Footprinting and Reconnaissance

Module Objectives

- Understanding Footprinting Concepts
- Understanding Footprinting Through Search Engines and Advanced Google Hacking Techniques
- Understanding Footprinting Through Web Services and Social Networking Sites
- Understanding Website Footprinting and Email Footprinting
- Understanding WHOIS, DNS, and Network Footprinting
- Understanding Footprinting Through Social Engineering
- Understanding Different Footprinting Tools and Countermeasures

Module Flow

1 Footprinting Concepts

2 Footprinting Methodology

3 Footprinting Tools

4 Footprinting Countermeasures

What is Footprinting?

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

Types of Footprinting

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

Information Obtained in Footprinting

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

Objectives of Footprinting

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

Passive footprinting techniques include:

- Finding information through search engines
- Finding the Top-level Domains (TLDs) and sub-domains of a target through web services
- Collecting location information on the target through web services
- Performing people search using social networking sites and people search services
- Gathering financial information about the target through financial services
- Gathering infrastructure details of the target organization through job sites
- Collecting information through deep and dark web footprinting
- Determining the operating systems in use by the target organization

- Performing competitive intelligence
- Monitoring the target using alert services
- Gathering information using groups, forums, blogs, and NNTP Usenet newsgroups
- Collecting information through social engineering on social networking sites
- Extracting information about the target using Internet archives
- Gathering information using business profile sites
- Monitoring website traffic of the target
- Tracking the online reputation of the target

Active footprinting techniques include:

- Querying published name servers of the target
- Searching for digital files
- Extracting website links and gathering wordlists from the target website
- Extracting metadata of published documents and files
- Gathering website information using web spidering and mirroring tools
- Gathering information through email tracking
- Harvesting email lists
- Performing Whois lookup
- Extracting DNS information
- Performing traceroute analysis
- Performing social engineering

Organization Information: Such information about an organization is available from its website. In addition, you can query the target's domain name against the Whois database and obtain valuable information.

The information collected includes:

- Employee details (employee names, contact addresses, designations, and work experience)
- Addresses and mobile/telephone numbers
- Branch and location details
- Partners of the organization
- Web links to other company-related sites
- Background of the organization
- Web technologies
- News articles, press releases, and related documents
- Legal documents related to the organization
- Patents and trademarks related to the organization

Network Information: You can gather network information by performing Whois database analysis, trace routing, and so on.

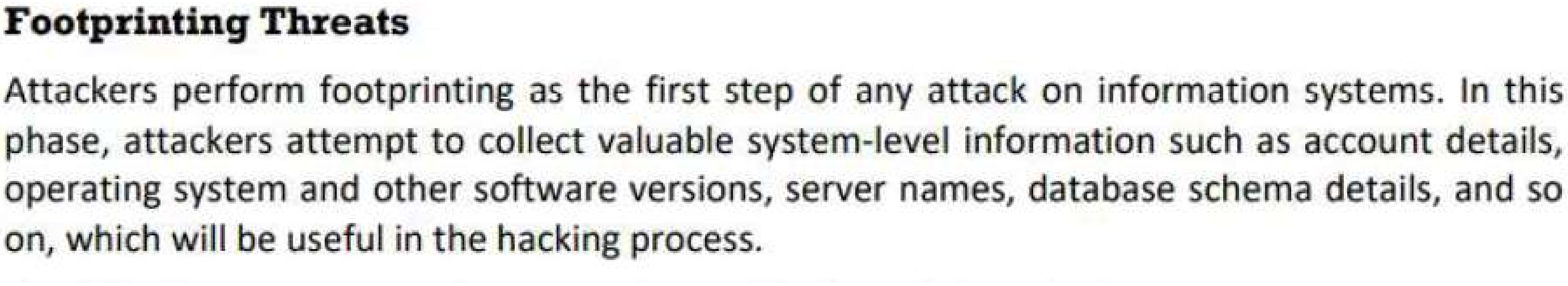
The information collected includes:

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

System Information: You can gather system information by performing network footprinting, DNS footprinting, website footprinting, email footprinting, and so on.

The information collected includes:

- Web server OS
- Location of web servers
- Publicly available email addresses
- Usernames, passwords, and so on.



Footprinting Threats

Attackers perform footprinting as the first step of any attack on information systems. In this phase, attackers attempt to collect valuable system-level information such as account details, operating system and other software versions, server names, database schema details, and so on, which will be useful in the hacking process.

The following are assorted threats made possible through footprinting:

- **Social Engineering**: Without using any intrusion methods, hackers directly and indirectly collect information through persuasion and other means. Hackers gather crucial information from willing employees who are unaware of the hackers' intent.
- **System and Network Attacks**: Footprinting enables an attacker to perform system and network attacks. Thus, attackers can gather information related to the target organization's system configuration, the operating system running on the machine, and so on. Using this information, attackers can find vulnerabilities in the target system and then exploit such vulnerabilities. They can then take control of a target system or the entire network.

- **Information Leakage**: Information leakage poses a threat to any organization. If sensitive information of an entity falls into the hands of attackers, they can mount an attack based on the information or alternatively use it for monetary benefit.
- **Privacy Loss**: Through footprinting, hackers can access the systems and networks of the organization and even escalate the privileges up to admin levels, resulting in the loss of privacy for the organization as a whole and for its individual personnel.
- **Corporate Espionage**: Corporate espionage is a central threat to organizations, as competitors often aim to attempt to secure sensitive data through footprinting. Through this approach, competitors can launch similar products in the market, alter prices, and generally undermine the market position of a target organization.
- **Business Loss**: Footprinting can have a major effect on organizations such as online businesses and other e-commerce websites as well as banking and finance-related businesses. Billions of dollars are lost every year due to malicious attacks by hackers.

Module Flow

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

Search Engines

Footprinting through Search Engines

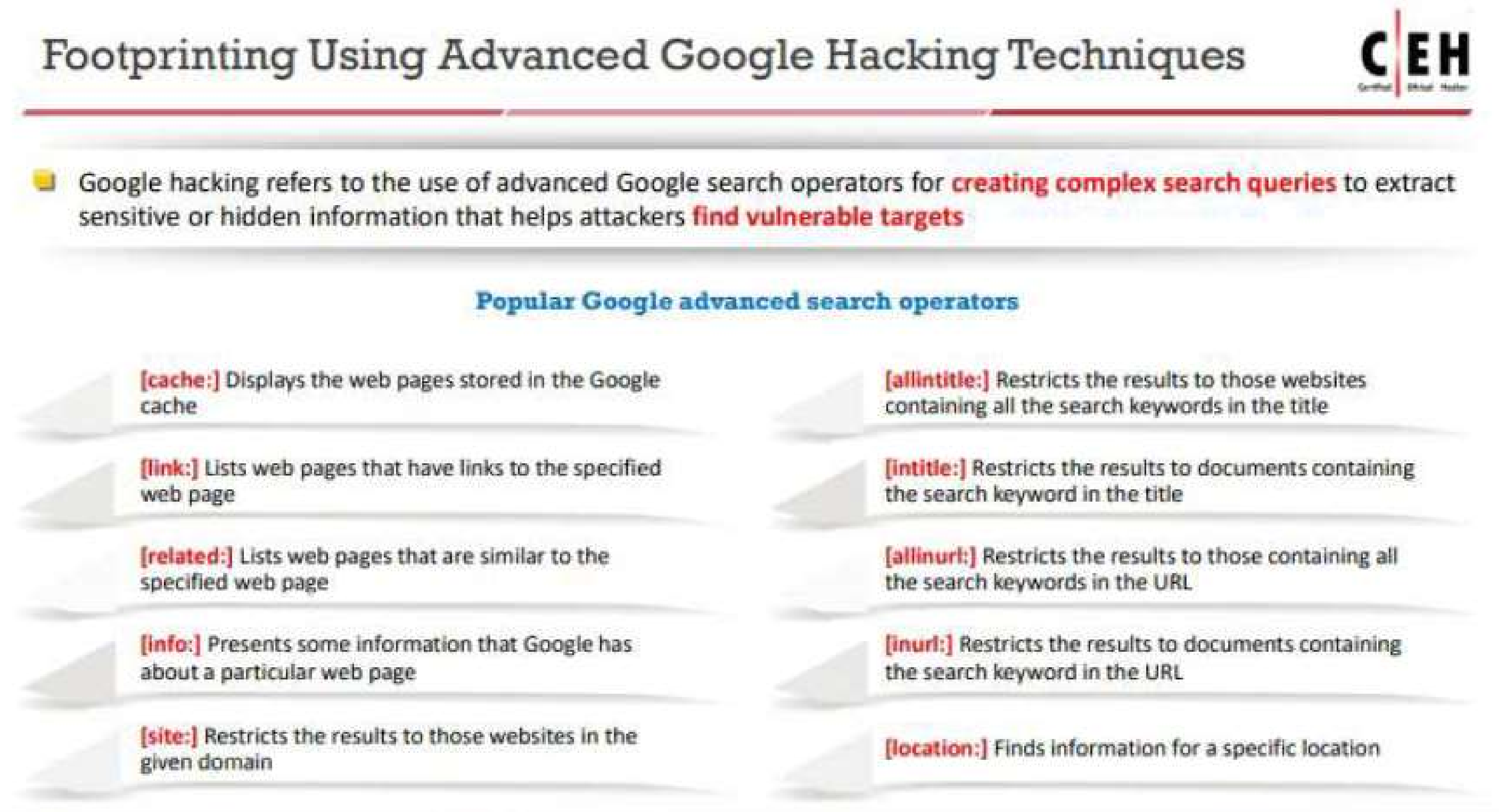
Footprinting through Search Engines

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

- Major search engines:

