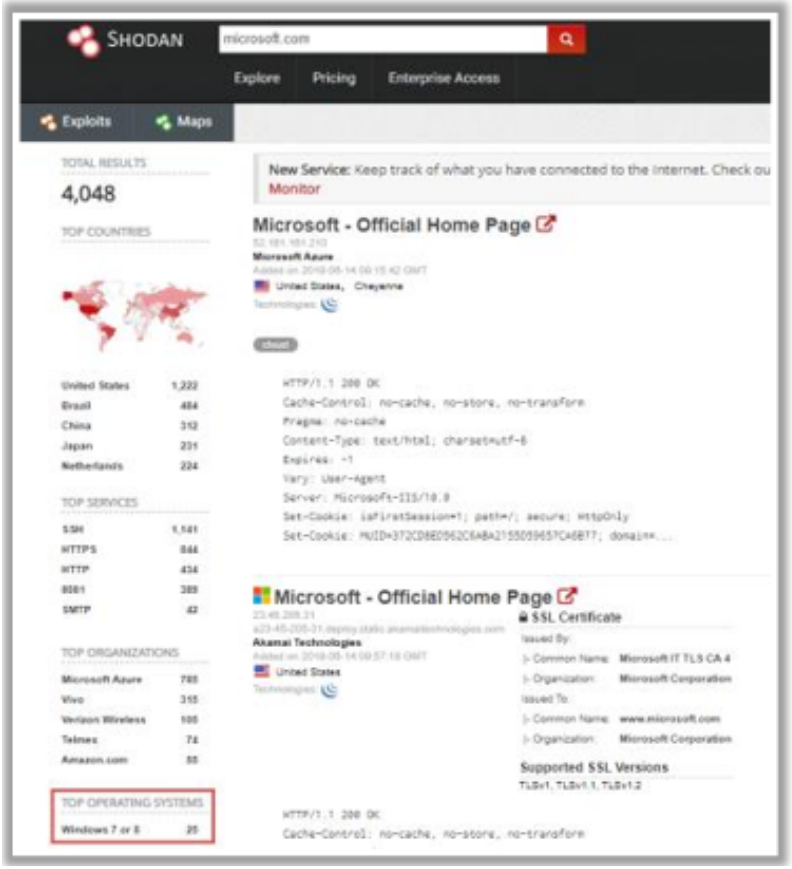
It is used to access the deep and dark web where it acts as a **default VPN** for the user and bounces the network IP address through several servers before interacting with the web



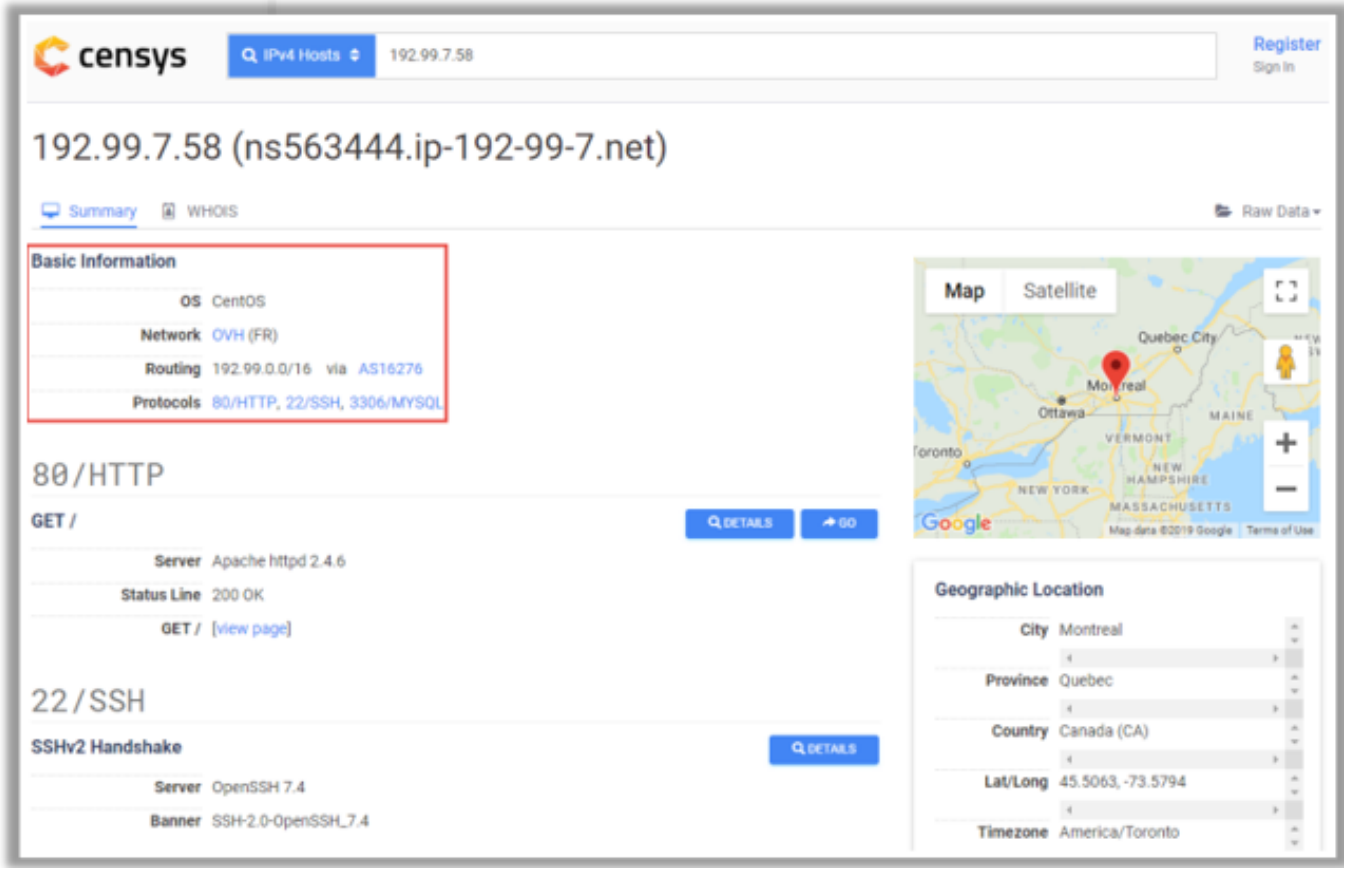
https://www.torproject.org

9. Determining the Operating System

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



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



10. 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

10. Competitive Intelligence Gathering (cont.)

When Did this Company Begin? How Did it Develop?

- **Information Resource Sites**
  - **EDGAR Database**
    https://www.sec.gov/edgar.shtml
  - **D & B Hoovers**
    http://www.hoovers.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
  - **Alexa**
    https://www.alexa.com
  - **Euromonitor**
    https://www.euromonitor.com

What Expert Opinions Say About the Company?

- **Information Resource Sites**
  - **SEMRush**
    https://www.semrush.com
  - **AttentionMeter**
    http://www.attentionmeter.com
  - **ABI/INFORM Global**
    https://www.proquest.com
  - **SimilarWeb**
    https://www.similarweb.com

11. Other Techniques for Footprinting through Web Services

Information Gathering Using Business Profile Sites

- Business profile sites contain the **business information** of companies located in a particular region, which includes their contact information and can be viewed by anyone
- Attackers use business profile sites, such as **opencorporates** and **Crunchbase**, to gather important information about the target organizations, such as their location, addresses, contact information, and employee database

Monitoring Targets Using Alerts

- Alerts are **content monitoring services** that automatically provide **up-to-date information** based on your preference, usually via email or SMS
- Tools, such as **Google Alerts** and **Twitter Alerts**, help attackers to track mentions of the organization's name, member names, website, or any people or projects

Tracking Online Reputation of the Target

- Online Reputation Management (ORM) is a process of **monitoring a company's reputation on the Internet** and taking certain measures to minimize the negative search results/reviews and thereby improve its brand reputation
- Attackers use ORM tracking tools, such as Trackur and Brand24, to track a company's online reputation, search engine ranking information, email notifications when a company is mentioned online, and social news about the company

11. Other Techniques for Footprinting through Web Services (cont.)

Information Gathering Using Groups, Forums, and Blogs

- Groups, forums, and blogs provide sensitive information about a target, such as **public network information**, **system information**, and **personal information**
- Attackers register with fake profiles in **Google groups**, **Yahoo groups**, etc. and try to join the target organization's employee groups, where they share personal and company information

Information Gathering Using NNTP Usenet Newsgroups

- Usenet newsgroup is a repository containing a **collection of notes or messages** on various subjects and topics that are submitted by the users over the Internet
- Attackers can search the Usenet newsgroups, such as Newshosting and Eweka, to find valuable information about the **operating systems**, **software**, **web servers**, etc. used by the target organization

FOOTPRINTING VIA SOCIAL NETWORKING SITES

c. Footprinting through Social Networking Sites

- While footprinting through social networking sites may seem similar to footprinting through social engineering (which is discussed in greater detail later), there are some differences between the two methods.
- In **footprinting through social engineering**, the attacker **tricks people into revealing information**, whereas **in footprinting through social networking sites**, the attacker **gathers information available on those sites.**

1. 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

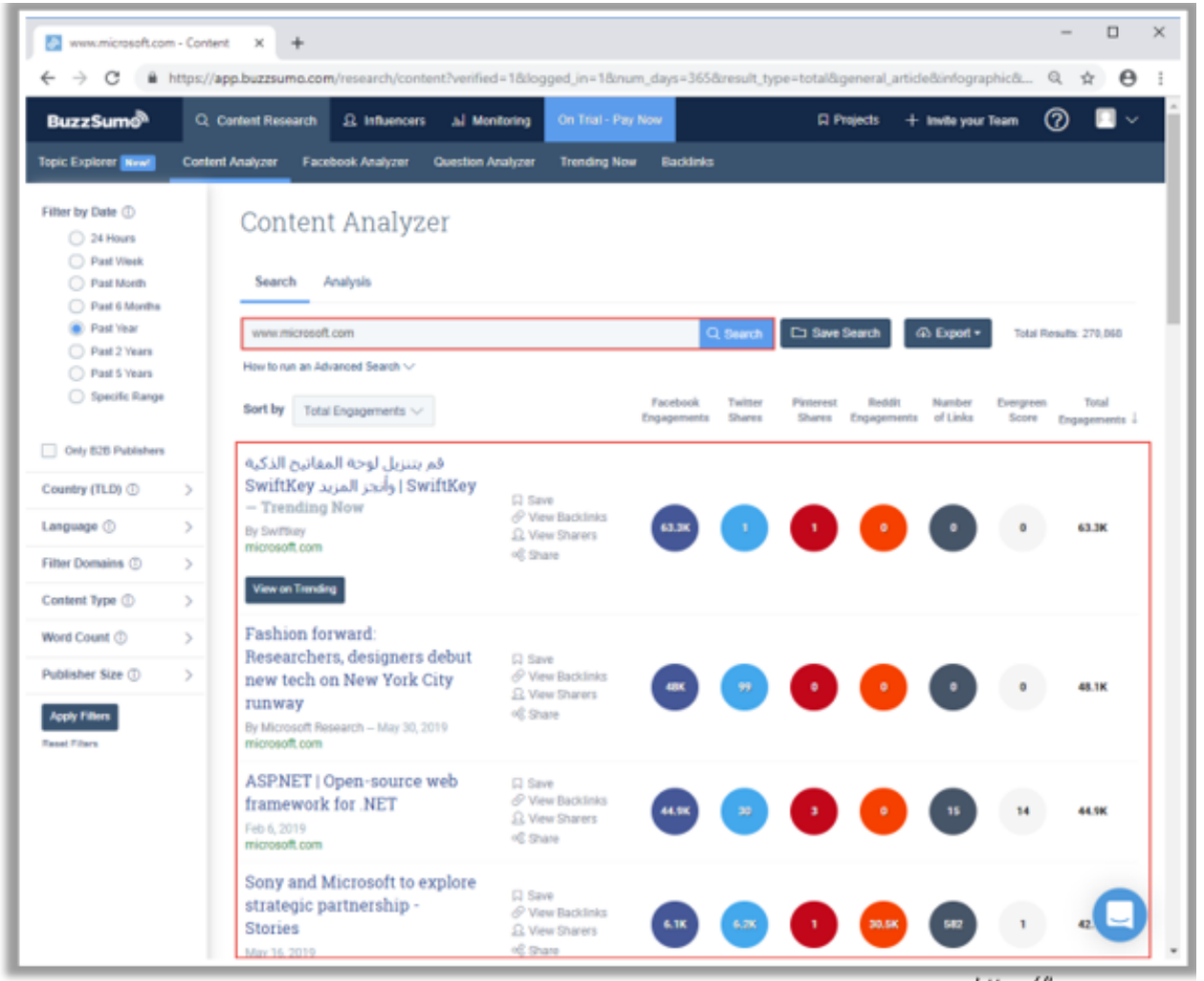
2. General Resources for Locating Information from Social Media Sites

- 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



https://buzzsumo.com

3. Conducting Location Search on Social Media Sites

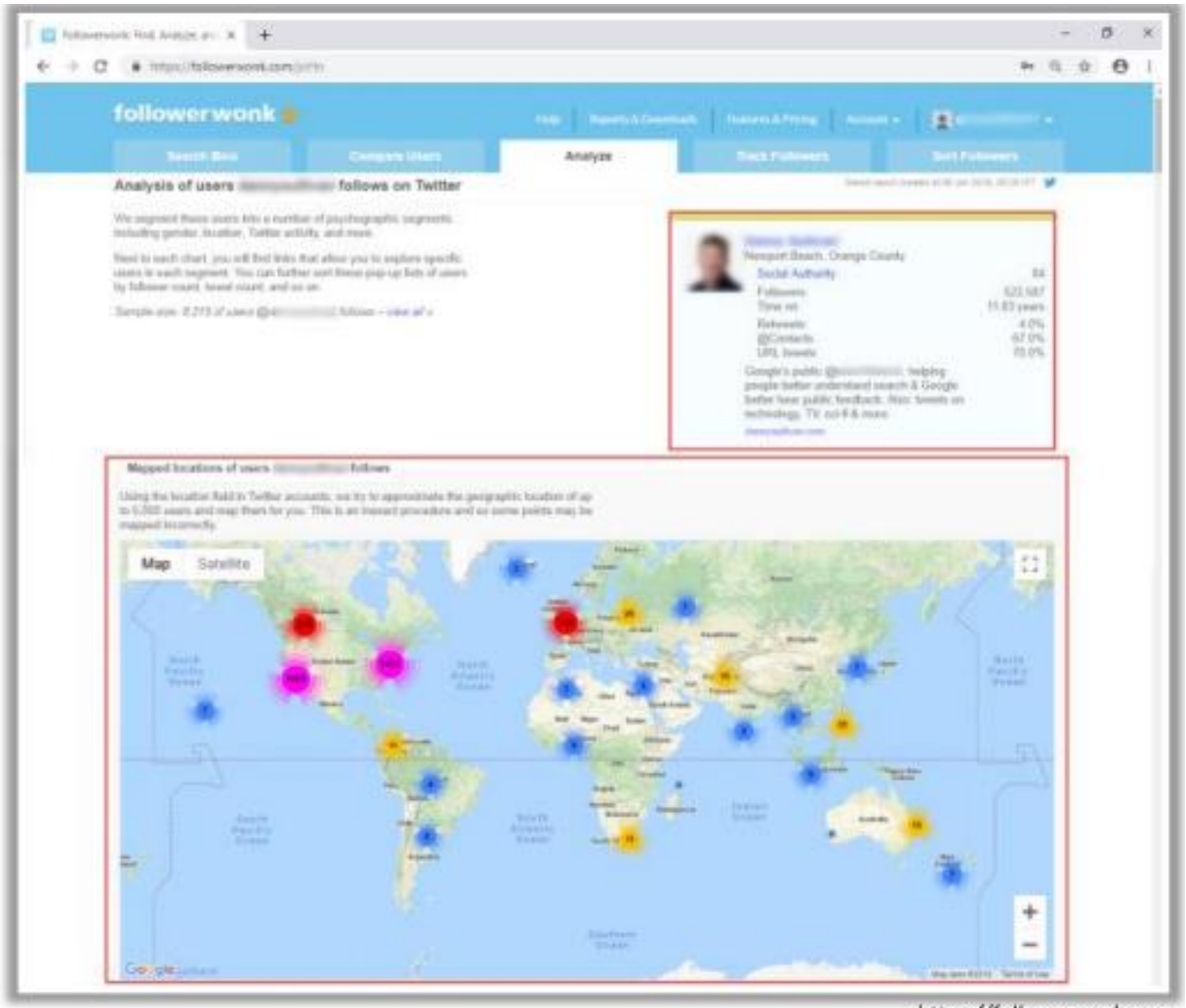
- Conducting location search on social media sites, such as Twitter, Instagram, and Facebook, helps attackers in **detecting the geolocation of the target**

