

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

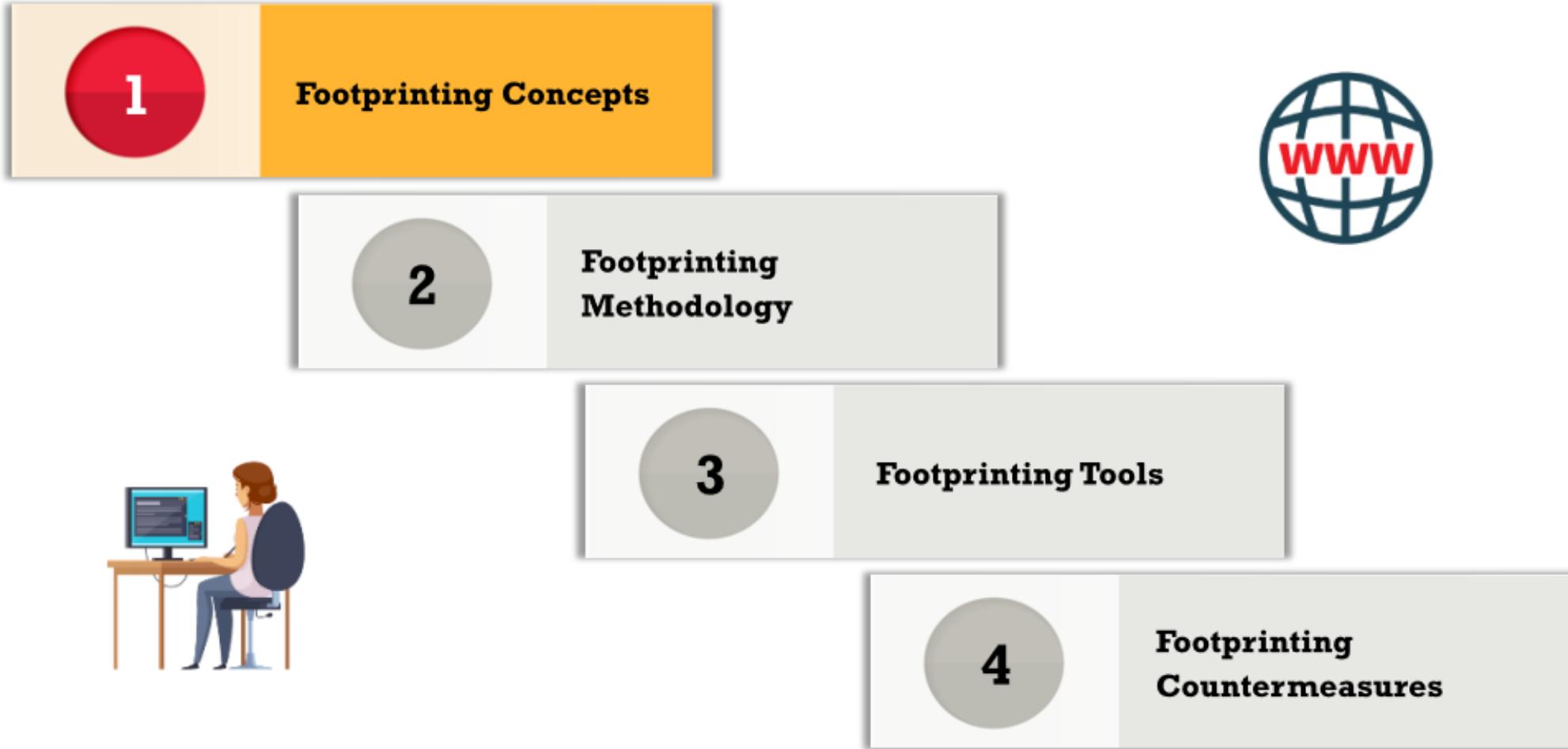
At the end of this module, you will be able to:

- 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



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.

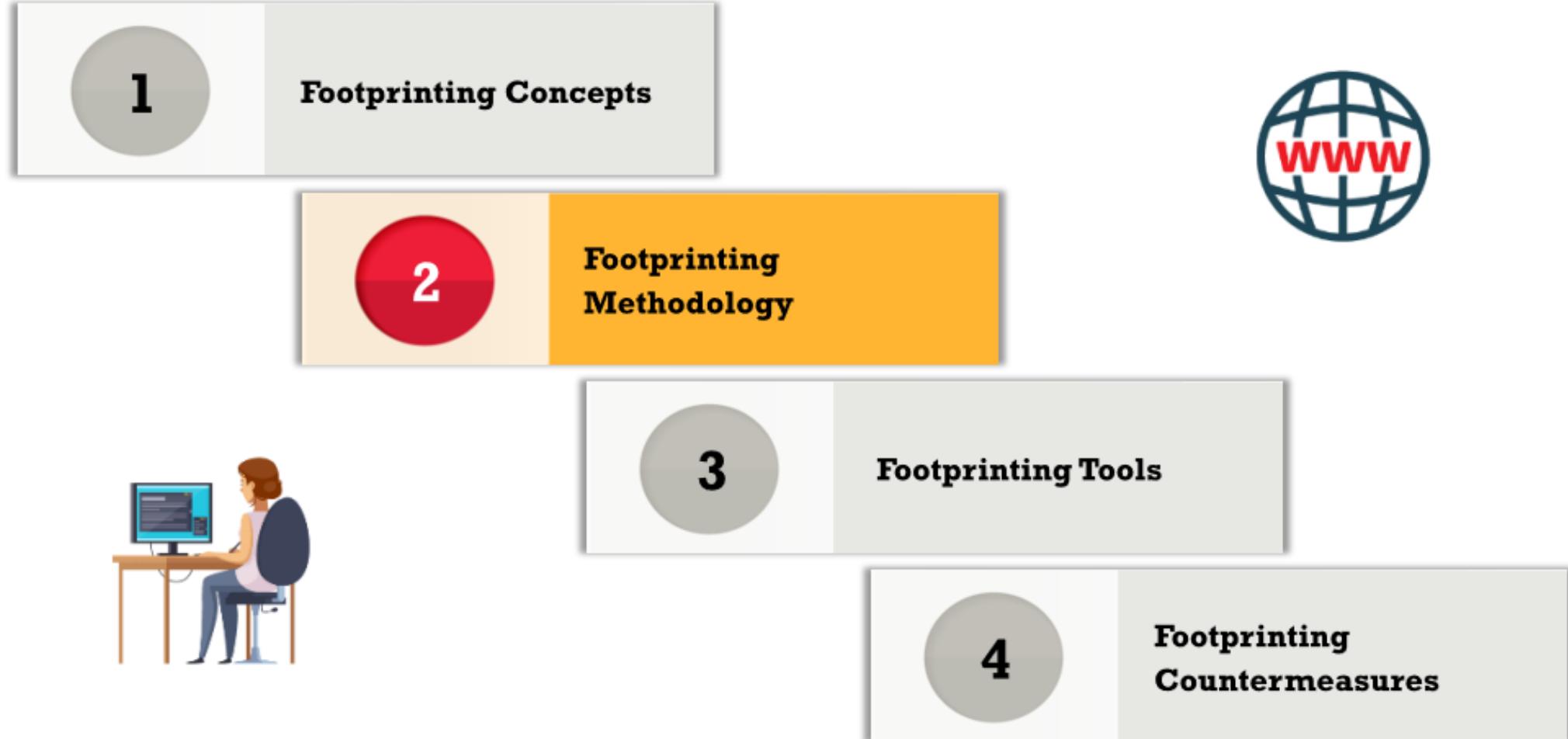
3. Identify Vulnerabilities:

- 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



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.

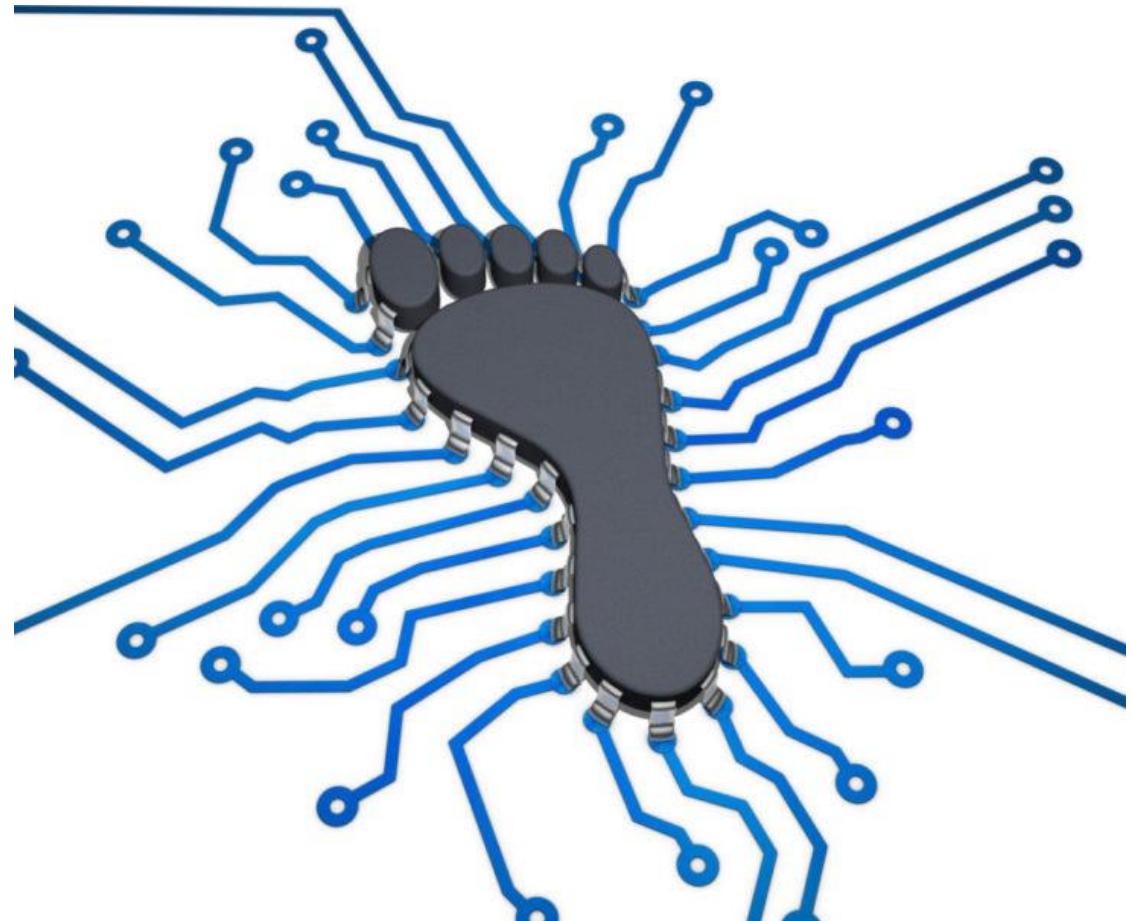
Key Deliverables:

- **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:



- 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 **publicly 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



Google Hacking Database

Category Any Author Begin typing...

Filters Reset All

Show 15 Quick Search

Date Added	Dork	Category	Author
2019-05-23	"please sign in" "sign in" "gophish" +"login"	Pages Containing Login Portals	edm0nd
2019-05-23	intitle:"LaserJet" "Device status" "Supplies summary"	Various Online Devices	Robert Marmorstein
2019-05-23	inurl:github.com intext:.ftpconfig -issues	Files Containing Juicy Info	vocuzi
2019-05-21	inurl:bc.googleusercontent.com intitle:index of	Sensitive Directories	acc3ssp0int
	intitle:"admin console" inurl:login site:"*.edu" "site:"*.gov" "site:"*.net" -	Pages Containing Login Portals	acc3ssp0int
2019-05-21	site:"*.com -help -guide -documentation -release -notes -configure -support -price -cant		

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

NETCRAFT

Hostnames matching *.microsoft.com

► Search with another pattern?

First 500 results (showing 41 to 60)

Site	First seen	Netblock	OS	Site Report
41. social.technet.microsoft.com	August 2008	Akamai Technologies	Linux	Report
42. appforoffice.microsoft.com	October 2013	Akamai International, BV	Linux	Report
43. examregistration.microsoft.com	October 2014	Microsoft Corporation	Windows Server 2016	Report
44. login.microsoft.com		Microsoft Corporation	Windows Server 2008	Report
45. myanalytics.microsoft.com	March 2019	Microsoft Corp	Windows Server 2016	Report
46. o15.officerestr.microsoft.com	May 2012	Microsoft Corporation	Windows Server 2016	Report
47. statics.teams.microsoft.com	December 2016	Microsoft Corporation	unknown	Report
48. emea.flow.microsoft.com		Microsoft Corp	Windows Server 2016	Report
49. powerusers.microsoft.com	June 2016	Lithium Technologies, Inc.	F5 BIG-IP	Report
50. mirc-blog.microsoft.com		Microsoft Corporation	Windows Server 2016	Report

<https://www.netcraft.com>

PuTTY - [root@parrot: ~]#

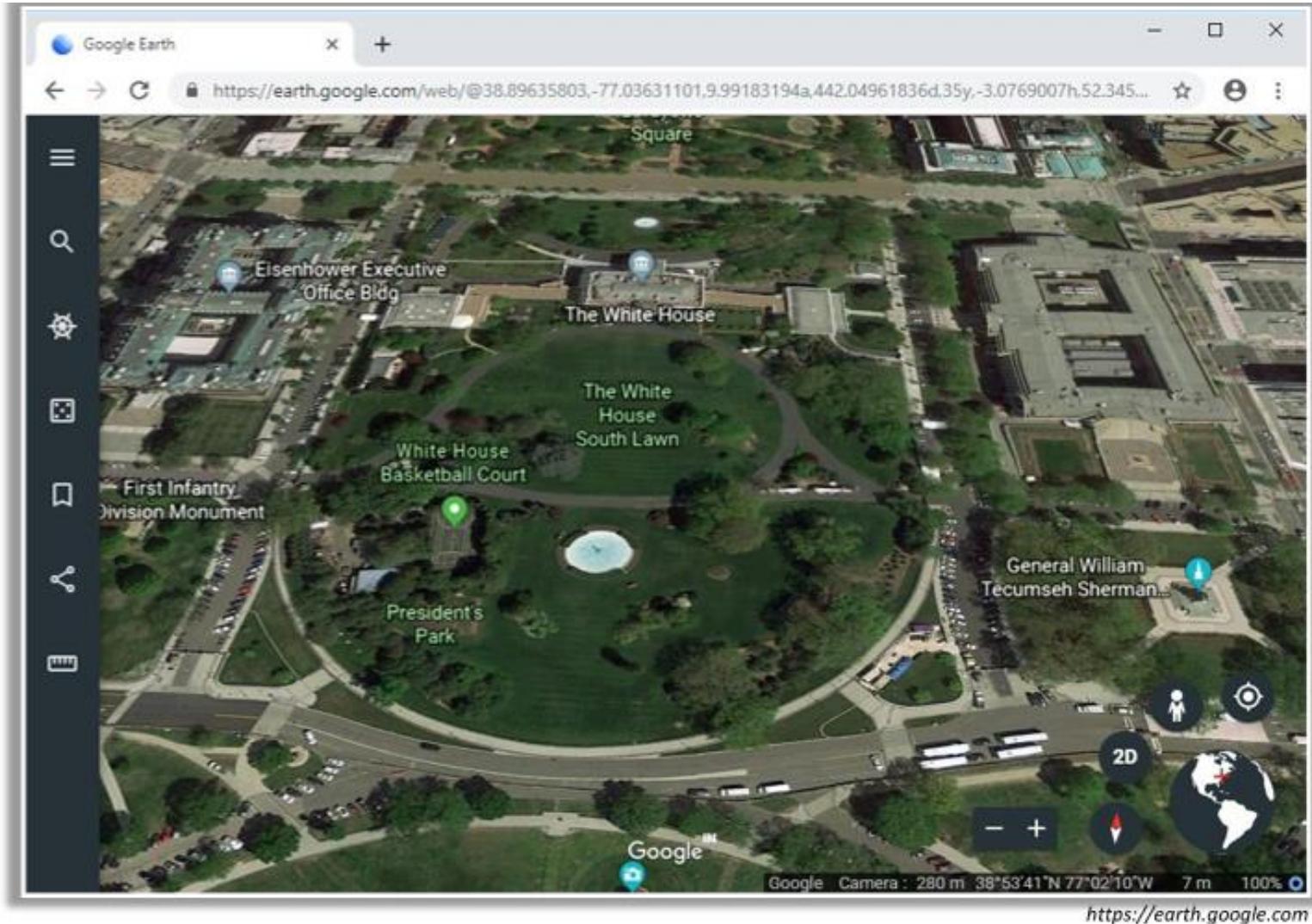
```
# sublist3r -d google.com
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for google.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 853
www.google.com
alt.aspmx.l.google.com
client.l.google.com
clients.l.google.com
gmail-smtp-mas.l.google.com
misc-anycast.l.google.com
31.google.com
360suite.google.com
clients-2.google.com
www.google.com
aboutme.google.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



NAME PHONE BACKGROUND CHECK MORE +

Search results for **Nicolas Cage in United States**

Narrow your results by: Middle Initial: All M.I. Age: All Ages State: All States City: All Cities Filter

We found 43 people that match Nicolas Cage in United States

1. Get the report on Nicolas Coppola Cage , age —		Get more details		
Has lived in	Has worked at	Has studied at	Related to	DOB Phone Address
New Orleans, LA Encino, CA Middletown, RI Los Angeles, CA View all	Saturn Films Brett Ratner Saturn Productions	Hinds Community College Beverly Hills High School	Alice Kim	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

2. Get the report on Nicolas Cage , age 30		Get more details		
Has lived in	Has worked at	Has studied at	Related to	DOB Phone Address
Daytona Beach, FL Ormond Beach, FL Orlando, FL	Orlando Style Magazine	Wheaton - Warrenville South High School	Douglas Cage Nicholas Cage Julie Cage Dylan Cage	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

3. Get the report on Nicolas Cage , age —		Get more details		
Has lived in	Has worked at	Has studied at	Related to	DOB Phone Address
Merrifield, VA Vienna, VA Virginia Beach, VA Baltimore, MD View all	Internal Revenue Service Federal Bureau of Investigation Amnesty International Food & Water Watch View all	Nordhoff High School		<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

<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

```
[*] Target: microsoft
[*] Searching LinkedIn.
```

Attackers search on LinkedIn to obtain employee details