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

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



Footprinting Using Advanced Google Hacking Techniques

- 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

- **inanchor**: This operator restricts results to only the pages containing the query terms specified in the anchor text on links to the page.

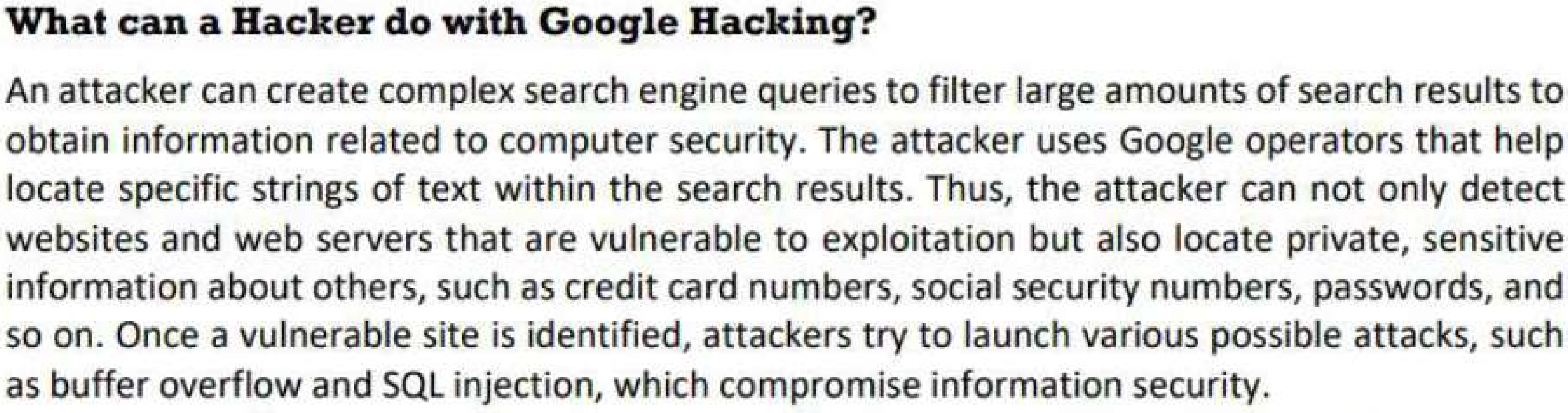
  For example, the [Anti-virus inanchor:Norton] query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus."

- **allinanchor**: This operator restricts results to only the pages containing all query terms specified in the anchor text on links to the pages.

  For example, the [allinanchor: best cloud service provider] query returns only pages for which the anchor text on links to the pages contains the words "best," "cloud," "service," and "provider."

- **Filetype:** This operator allows you to search for results based on a file extension.

  For Example, [jasmine:jpg] will provide jpg files based on jasmine.



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.

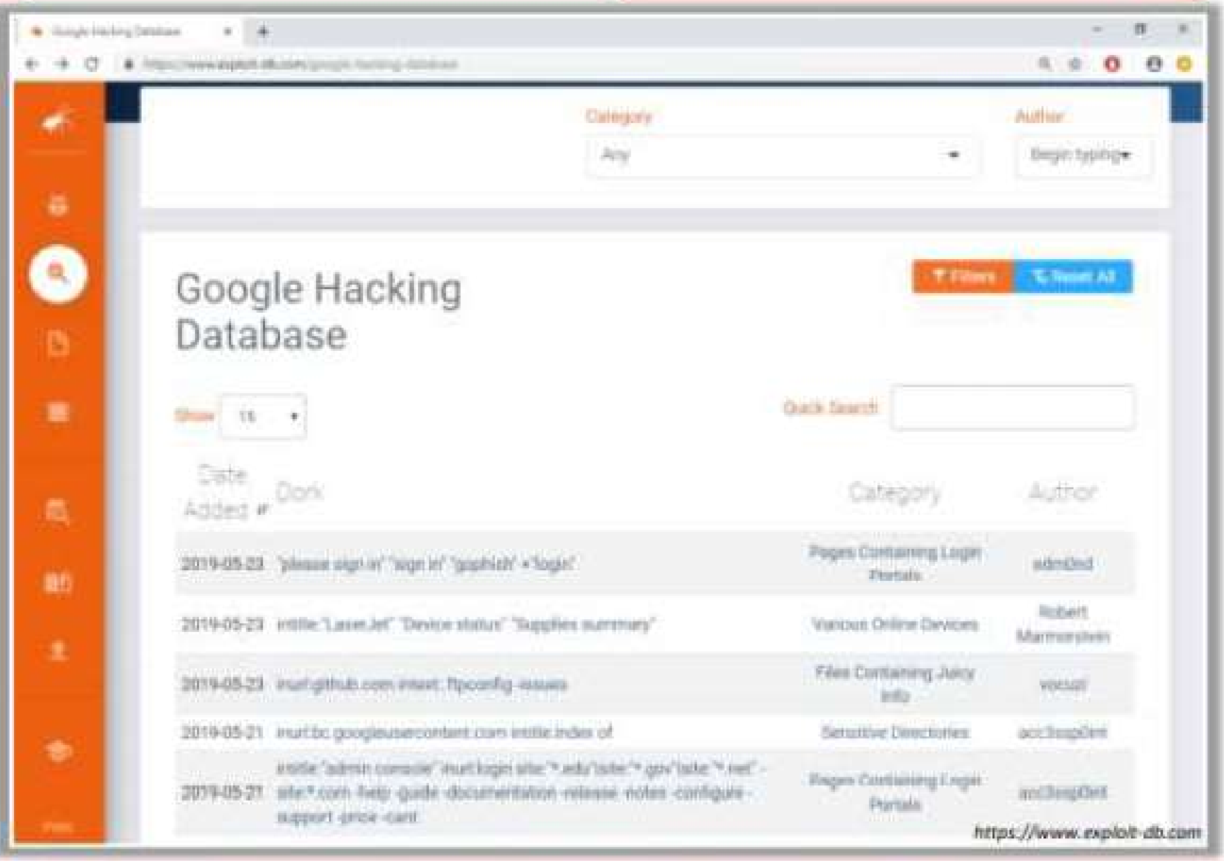
Examples of sensitive information on public servers that an attacker can extract with the help of Google Hacking Database (GHDB) queries include:

- Error messages that contain sensitive information
- Files containing passwords
- Sensitive directories
- Pages containing logon portals
- Pages containing network or vulnerability data, such as IDS, firewall logs, and configurations
- Advisories and server vulnerabilities
- Software version information
- Web application source code
- Connected IoT devices and their control panels, if unprotected
- Hidden web pages such as intranet and VPN services