- Attackers use online tools, such as **Followerwonk**, **Hootsuite**, and **Sysomos**, 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

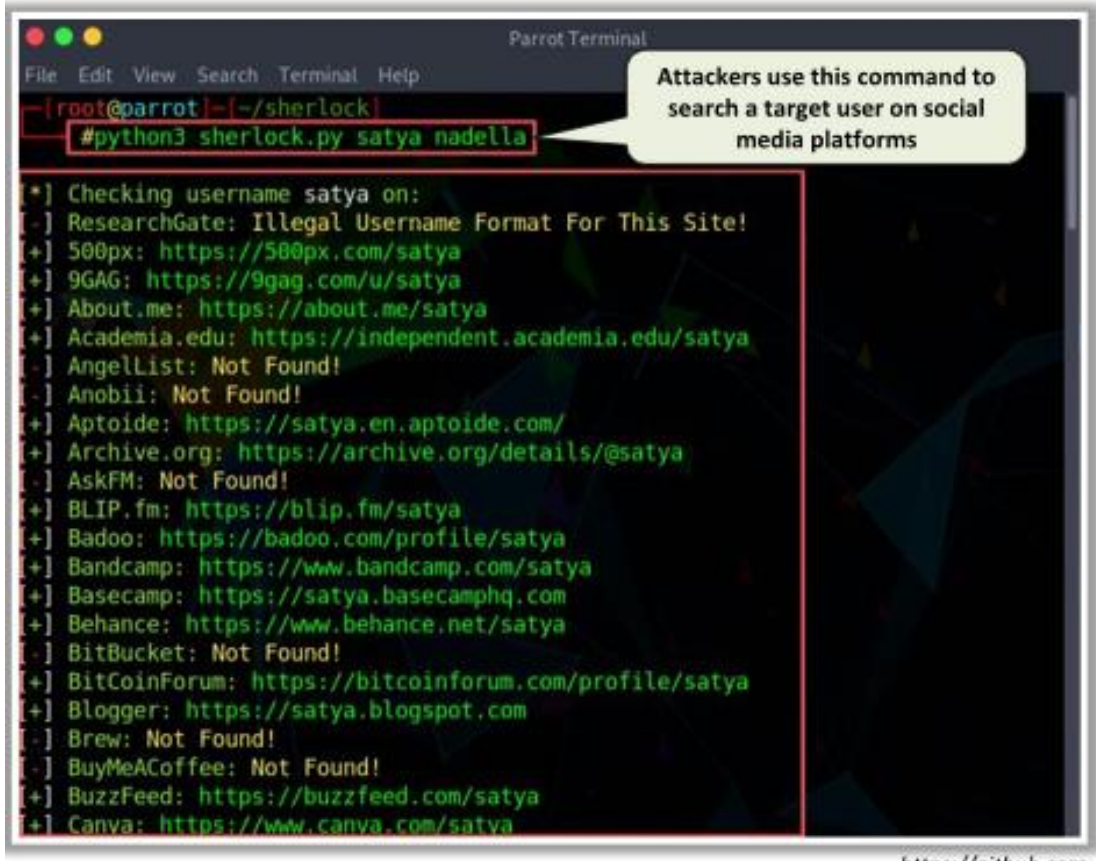
Followerwonk helps to explore and grow one's social graph by digging deeper into Twitter analytics



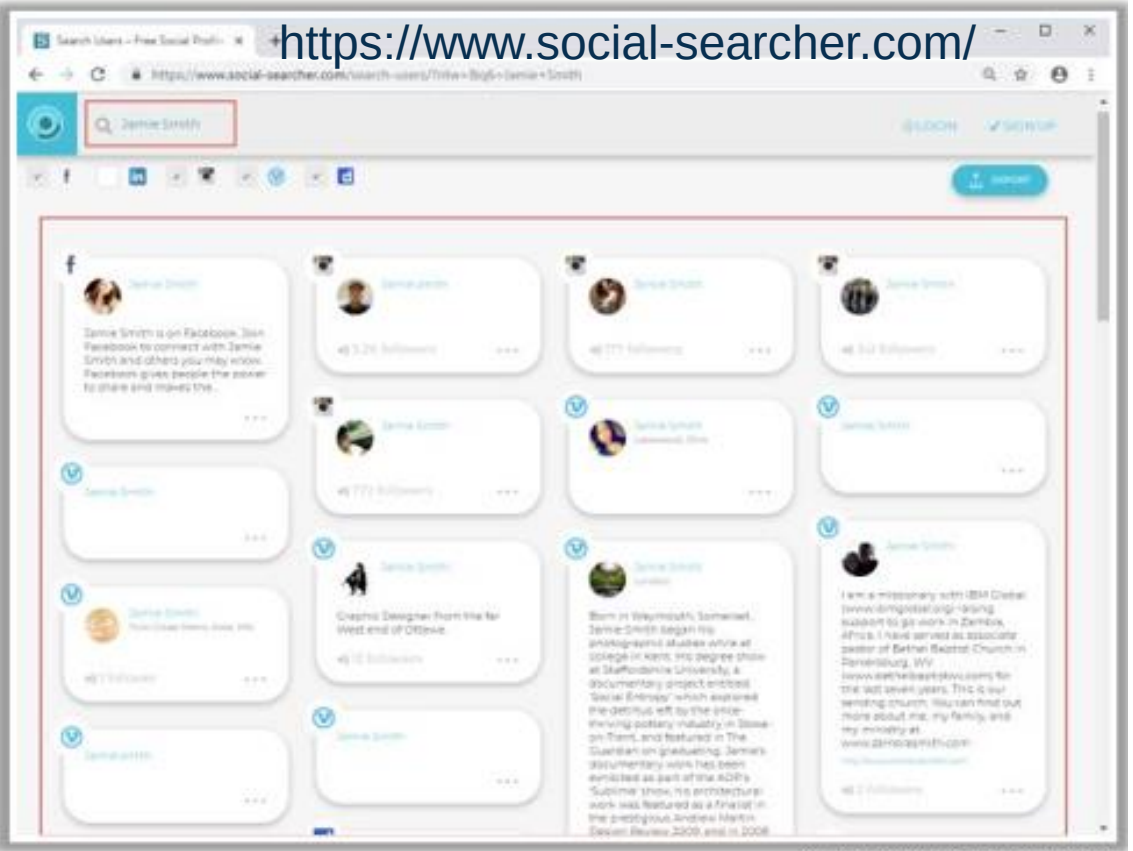
https://followerwonk.com

4. 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
Social Searcher	Social Searcher allows you to search for content in social networks in real-time and provides deep analytics data



https://github.com



https://www.social-searcher.com

WEBSITE FOOTPRINTING

Website Footprinting

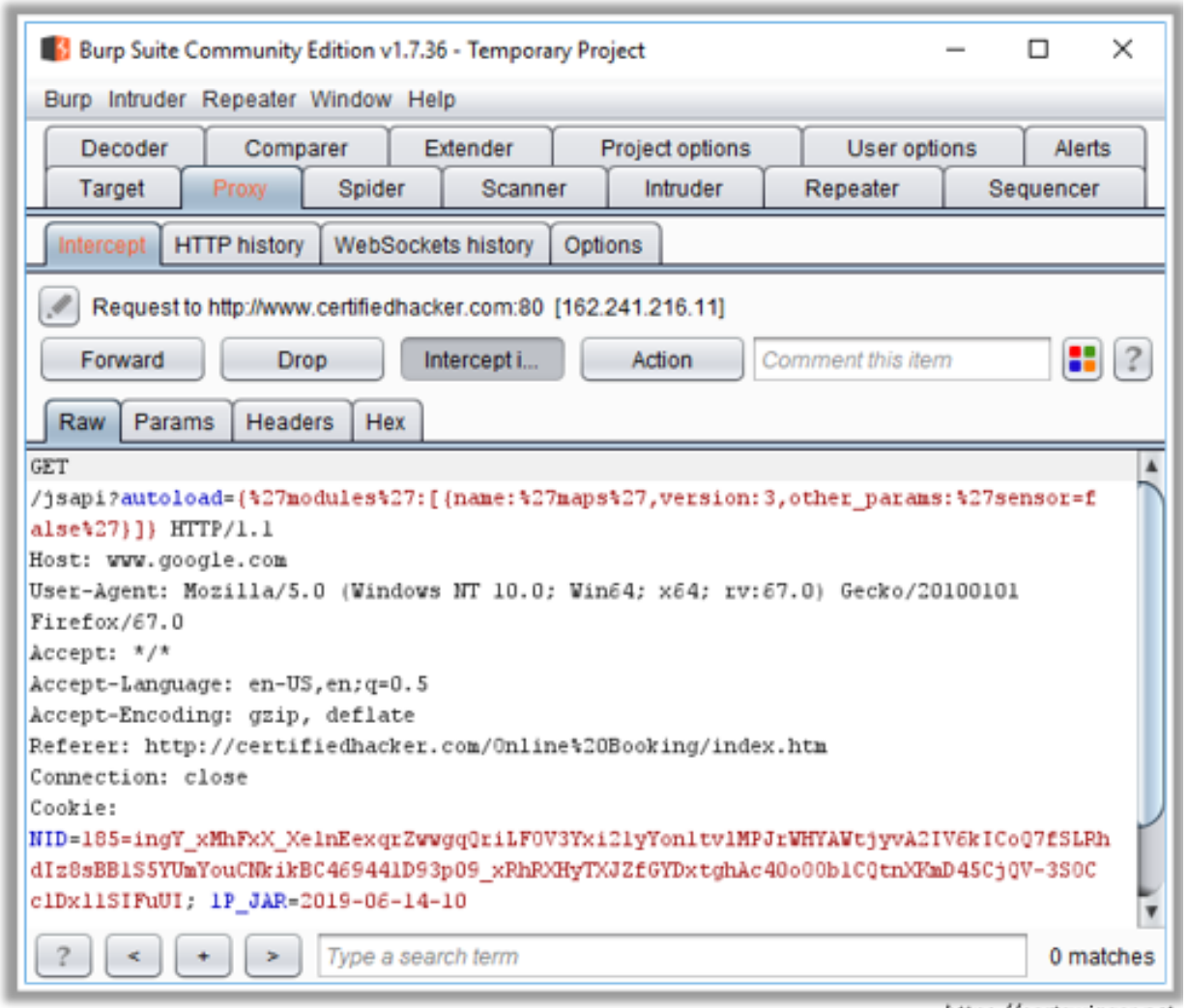
- Website footprinting refers to the **monitoring and analysis of the target organization's website** for information

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**, **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



https://portswigger.net

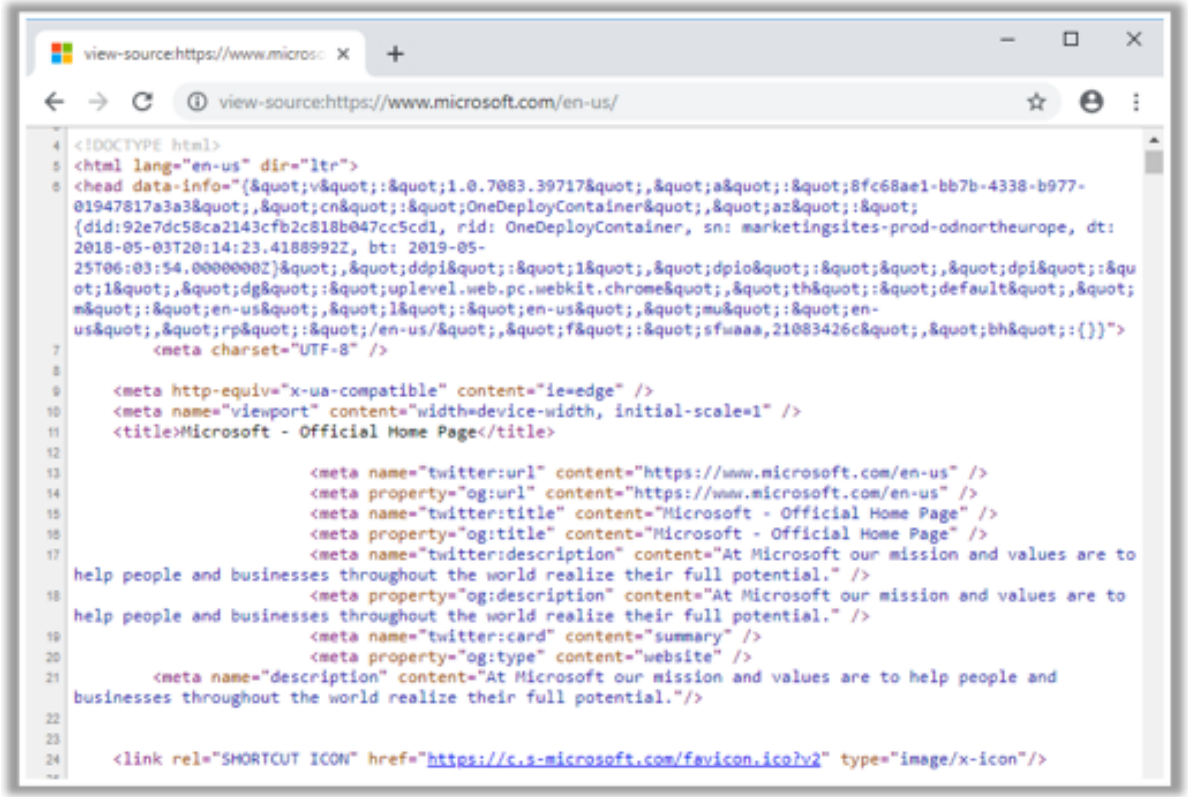
Cont.