```
Parrot Terminal
File Edit View Search Terminal Help
[*] Users found: 80
-----
Amrita Shanbhag - Software Engineer II - Microsoft
Andrew Wilson - Chief Digital Officer - Microsoft
Arun Rajappa - Director of Product Management - Microsoft
Ashis Roy - Group Development Manager - Microsoft
Ashish Shah - Director Of Engineering - Microsoft
Brad Smith - President - Microsoft
Brendan Burns - Corporate Vice President - Microsoft
Brian Holt - Senior Program Manager - Microsoft
Charles Lamanna - Corporate Vice President - Microsoft
Charu Srinivasan - Microsoft
Chetan Parulekar - Partner Group Manager - Microsoft
Chris L. - Senior Director Software Partnerships - Microsoft
Dalan Mendonca - Product Manager - Microsoft
David Cattanach - Azure Technical Trainer - Microsoft
David Fowler - Partner Software Architect - Microsoft
David Maltz - Distinguished Engineer - Microsoft
Deepak Menon - Partner Director - Microsoft
Dharma Shukla - Technical Fellow - Microsoft
Dominic Williamson - Senior Program Manager - Microsoft
Doug Burger - Technical Fellow - Microsoft

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

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

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

```
[+] Emails found:
-----
msdnmg@microsoft.com
tomas@contoso.onmicrosoft.com
user@contoso.onmicrosoft.com
Rome.Li@microsoft.com
v-lanz@microsoft.com
support@microsoft.com
delist@messaging.microsoft.com
homepage@microsoft.com
postmaster@ul.onmicrosoft.com
TheWebInterfaceShouldBeRadicallyRefactoredJohnR.DouceurJonHowellBryanParnojohndo
howellparno@microsoft.com
quarantine@messaging.microsoft.com
hicwhql@microsoft.com
ctcwhql@microsoft.com
age3support@microsoft.com
...STOR.WW.00.EN.MSF.RMD.TS.T1S.SPT.00.EM@css.one.microsoft.com
pexdata@microsoft.com
brohrer@microsoft.com
rightlicense@microsoft.com
```

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



Google Finance - NASDAQ:GOOGL

Alphabet Inc (NASDAQ:GOOGL)

1,041.20 -2.95 (-0.28%)

Range: 1,039.26 - 1,048.74 | Dividend: - | EPS: 29.94 | Shares: 296.26M | P/E: 34.77

After Hours: 1,041.20 +0.00 (0.00%) | Vol / Avg: 0.00160M | Beta: 0.91 | Mkt cap: 717.82B | Instl. own: 81%

Dow Jones: 23,439.70 | 0.07% | Nasdaq: 6,757.60 | 0.10% | Technology: 1,041.20 | -0.28% | More results

Add to portfolio | More results

Company Summary News Option chain Related companies Financiers Markets

News: The Brilliance Of Alphabet's YouTube Strategy Seeking Alpha - 3 hours ago

Alphabet Inc. Plans A Beta City Co Design - Oct 17, 2017

Alphabet Inc (GOOG, GOOGL) Delivers Earnings Beat U.S. News & World Report - Oct 26, 2017

GOOG, GOOGL earnings call for the period ending September 30, 2017 Motley Fool - Oct 30, 2017

How Alphabet thinks of capital allocation and acquisitions Motley Fool - Oct 31, 2017

Waymo Works To Build Trust As First Pilot- Motley Fool - Oct 31, 2017

All news for Alphabet Inc > | Subscribe

Related companies

Company name	Exchange	Currency	Price	Change	Chg %	Earnings per share	P/E ratio	Mkt Cap	Dividend	Total debt to assets	Return on avg assets	Return on avg equity	Operating margin	Net profit margin
GOOGL, Alphabet Inc	NASDAQ	USD	1,041.20	-2.55	-0.28%	29.94	34.77	717.82B	0.00	2.35	12.37	15.02	26.27	21.58
BIDU (Baidu Inc (ADR))	NASDAQ	USD	217.37	-0.63	-0.28%	7.07	33.56	82.31B	16.43	7.03	12.84	14.24	16.44	8.93
YNDX Yandex NV	NASDAQ	USD	31.62	+0.63	+2.03%	0.33	95.20	10.30B	1.53	6.00	9.24	16.99	15.37	12.57
MSFT Microsoft Corpora...	NASDAQ	USD	83.93	+0.05	+0.07%	2.95	28.39	647.49B	1.53	34.43	9.95	26.55	24.76	23.57
UNVGY Lenovo Group Limi...	OTCMKTS	USD	11.54	-0.09	-0.77%	0.53	21.95	6.43B	0.68	11.17	2.04	15.14	1.56	1.23
VZ Verizon Communic...	NASDAQ	USD	173.97	-0.70	-0.40%	9.19	18.94	893.22B	2.40	30.82	13.87	36.87	26.76	21.09
AAPL Apple Inc.	NYSE	USD	44.75	-0.13	-0.29%	3.90	11.48	182.55B	2.27	44.25	5.57	67.40	21.48	10.80
IBA Int'l Business Ma...	NYSE	USD	148.40	-0.76	-0.51%	11.98	12.38	137.39B	5.50	35.90	10.42	73.10	15.43	14.87
FBB Facebook Inc	NASDAQ	USD	178.77	+0.31	+0.17%	5.38	33.23	519.47B	0.00	0.00	17.87	19.70	44.96	36.97
TWTR Twitter Inc.	NYSE	USD	20.17	-0.15	-0.74%	-0.51	14.90B	24.00	4.06	-10.18	-14.52	-18.06		
GOOG Google Inc - Com...	NASDAQ	USD	568.67											

Advertisement

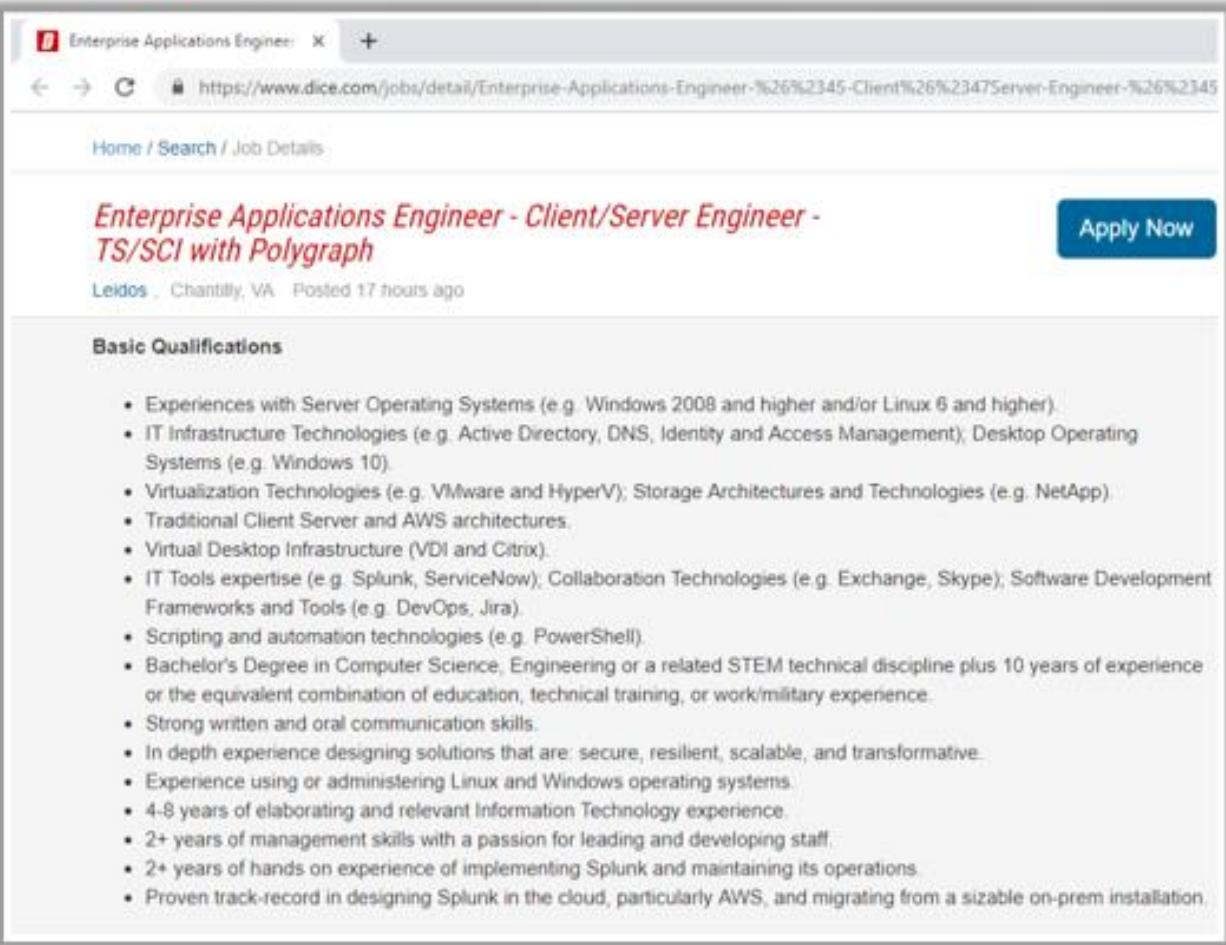
Google Cloud Platform Try Google Cloud Platform free with a \$300 credit. Google Cloud Platform >

Events Add GOOGL to my calendar Jan 24, 2018 Q4 2017 Alphabet Inc Earnings Release (Estimated) - 4:00PM EST - Nov 28, 2017 Alphabet Inc at Credit Suisse Technology, Media and Telecom Conference - 1:00PM EST -

<https://www.google.com/finance>

7. Footprinting through Job Sites

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

A screenshot of a job listing on Dice.com. The title is "Enterprise Applications Engineer - Client/Server Engineer - TS/SCI with Polygraph" at Leidos in Chantilly, VA, posted 17 hours ago. The "Apply Now" button is visible. Below the title, under "Basic Qualifications", there is a bulleted list of requirements.

- Experiences with Server Operating Systems (e.g. Windows 2008 and higher and/or Linux 6 and higher).
- IT Infrastructure Technologies (e.g. Active Directory, DNS, Identity and Access Management); Desktop Operating Systems (e.g. Windows 10).
- Virtualization Technologies (e.g. VMware and HyperV); Storage Architectures and Technologies (e.g. NetApp).
- Traditional Client Server and AWS architectures.
- Virtual Desktop Infrastructure (VDI and Citrix).
- IT Tools expertise (e.g. Splunk, ServiceNow); Collaboration Technologies (e.g. Exchange, Skype); Software Development Frameworks and Tools (e.g. DevOps, Jira).
- Scripting and automation technologies (e.g. PowerShell).
- Bachelor's Degree in Computer Science, Engineering or a related STEM technical discipline plus 10 years of experience or the equivalent combination of education, technical training, or work/military experience.
- Strong written and oral communication skills.
- In depth experience designing solutions that are: secure, resilient, scalable, and transformative.
- Experience using or administering Linux and Windows operating systems.
- 4-8 years of elaborating and relevant Information Technology experience.
- 2+ years of management skills with a passion for leading and developing staff.
- 2+ years of hands on experience of implementing Splunk and maintaining its operations.
- Proven track-record in designing Splunk in the cloud, particularly AWS, and migrating from a sizable on-prem installation.

<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

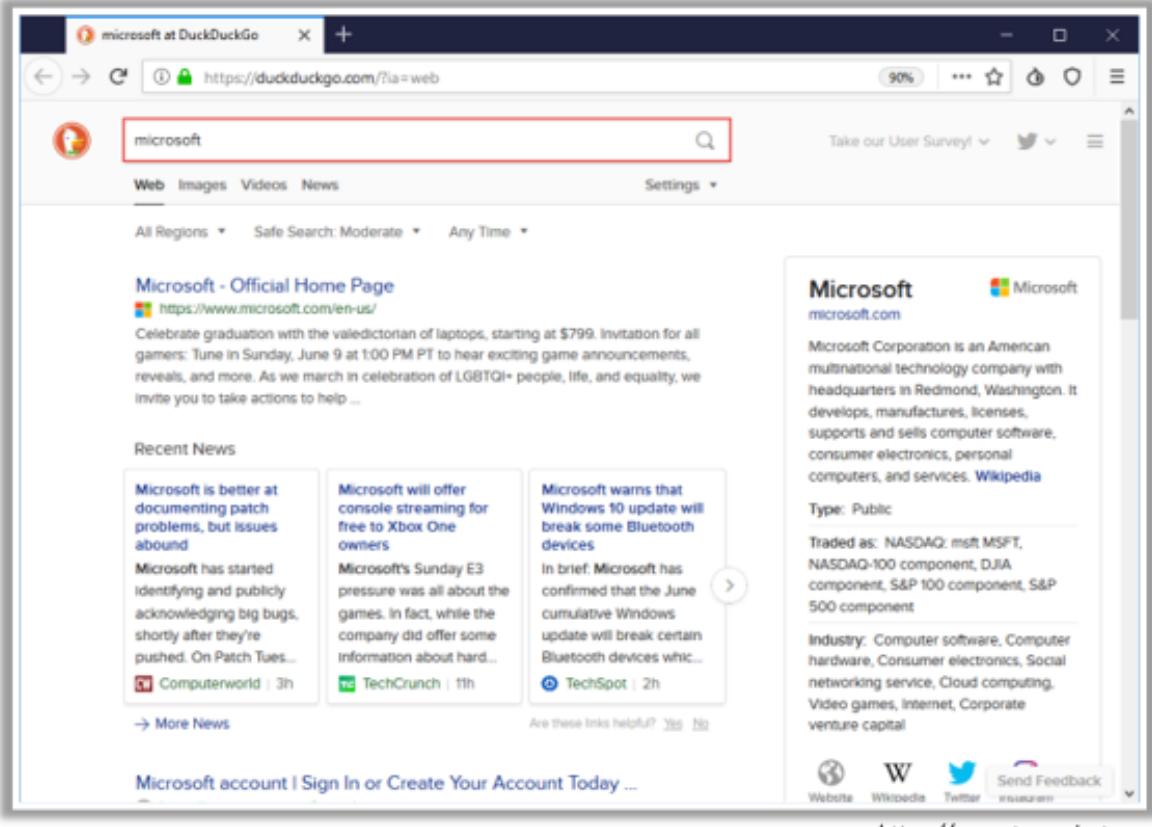
Dark web or Darknet

- 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

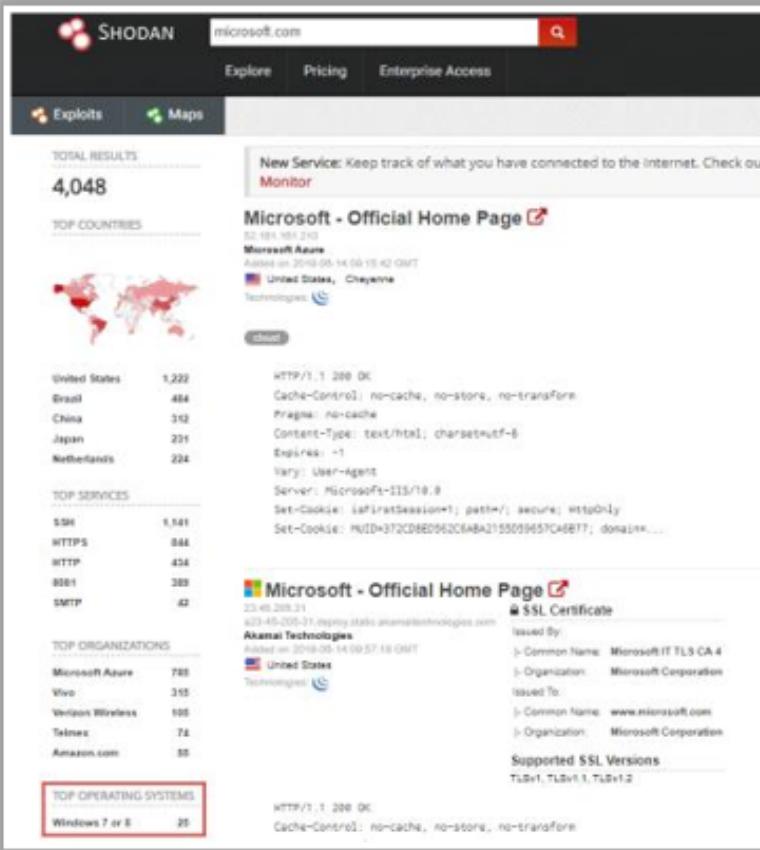
It is used to access the deep and dark web where it acts as a **default VPN** for the user and bounces the network IP address through several servers before interacting with the web



<https://www.torproject.org>

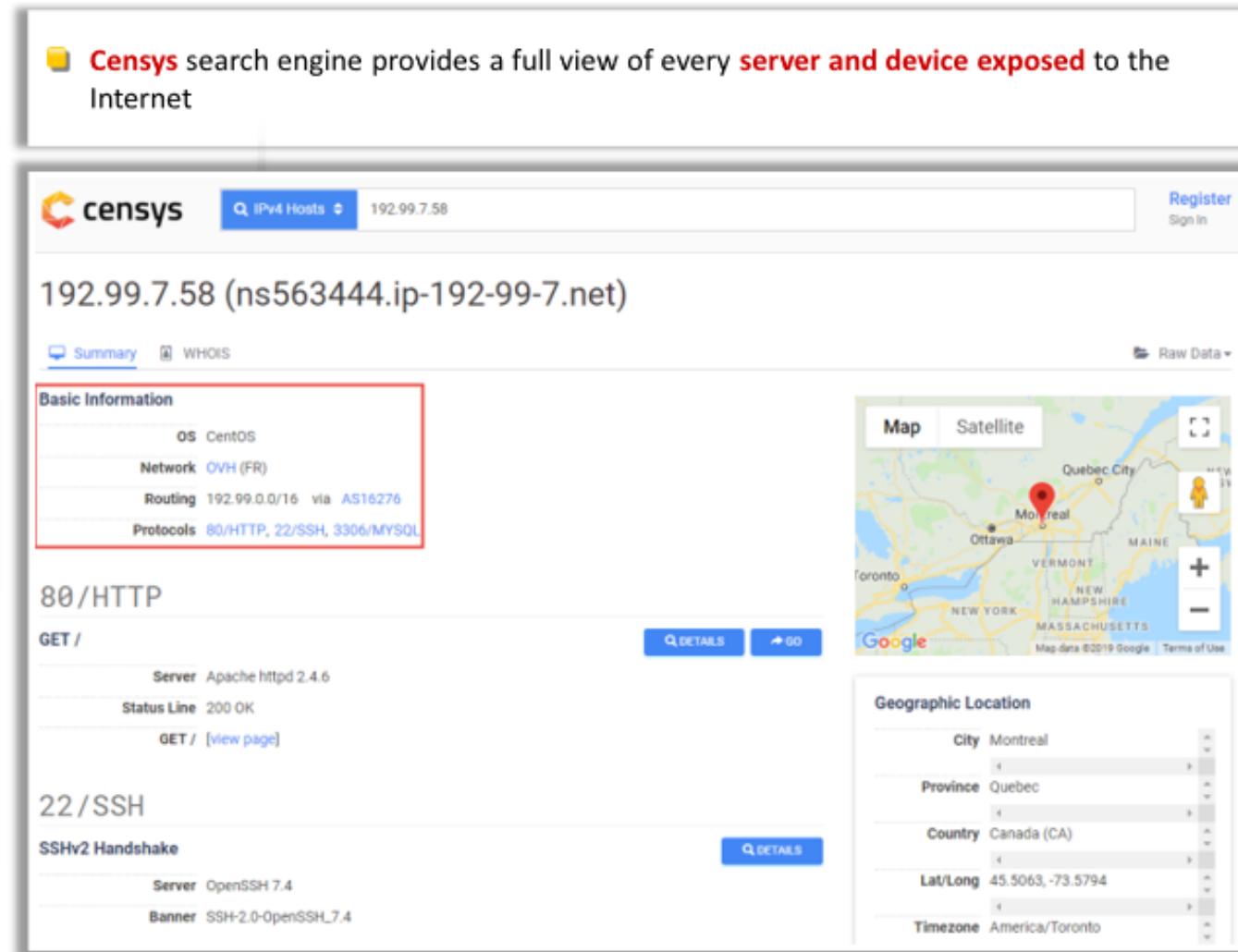
9. Determining the Operating System

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



The screenshot shows the SHODAN search results for 'microsoft.com'. It includes a search bar with 'microsoft.com', navigation links for 'Explore', 'Pricing', and 'Enterprise Access', and tabs for 'Exploits' and 'Maps'. The main area displays 'TOTAL RESULTS: 4,048' and a 'TOP COUNTRIES' section with a world map and a table. The table lists countries and their counts: United States (1,222), Brazil (484), China (312), Japan (231), and Netherlands (224). Below this is a 'TOP SERVICES' section with tables for SSH, HTTPS, HTTP, 8081, and SMTP. A detailed result for 'Microsoft - Official Home Page' is shown, including its IP address (23.45.205.31), SSL certificate from Axamai Technologies, and a snippet of the page content.