Google Hacking Database

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

EXPLOIT DATABASE



Google Hacking Database

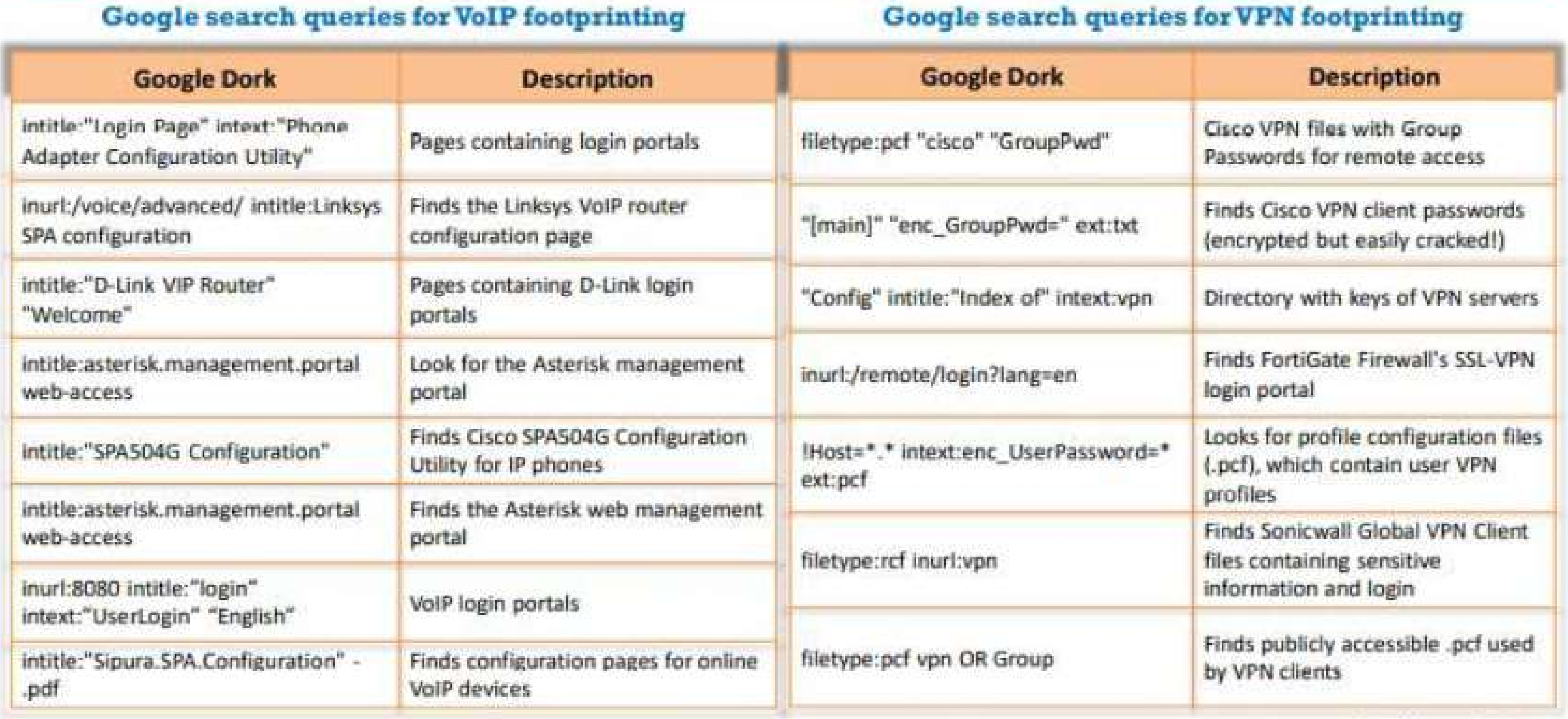
Date Added	Dork	Category	Author
2019-05-23	"please sign in" "sign in" "gophish" +"login"	Pages Containing Login Portals	edm0nd
2019-05-23	intitle:"LaserJet" "Device status" "Supplies summary"	Various Online Devices	Robert Marmorstein
2019-05-23	inurl:github.com intext:.ftpconfig -issues	Files Containing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

https://www.exploit-db.com

Google Hacking Database Categories:

- Footholds
- Files Containing Usernames
- Sensitive Directories
- Web Server Detection
- Vulnerable Files
- Vulnerable Servers
- Error Messages
- Files Containing Juicy Info
- Files Containing Passwords
- Sensitive Online Shopping Info
- Network or Vulnerability Data
- Pages Containing Login Portals
- Various Online Devices
- Advisories and Vulnerabilities

VoIP and VPN Footprinting through Google Hacking Database



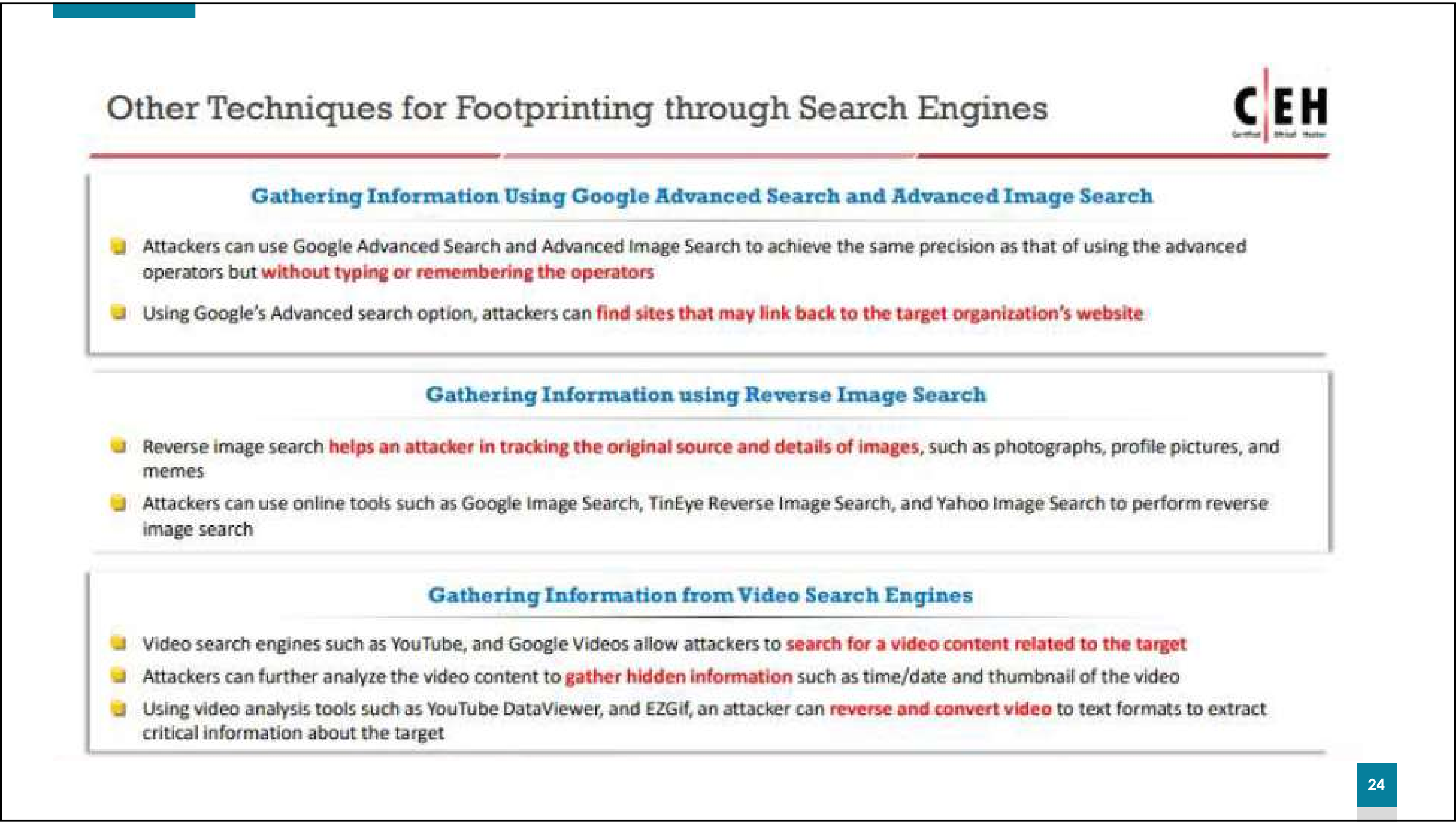
Google search queries for VoIP footprinting

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



Other Techniques for Footprinting through Search Engines

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

Other Techniques for Footprinting through Search Engines (Cont'd)