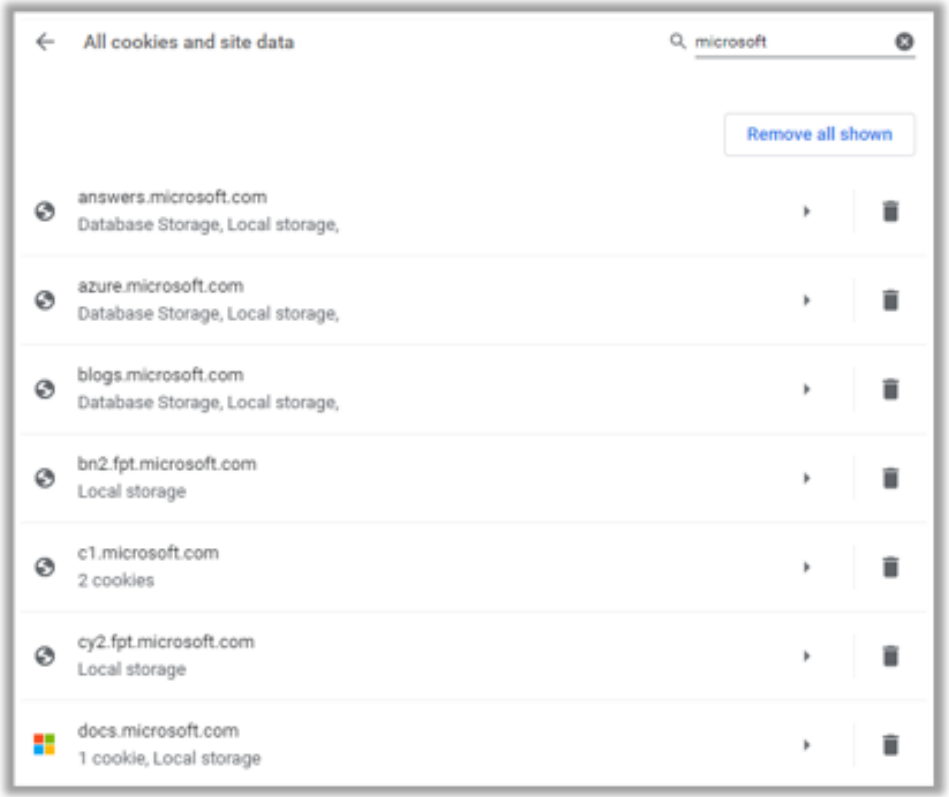
Examining the HTML source code may provide

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

Examining cookies may provide

- Software in use and its behavior
- Scripting platforms used



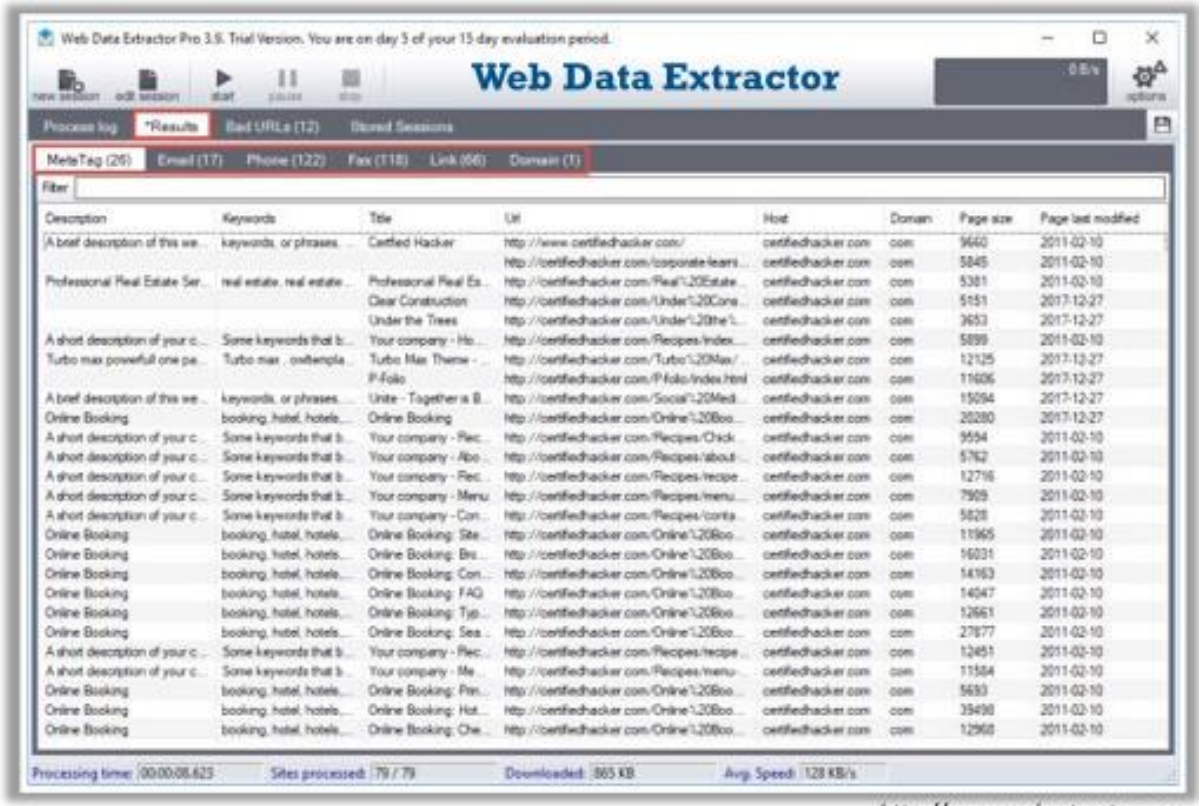


1. Website Footprinting using Web Spiders

- 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

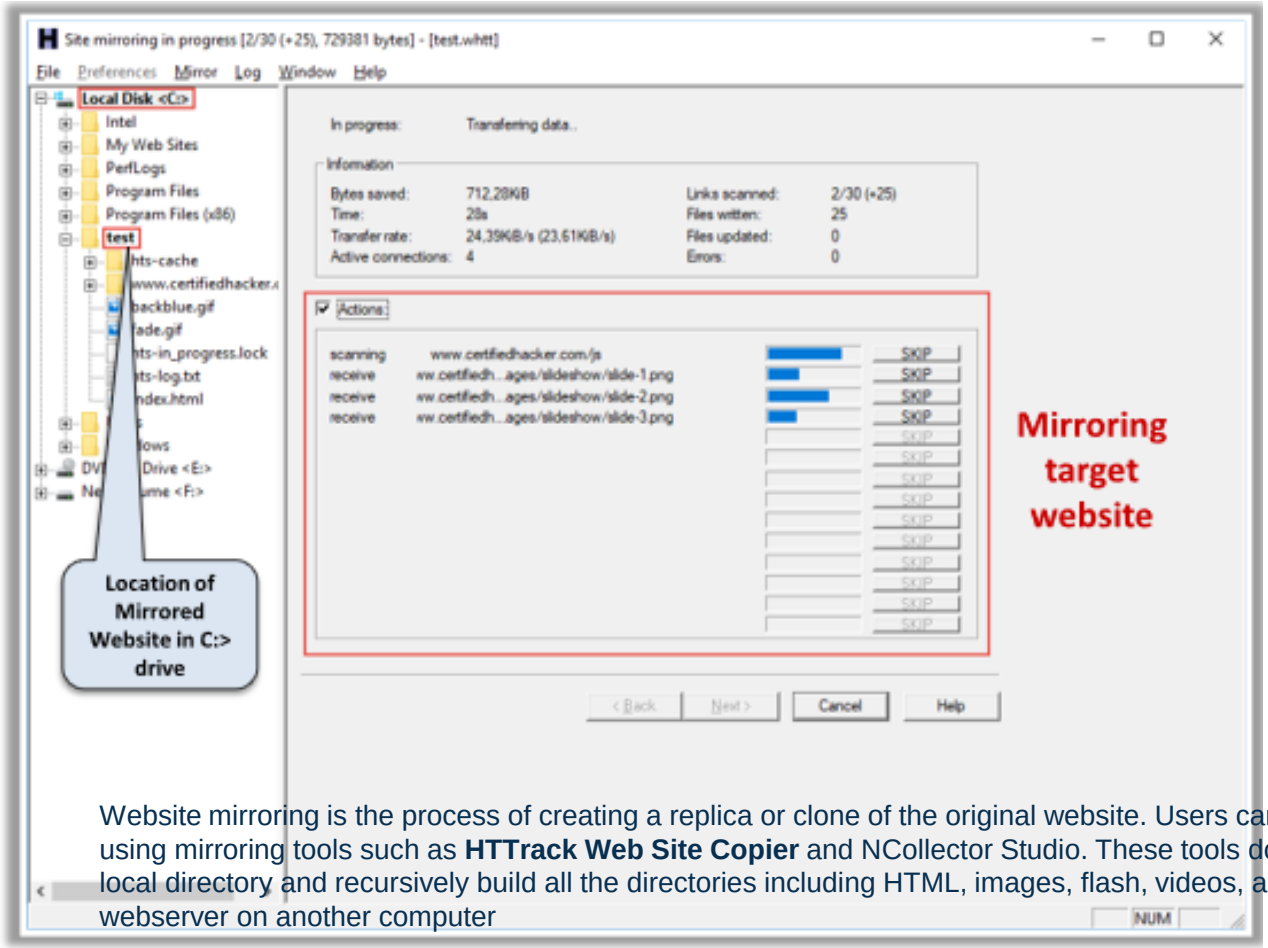
- Attackers use **standard web browsers** to walk through the target website functionalities
- The incoming and outgoing **traffic of the target website is monitored** and analyzed by tools that include features of both a web spider and an intercepting proxy
- Attackers use tools such as **Burp Suite**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



http://www.webextractor.com

2. Mirroring Entire Website

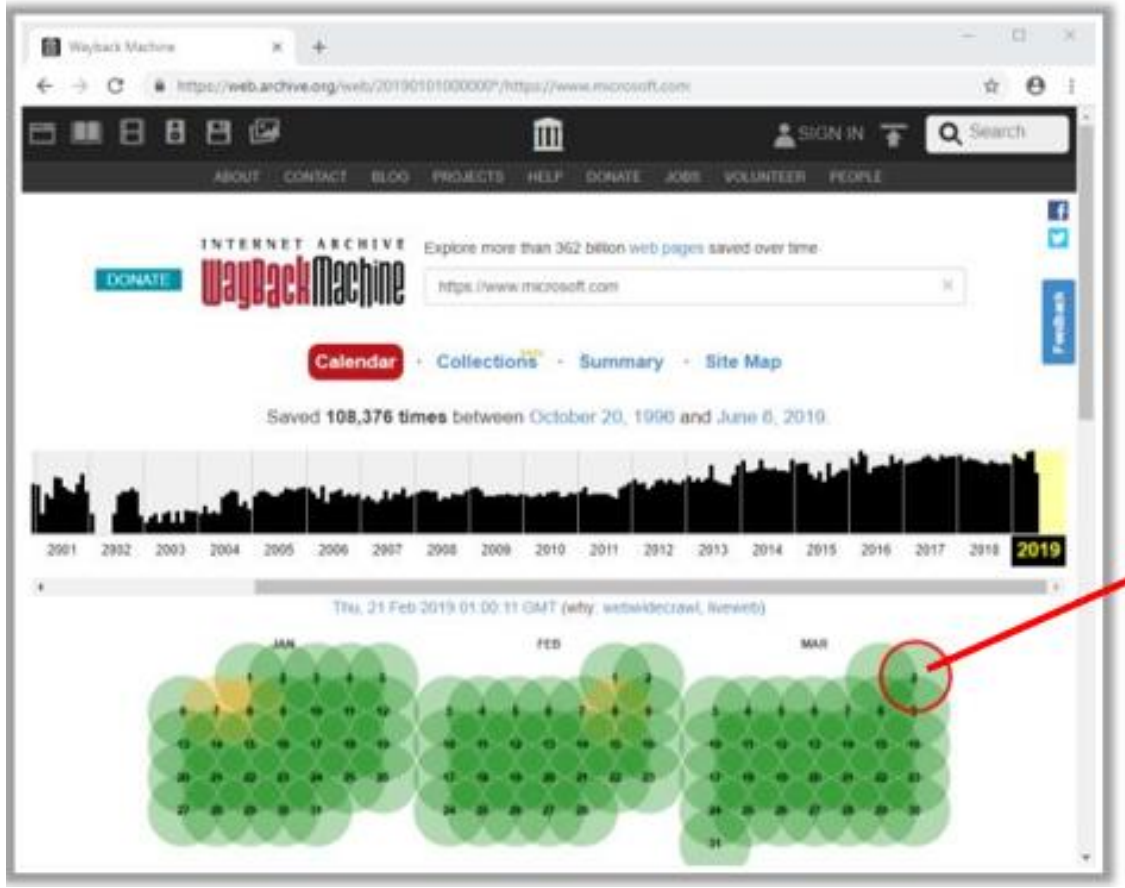
- Mirroring an entire website onto a local system enables an attacker to browse website offline; it also assists in finding **directory structure** and other valuable information from the mirrored copy without sending multiple requests to web server
- Web mirroring tools, such as HTTrack Web Site Copier, and NCollector Studio, 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