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



The screenshot shows the Censys search results for the IP address 192.99.7.58. The interface includes a search bar with 'IPv4 Hosts' and '192.99.7.58', and links for 'Register' and 'Sign In'. The main content area shows the IP address '192.99.7.58 (ns563444.ip-192-99-7.net)'. It features a 'Summary' tab (selected) and a 'WHOIS' tab. A red box highlights the 'Basic Information' section, which contains details about the OS (CentOS), Network (OVH (FR)), Routing (192.99.0.0/16 via AS16276), and Protocols (80/HTTP, 22/SSH, 3306/MYSQL). Below this are sections for '80/HTTP' (GET /, Server: Apache httpd 2.4.6, Status Line: 200 OK) and '22/SSH' (SSHv2 Handshake, Server: OpenSSH 7.4, Banner: SSH-2.0-OpenSSH_7.4). On the right side, there is a map showing the location of the IP address in Montreal, Quebec, Canada, with a red marker. A sidebar on the right allows setting geographic location parameters like City, Province, Country, Lat/Long, and Timezone.

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 | 6 Social engineering employees |
| 2 Search engines, Internet, and online database | 7 Product catalogs and retail outlets |
| 3 Press releases and annual reports | 8 Analyst and regulatory reports |
| 4 Trade journals, conferences, and newspapers | 9 Customer and vendor interviews |
| 5 Patent and trademarks | 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	What Organizations Do	What Attacker Gets
Maintain profile	Contact info, location, etc.	User surveys	Business strategies
Connect to friends, chat	Friends list, friends' info, etc.	Promote products	Product profile
Share photos and videos	Identity of family members, interests, etc.	User support	Social engineering
Play games, join groups	Interests	Recruitment	Platform/technology
Create events	Activities	Background check to hire employees	Type of business

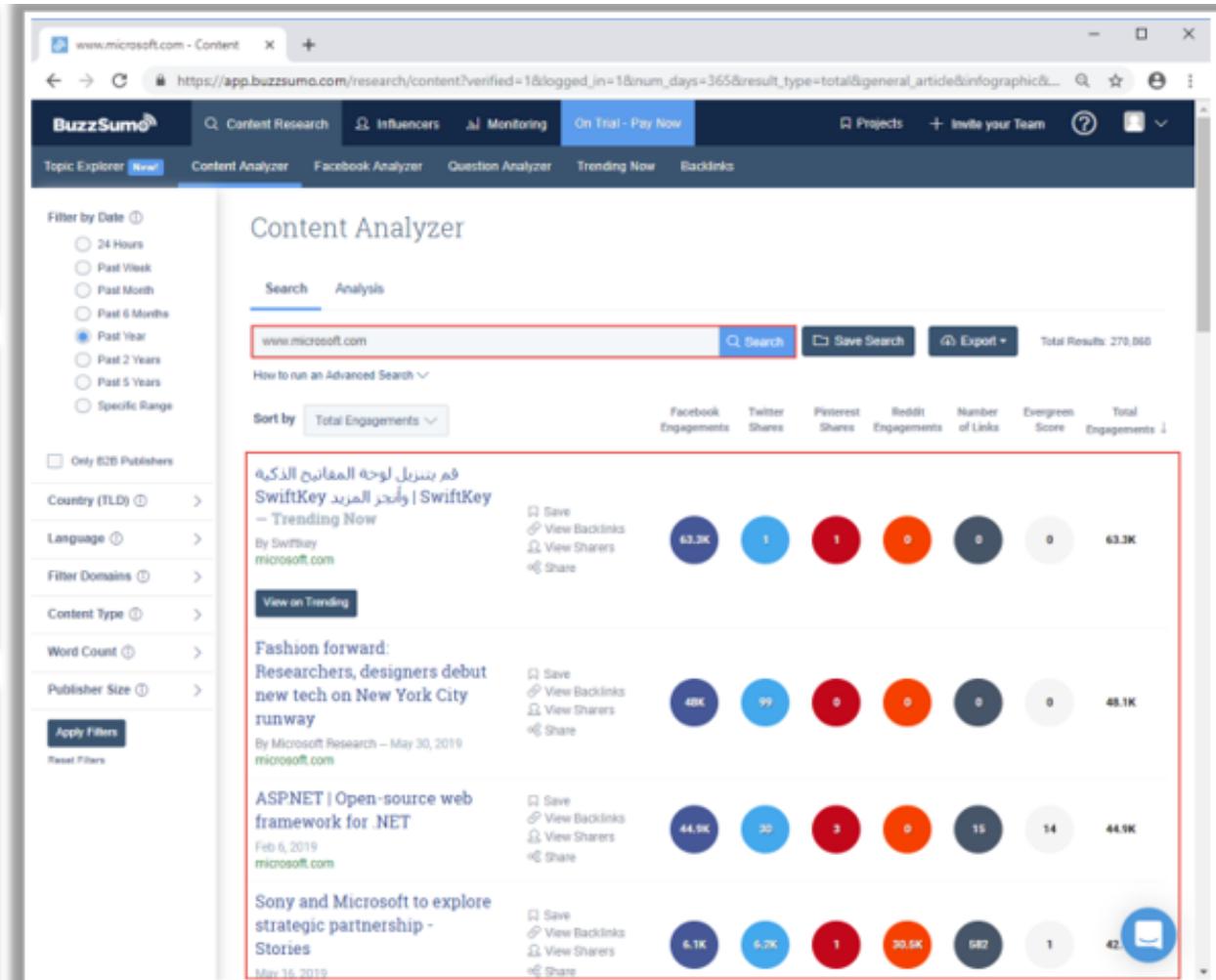
2. General Resources for Locating Information from Social Media Sites

- 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

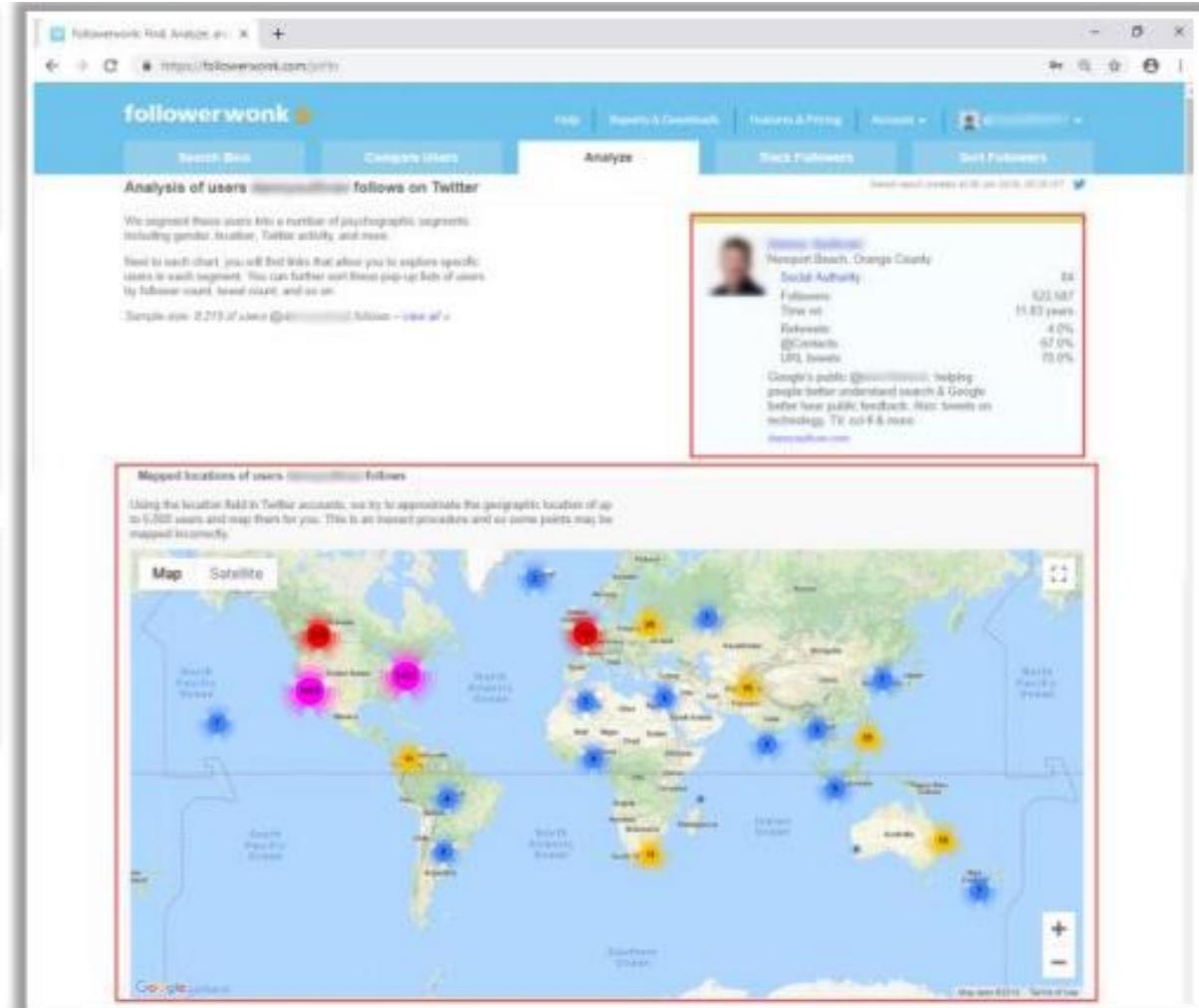
- Conducting location search on social media sites, such as Twitter, Instagram, and Facebook, helps attackers in **detecting the geolocation of the target**

- 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

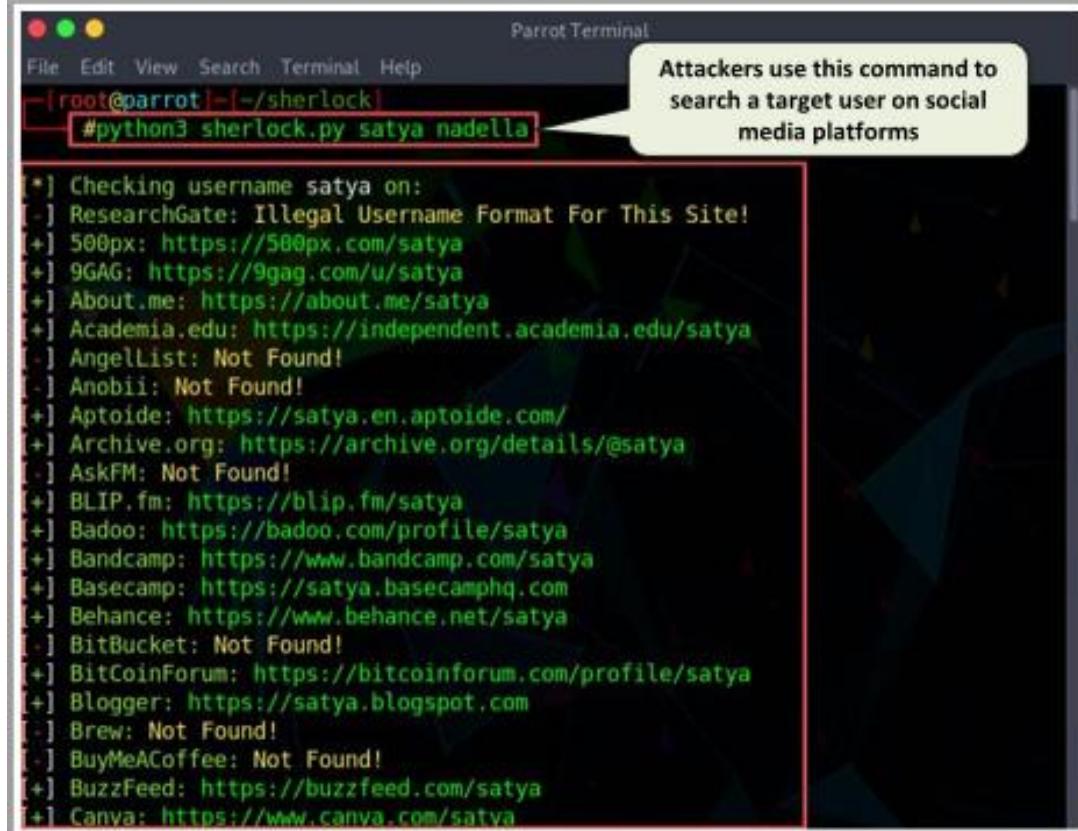


<https://followerwonk.com>

4. Tools for Footprinting through Social Networking Sites

Sherlock

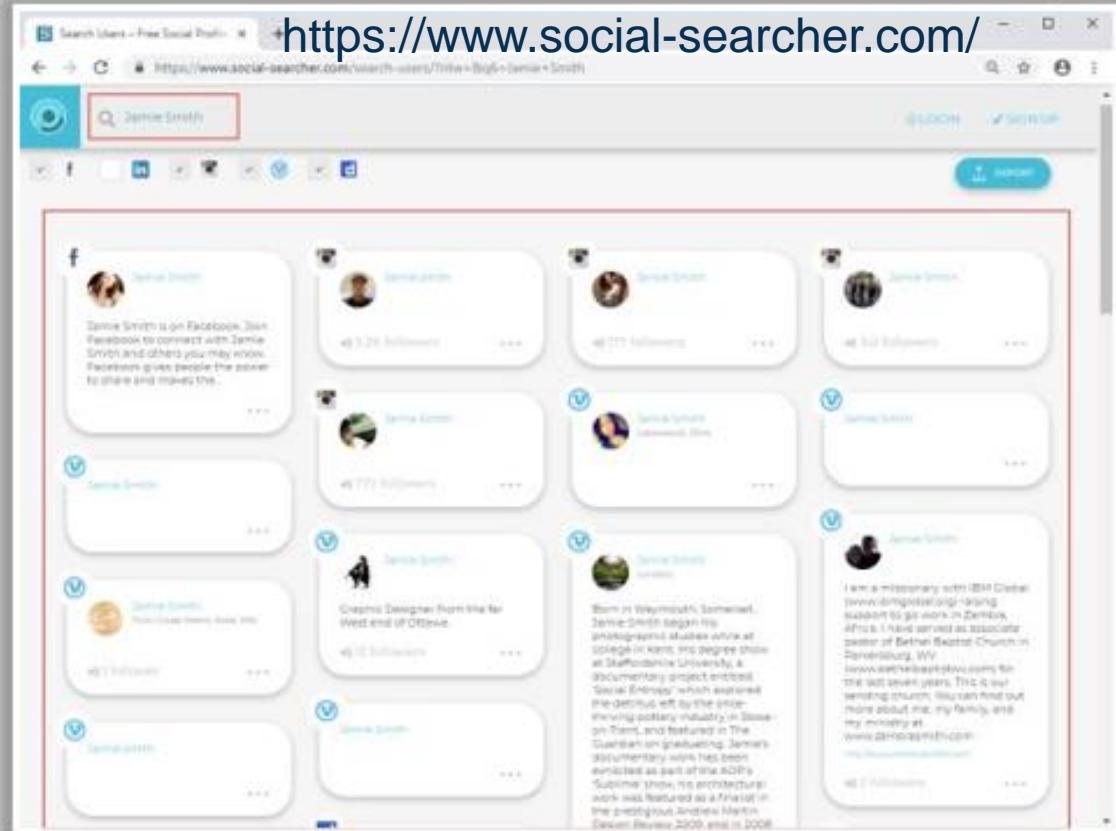
Sherlock tool is used to search a vast number of social networking sites for a target username



```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]# cd ~/sherlock
[root@parrot]# python3 sherlock.py satya nadella
[*] Checking username satya on:
[+] ResearchGate: Illegal Username Format For This Site!
[+] 500px: https://500px.com/satya
[+] 9GAG: https://9gag.com/u/satya
[+] About.me: https://about.me/satya
[+] Academia.edu: https://independent.academia.edu/satya
[+] AngelList: Not Found!
[+] Anobii: Not Found!
[+] Aptoide: https://satya.en.aptoide.com/
[+] Archive.org: https://archive.org/details/@satya
[+] AskFM: Not Found!
[+] BLIP.fm: https://blip.fm/satya
[+] Badoo: https://badoo.com/profile/satya
[+] Bandcamp: https://www.bandcamp.com/satya
[+] Basecamp: https://satya.basecamphq.com
[+] Behance: https://www.behance.net/satya
[+] BitBucket: Not Found!
[+] BitCoinForum: https://bitcoinforum.com/profile/satya
[+] Blogger: https://satya.blogspot.com
[+] Brew: Not Found!
[+] BuyMeACoffee: Not Found!
[+] BuzzFeed: https://buzzfeed.com/satya
[+] Canva: https://www.canva.com/satya
```

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/>

The screenshot shows a web browser displaying search results for the query "Jamie Smith". The results are presented in a grid of cards, each representing a different profile or piece of content found across various social media platforms. The profiles include basic information like names, profile pictures, and follower counts.