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

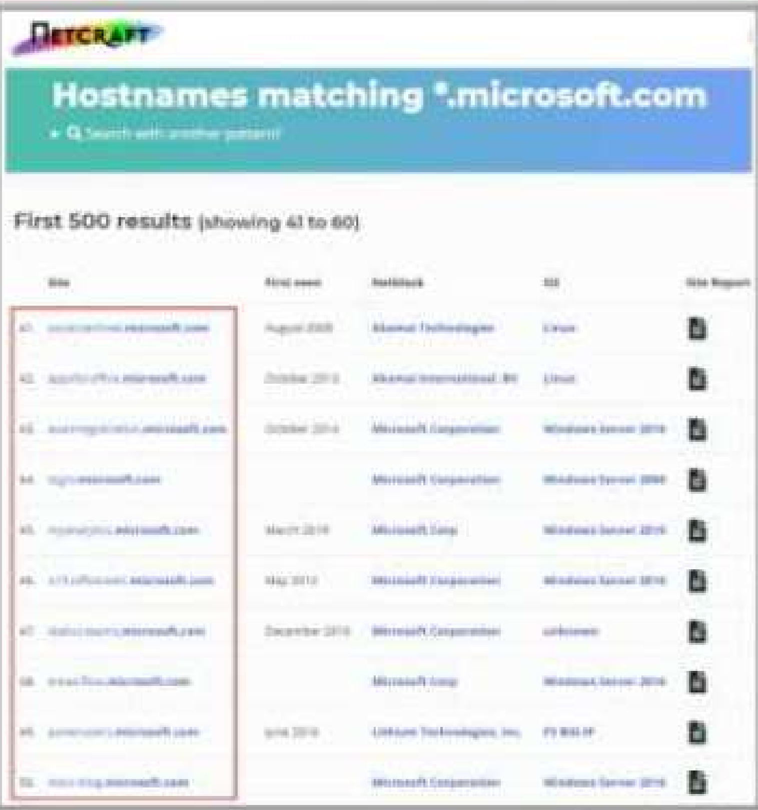
Gathering Information from IoT Search Engines

- 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 through Web Services

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

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



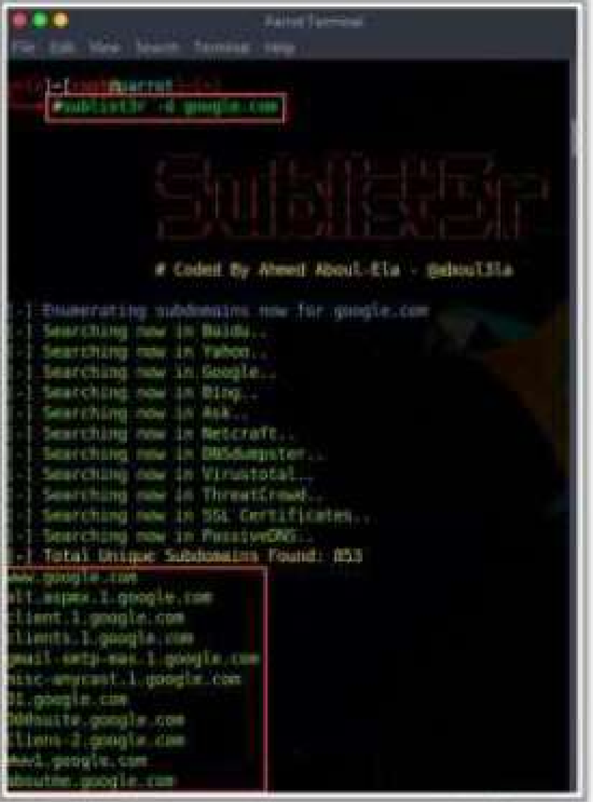
Hostnames matching *.microsoft.com

Search with another pattern!

First 500 results (showing 41 to 60)

	Site	First seen	Netblock	OS	Site Report
41.	[illegible].microsoft.com	August 2008	Akamai Technologies	Linux	🗎
42.	[illegible].microsoft.com	October 2013	Akamai International, BV	Linux	🗎
43.	[illegible].microsoft.com	October 2014	Microsoft Corporation	Windows Server 2016	🗎
44.	[illegible].microsoft.com		Microsoft Corporation	Windows Server 2008	🗎
45.	[illegible].microsoft.com	March 2019	Microsoft Corp	Windows Server 2016	🗎
46.	[illegible].microsoft.com	May 2013	Microsoft Corporation	Windows Server 2016	🗎
47.	[illegible].microsoft.com	December 2019	Microsoft Corporation	unknown	🗎
48.	[illegible].microsoft.com		Microsoft Corp	Windows Server 2016	🗎
49.	[illegible].microsoft.com	June 2019	[illegible] Technologies, Inc.	F5 BIG-IP	🗎
50.	[illegible].microsoft.com		Microsoft Corporation	Windows Server 2016	🗎

https://www.netcraft.com

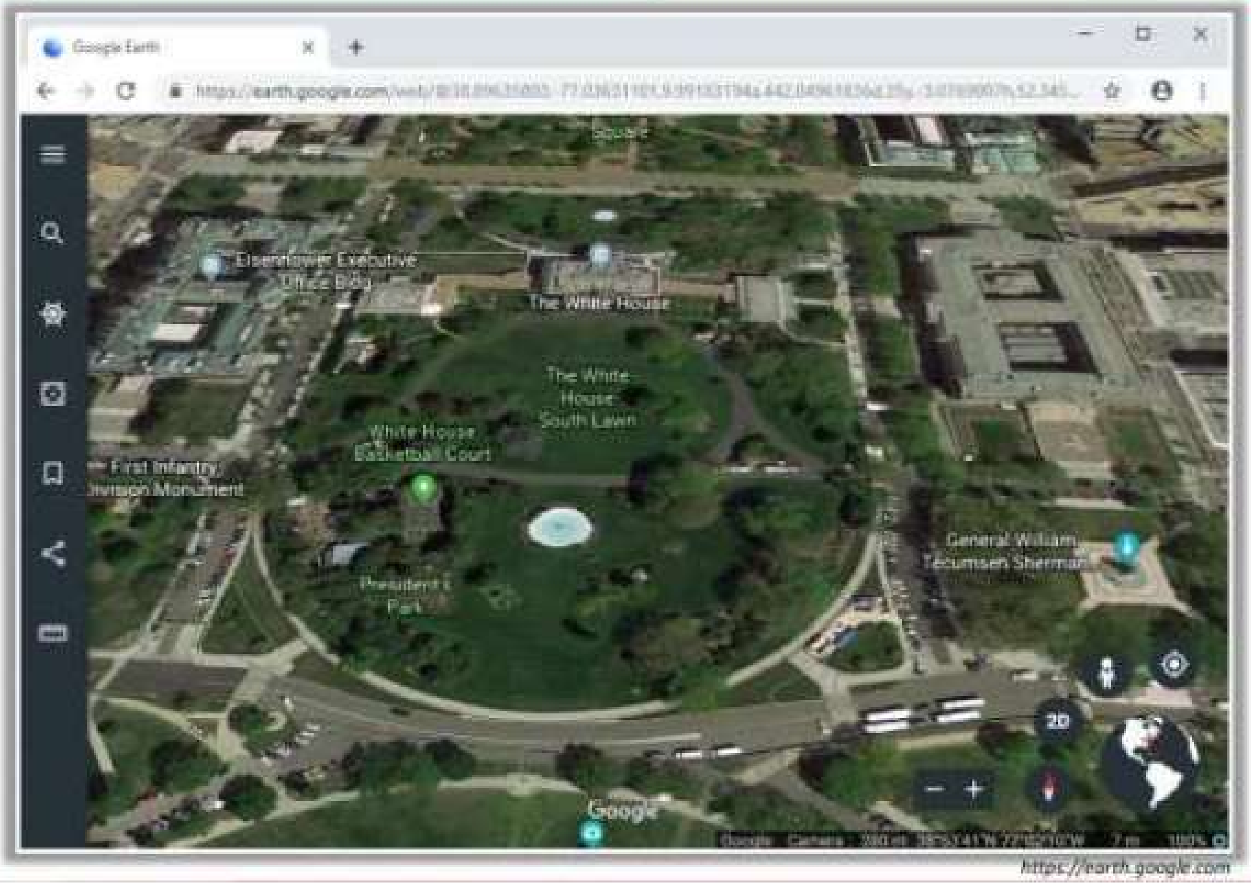


```
┌─[root@parrot]─[~]
└──╼ #sublist3r -d google.com

        Sublist3r

        # 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-msa.l.google.com
misc-anycast.l.google.com
[illegible].google.com
[illegible].google.com
clients-2.google.com
[illegible].google.com
aboutme.google.com
```

https://github.com

Finding the Geographical Location of the Target

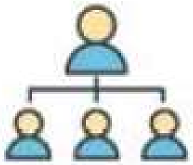
- Attackers use tools, such as **Google Earth**, **Google Maps**, and **Wikimapia**, to obtain the physical location of the target, which helps them to perform social engineering and other non-technical attacks
- These tools help attackers to find or locate entrances to buildings, security cameras, gates,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