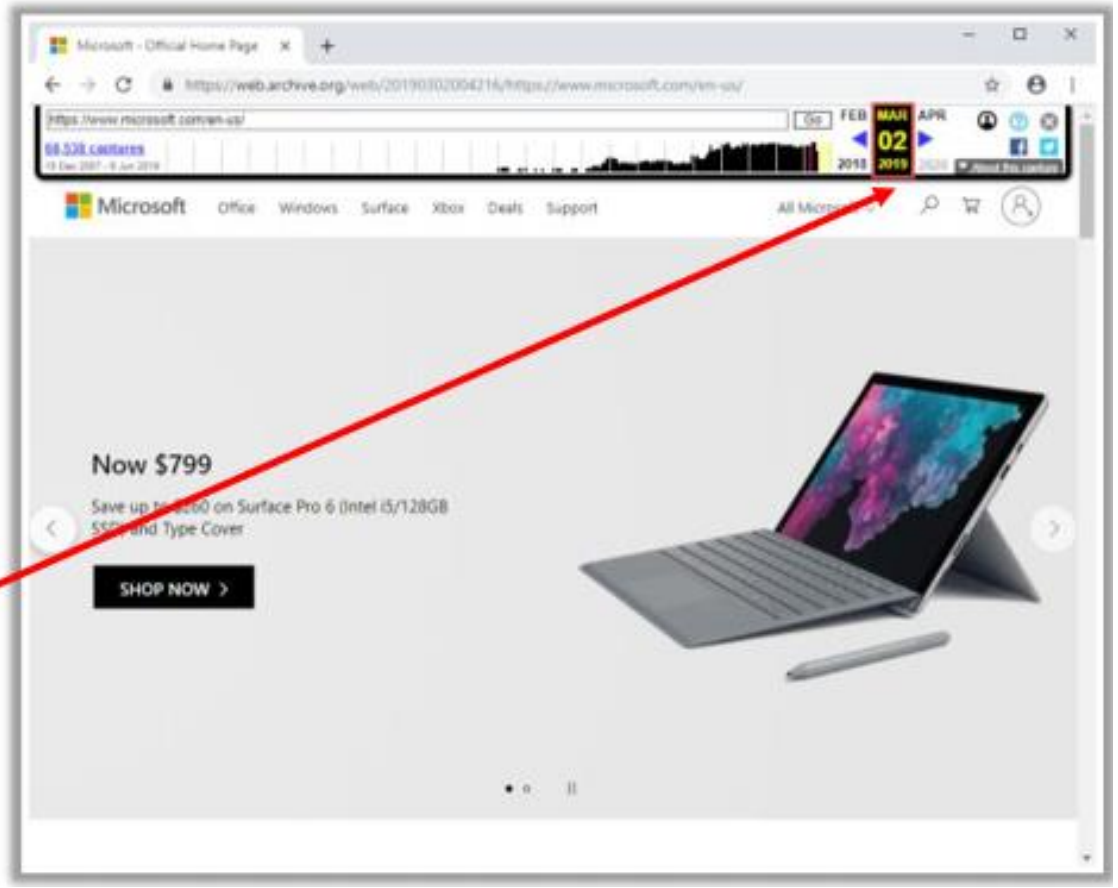


Website mirroring is the process of creating a replica or clone of the original website. Users can duplicate websites using mirroring tools such as **HTTrack Web Site Copier** and NCollector Studio. These tools download a website to a local directory and recursively build all the directories including HTML, images, flash, videos, and other files from the webserver on another computer

3. Extracting Website Information from https://archive.org **

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



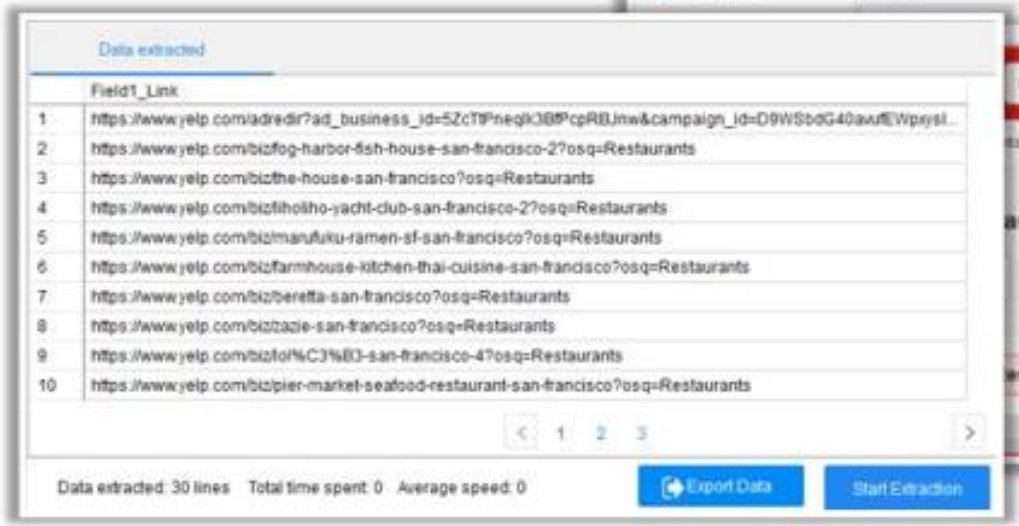


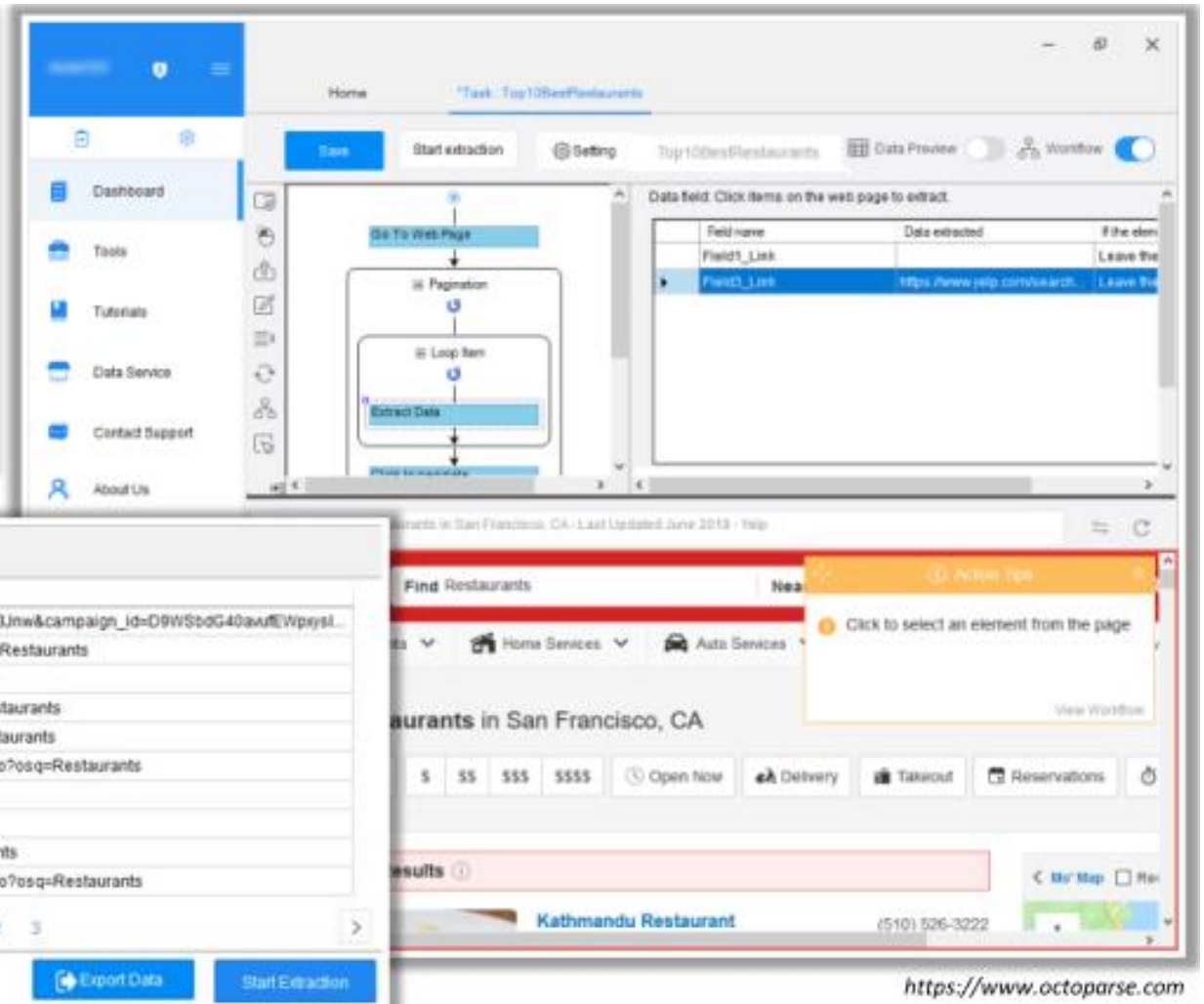
4. Extracting Website Links

- Extracting website links is an important part of website footprinting where an attacker analyses a target website to **determine its internal and external links**
- Attackers can use various online tools, such as **Octoparse**, **Netpeak Spider**, and **Link Extractor**, to extract linked images, scripts, iframes, and URLs of the target website

Octoparse

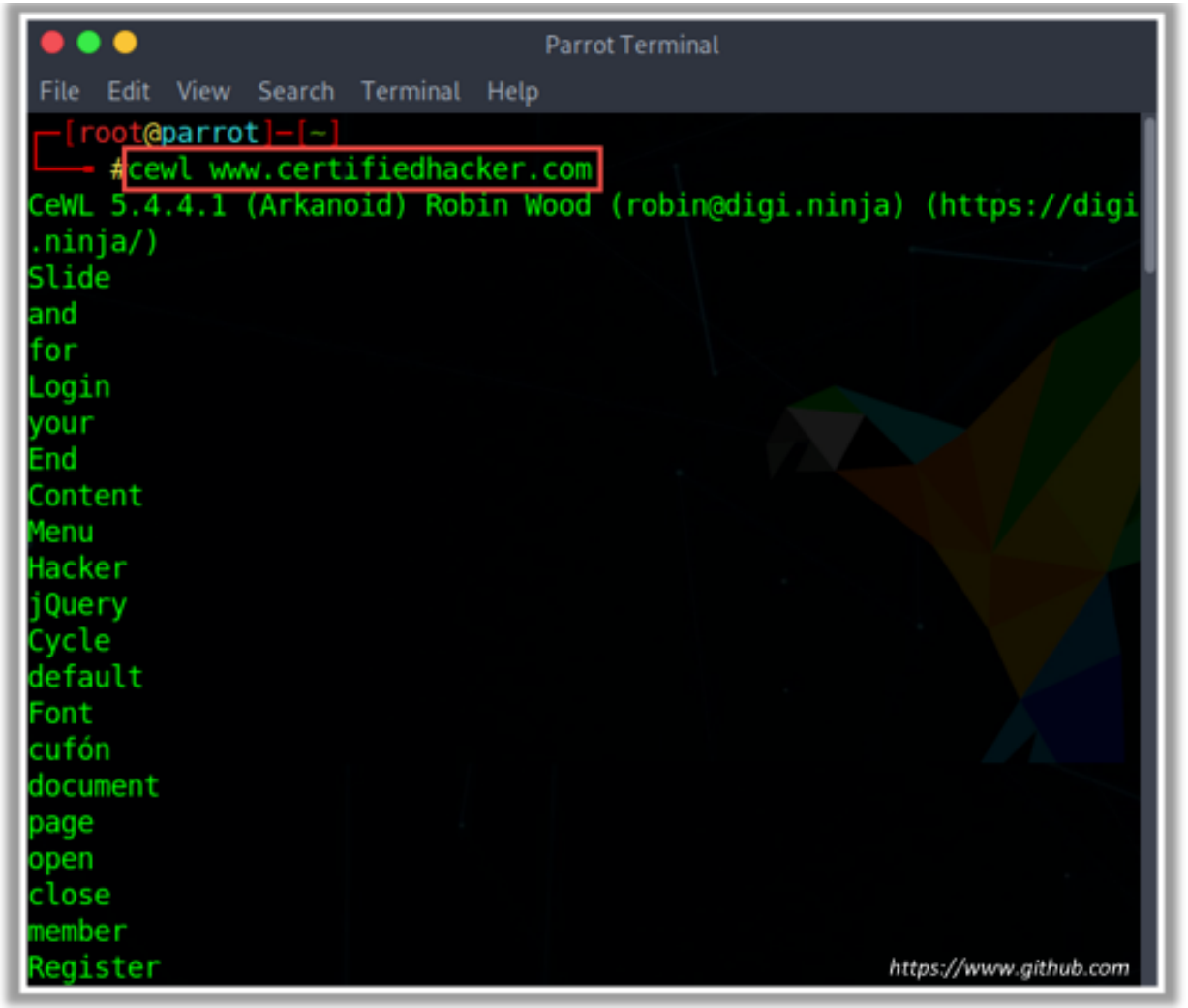
Octoparse offers **automatic data extraction** as it quickly scrapes web data without coding and turns web pages into structured data





5. Gathering Wordlist from the Target Website

- Attackers **gather a list of words available on the target website** to brute-force the email addresses gathered through search engines, social networking sites, web spidering, etc.
- Attackers use **CeWL** tool to gather a list of words from the target website
- Use the following command to extract all the words available on the target website:
  - `cewl www.certifiedhacker.com`



6. Extracting Metadata of Public Documents

- Useful information may reside on the target organization's website in the form of **pdf documents**, **Microsoft Word files**, etc.
- Attackers use metadata extraction tools, such as **Metagoofil**, **Exiftool**, and Web Data Extractor, to extract metadata and hidden information
- Attackers use this information to perform **social engineering** and other attacks

Metagoofil

Metagoofil **extracts the metadata of public documents** (pdf, doc, xls, ppt, docx, pptx, xlsx, etc.) belonging to a target company

```
****************************************
* Metagoofil Ver 2.1 -                 *
* Christian Martorella                 *
* Edge-Security.com                    *
* cmartorella_at_edge-security.com     *
* Blackhat Arsenal Edition             *
****************************************

[-] Starting online search...

[-] Searching for doc files, with a limit of 200
        Searching 100 results...
        Searching 200 results...
Results: 4 files found
Starting to download 50 of them:
----------------------------------------

[1/50] /webhp?hl=en
Error downloading /webhp?hl=en
[2/50] /intl/en/ads
Error downloading /intl/en/ads
[3/50] /services
Error downloading /services
[4/50] /intl/en/policies/

[-] Searching for pdf files, with a limit of 200
        Searching 100 results...
        Searching 200 results...
Results: 34 files found
Starting to download 50 of them:
```

https://code.google.com

7. Other Techniques for Website Footprinting

Monitoring Web Pages for Updates and Changes

- Attackers use web updates monitoring tools, such as **WebSite-Watcher** and **VisualPing**, to detect changes or updates in a target website, and they analyze the gathered information to detect underlying vulnerabilities in the target website

Searching for Contact Information, Email Addresses, and Telephone Numbers from Company Website

- Attackers can search the target company's website to **obtain crucial information** about the company, such as the company's contact details, location, partner information, news, and links to other sites

Searching for Web Pages Posting Patterns and Revision Numbers

- Attackers can search for **copyright notices** and revision numbers on the web and can use these details to perform deep analyses on the target organization

Monitoring Website Traffic of Target Company

- Attackers use website traffic monitoring tools, such as **Web-Stat**, **Alexa**, and **Monitis**, to collect information about the target company's website, such as total visitors, page views, bounce rate, and site ranking

EMAIL FOOTPRINTING

Email Footprinting

This section describes:

- How to track email communications
- How to collect information from email headers, and
- Email tracking tools

1. 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 such attacks

```
Delivered-To: [redacted]@gmail.com
Received: by 2002:a8a:a99:0:0:0:0:0 with SMTP
        Sun, 9 Jun 2019 21:09:48 -0700 (PDT)
Return-Path: <[redacted]@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id v17sor28[redacted]09.48
        for <[redacted]@gmail.com>
        (Google Transport Security);
        Sun, 09 Jun 2019 21:09:48 -0700 (PDT)
Received-SPF: pass (google.com: domain of [redacted]@gmail.com designates 209.85.220.41 as
permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@gmail.com header.s=20161025 header.b=s6SMnvzN;
       spf=pass (google.com: domain of [redacted]@gmail.com designates 209.85.220.41 as
permitted sender) smtp.mailfrom=[redacted]@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
DKIM-Signature: v=1; a=rsa-sha256; [redacted]
        d=gmail.com; s=20161025;
        h=mime-version:from:date:message-id:subject:to;
        bh=nheQC6dgq1LhKwkOykBx4gYW0VwtRRaK2KrErWhvfCg=;
        b=s6SMnvzNwWAeedUZF5r7LGPdGSiUyxSKDxvLIBGHvEcf/pIIqx8KkNR2JGfOMPVXAL
         e763O+SPbK+M54CPx9hkvdbYhbcVgUZFuEvp3J/fPvIliT7Blf8jGXWqvvxwQhTH4+/g
         XeIE0g6h98SYL4lvePj8I9hw1xvjym8QYRoCgEqWE8JVRfqmNcOxNBa6yoxuOVIJRT0A
         aFdUZS3KJMWbG8gBU6hS+bHrr3no37OYJgLlh/YwkLTx76h7BgDYBzHcyg+ZPA+HvK5K
         3BWvrqeaGvGeZWh6xaS6LNmhf7CIuuxa/skSls1pfsKIeJv1qeCAV0Cqi34JC292HRn2
         YCxw==
MIME-Version: 1.0
From: [redacted] <[redacted]@gmail.com>
Date: Mon, 10 Jun 2019 09:39:37 +0530
Message-ID: <CA++=zy1VzQ1gFmUDByZzqE9OSbjwFYK7[redacted]com>
Subject: Check Out Daily News Feed
To: [redacted]@gmail.com
```

The address from which the message was sent

Date and time received by the originator's email servers

Sender's IP address

Sender's mail server

Authentication system used by sender's mail server

Sender's full name

Date and time of message sent

Cont.