<https://github.com>

<https://www.social-searcher.com>

WEBSITE FOOTPRINTING

Website Footprinting

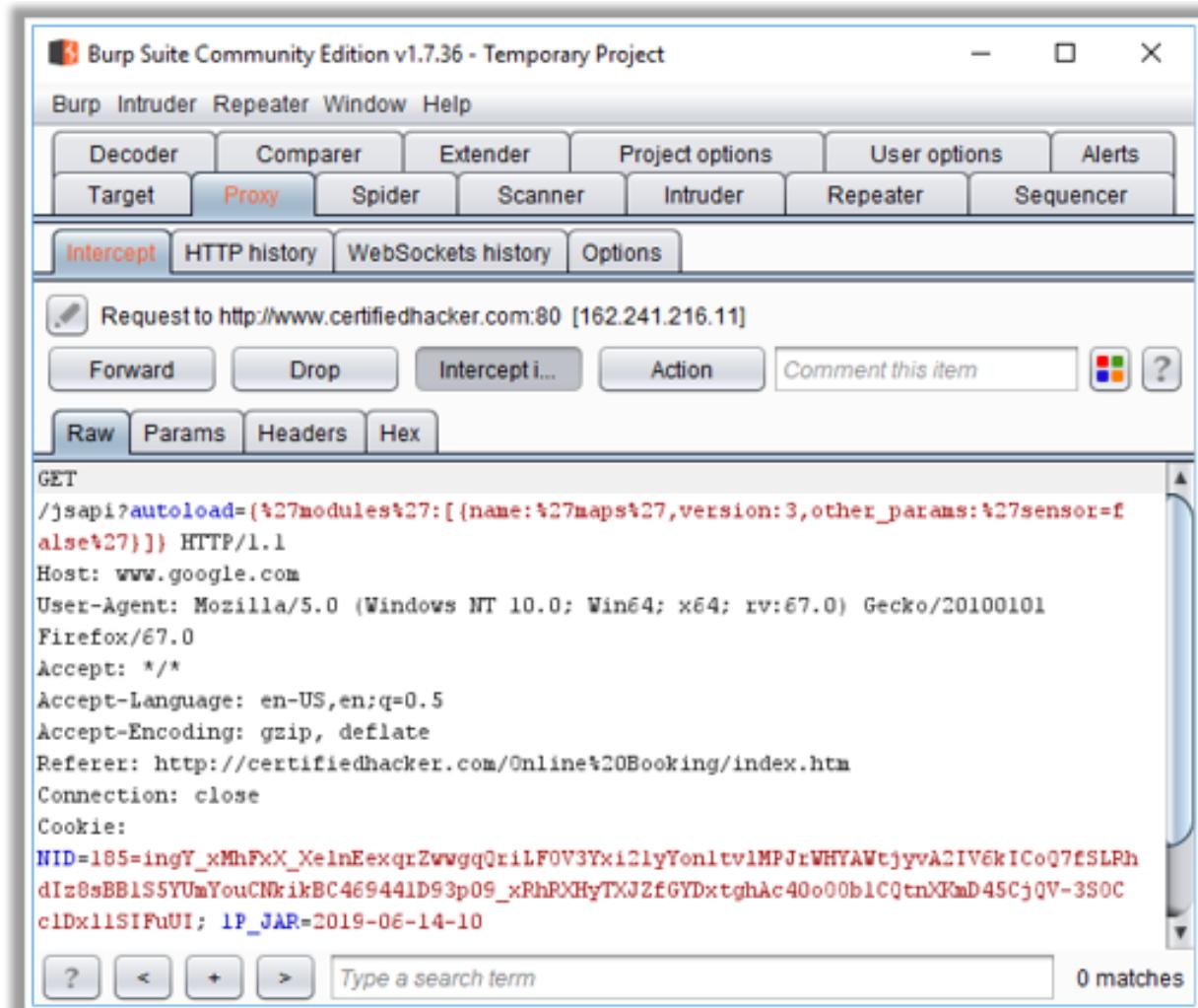
- Website footprinting refers to the **monitoring and analysis of the target organization's website** for information

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



```

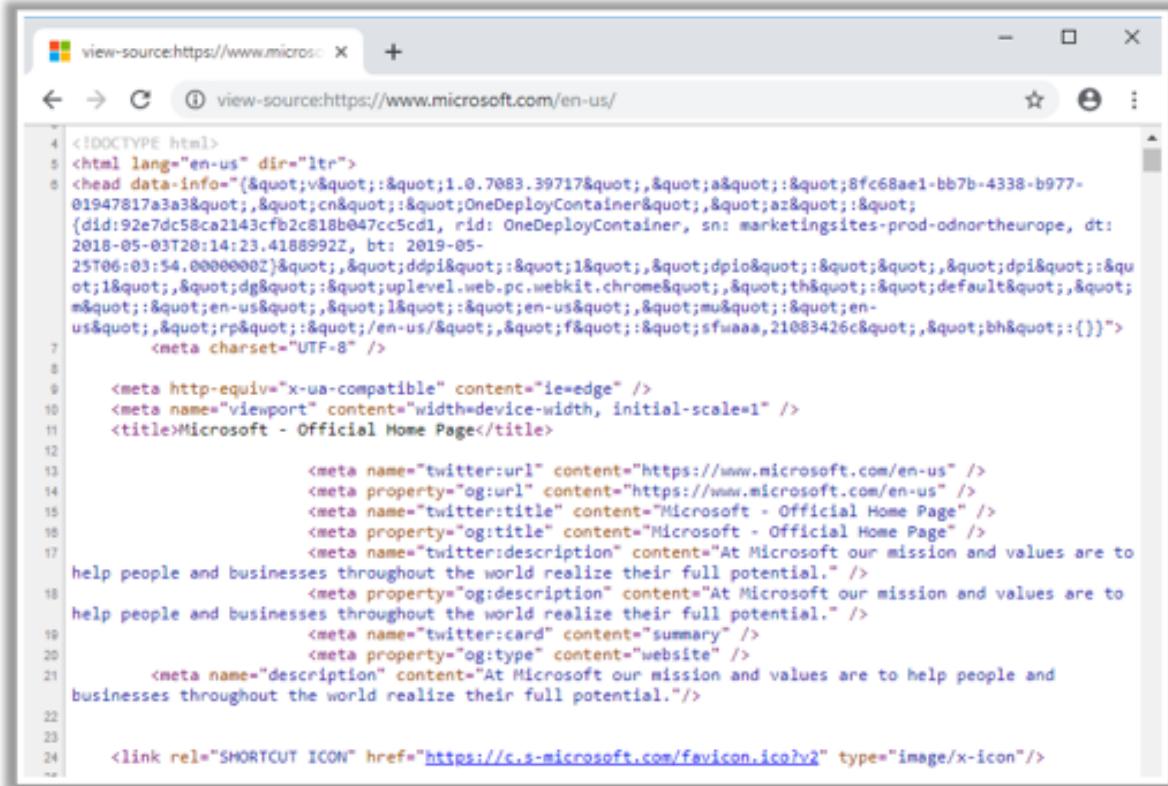
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Decoder Comparer Extender Project options User options Alerts
Target Proxy Spider Scanner Intruder Repeater Sequencer
Intercept HTTP history WebSockets history Options
Request to http://www.certifiedhacker.com:80 [162.241.216.11]
Forward Drop Intercept... Action Comment this item
Raw Params Headers Hex
GET
/jsapi?autoload=[{"modules": [{"name": "maps", "version": 3, "other_params": "sensor=false"}]] HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101
Firefox/67.0
Accept: /*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://certifiedhacker.com/Online%20Booking/index.htm
Connection: close
Cookie:
NID=185=ingY_xMhFxX_XelnEexqrZwwgqQriLF0V3Yxi2lyYonltvlMPJrWHYAWtjyvA2IV6kICoQ7fSLRhdIz8sBB1SSYUmYouCmkikBc469441D93p09_xRhRXHyTXJZfGYDxtghAc40o00b1CQtnXKmD45CjQV-3SOCc1Dx1lSIFuUI; 1P_JAR=2019-06-14-10
?
< + > Type a search term 0 matches
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



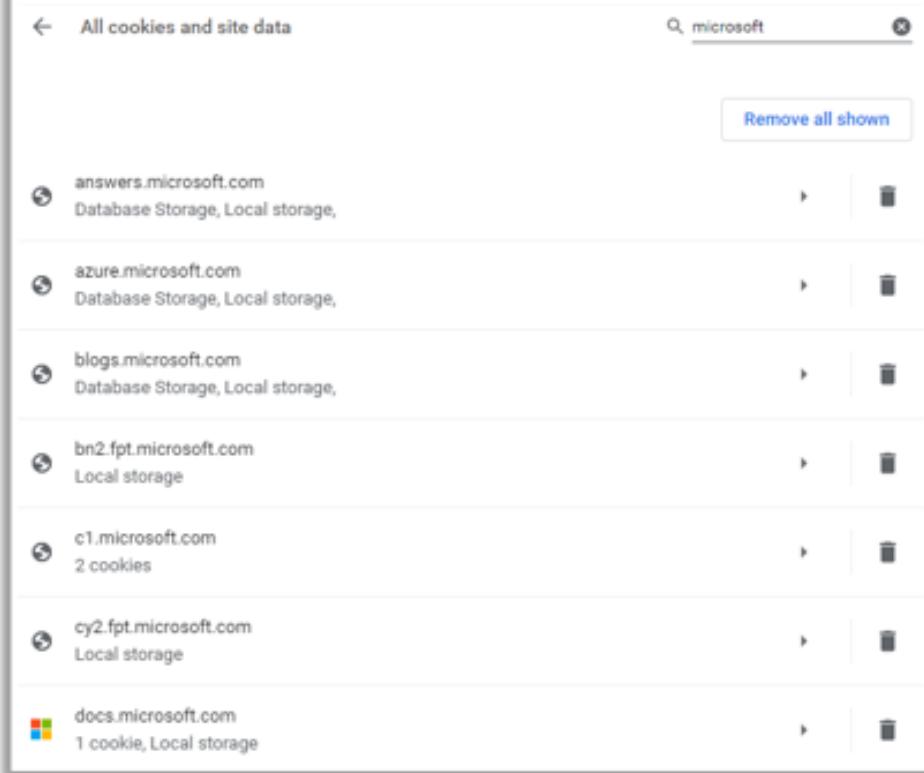
```