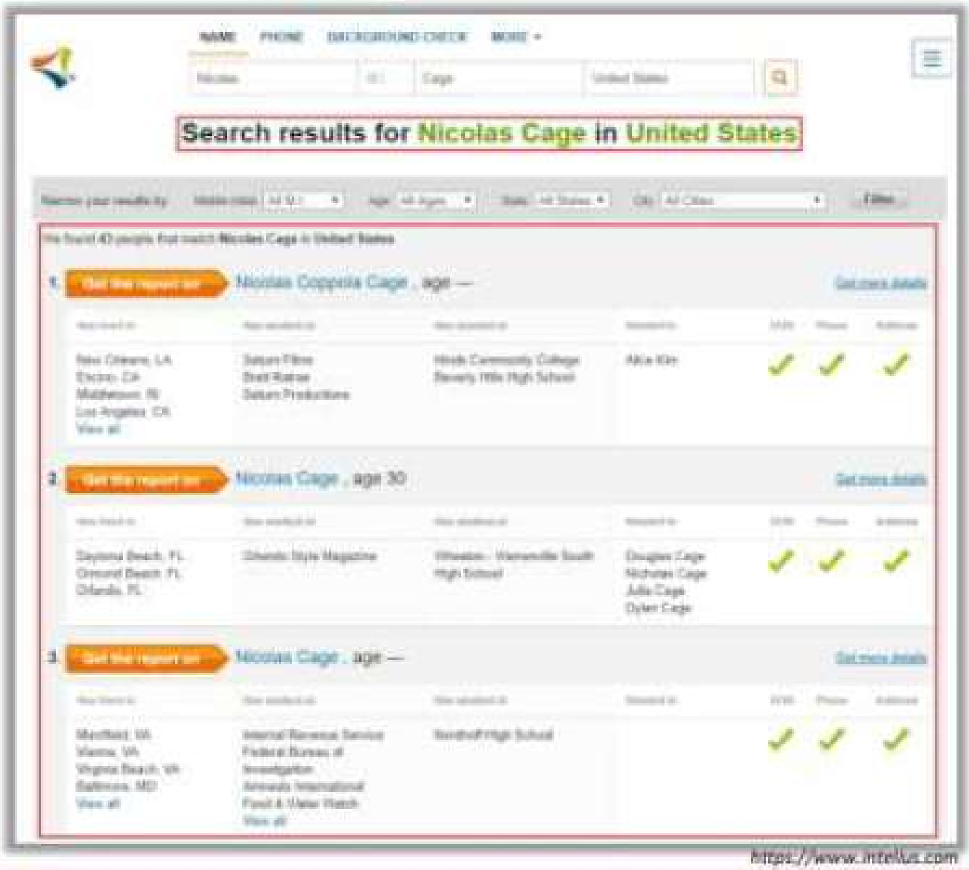

Google Earth
Square
Eisenhower Executive Office Bldg
The White House
The White House South Lawn
White House Basketball Court
First Infantry Division Monument
President's Park
General William Tecumseh Sherman
2D
Google

https://earth.google.com

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





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

We found 40 people that match Nicolas Cage in United States

1. Nicolas Coppola Cage , age —

Has lived in	Has worked at	Has studied at	Related to	SSN	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	✓	✓	✓

2. Nicolas Cage , age 30

Has lived in	Has worked at	Has studied at	Related to	SSN	Phone	Address
Daytona Beach, FL Ormond Beach, FL Orlando, FL	Orlando Style Magazine	Wheaton - Warrenville South High School	Douglas Cage Nicholas Cage Julia Cage Dylan Cage	✓	✓	✓

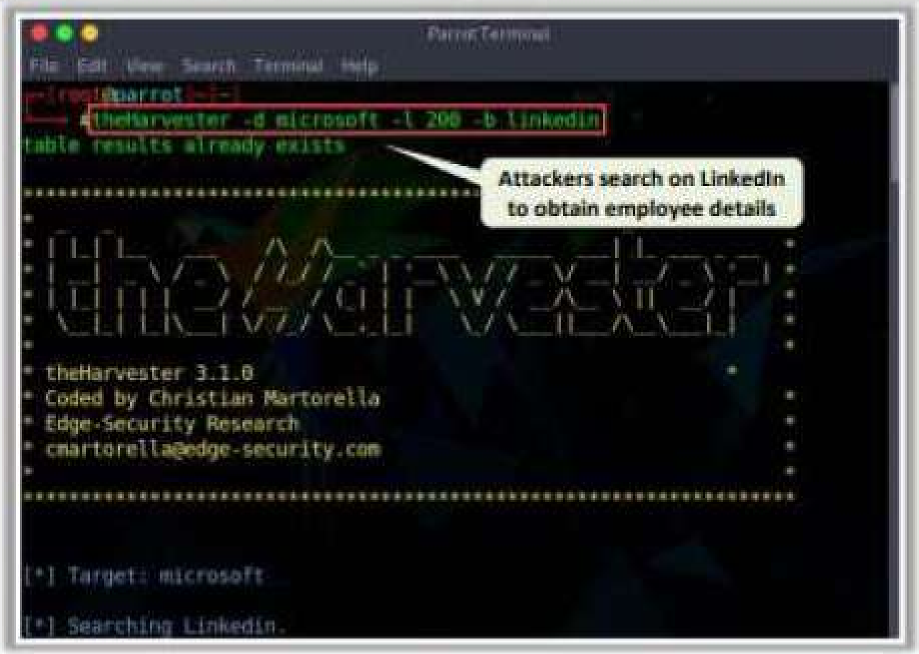
3. Nicolas Cage , age —

Has lived in	Has worked at	Has studied at	Related to	SSN	Phone	Address
Manfield, VA Vienna, VA Virginia Beach, VA Baltimore, MD View all	Internal Revenue Service Federal Bureau of Investigation Animals International Food & Water Watch View all	Nordhoff High School		✓	✓	✓

https://www.intelius.com

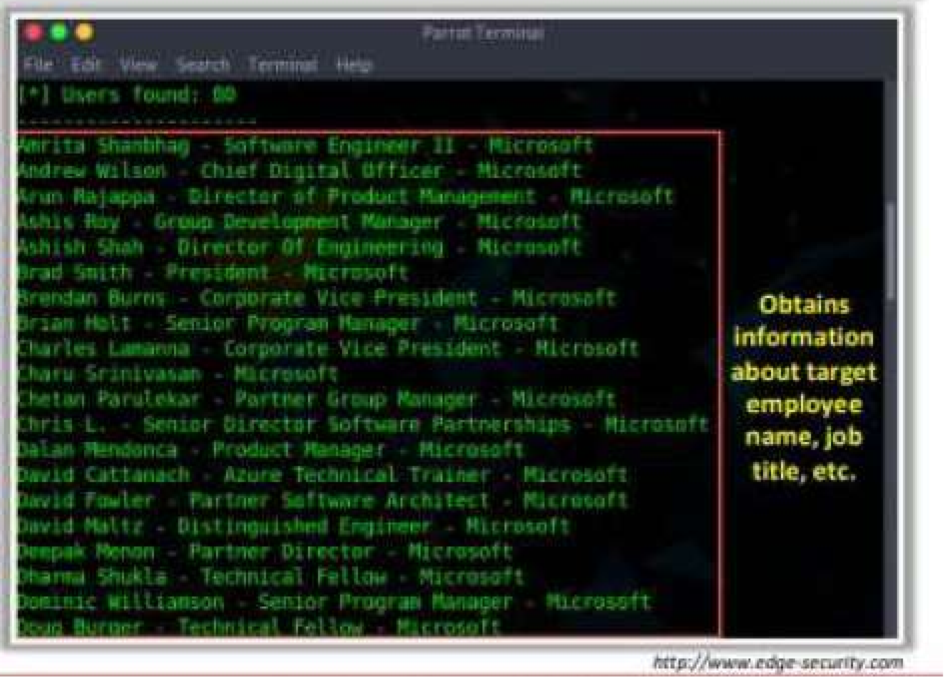
Gathering Information from LinkedIn

- 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



```
┌─[root@parrot]─[~]
└──╼ #theHarvester -d microsoft -l 200 -b linkedin
table results already exists

*******************************************************************
*                                                                 *
* theHarvester 3.1.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: microsoft

[*] Searching Linkedin.
```