Information about the victim gathered using email tracking tools includes:

1. **Recipient's System IP address**: Allows tracking of the recipient's IP address
2. **Geolocation**: Estimates and displays the location of the recipient on the map and may even calculate the distance from the attacker's location
3. **Email Received and Read**: Notifies the attacker when the email is received and read by the recipient
4. **Read Duration**: The time spent by the recipient in reading the email sent by the sender
5. **Proxy Detection**: Provides information about the type of server used by the recipient
6. Links: Checks whether the links sent to the recipient through email have been checked
7. **Operating System and Browser information**: Reveals information about the operating system and the browser used by the recipient. The attacker can use this information to find loopholes in that version of the operating system and browser to launch further attacks
8. **Forward Email**: Determines whether the email sent to the user is forwarded to another person
9. **Device Type**: Provides information about the type of device used to open and read the email, e.g., desktop computer, mobile device, or laptop
10. **Path Travelled**: Tracks the path through which the email traveled via email transfer agents from source to destination system

2. collect information from email headers

An email header contains the details of the sender, routing information, addressing scheme, date, subject, and recipient. Email headers also help attackers to trace the routing path taken by an email before it is delivered to the recipient. Each email header is a useful source of information for an attacker to launch attacks against the target. The process of viewing the email header varies with different email programs.

Commonly used email programs:

- eM Client
- Mailbird Lite
- Hiri
- Mozilla Thunderbird
- Spike
- Claws Mail
- SmarterMail Webmail
- Outlook

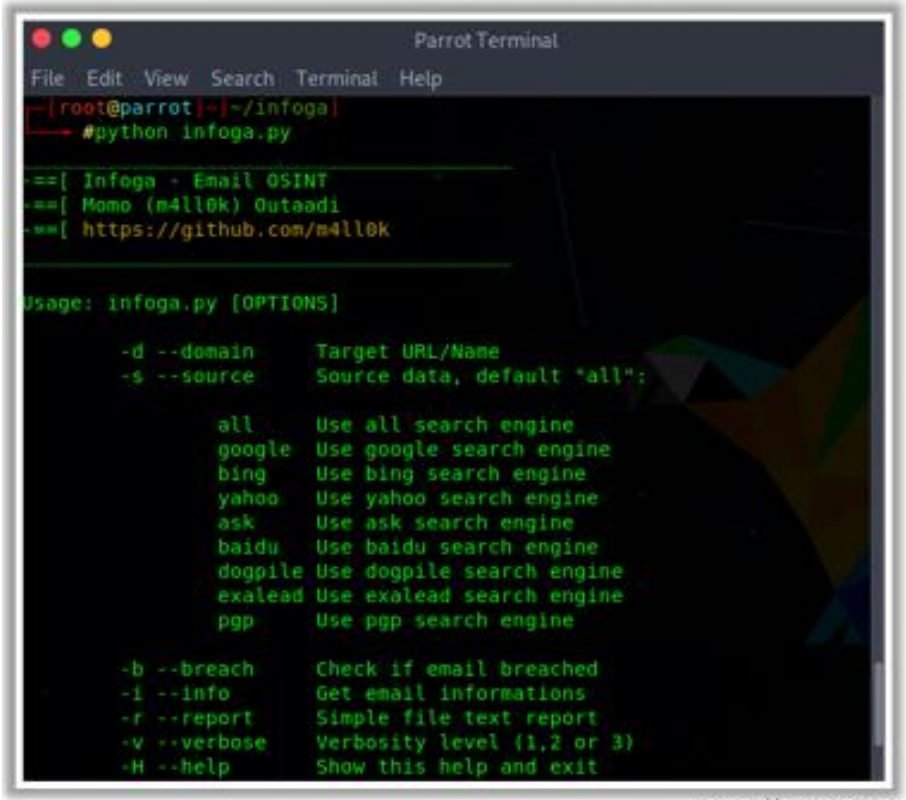
The email header contains the following information:

- Sender's mail server
- Date and time of receipt by the originator's email servers
- Authentication system used by the sender's mail server
- Data and time of sending the message
- A unique number assigned by mx.google.com to identify the message
- Sender's full name
- Sender's IP address and address from which the message was sent

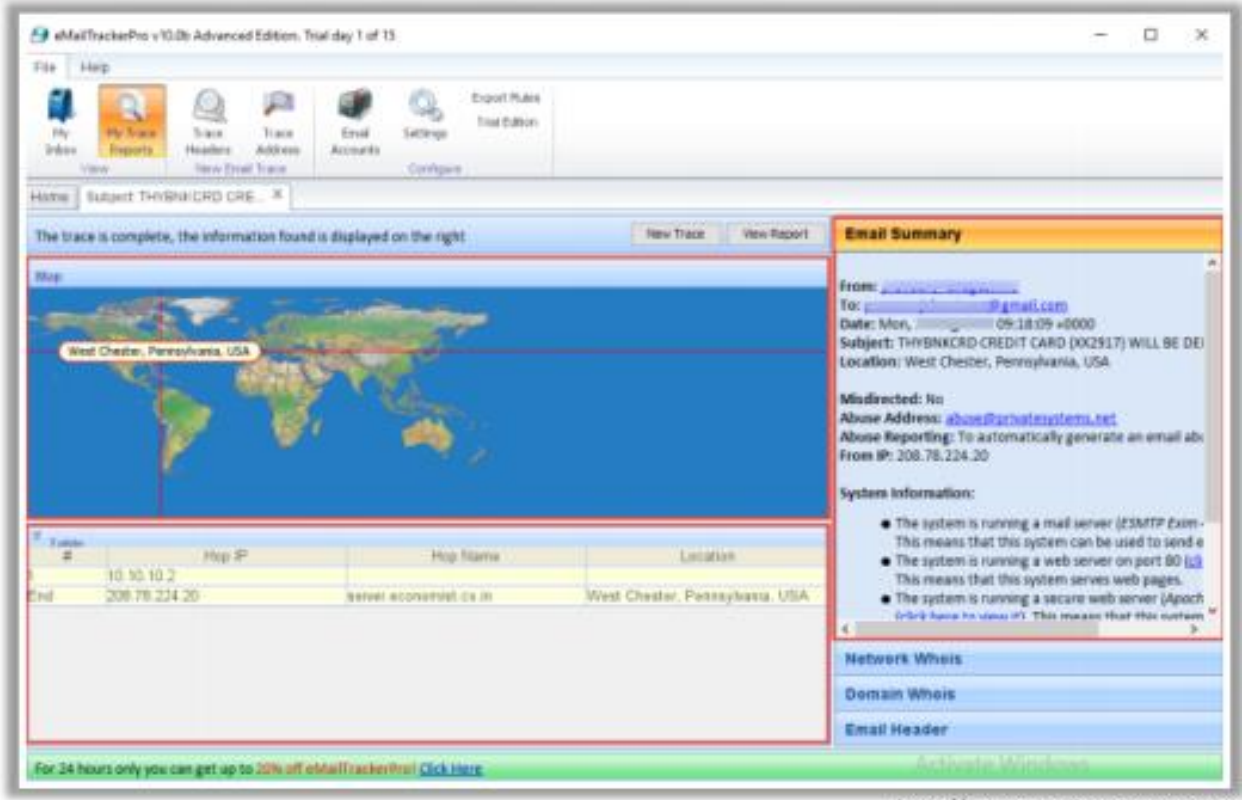
The attacker can trace and collect all this information by performing a detailed analysis of the complete email header.

3. 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



https://github.com



http://www.emailtrackerpro.com

WHOIS FOOTPRINTING

Whois Footprinting

- **Gathering network-related information** such as “Whois” information about the target organization is important when planning an attack.
- In this section, we will discuss Whois footprinting, which helps in
  - Gathering domain information such as information regarding the owner of an organization, its registrar, registration details, its name server, and contact information.
  - How to perform a Whois lookup
  - Analyze the Whois lookup results
  - Find IP geolocation information
  - Tools used to gather Whois information

1. 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

AFRINIC

RIPE NCC

lacnic

APNIC

2. 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

IP Address	207.46.232.182
Country	Singapore [SG]
Region	Singapore
City	Singapore
Coordinates of City	1.289670, 103.850070 (1°17'23"N 103°51'0"E)
ISP	Microsoft Corporation
Local Time	10 Jun, 2019 07:10 PM (UTC +08:00)
Domain	microsoft.com
Net Speed	(COMP) Company/T1
IDD & Area Code	(65) 06
ZIP Code	179431
Weather Station	Singapore (SNXX0006)

https://www.ip2location.com

DNS FOOTPRINTING

DNS Footprinting

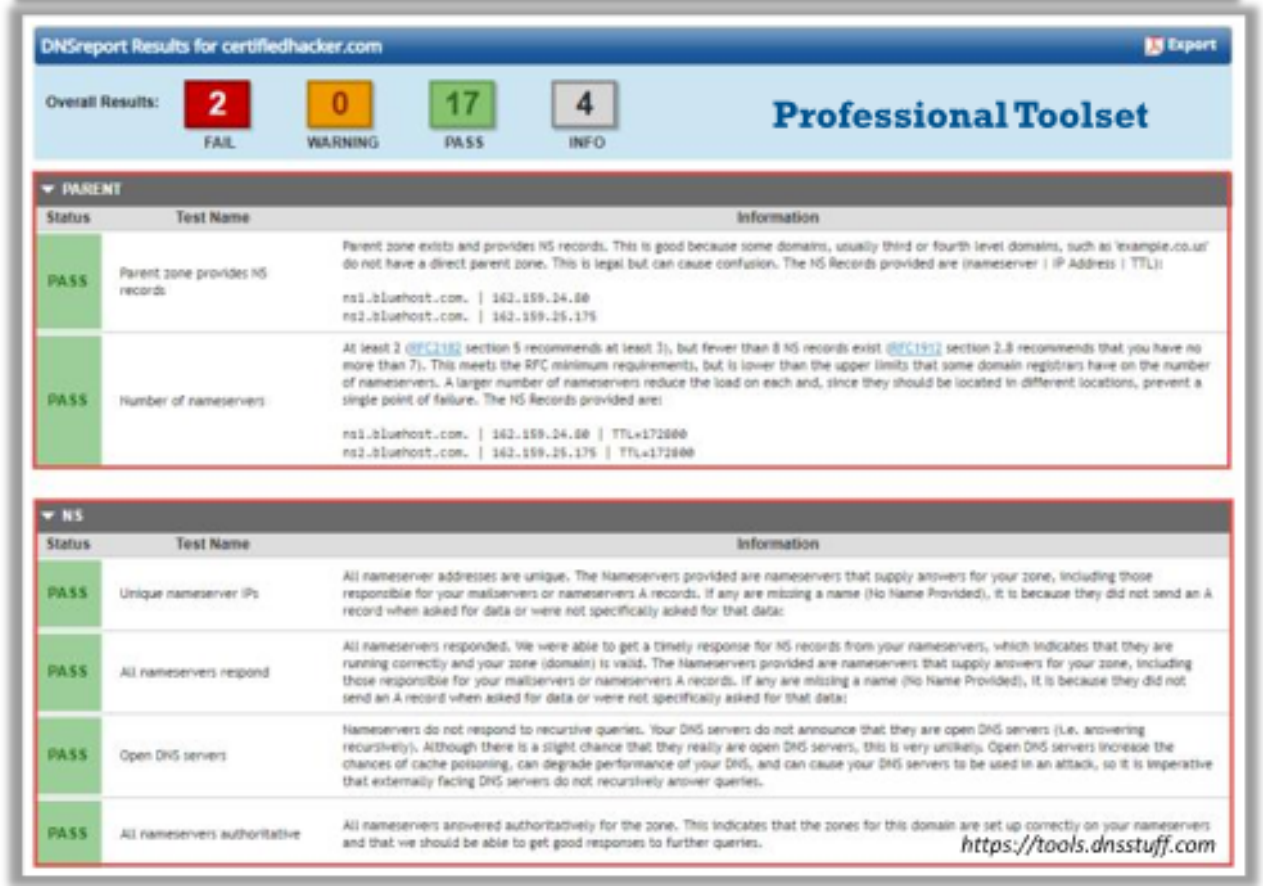
- After collecting Whois records about the target, the next phase in the footprinting methodology is DNS footprinting.
- Attackers **perform DNS footprinting to gather information about DNS servers, DNS records, and types of servers used** by the target organization.
- This information helps attackers to **identify the hosts connected** in the target network and perform further exploitation on the target organization.
- DNS footprinting reveals information about DNS zone data.
  - DNS domain names,
  - computer names,
  - IP addresses, and much more information about a network.
- An attacker uses DNS information to determine key hosts in the network and then performs social engineering attacks to gather even more information.