4 <!DOCTYPE html>
5 <html lang="en-us" dir="ltr">
6 <head data-info="("v="1.0.7083.39717","a="8fc68ae1-bb7b-4338-b977-
01947817a3a3","cn="OneDeployContainer","az=")&quot;
7 (did:92e7dc58ca2143cfb2c818b047cc5cd1, rid: OneDeployContainer, sn: marketingsites-prod-odnortheurope, dt:
2018-05-03T20:14:12.4188992Z, bt: 2019-05-
25T06:03:54.0000000Z)&quot;,&quot;ddpi="1&quot;,&quot;dpio="1&quot;,&quot;dpi="1&quot;,
8 &quot;dg="1&quot;,&quot;uplevel.web.pc.webkit.chrome="1&quot;,&quot;th="1&quot;,&quot;default="1&quot;,
9 &quot;en-us="1&quot;,&quot;en-us&quot;,&quot;mu="1&quot;,&quot;en-
10 us="1&quot;,&quot;rp="1&quot;,&quot;en-us/&quot;,&quot;f="sfwaaa,21083426c&quot;,&quot;bh="1&quot;,&quot;()=")
11 <meta charset="UTF-8" />
12
13 <meta http-equiv="x-ua-compatible" content="ie=edge" />
14 <meta name="viewport" content="width=device-width, initial-scale=1" />
15 <title>Microsoft - Official Home Page</title>
16
17 <meta name="twitter:url" content="https://www.microsoft.com/en-us" />
18 <meta property="og:url" content="https://www.microsoft.com/en-us" />
19 <meta name="twitter:title" content="Microsoft - Official Home Page" />
20 <meta property="og:title" content="Microsoft - Official Home Page" />
21 <meta name="twitter:description" content="At Microsoft our mission and values are to
help people and businesses throughout the world realize their full potential." />
22 <meta property="og:description" content="At Microsoft our mission and values are to
help people and businesses throughout the world realize their full potential." />
23 <meta name="twitter:card" content="summary" />
24 <meta property="og:type" content="website" />
25 <meta name="description" content="At Microsoft our mission and values are to help people and
businesses throughout the world realize their full potential."/>
26
27 <link rel="SHORTCUT ICON" href="https://c.s-microsoft.com/favicon.ico?v2" type="image/x-icon"/>

```

Examining cookies may provide

- Software in use and its behavior
- Scripting platforms used



Domain	Type	Count
answers.microsoft.com	Database Storage, Local storage	1
azure.microsoft.com	Database Storage, Local storage	1
blogs.microsoft.com	Database Storage, Local storage	1
bn2.fpt.microsoft.com	Local storage	1
c1.microsoft.com	2 cookies	2
cy2.fpt.microsoft.com	Local storage	1
docs.microsoft.com	1 cookie, Local storage	1

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



Web Data Extractor

Web Data Extractor Pro 3.9. Trial Version. You are on day 5 of your 15 day evaluation period.

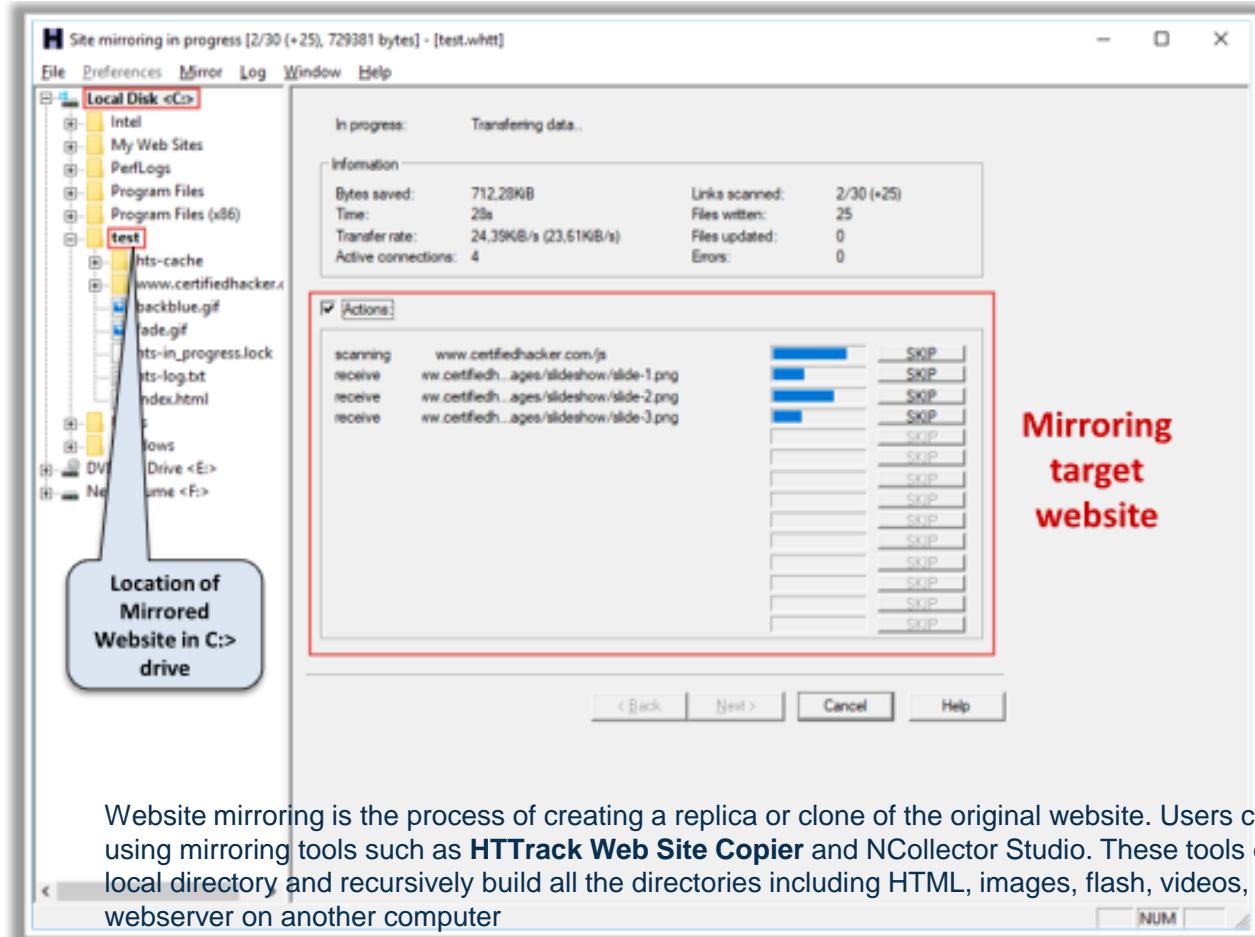
Description	Keywords	Title	URL	Host	Domain	Page size	Page last modified
A brief description of this we...	keywords, or phrases...	Certified Hacker	http://www.certifiedhacker.com/	certifiedhacker.com	.com	3640	2011-02-10
Professional Real Estate Ser...	real estate, real estate...	Professional Real Es...	http://certifiedhacker.com/Real%20Estate...	certifiedhacker.com	.com	5845	2011-02-10
Dear Construction		Dear Construction	http://certifiedhacker.com/Under%20Construction	certifiedhacker.com	.com	5381	2011-02-10
Under the Trees		Under the Trees	http://certifiedhacker.com/Under%20the%20Trees	certifiedhacker.com	.com	3653	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Ho...	http://certifiedhacker.com/Recipes/Index	certifiedhacker.com	.com	5899	2011-02-10
Turbo max powerful one pe...	Turbo max , examp...	Turbo Max Theme -	http://certifiedhacker.com/Turbo%20Max%20...	certifiedhacker.com	.com	12125	2011-02-10
IP-Folio		IP-Folio	http://certifiedhacker.com/IP-Folio/Index.html	certifiedhacker.com	.com	11606	2011-02-10
Unite - Together is B...	keywords, or phrases...	Unite - Together is B...	http://certifiedhacker.com/Social%20Media	certifiedhacker.com	.com	15094	2011-02-10
Online Booking		Online Booking	http://certifiedhacker.com/Online%20Booking	certifiedhacker.com	.com	20280	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Rec...	http://certifiedhacker.com/Recipes/Check...	certifiedhacker.com	.com	9594	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Abe...	http://certifiedhacker.com/Recipes/about	certifiedhacker.com	.com	5762	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Rec...	http://certifiedhacker.com/Recipes/recipe	certifiedhacker.com	.com	12716	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Menu	http://certifiedhacker.com/Recipes/menu	certifiedhacker.com	.com	7909	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Con...	http://certifiedhacker.com/Recipes/contact	certifiedhacker.com	.com	5621	2011-02-10
Online Booking		Online Booking: Site	http://certifiedhacker.com/Online%20Booking	certifiedhacker.com	.com	11965	2011-02-10
Online Booking		Online Booking: Bra...	http://certifiedhacker.com/Online%20Booking	certifiedhacker.com	.com	16031	2011-02-10
Online Booking		Online Booking: Con...	http://certifiedhacker.com/Online%20Booking	certifiedhacker.com	.com	14163	2011-02-10
Online Booking		Online Booking: FAQ	http://certifiedhacker.com/Online%20Booking	certifiedhacker.com	.com	14047	2011-02-10
Online Booking		Online Booking: Typ...	http://certifiedhacker.com/Online%20Booking	certifiedhacker.com	.com	12661	2011-02-10
Online Booking		Online Booking: Sea...	http://certifiedhacker.com/Online%20Booking	certifiedhacker.com	.com	27877	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Rec...	http://certifiedhacker.com/Recipes/recipe	certifiedhacker.com	.com	12481	2011-02-10
A short description of your c...	Some keywords that b...	Your company - Men...	http://certifiedhacker.com/Recipes/menu	certifiedhacker.com	.com	11584	2011-02-10
Online Booking		Online Booking: Pri...	http://certifiedhacker.com/Online%20Booking	certifiedhacker.com	.com	5693	2011-02-10
Online Booking		Online Booking: Hot...	http://certifiedhacker.com/Online%20Booking	certifiedhacker.com	.com	35400	2011-02-10
Online Booking		Online Booking: Che...	http://certifiedhacker.com/Online%20Booking	certifiedhacker.com	.com	12968	2011-02-10

Processing time: 00:00:08.623 Sites processed: 79 / 79 Downloaded: 385 KB Avg. Speed: 128 KB/s

<http://www.webextractor.com>

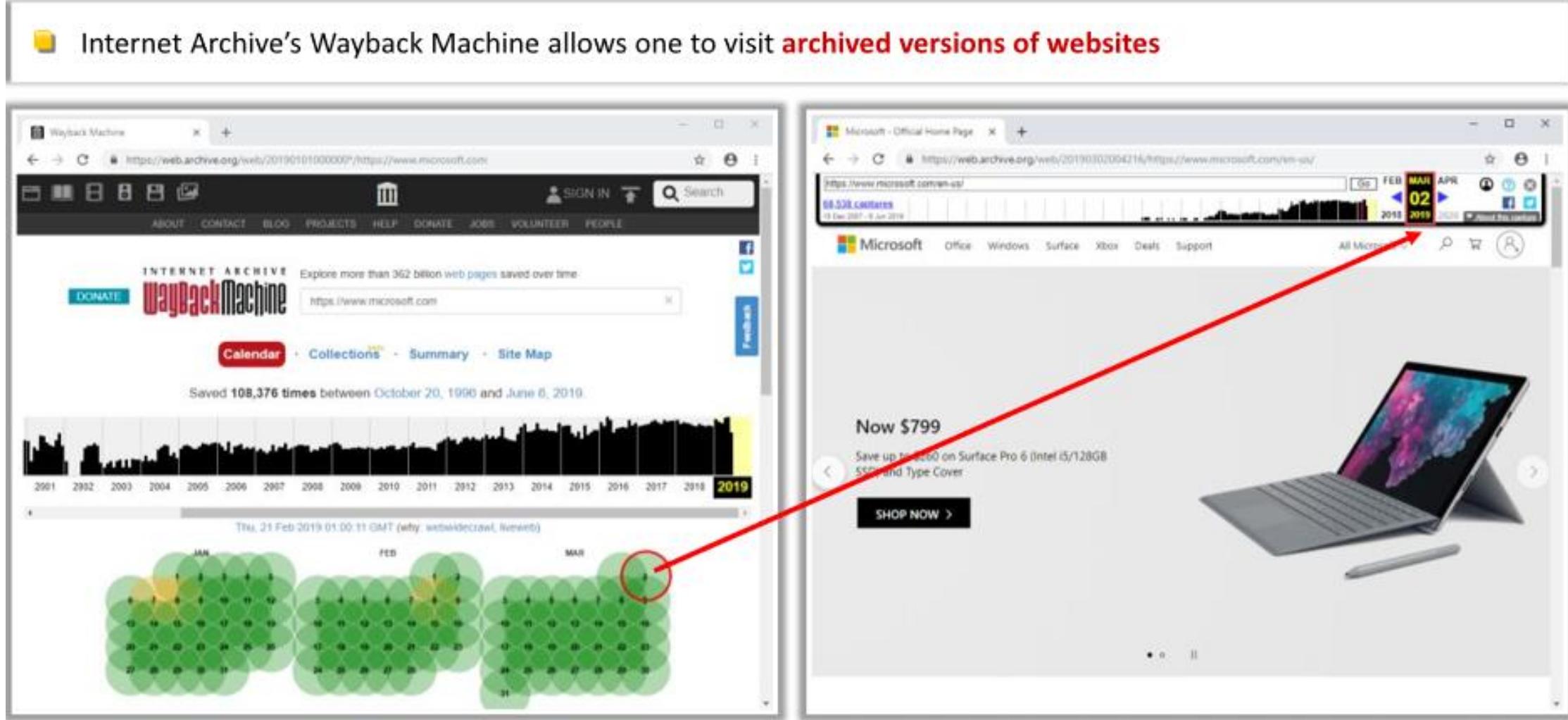
2. Mirroring Entire Website

- 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



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

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

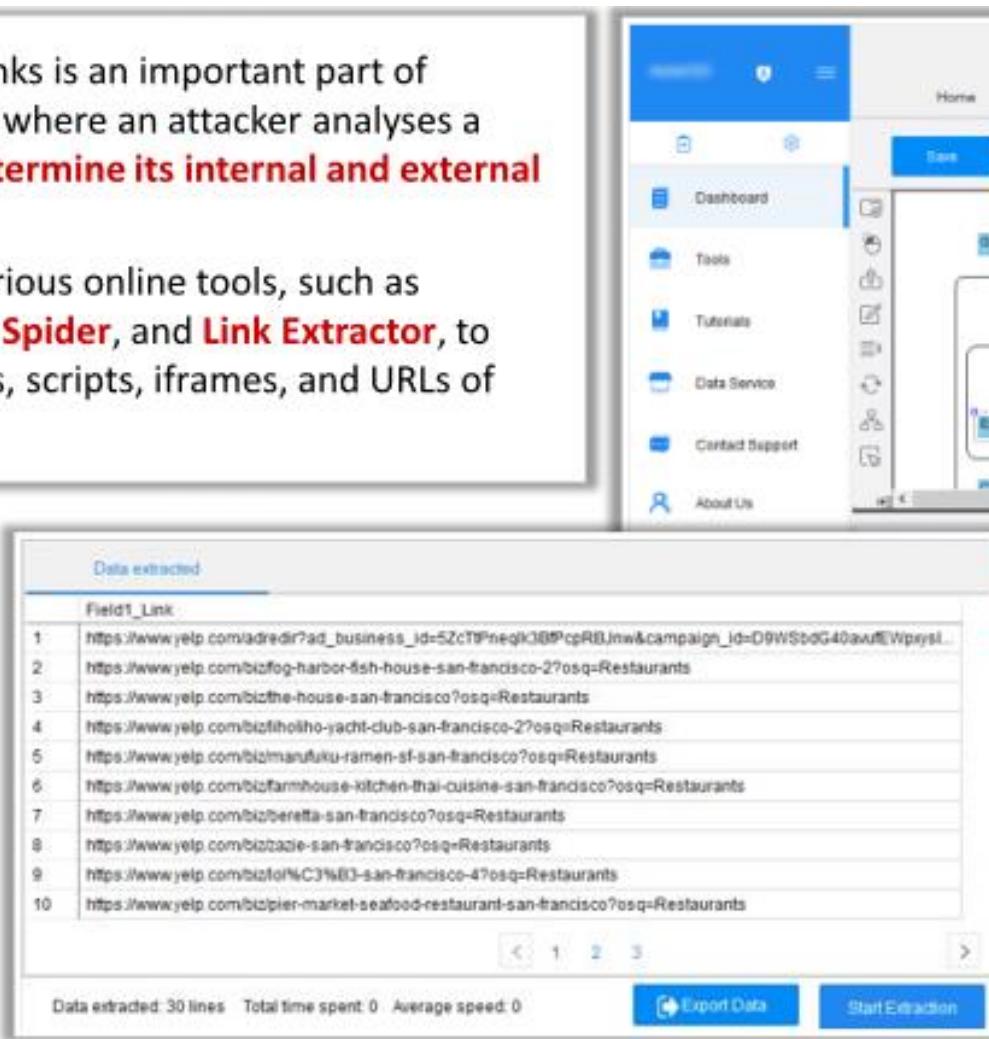


4. Extracting Website Links

- 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

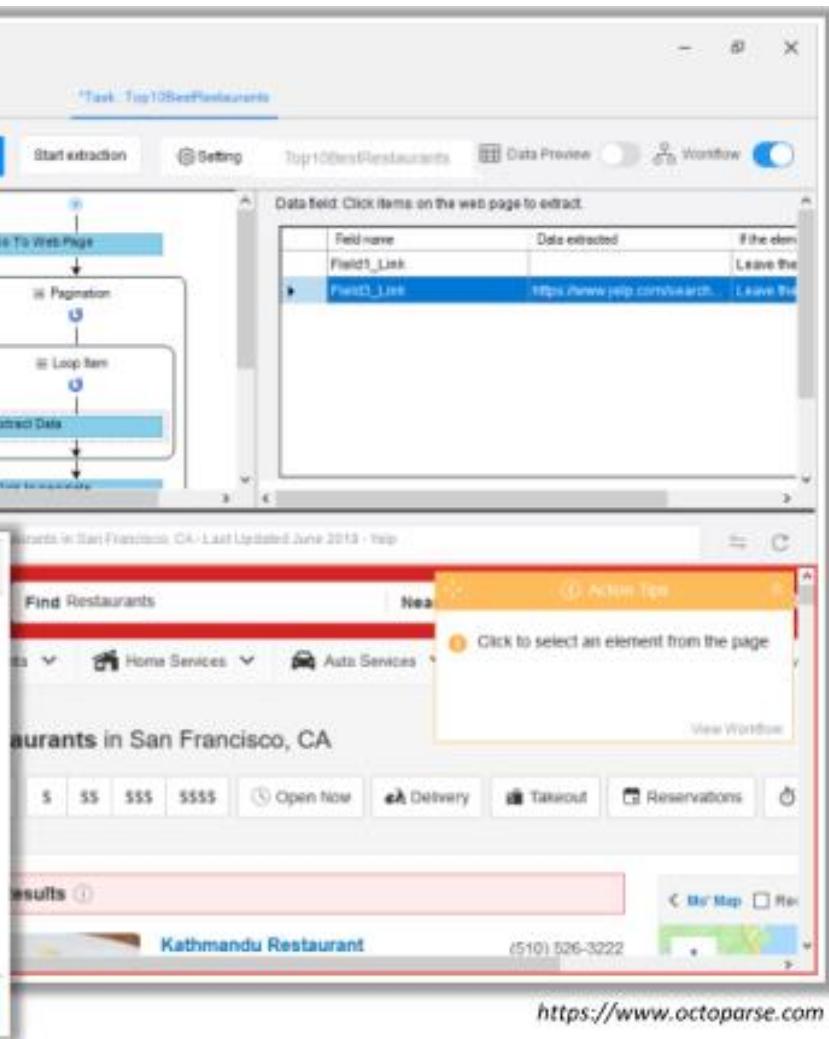
Octoparse

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



Data extracted		
	Field1_Link	
1	https://www.yelp.com/biz/adredin?ad_business_id=5ZctIPneqjKOBPcpREJmw&campaign_id=D9WSodG40avufEWpysl...	
2	https://www.yelp.com/biz/fog-harbor-fish-house-san-francisco-2?osq=Restaurants	
3	https://www.yelp.com/biz/the-house-san-francisco?osq=Restaurants	
4	https://www.yelp.com/biz/hiho-yacht-club-san-francisco-2?osq=Restaurants	
5	https://www.yelp.com/biz/manduku-ramen-st-san-francisco?osq=Restaurants	
6	https://www.yelp.com/biz/farmhouse-kitchen-thai-cuisine-san-francisco?osq=Restaurants	
7	https://www.yelp.com/biz/beretta-san-francisco?osq=Restaurants	
8	https://www.yelp.com/biz/zazzie-san-francisco?osq=Restaurants	
9	https://www.yelp.com/biz/oro%C3%B3-san-francisco-4?osq=Restaurants	
10	https://www.yelp.com/biz/pier-market-seafood-restaurant-san-francisco?osq=Restaurants	

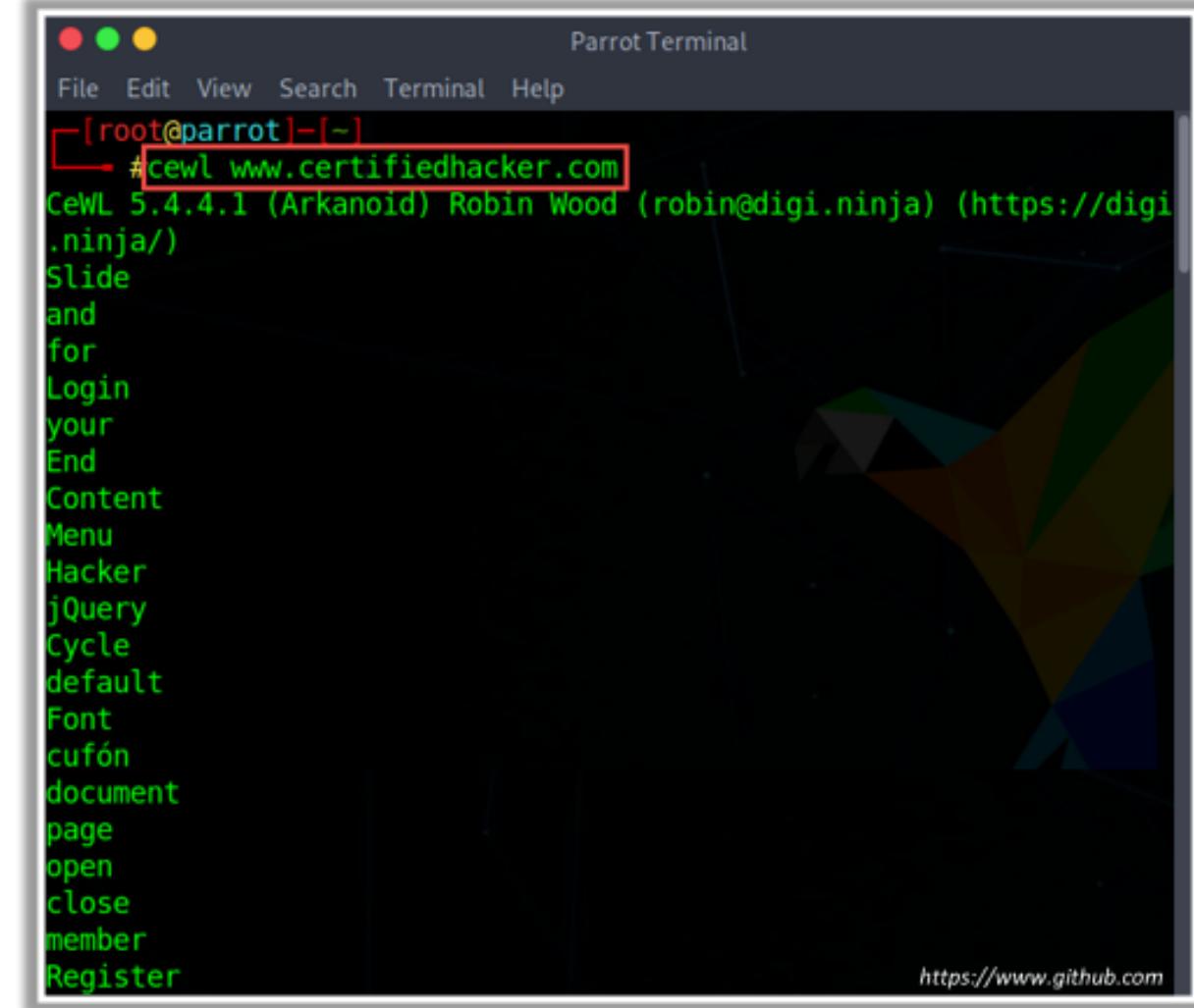
Data extracted: 30 lines Total time spent: 0 Average speed: 0 [Export Data](#) [Start Extraction](#)



https://www.yelp.com/search?find_desc=Restaurants&find_loc=San+Francisco,+CA&last_update=June+2013+10+ago

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`



```
[root@parrot] ~
# cewl www.certifiedhacker.com
CeWL 5.4.4.1 (Arkanoid) Robin Wood (robin@digi.ninja) (https://digi
.ninja/)
Slide
and
for
Login
your
End
Content
Menu
Hacker
jQuery
Cycle
default
Font
cufón
document
page
open
close
member
Register
```

<https://www.github.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 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 v17sor284449sor
 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; c=relaxed/relaxed;
 d=gmail.com; s=20161025;
 h=mime-version:from:date:message-id:subject:to;
 bh=nheQC6dgq1LhKwkOyK8x4gYW0WvtRRaK2KrErWhvfCg=;
 b=s6SMnvzNwMAeedUZF5r7LGPdGStUyx5KDxvLIBGHvEcF/pIIqx8KkNR2JGFOMPVXAL
 e7630+SPbK+M54CPx9hkvdbYhbcVgUZFuEvp3J/fPvIliT7Blf8jGXWqvvxwQhTH4+/g
 XeIE0g6h98SYL4lvePj8I9hw1xvjym8QYRoCgEqWE8JVRfqmNc0xBa6yoxuOVIJRT8A
 aFdUZS3KJMlbG8gBU6hS+bHrr3no370YJgLlh/YwkLTx76h7BgDYBzHcyg+ZPA+HvK5K
 3BWvrqeaGvGeZWh6xaS6LNmhf7CIuuxa/sk5ls1pfsK1eJv1qeCAV0Cq134JC292HRn2
 YCxw==
 MIME-Version: 1.0
 From: **[REDACTED] <[REDACTED] @gmail.com>**
 Date: **Mon, 10 Jun 2019 09:39:37 +0530**
 Message-ID: <CA++=zy1VzQ1gFmUDByZzqE90SbjwFYK/jcs...@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

Parrot Terminal