Attackers search on LinkedIn to obtain employee details



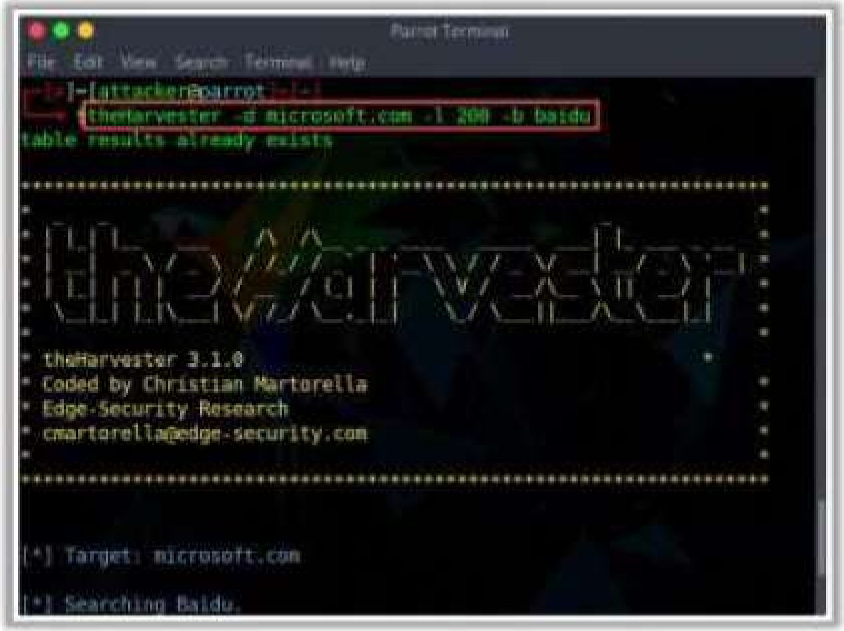
```
[*] Users found: 80
---------------------
Amrita Shanbhag - Software Engineer II - Microsoft
Andrew Wilson - Chief Digital Officer - Microsoft
Arun Rajappa - Director of Product Management - Microsoft
Ashis Roy - Group Development Manager - Microsoft
Ashish Shah - Director Of Engineering - Microsoft
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
Dhanma Shukla - Technical Fellow - Microsoft
Dominic Williamson - Senior Program Manager - Microsoft
Doug Burger - Technical Fellow - Microsoft
```

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

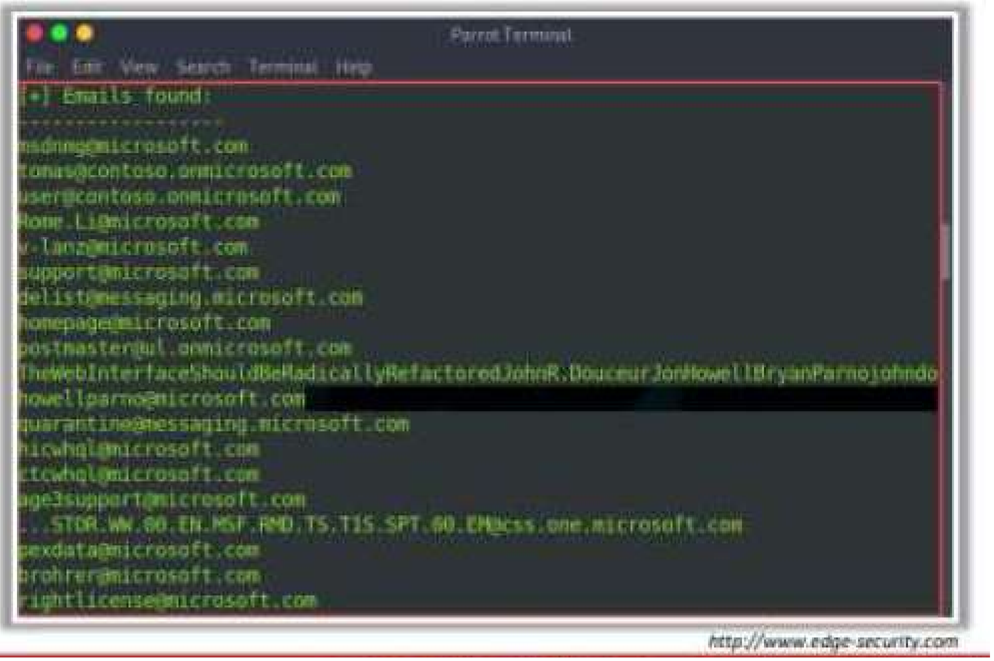
http://www.edge-security.com

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



```
┌─[attacker@parrot]─[~]
└──╼ $theHarvester -d microsoft.com -l 200 -b baidu
table results already exists

*******************************************************************
*                                                                 *
*                                                                 *
* theHarvester 3.1.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: microsoft.com

[*] Searching Baidu.
```

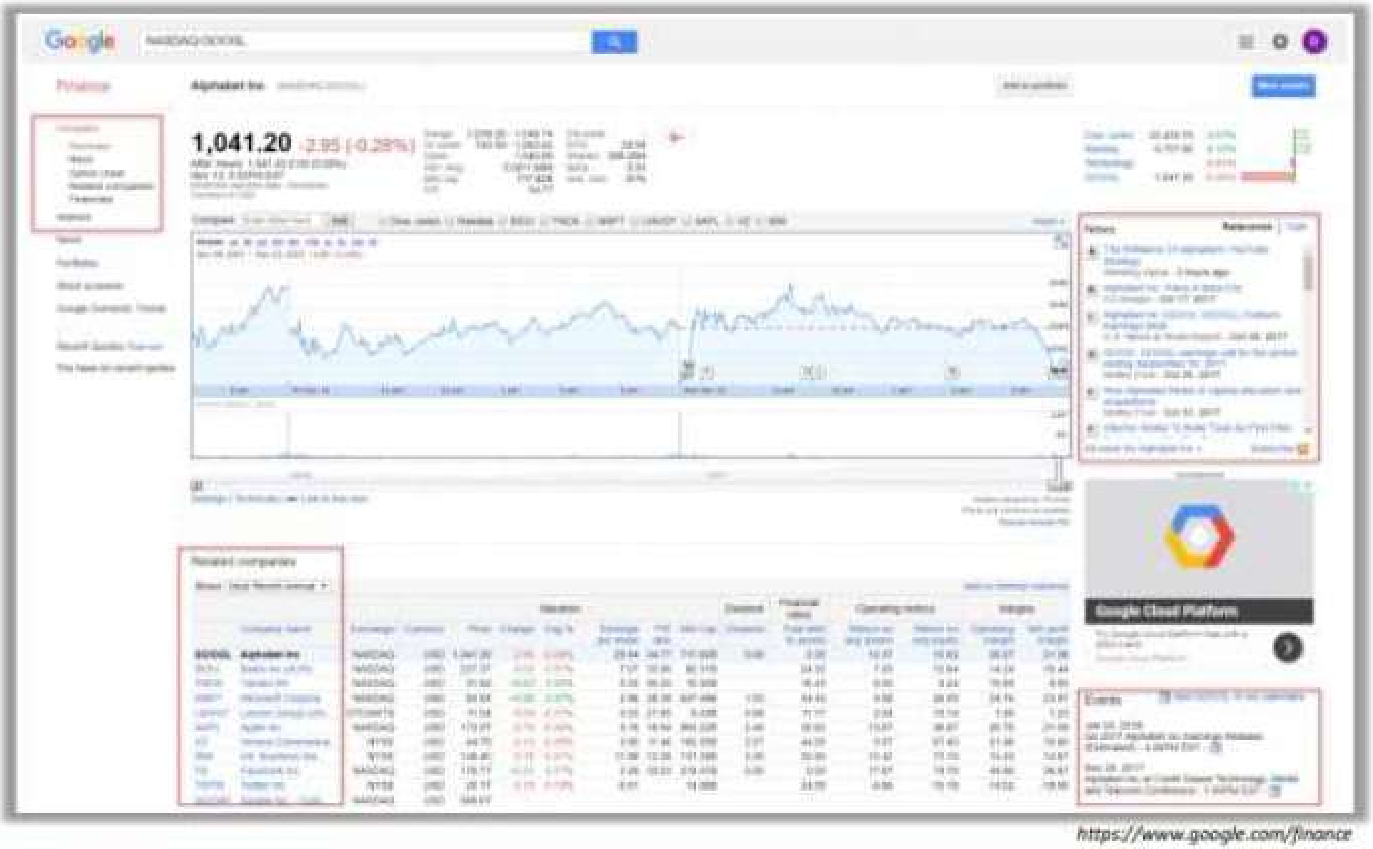


```
[+] Emails found:
------------------
msdnmg@microsoft.com
tomas@contoso.onmicrosoft.com
user@contoso.onmicrosoft.com
Rome.Li@microsoft.com
v-lanz@microsoft.com
support@microsoft.com
delist@messaging.microsoft.com
homepage@microsoft.com
postmaster@ul.onmicrosoft.com
TheWebInterfaceShouldBeRadicallyRefactoredJohnR.DouceurJonHowellBryanParnojohndo
howellparno@microsoft.com [redacted]
quarantine@messaging.microsoft.com
hicwhql@microsoft.com
ctowhql@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
```