1. 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

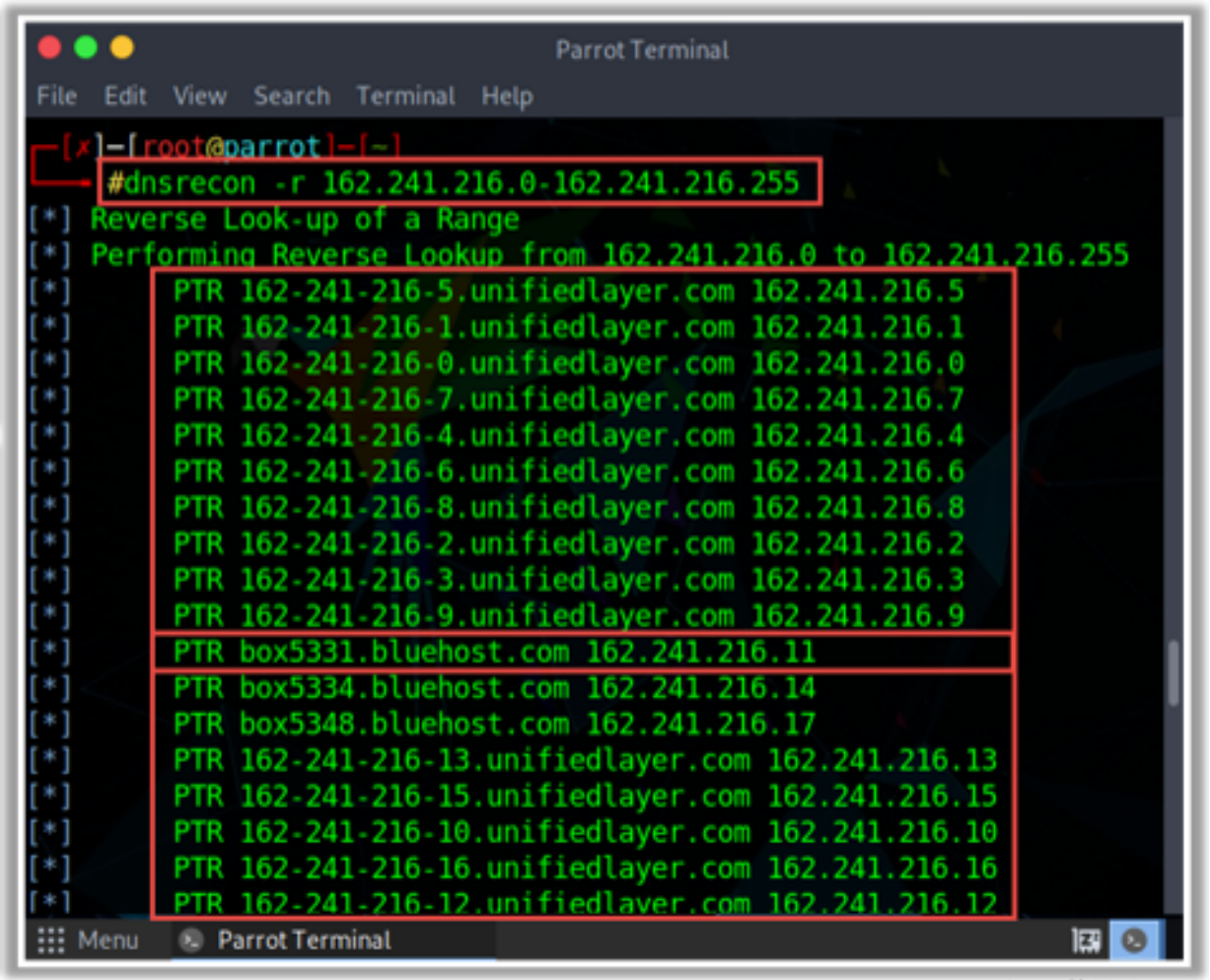
- Attackers query DNS servers using DNS interrogation tools, such as Professional Toolset and DNS Records, to **retrieve the record structure** that contains information about the target DNS



2. 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**, to perform the reverse DNS lookup on the target host
- Attackers can also find the other domains that share the same web server, using tools such as **Reverse IP Domain Check**

https://www.yougetsignal.com



https://github.com

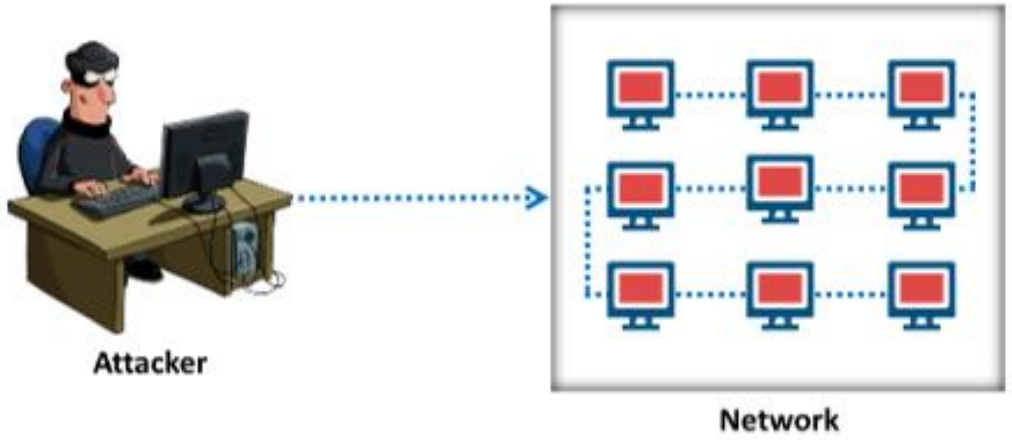
NETWORK FOOTPRINTING

Network Footprinting

- The next step after retrieving the DNS information is gathering network-related information.
- Network footprinting, a method of **gathering the footprint of the target organization's network**.
- This section describes how to locate the network range, traceroute analysis, and traceroute tools.

1. 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 ASSIGNMENT
Origin AS	*not provided*
Registration	Mon, 31 Mar 1997 05:00:00 GMT (Mon Mar 31 1997 local time)
Last Changed	Wed, 21 Aug 2013 00:16:49 GMT (Wed Aug 21 2013 local time)
Self	https://rdap.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
Kind	Org
Full Name	Microsoft Corporation
Handle	MSFT
Address	One Microsoft Way Redmond WA 98052 United States
Roles	Registrant
Registration	Fri, 10 Jul 1998 03:00:00 GMT (Fri Jul 10 1998 local time)
Last Changed	Sat, 28 Jan 2017 13:32:29 GMT (Sat Jan 28 2017 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://cert.microsoft.com.

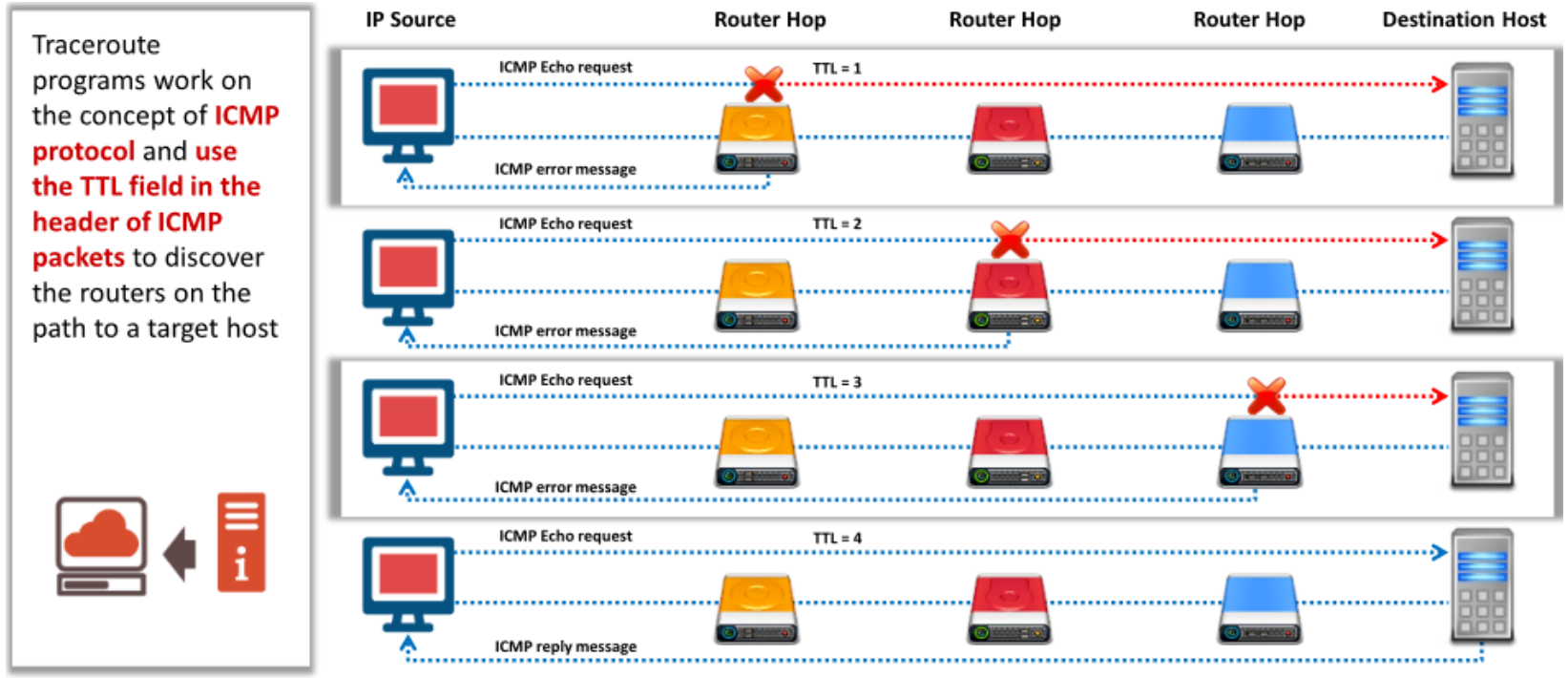
Network Whois Record

Queried whois.arin.net with "207.46.232.182"

2. Traceroute

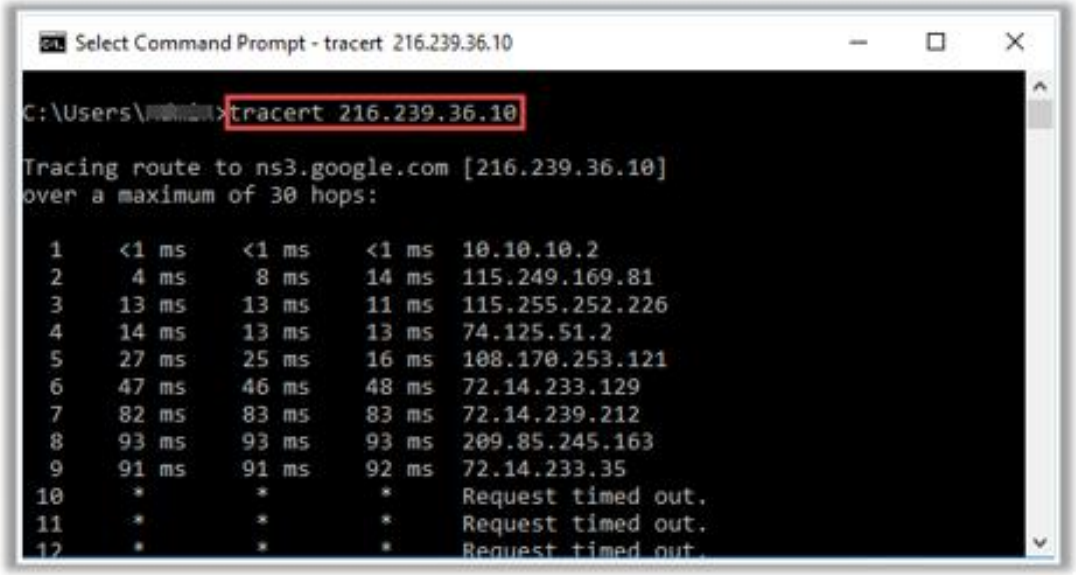
- Finding the route of the target host on the network is necessary to test against man-in-the-middle attacks and other related attacks.
- Most operating systems come with a Traceroute utility to perform this task. It **traces the path or route through which the target host packets travel in the network**.