```

File Edit View Search Terminal Help
[root@parrot] ~ /infoga
[root@parrot] ~ /infoga
#python infoga.py

==[ Infoga - Email OSINT
==[ Momo (m4ll0k) Outtaadi
==[ https://github.com/m4ll0k

Usage: infoga.py [OPTIONS]

  -d --domain    Target URL/Name
  -s --source     Source data, default "all";
      all: Use all search engine
      google: Use google search engine
      bing: Use bing search engine
      yahoo: Use yahoo search engine
      ask: Use ask search engine
      baidu: Use baidu search engine
      dogpile: Use dogpile search engine
      exalead: Use exalead search engine
      PGP: Use pgp search engine

  -b --breach    Check if email breached
  -i --info      Get email informations
  -r --report    Simple file text report
  -v --verbose   Verbosity level (1,2 or 3)
  -H --help      Show this help and exit

```

<https://github.com>

eMailTrackerPro v10.0b Advanced Edition, Trial day 1 of 15.

File Help

My Index My Trace Reports Trace Headers Trace Address New Email Trace Email Accounts Settings Export Rules Configure

Home Subject THYBNKCRD CREDIT CARD (X2917) WILL BE DEI

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

New Trace View Report

Email Summary

From: [REDACTED] To: [REDACTED]@gmail.com Date: Mon, [REDACTED] 09:18:09 +0000 Subject: THYBNKCRD CREDIT CARD (X2917) WILL BE DEI Location: West Chester, Pennsylvania, USA

Misdirected: No Abuse Address: abuse@abuse-mailer.net Abuse Reporting: To automatically generate an email abo From IP: 208.78.224.20

System Information:

- The system is running a mail server (SMTP). This means that this system can be used to send e
- The system is running a web server on port 80 (HTTP). This means that this system serves web pages.
- The system is running a secure web server (Apache 2.4.18). Apache is status OK. This means that this system is running a web server.

Network Whois Domain Whois Email Header

For 24 hours only you can get up to 20% off eMailTrackerTrial Click Here

<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)



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

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

DNSReport Results for certifiedhacker.com

Overall Results: **2 FAIL** **0 WARNING** **17 PASS** **4 INFO**

Professional Toolset

PARENT			Information
Status	Test Name		
PASS	Parent zone provides NS records	Parent zone exists and provides NS records. This is good because some domains, usually third or fourth level domains, such as 'example.co.uk' do not have a direct parent zone. This is legal but can cause confusion. The NS Records provided are (nameserver IP Address TTL): ns1.bluehost.com. 162.159.24.00 ns1.bluehost.com. 162.159.25.175	
PASS	Number of nameservers	At least 2 (RFC1912 section 5 recommends at least 3), but fewer than 8 NS records exist. RFC1912 section 2.8 recommends that you have no more than 7). This meets the RFC minimum requirements, but is lower than the upper limits that some domain registrars have on the number of nameservers. A larger number of nameservers reduce the load on each and, since they should be located in different locations, prevent a single point of failure. The NS Records provided are: ns1.bluehost.com. 162.159.24.00 TTL=172800 ns2.bluehost.com. 162.159.25.175 TTL=172800	

NS			Information
Status	Test Name		
PASS	Unique nameserver IPs	All nameserver addresses are unique. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data.	
PASS	All nameservers respond	All nameservers responded. We were able to get a timely response for NS records from your nameservers, which indicates that they are running correctly and your zone (domain) is valid. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data.	
PASS	Open DNS servers	Nameservers do not respond to recursive queries. Your DNS servers do not announce that they are open DNS servers (i.e. answering recursively). Although there is a slight chance that they really are open DNS servers, this is very unlikely. Open DNS servers increase the chances of cache poisoning, can degrade performance of your DNS, and can cause your DNS servers to be used in an attack, so it is imperative that externally facing DNS servers do not recursively answer queries.	
PASS	All nameservers authoritative	All nameservers answered authoritatively for the zone. This indicates that the zones for this domain are set up correctly on your nameservers and that we should be able to get good responses to further queries.	

<https://tools.dnsstuff.com>

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**



yougetsignal

Reverse IP Domain Check

Remote Address: www.certifiedhacker.com Check

Found 7 domains hosted on the same web server as www.certifiedhacker.com (162.241.216.11).

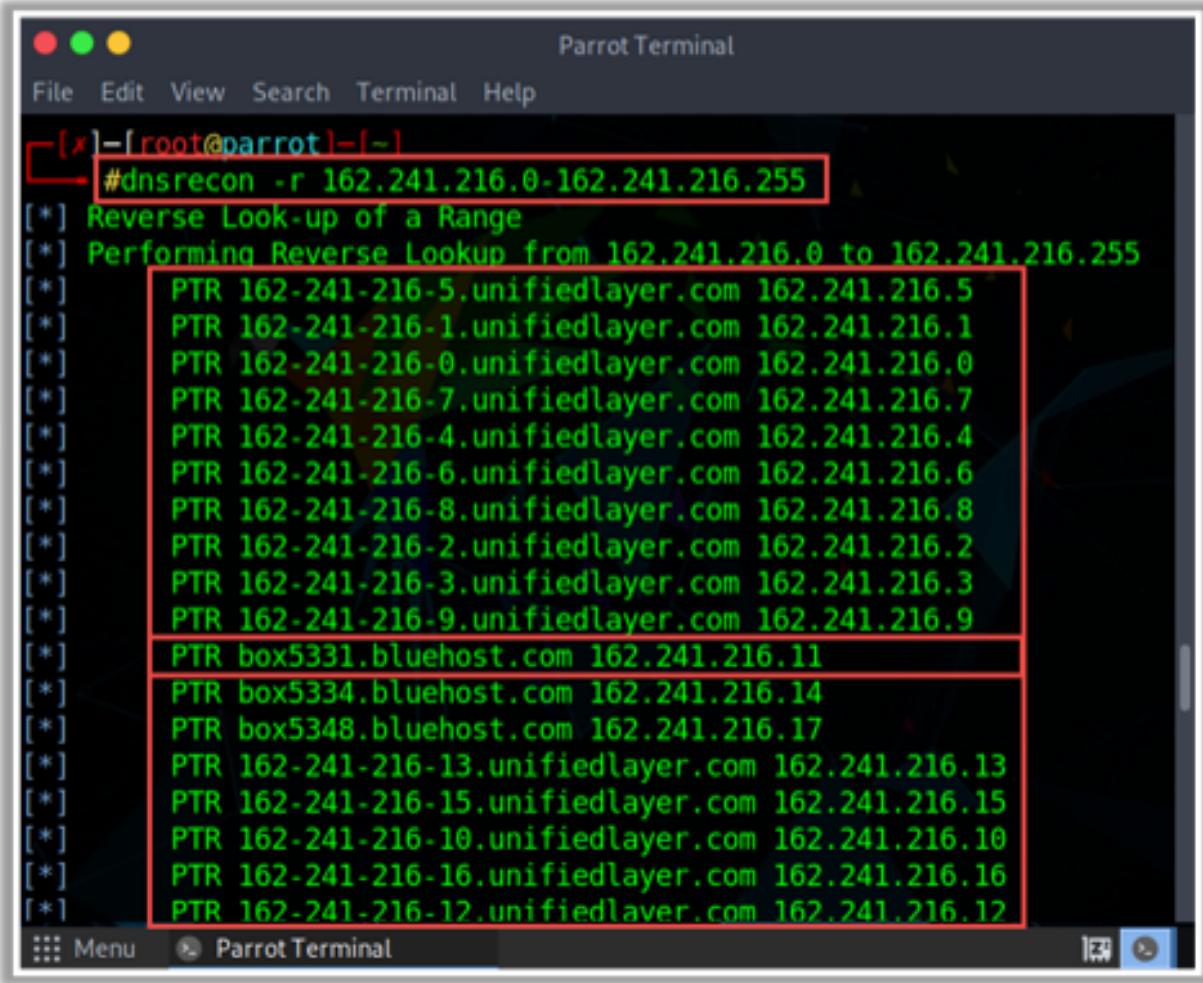
bongkille.com	box5331.bluehost.com
certifiedhacker.com	humancarehealth.com
oakoffer.com	www.certifiedhacker.com
www.lisit.org	

about
Note: For those of you interested, as of May 2014, my database has grown to over 100 million domain names. I am now offering this domain list for purchase.

A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on that same web server. Data is gathered from search engine results, which are not guaranteed to be complete. IP-Address.org provides interesting visual reverse IP lookup tool. Knowing the other web sites hosted on a web server is important from both an SEO and web filtering perspective, particularly for those on [shared web hosting](#) plans.

[More about this tool.](#) Set an API Key

<https://www.yougetsignal.com>



Parrot Terminal

```
[x]-[root@parrot]-[~]
#dnsrecon -r 162.241.216.0-162.241.216.255
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 162.241.216.0 to 162.241.216.255
[*] PTR 162-241-216-5.unifiedlayer.com 162.241.216.5
[*] PTR 162-241-216-1.unifiedlayer.com 162.241.216.1
[*] PTR 162-241-216-0.unifiedlayer.com 162.241.216.0
[*] PTR 162-241-216-7.unifiedlayer.com 162.241.216.7
[*] PTR 162-241-216-4.unifiedlayer.com 162.241.216.4
[*] PTR 162-241-216-6.unifiedlayer.com 162.241.216.6
[*] PTR 162-241-216-8.unifiedlayer.com 162.241.216.8
[*] PTR 162-241-216-2.unifiedlayer.com 162.241.216.2
[*] PTR 162-241-216-3.unifiedlayer.com 162.241.216.3
[*] PTR 162-241-216-9.unifiedlayer.com 162.241.216.9
[*] PTR box5331.bluehost.com 162.241.216.11
[*] PTR box5334.bluehost.com 162.241.216.14
[*] PTR box5348.bluehost.com 162.241.216.17
[*] PTR 162-241-216-13.unifiedlayer.com 162.241.216.13
[*] PTR 162-241-216-15.unifiedlayer.com 162.241.216.15
[*] PTR 162-241-216-10.unifiedlayer.com 162.241.216.10
[*] PTR 162-241-216-16.unifiedlayer.com 162.241.216.16
[*] PTR 162-241-216-12.unifiedlayer.com 162.241.216.12
```

Menu Parrot Terminal

<https://github.com>

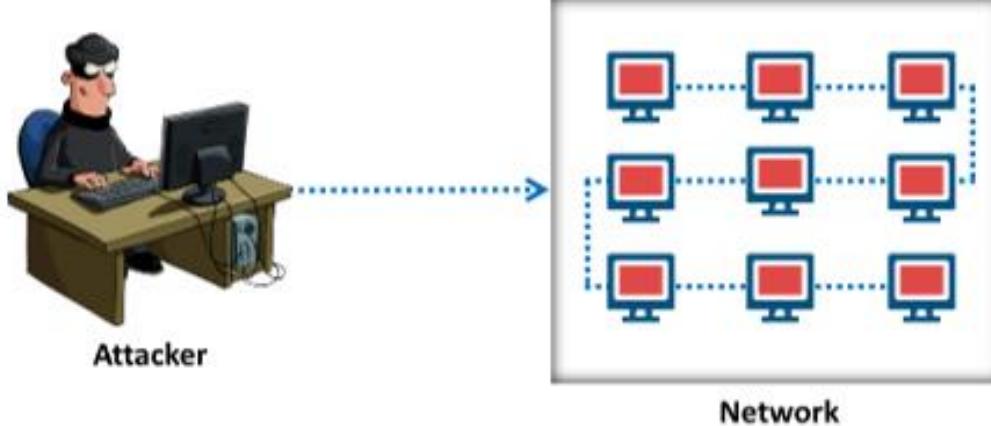
NETWORK FOOTPRINTING

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://dap.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

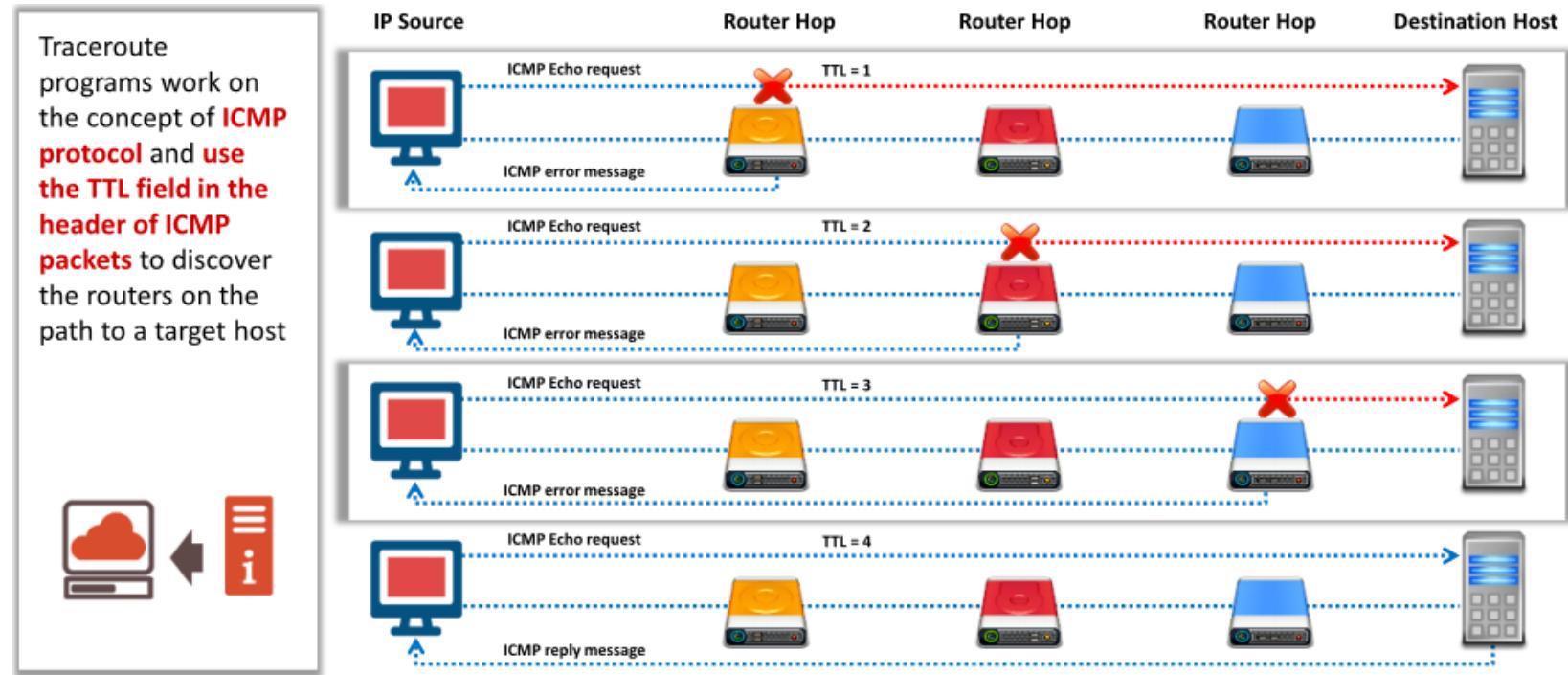
Related Entities ▾ 1 Entity

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**.



Cont,

IMCP Traceroute

```
Select Command Prompt - tracer 216.239.36.10
C:\Users\*****>tracert 216.239.36.10

Tracing route to ns3.google.com [216.239.36.10]
over a maximum of 30 hops:
1 <1 ms <1 ms <1 ms 10.10.10.2
2 4 ms 8 ms 14 ms 115.249.169.81
3 13 ms 13 ms 11 ms 115.255.252.226
4 14 ms 13 ms 13 ms 74.125.51.2
5 27 ms 25 ms 16 ms 108.170.253.121
6 47 ms 46 ms 48 ms 72.14.233.129
7 82 ms 83 ms 83 ms 72.14.239.212
8 93 ms 93 ms 93 ms 209.85.245.163
9 91 ms 91 ms 92 ms 72.14.233.35
10 * * * Request timed out.
11 * * * Request timed out.
12 * * * Request timed out.
```



TCP Traceroute

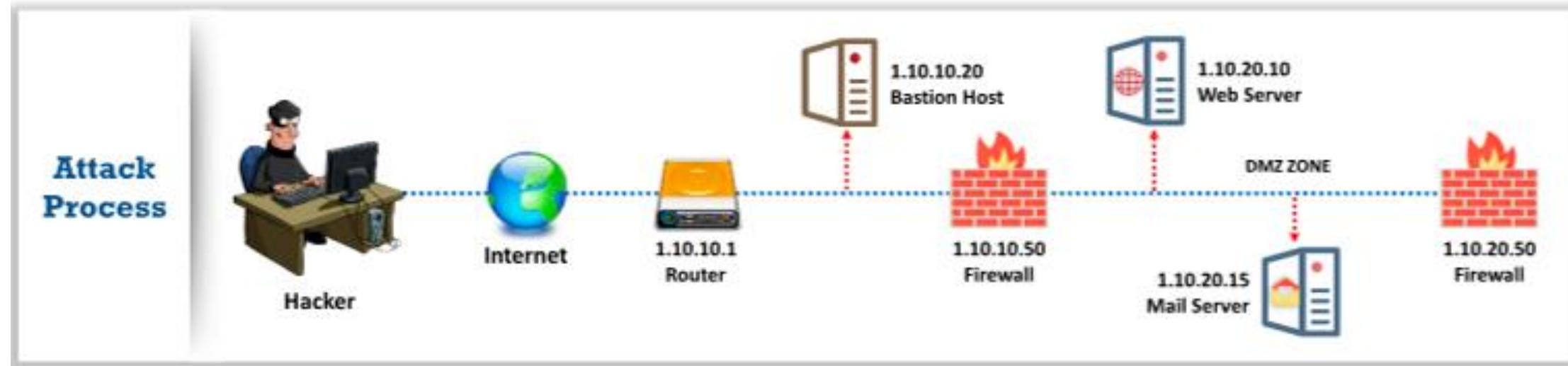
```
[root@parrot] ~
[root@parrot] ~ -> #tcptraceroute www.google.com
Running:
traceroute -T -O info www.google.com
traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
1 10.10.10.2 (10.10.10.2) 0.312 ms 0.172 ms 0.287 ms
2 maa05s05-in-f4.1e100.net (172.217.163.164) <syn,ack> 17.775 ms 17.367
ms 17.491 ms
```

UDP Traceroute