http://www.edge-security.com

Gathering Information from Financial Services

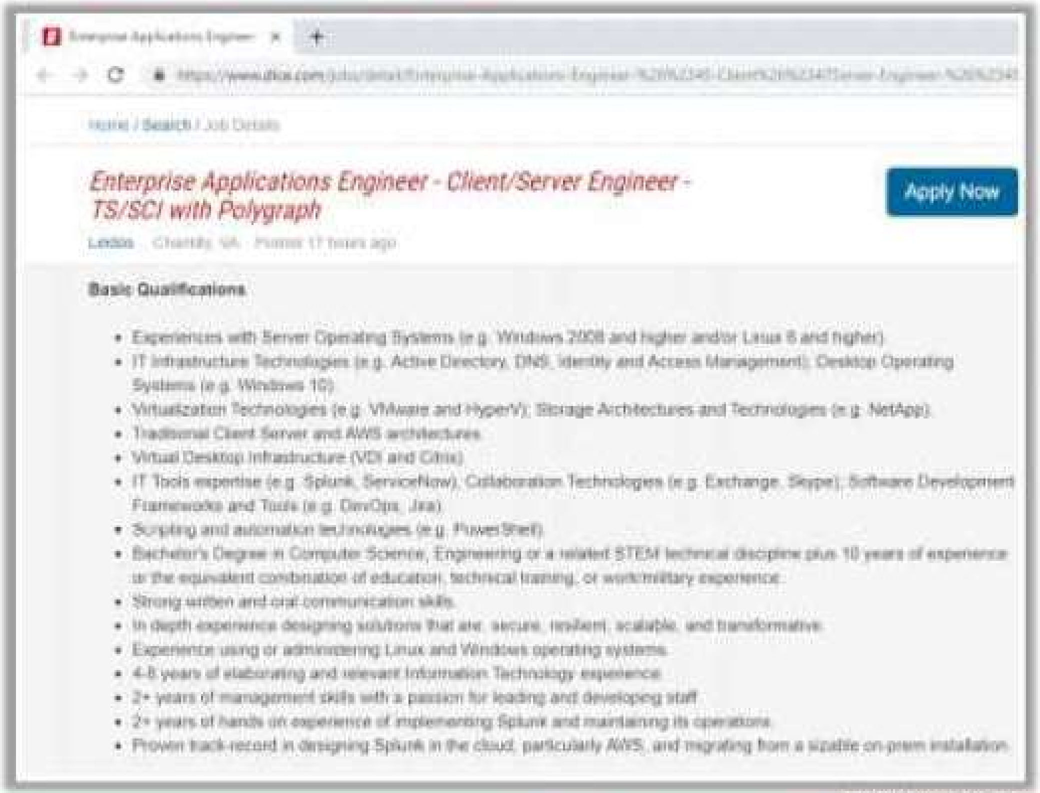
- Financial services, such as Google Finance, MSN Money, and Yahoo! Finance, provide useful information about the target company, such as the **market value of a company's shares**, **company profile**, and **competitor details**
- Attackers can use this information to perform service flooding, brute-force,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



https://www.google.com/finance

Footprinting through Job Sites

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


Enterprise Applications Engineer
https://www.dice.com/jobs/detail/Enterprise-Applications-Engineer-%20%2D%20-Client%2F%2F47Server-Engineer-%20%2D
Apply Now

Home / Search / Job Details

Enterprise Applications Engineer - Client/Server Engineer - TS/SCI with Polygraph

Leidos · Chantilly, VA · Posted 17 hours ago

Basic Qualifications

- 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
- 4-6 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**

Deep and Dark Web Footprinting

Deep web

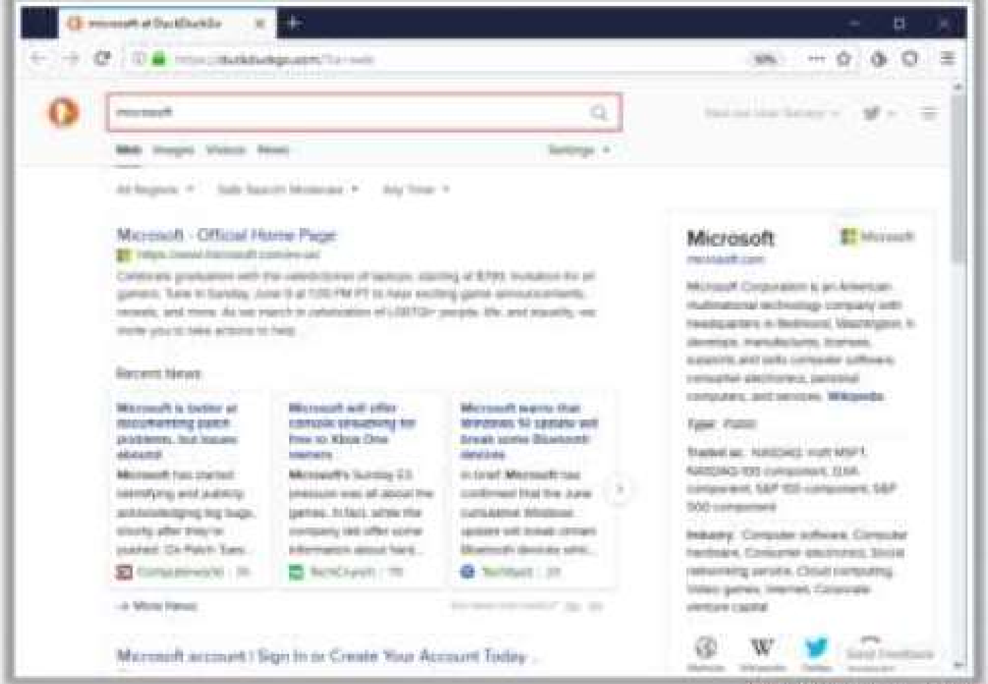
- It consists of web pages and contents that are **hidden and unindexed** and cannot be located using traditional web browsers and search engines
- It can be accessed by **search engines** like Tor Browser and The WWW Virtual Library

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.

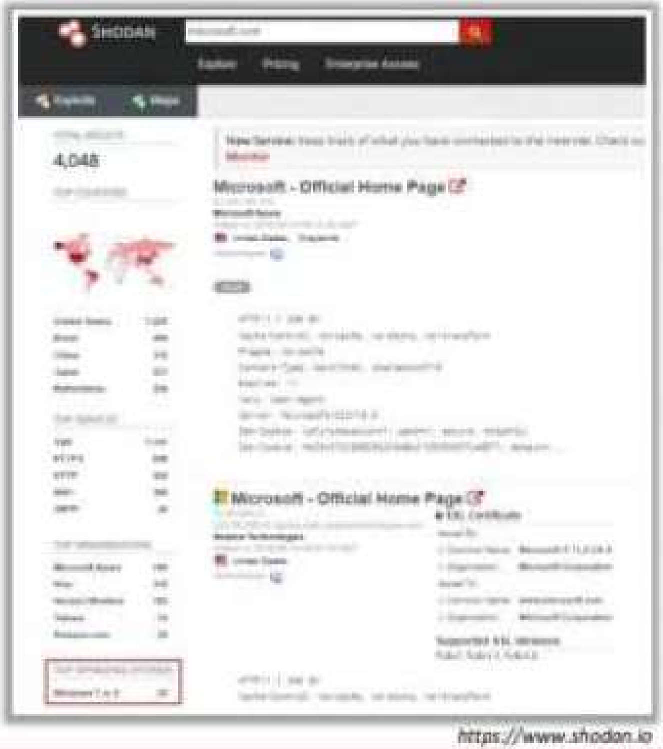
TOR Browser | It is used to access the deep and dark web where it acts as a **default VPN** for the user and bounces the network IP address through several servers before interacting with the web