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

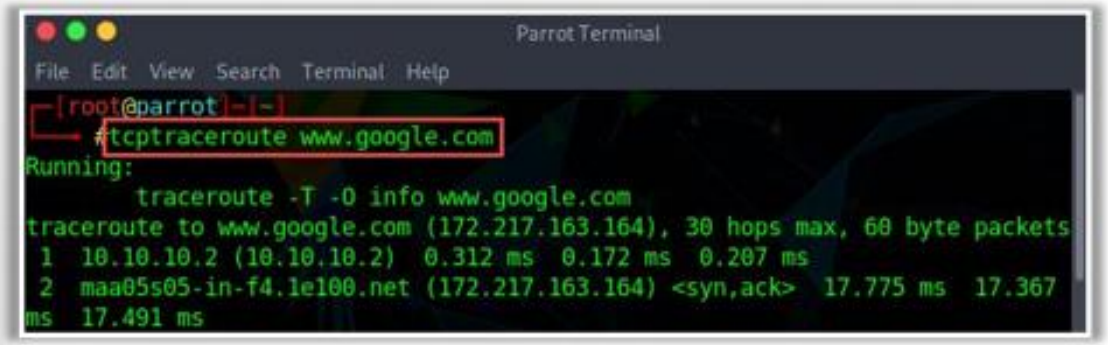


Cont,

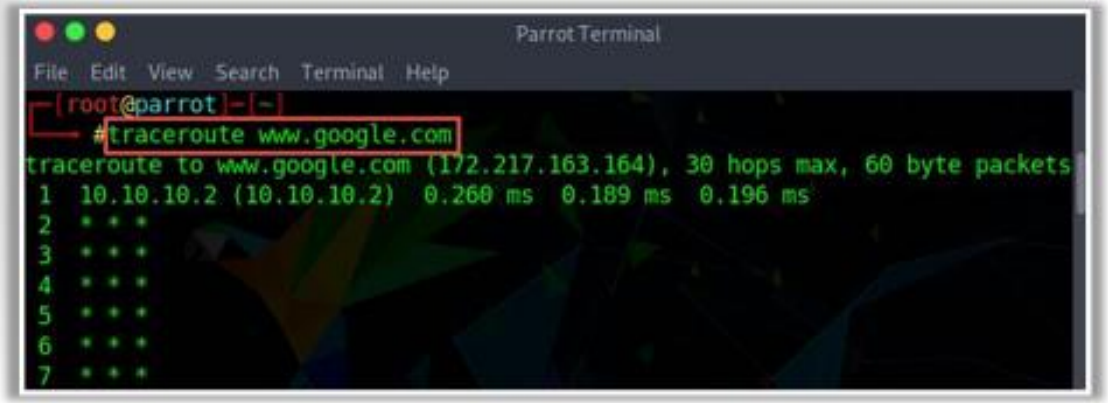
IMCP Traceroute



TCP Traceroute

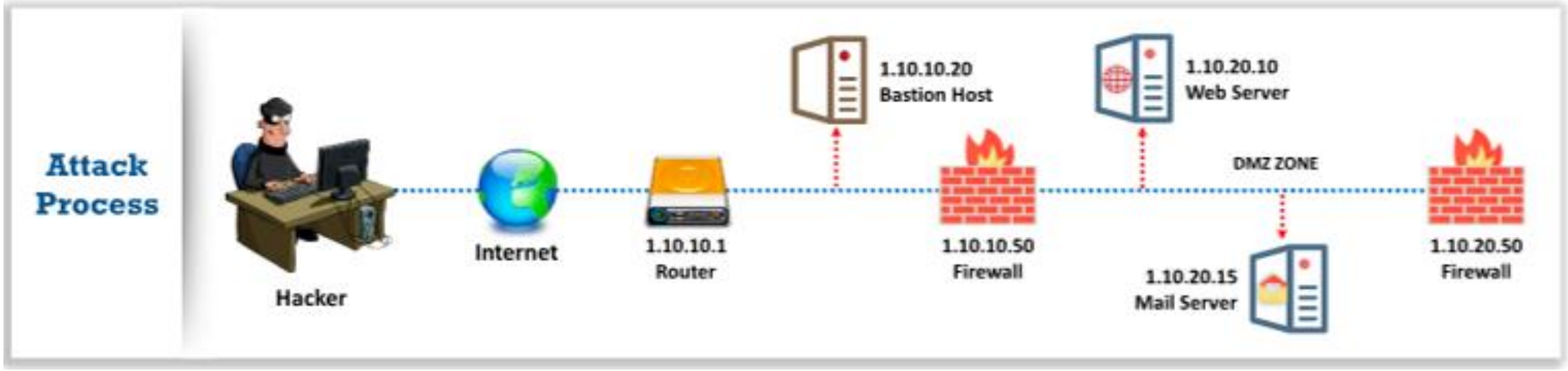


UDP Traceroute



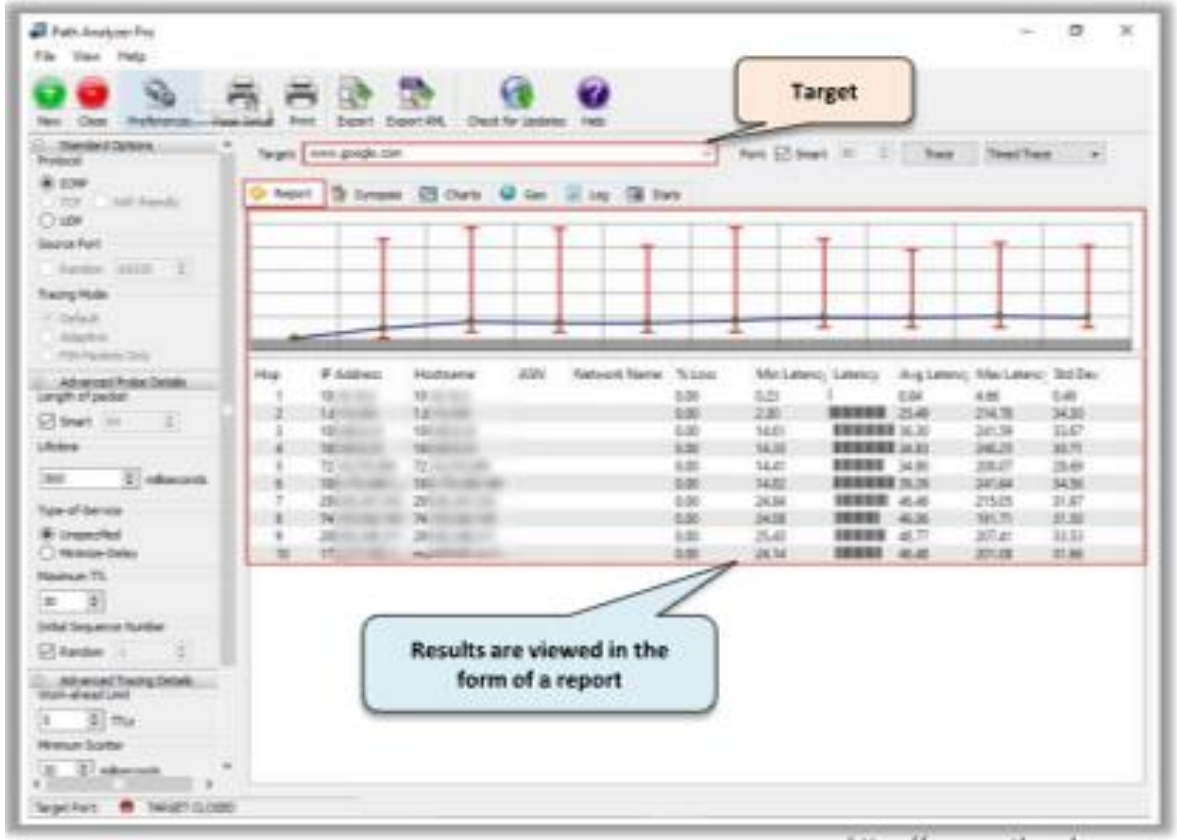
3. Traceroute Analysis

- Attackers conduct traceroute to extract information about **network topology**, **trusted routers**, and **firewall locations**
- 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 putting this information together, attackers can draw the **network diagram**

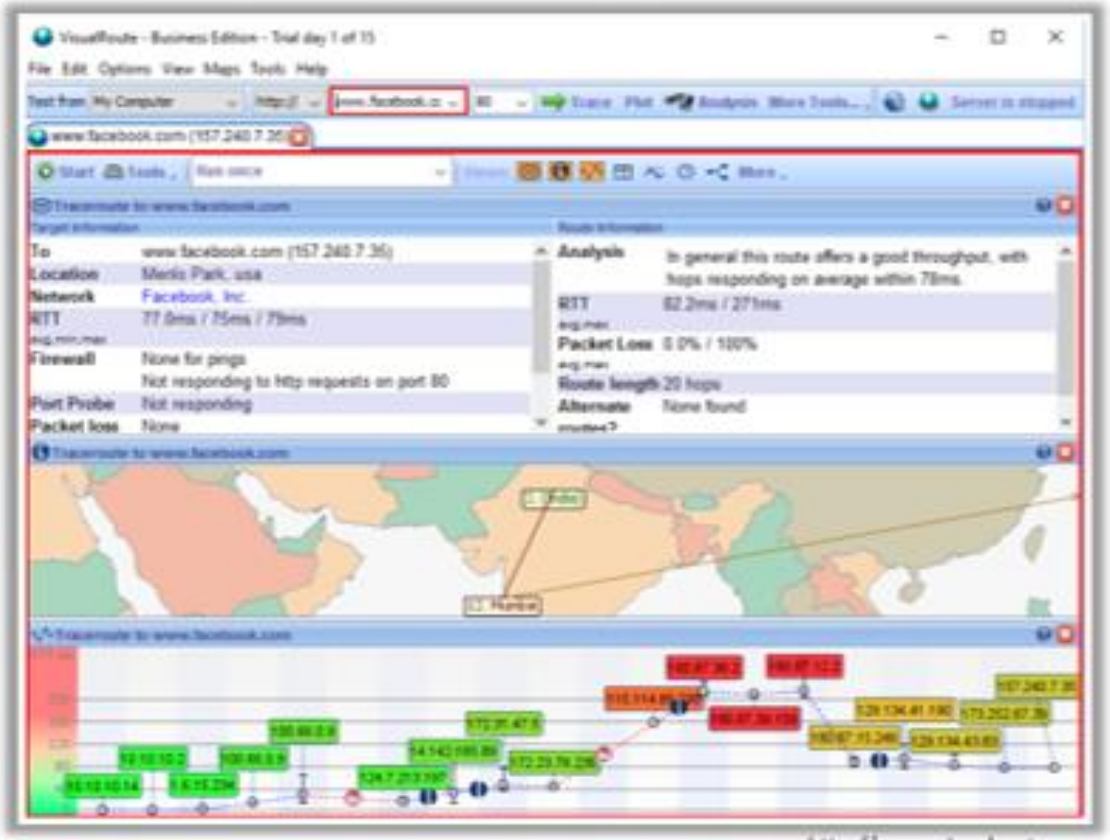


4. Traceroute Tools

Path Analyzer Pro	It **delivers network route tracing** with performance tests, DNS, Whois, and network resolution to investigate network issues
VisualRoute	It is a traceroute and network diagnostic tool that **identifies the geographical location of routers**, servers, and other IP devices



https://www.pathanalyzer.com



http://www.visualroute.com

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
- User names 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

The art of obtaining information from people by exploiting their weaknesses.

1. 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

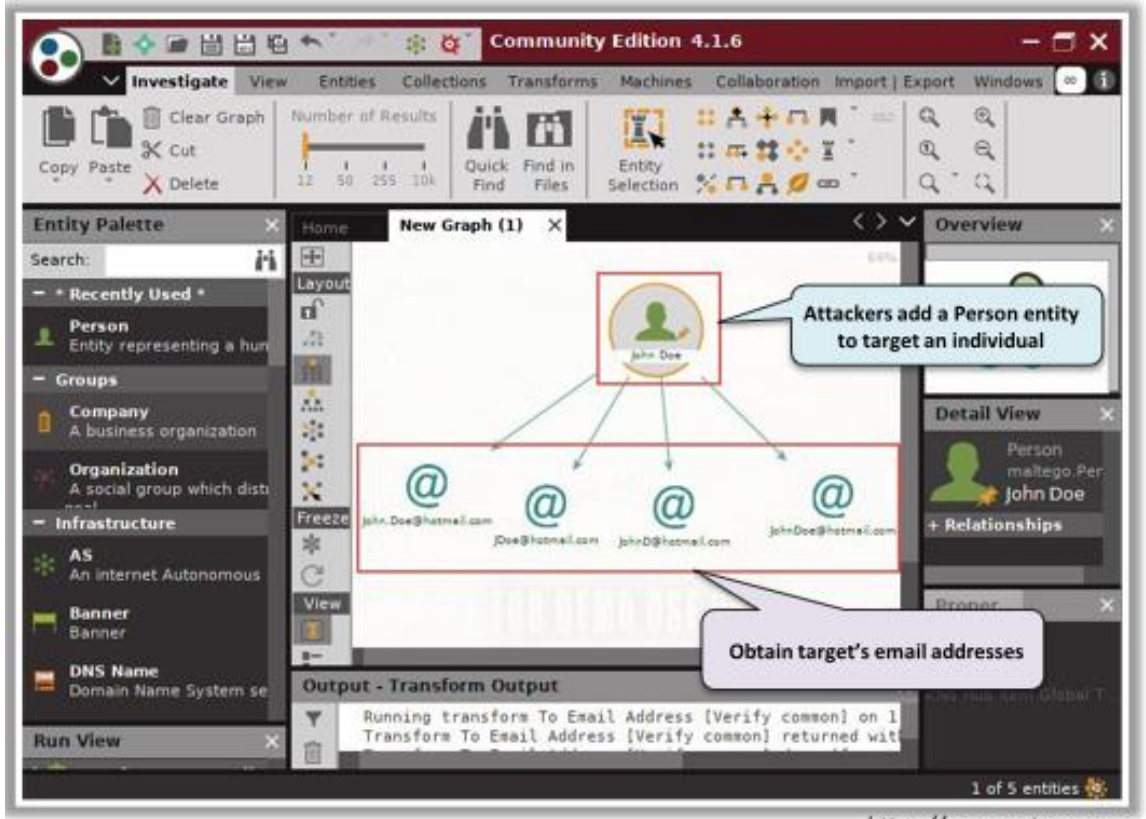
- **Pretending to be a legitimate or authorized person** and using the phone or other communication medium to mislead targets and trick them into revealing information

3. Footprinting Tools

1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting Tools
4. Footprinting Countermeasures