```
[root@parrot] ~
[root@parrot] ~ -> #traceroute www.google.com
traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
1 10.10.10.2 (10.10.10.2) 0.260 ms 0.189 ms 0.196 ms
2 * *
3 * *
4 * *
5 * *
6 * *
7 * *
```

3. Traceroute Analysis

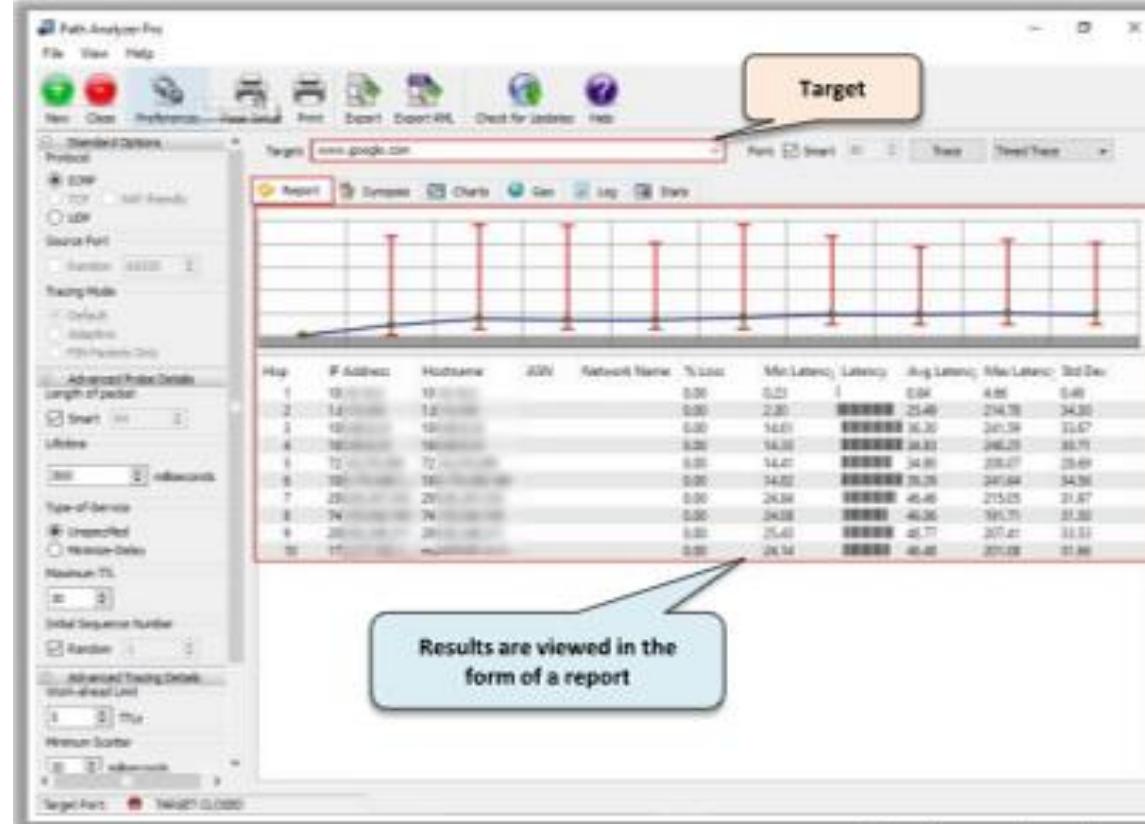
- Attackers conduct traceroute to extract information about **network topology**, **trusted routers**, and **firewall locations**
- For example, after running several **traceroutes**, an attacker might obtain the following information:
 - traceroute 1.10.10.20, second to last hop is 1.10.10.1
 - traceroute 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

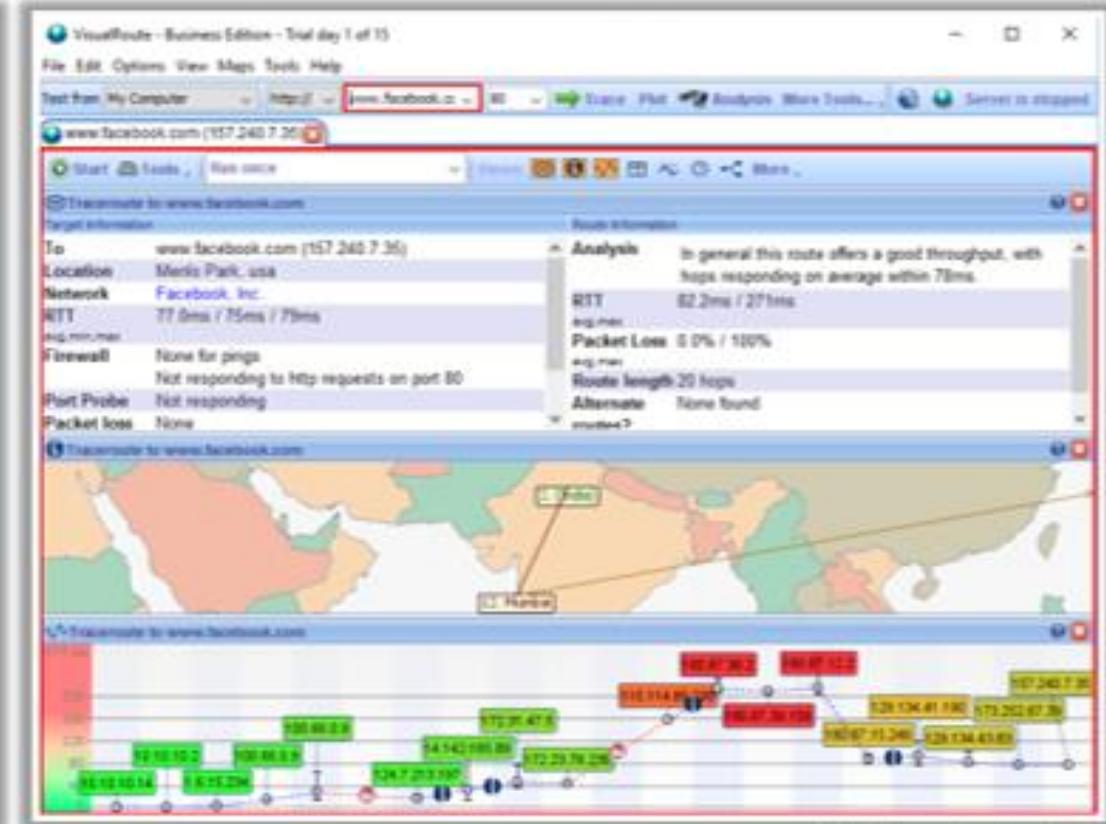
Path Analyzer Pro

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

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



Shoulder Surfing

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



Dumpster Diving

- ➊ Looking for treasure in someone else's trash
- ➋ 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.

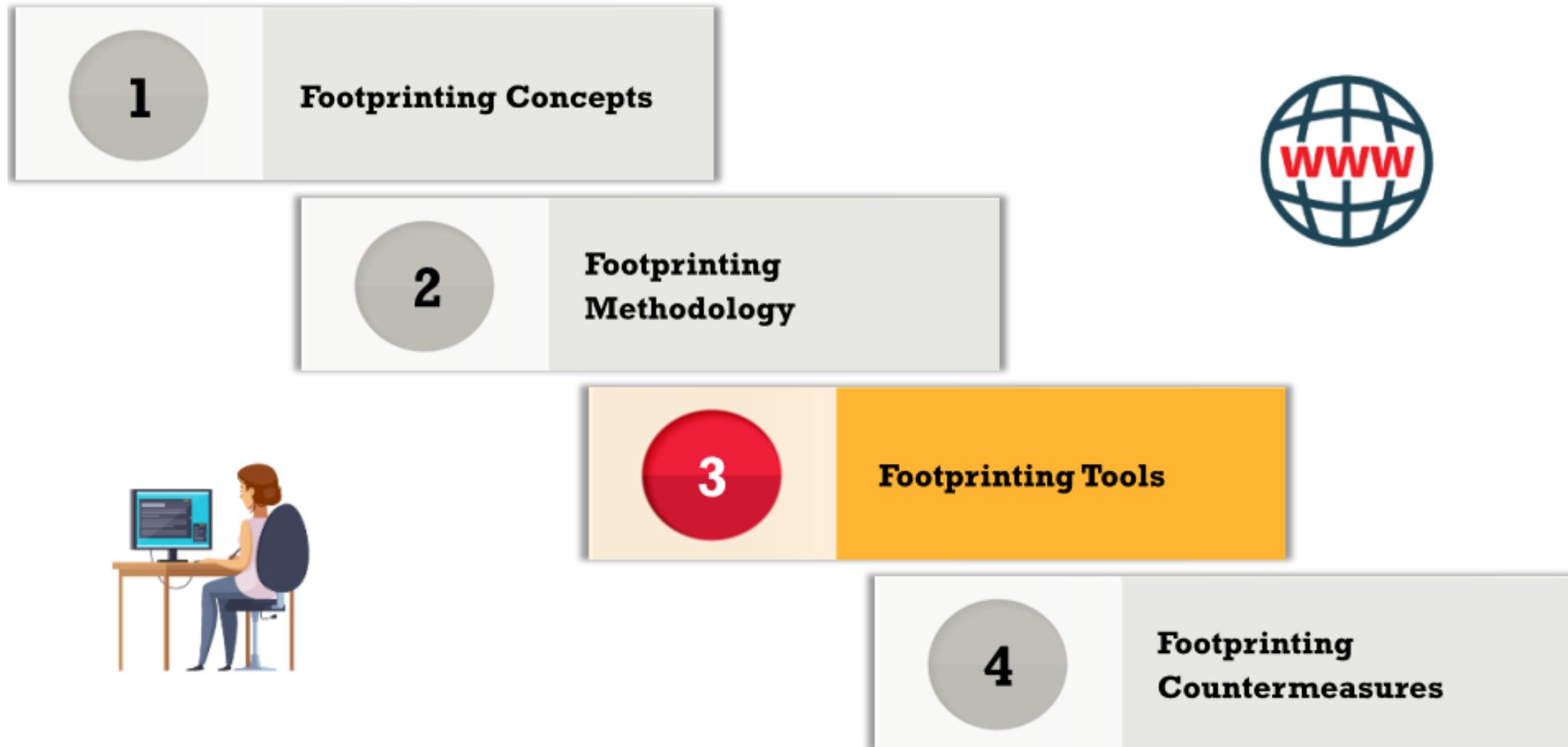


Impersonation

- ➊ 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



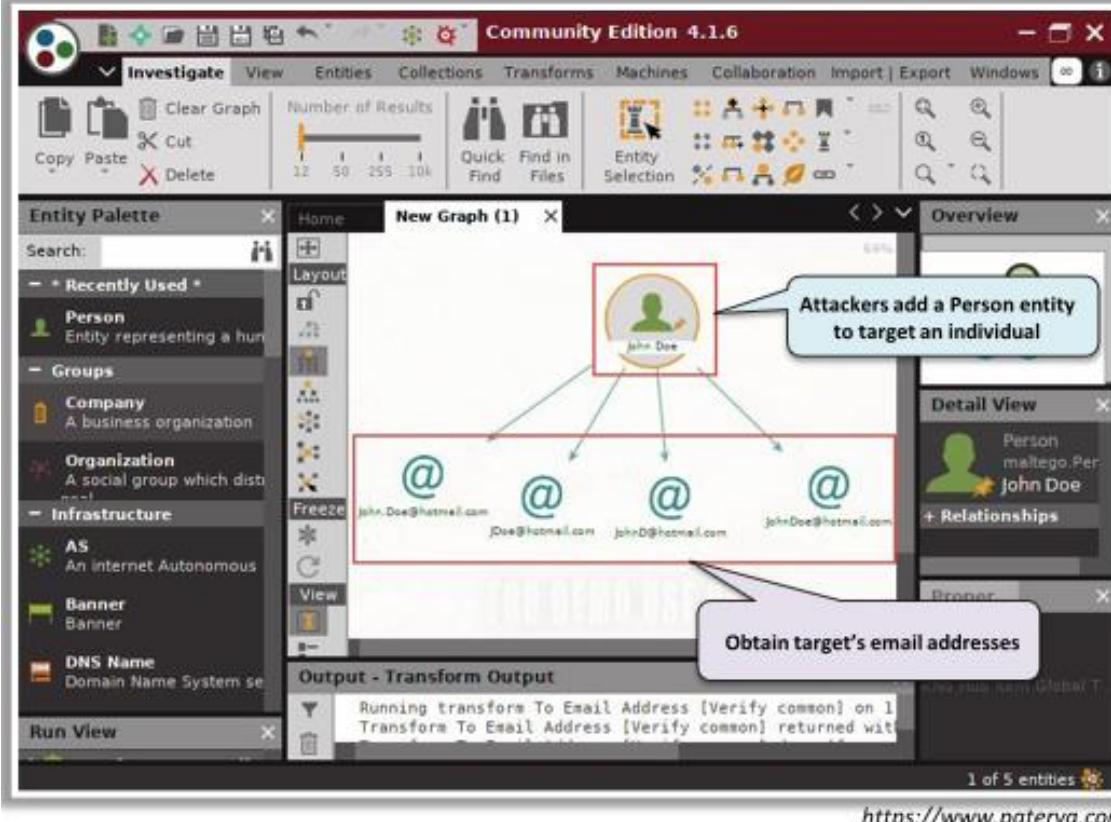
3. Footprinting Tools



Maltego and Recon-ng

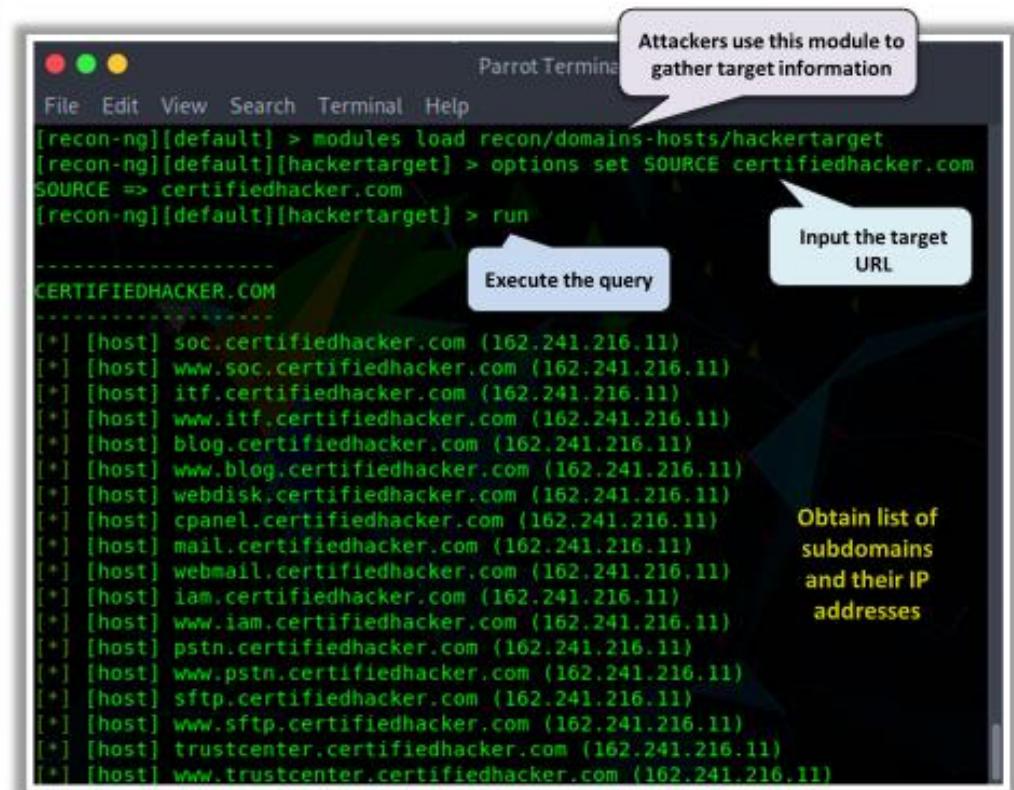
Maltego

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



```
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > options set SOURCE certifiedhacker.com
SOURCE => certifiedhacker.com
[recon-ng][default][hackertarget] > run
```

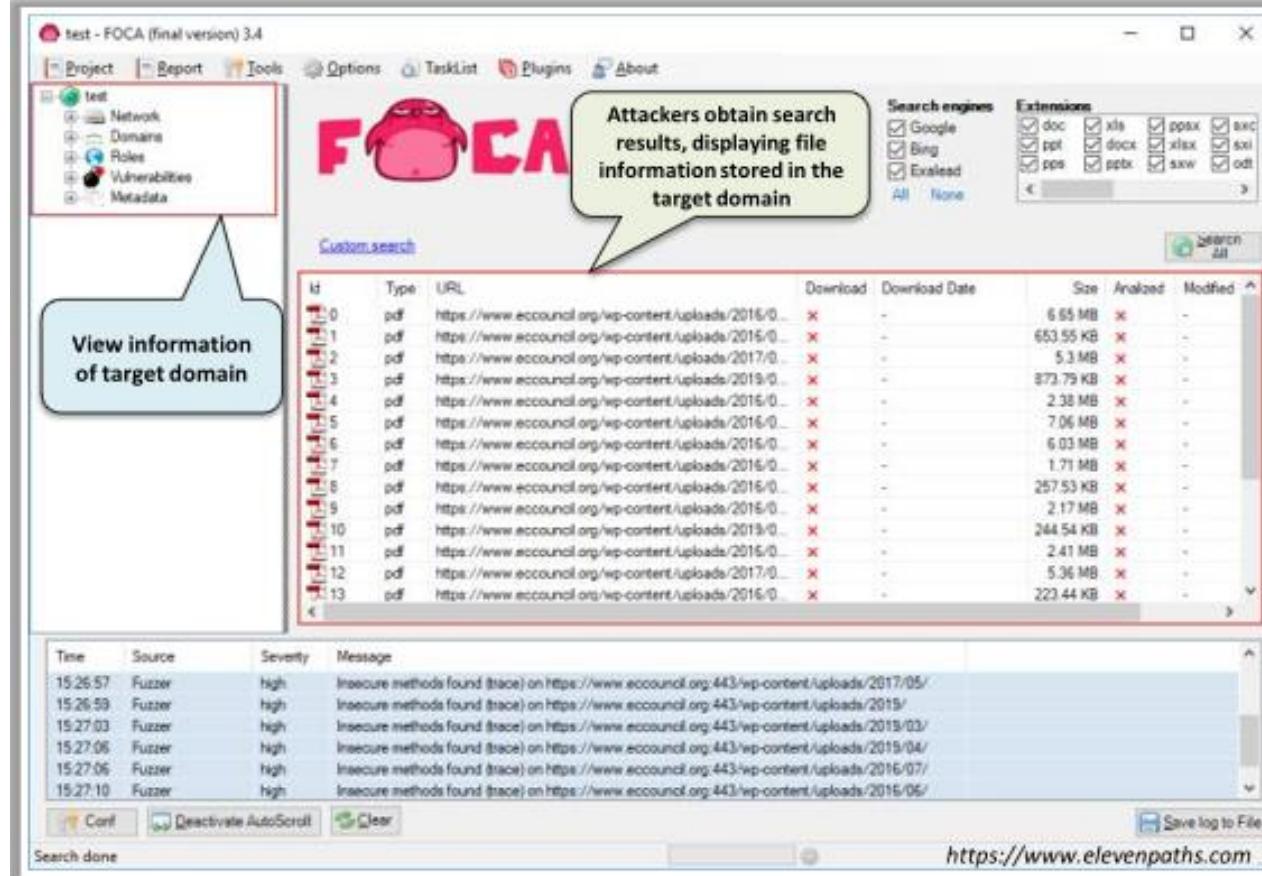
CERTIFIEDHACKER.COM