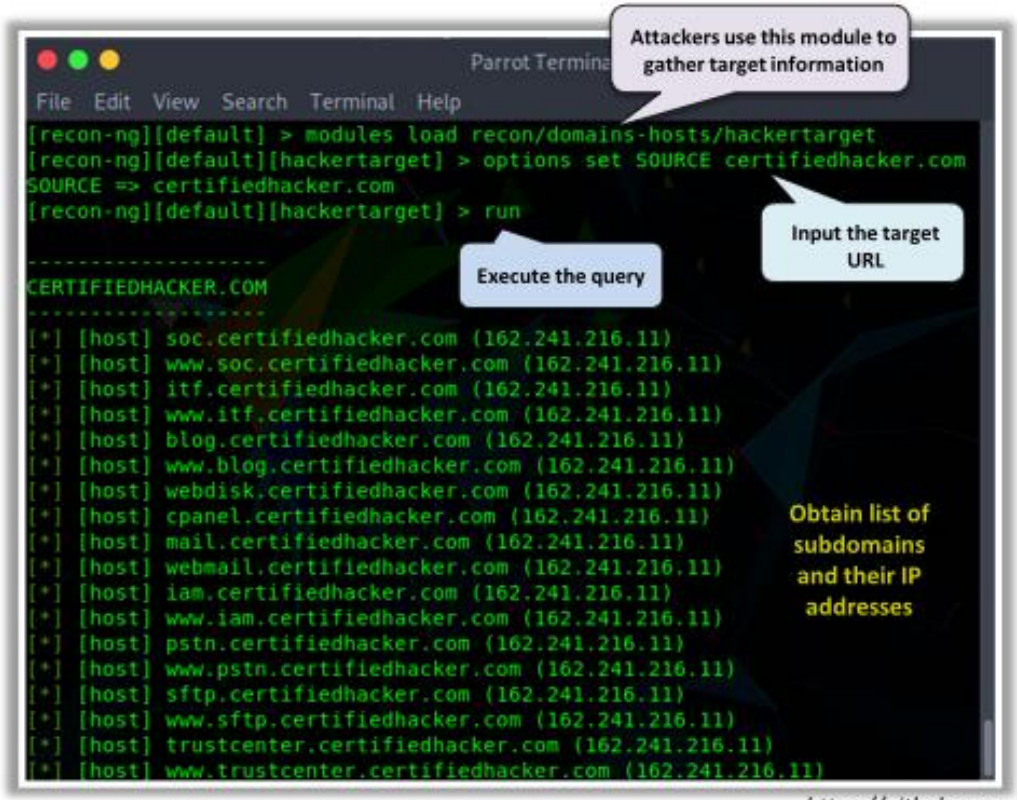
Maltego and Recon-ng

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



https://www.paterva.com

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

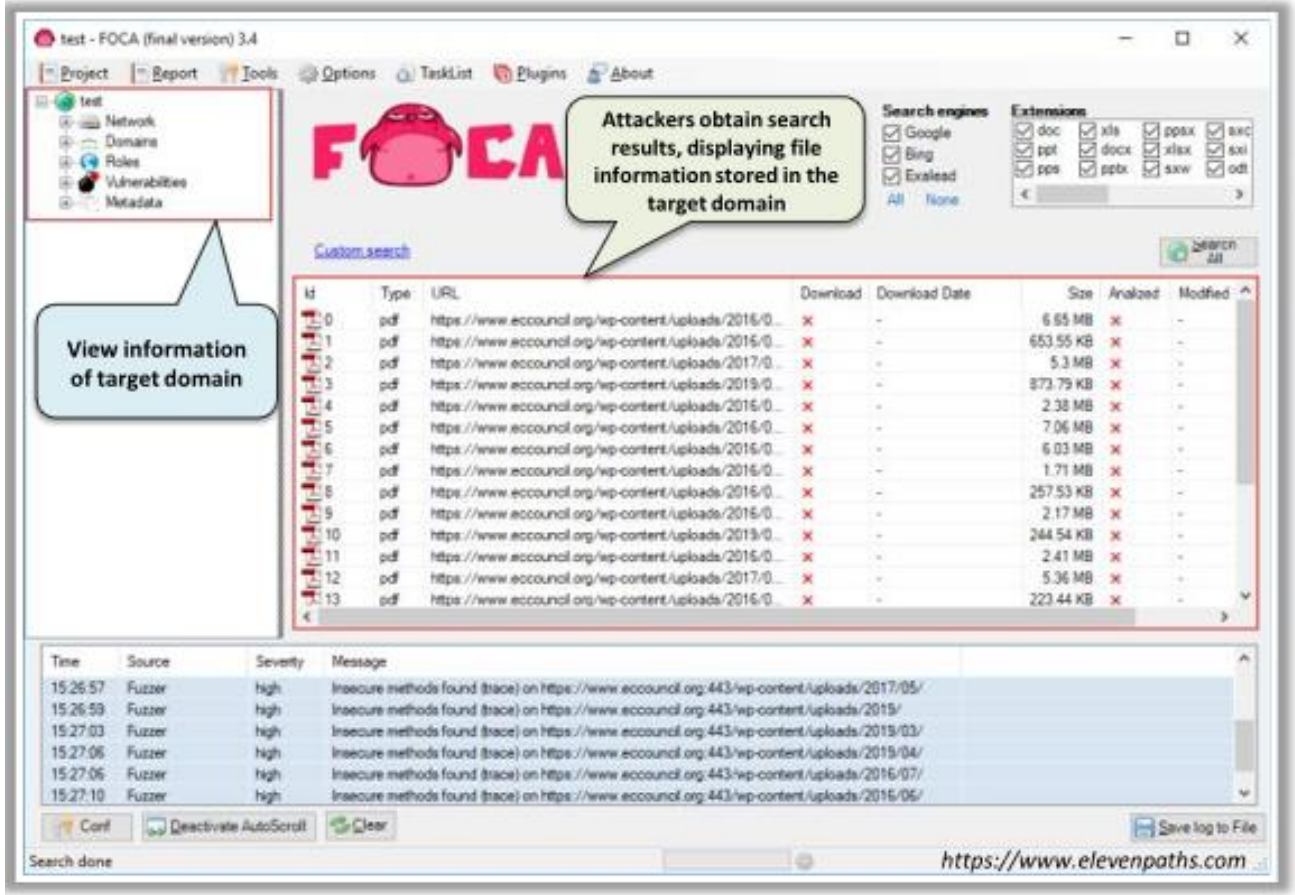


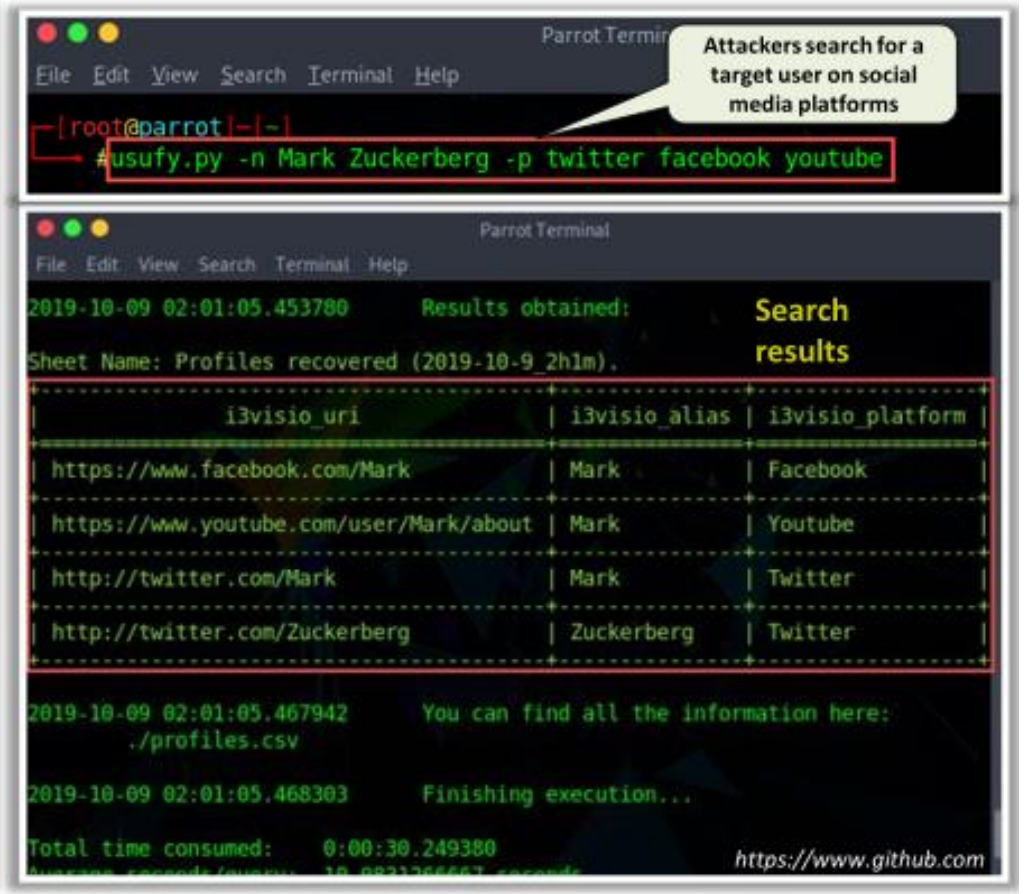
https://github.com

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

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

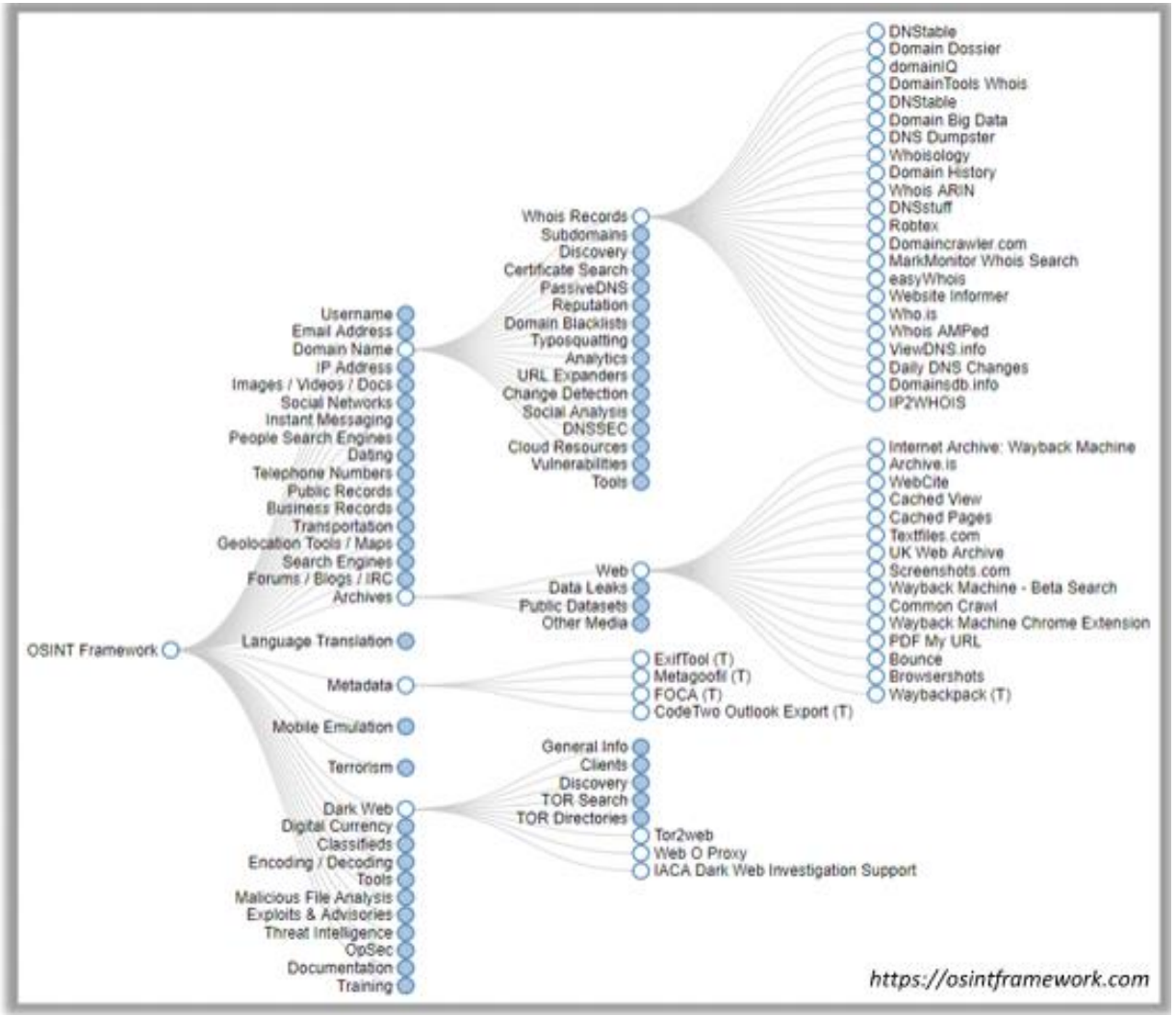




OSINT Framework

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



Other tools

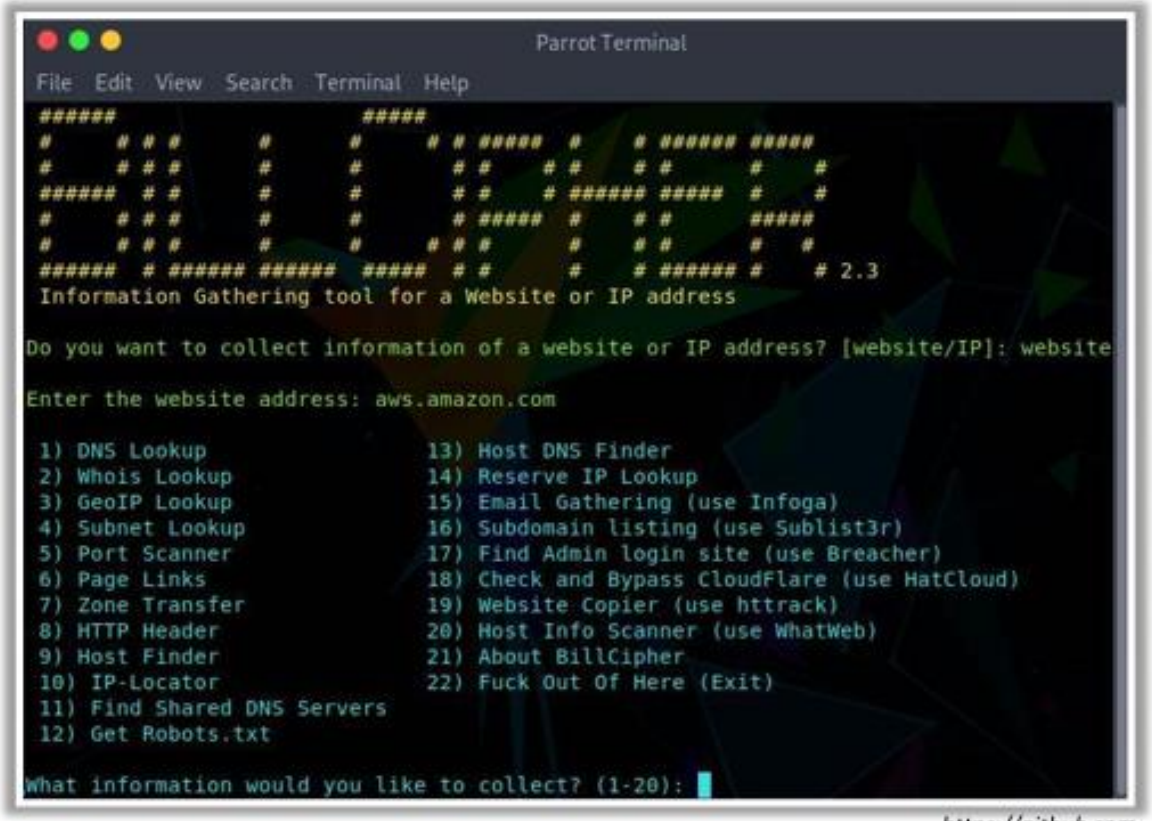
Recon-Dog

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

https://www.github.com

BillCipher

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



https://github.com

theHarvester

http://www.edge-security.com

Th3Inspector

https://github.com

Raccoon

https://github.com

Orb

https://github.com

PENTMENU

https://github.com

4. Footprinting Countermeasures

1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting Tools
4. 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 the website/Internet

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

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

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 web servers
4. Conduct periodic security awareness training to educate employees about various **social engineering tricks and risks**
5. Opt for privacy services on **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

Summary

- In this module, we have discussed the following:
  1. Footprinting concepts and the objectives of footprinting
  2. Various footprinting techniques, such as footprinting through search engines, footprinting through web services, and footprinting through social networking sites
  3. Website, email, Whois, and DNS footprinting
  4. Network footprinting and footprinting through social engineering
  5. Some important footprinting tools
  6. How organizations can defend against footprinting and reconnaissance activities

Review Questions

1. What Is FootPrinting?
2. What are the objectives of FootPrinting?
3. What are the FootPrinting Methodologies?

Class Activities

1. Go through the method of FP
    - Search engines
    - Web Services
    - Social Networking Sites
    - Website
    - Email
    - WHOIS
    - DNS
    - Network
2. Run one tool/technique for each of the method above.

Lab activities: Conduct Footprinting and Reconnaissance

1. **Identify the Target**
2. Passive Footprinting
3. Active Footprinting
4. Network Information Gathering
5. Social Engineering
6. Website Footprinting
7. DNS Footprinting
8. **Compile & Report**

- **Company or Organization**
  (for corporate reconnaissance)
- **IP Address or Network**
  (to identify services and ports)
- **Domain or Website**
  (to find vulnerabilities in web applications)
- **Individual or Person**
  (for social engineering / human factor attacks)

Question and Answer Session

Q & A

What To Expect Next Week

In Class

- 03_EHIR_Computer and Network Scanning

Preparation for Class

- VMs