```
[*] [host] soc.certifiedhacker.com (162.241.216.11)
[*] [host] www.soc.certifiedhacker.com (162.241.216.11)
[*] [host] itf.certifiedhacker.com (162.241.216.11)
[*] [host] www.itf.certifiedhacker.com (162.241.216.11)
[*] [host] blog.certifiedhacker.com (162.241.216.11)
[*] [host] www.blog.certifiedhacker.com (162.241.216.11)
[*] [host] webdisk.certifiedhacker.com (162.241.216.11)
[*] [host] cpanel.certifiedhacker.com (162.241.216.11)
[*] [host] mail.certifiedhacker.com (162.241.216.11)
[*] [host] webmail.certifiedhacker.com (162.241.216.11)
[*] [host] iam.certifiedhacker.com (162.241.216.11)
[*] [host] www.iam.certifiedhacker.com (162.241.216.11)
[*] [host] pstn.certifiedhacker.com (162.241.216.11)
[*] [host] www.pstn.certifiedhacker.com (162.241.216.11)
[*] [host] sftp.certifiedhacker.com (162.241.216.11)
[*] [host] www.sftp.certifiedhacker.com (162.241.216.11)
[*] [host] trustcenter.certifiedhacker.com (162.241.216.11)
[*] [host] www.trustcenter.certifiedhacker.com (162.241.216.11)
```

<https://aihub.com>

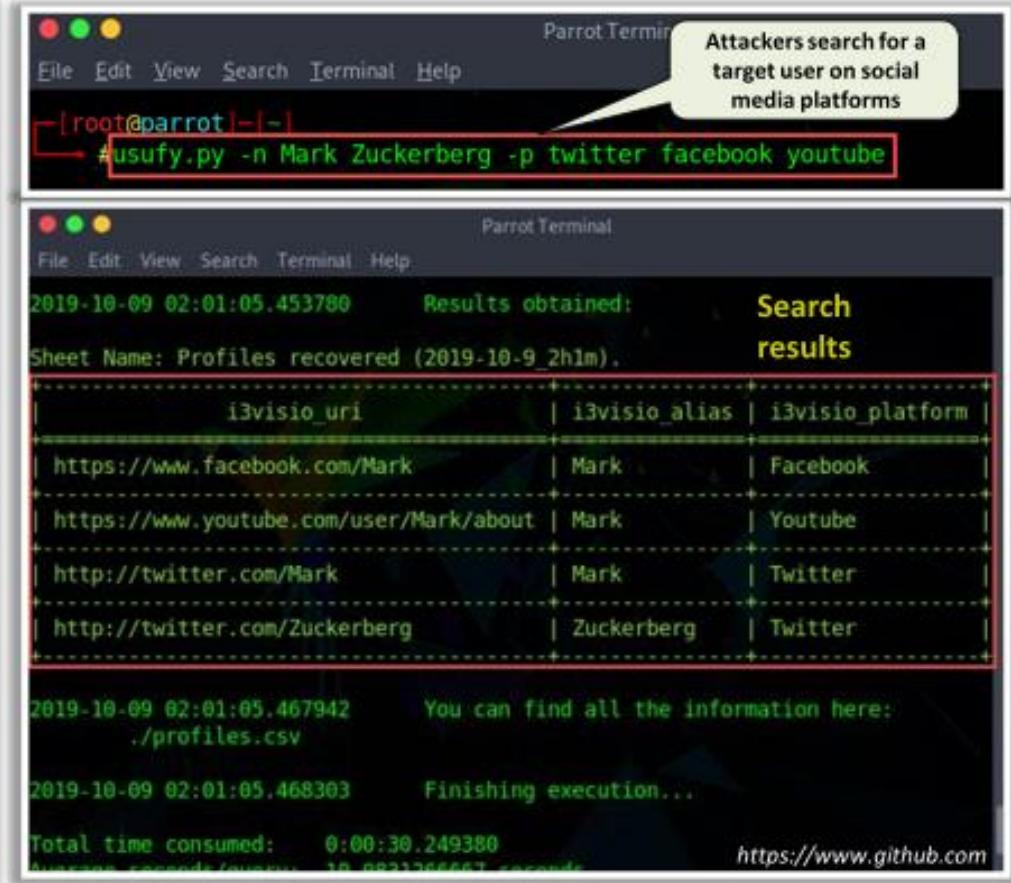
FOCA and OSRFramework

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



The screenshot shows the FOCA application window. On the left, there's a sidebar with a tree view of a project named 'test' containing Network, Domains, Roles, Vulnerabilities, and Metadata. A callout bubble points to this sidebar with the text 'View information of target domain'. The main area has a pink 'FOCA' logo and displays a table of search results. A callout bubble points to this table with the text 'Attackers obtain search results, displaying file information stored in the target domain'. The table columns include Id, Type, URL, Download, Download Date, Size, Analyzed, and Modified. Below the table is a log viewer showing messages from a 'Fuzzer' component. At the bottom, there's a status bar with the URL 'https://www.elevenpaths.com' and a 'Save log to File' button.

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

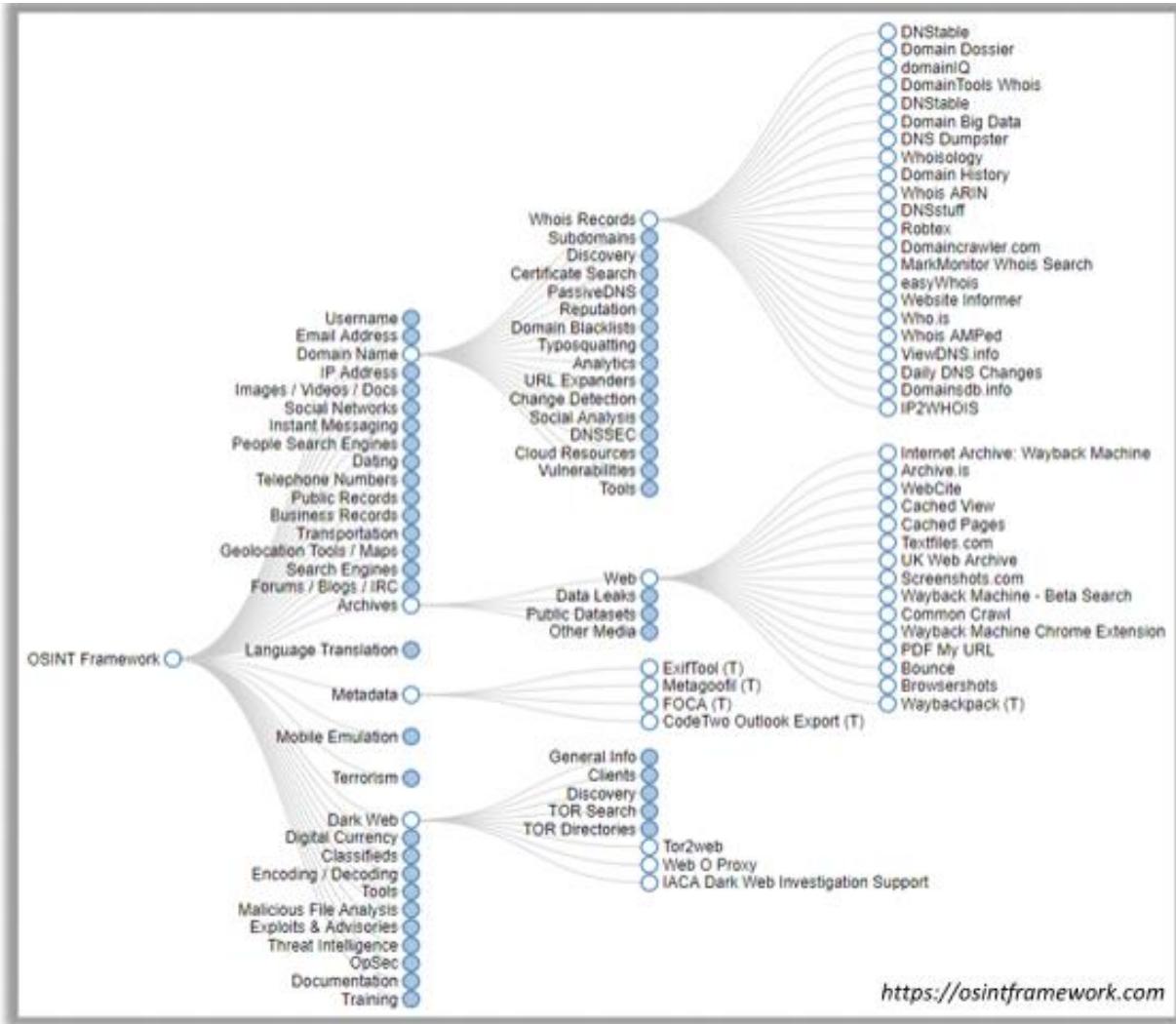


The screenshot shows two terminal windows. The top window is titled 'Parrot Terminal' and shows a command-line session where an attacker is searching for a target user on social media platforms using the 'usufy.py' script. The command is '#usufy.py -n Mark Zuckerberg -p twitter facebook youtube'. The bottom window is also a 'Parrot Terminal' and displays a table of search results under the heading 'Results obtained:'. The table has columns for 'Sheet Name', 'URL', 'Name', and 'Platform'. It lists several profiles recovered, such as 'Mark' on Facebook, YouTube, and Twitter, and 'Zuckerberg' on Twitter. The bottom terminal window also shows the command './profiles.csv' and the message 'Finishing execution...'. At the very bottom, it shows the total time consumed: 0:00:30.249380.

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



```

Parrot Terminal
File Edit View Search Terminal Help
[...]-[root@parrot:~/ReconDog]
└─# python dog
[...]
v2.0

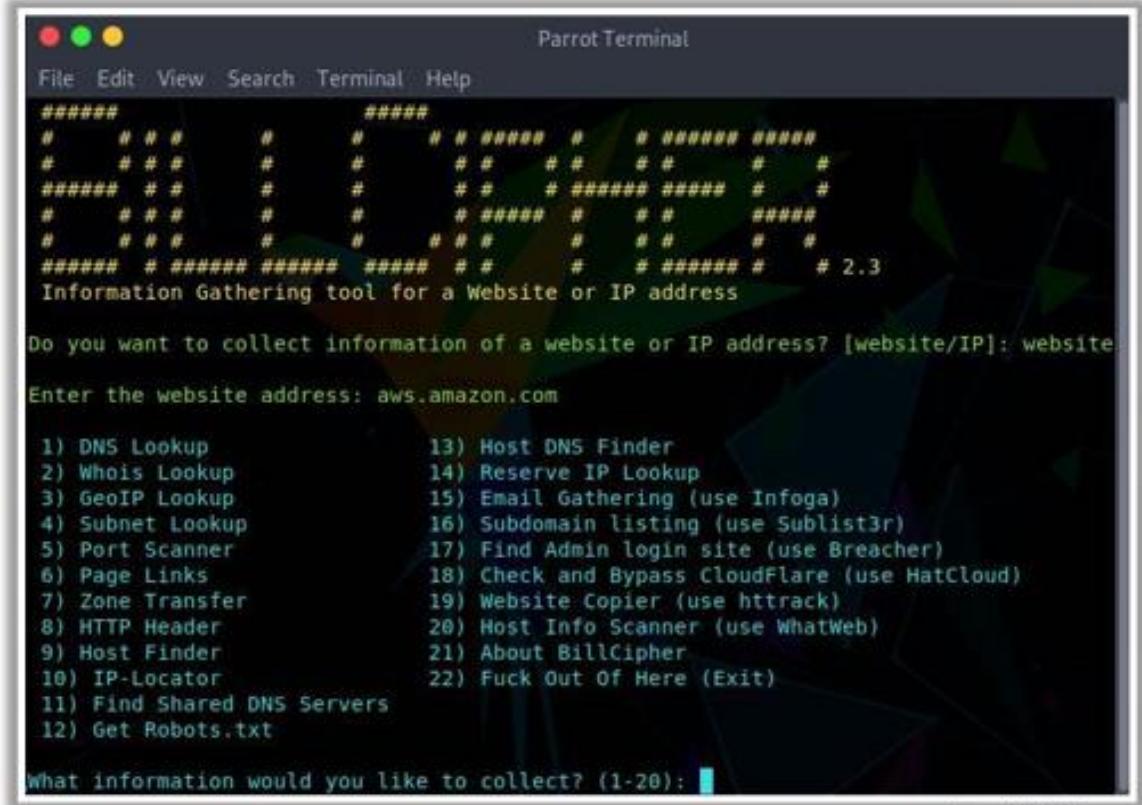
1. Censys
2. NS lookup
3. Port scan
4. Detect CMS
5. Whois lookup
6. Detect honeypot
7. Find subdomains
8. Reverse IP lookup
9. Detect technologies
0. All
-> 5
domain or ip> certifiedhacker.com
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2016-03-10T12:38:41Z
Creation Date: 2002-07-30T00:32:00Z
Registry Expiry Date: 2021-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8883337680
Domain Status: clientTransferProhibited https://icann.org/epp/clientTransferProhibited
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM

```

<https://www.github.com>

BillCipher

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



```

Parrot Terminal
File Edit View Search Terminal Help
#####
#   #   #   #   #
#   #   #   #   #
##### #   #   #   #   #
#   #   #   #   #   #
#   #   #   #   #   #
#####
#   #   #   #   #   #
#   #   #   #   #   #
#   #   #   #   #   #
#####
Information Gathering tool for a Website or IP address

Do you want to collect information of a website or IP address? [website/IP]: website
Enter the website address: aws.amazon.com

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

What information would you like to collect? (1-20): 1

```

<https://github.com>



theHarvester

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



Th3Inspector

<https://github.com>



Raccoon

<https://github.com>



Orb

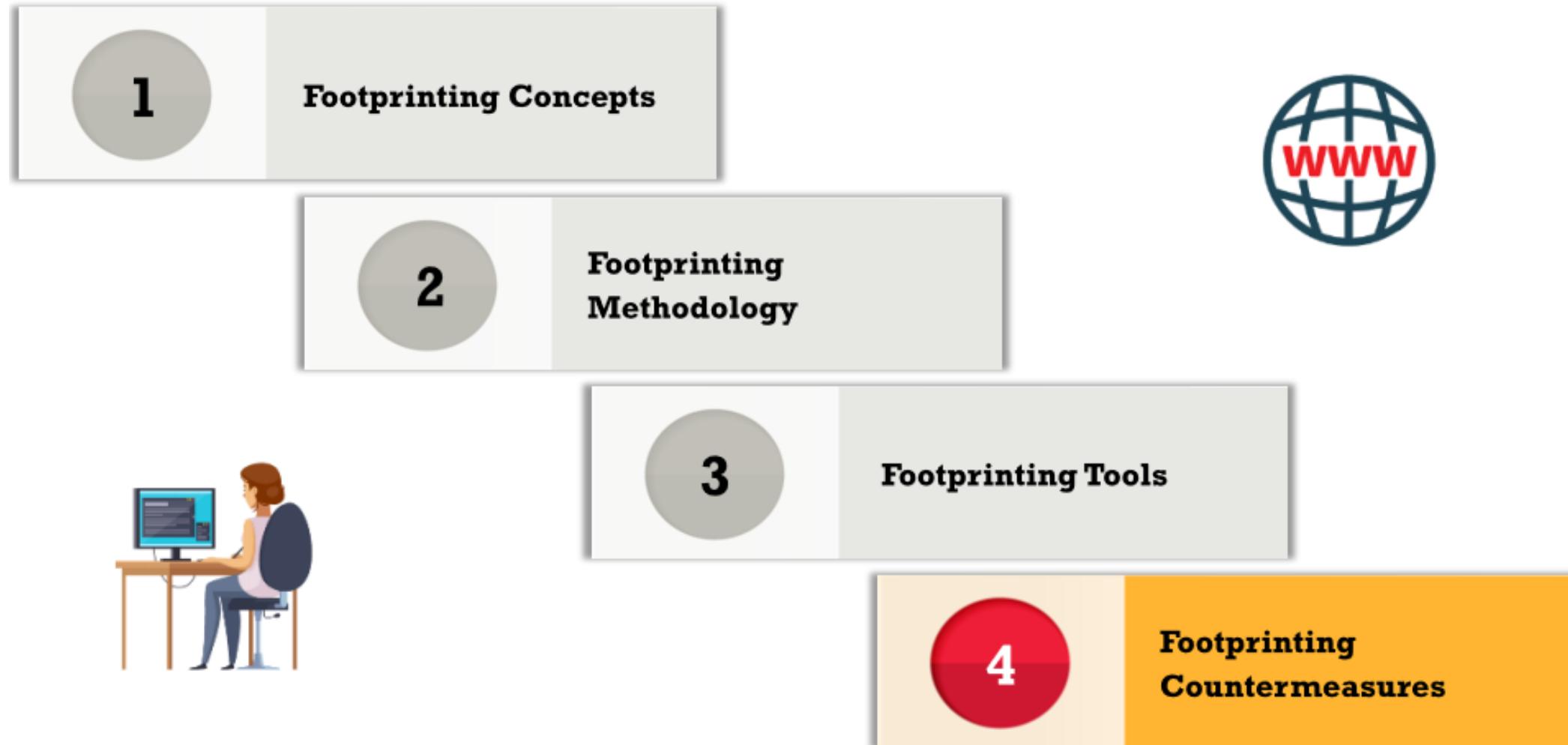
<https://github.com>



PENTMENU

<https://github.com>

4. Footprinting Countermeasures



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

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

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