Microsoft - Official Home Page
Recent News
Microsoft
Wikipedia
Microsoft account | Sign In or Create Your Account Today

https://www.torproject.org

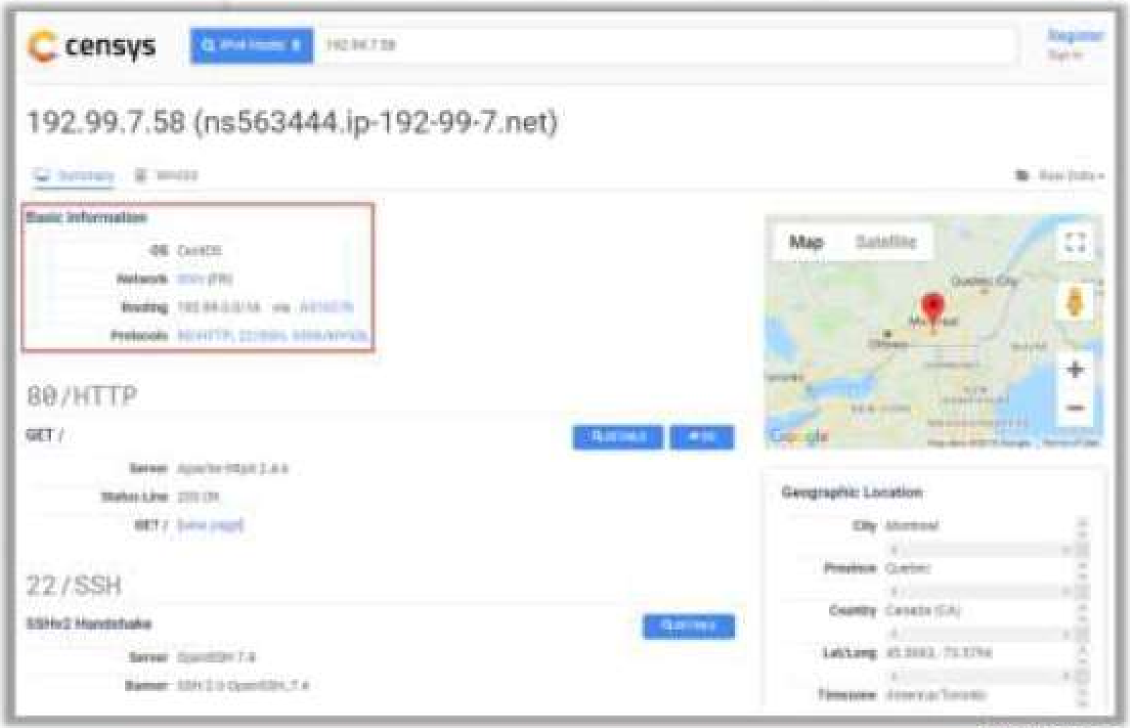
Determining the Operating System

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



https://www.shodan.io

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



192.99.7.58 (ns563444.ip-192-99-7.net)

Basic Information

OS CentOS

80/HTTP

GET /

Server Apache httpd 2.4.6

Status Line 200 OK

22/SSH

SSHv2 Handshake

Server OpenSSH 7.4

Banner SSH-2.0-OpenSSH_7.4

Geographic Location

City Montreal

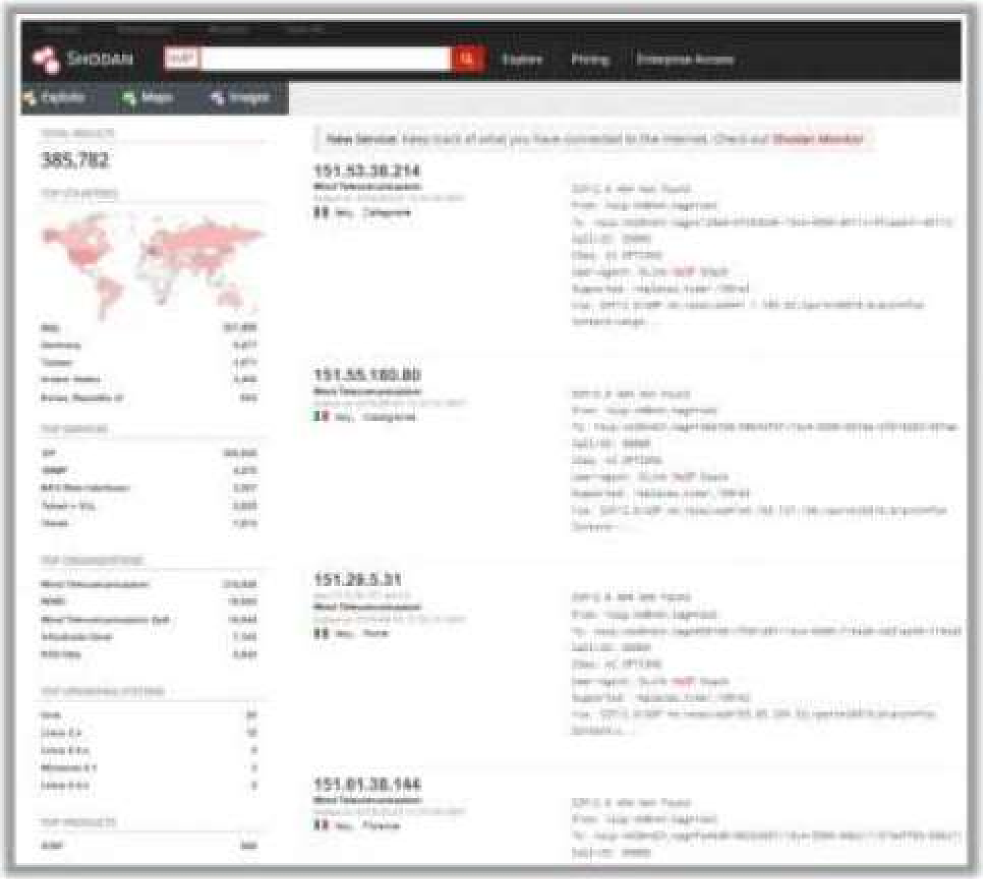
Province Quebec

Country Canada (CA)

Timezone America/Toronto

https://censys.io

VoIP and VPN Footprinting through SHODAN



385,782

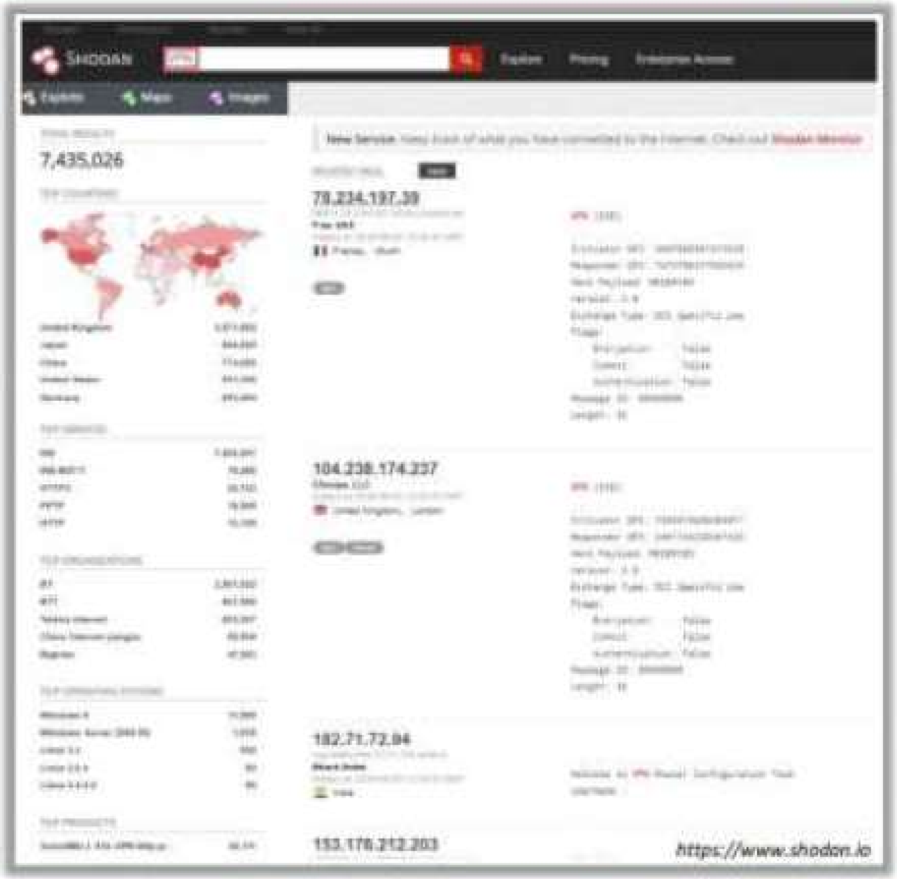
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

151.53.38.214

151.55.180.80

151.29.5.31

151.81.38.144



7,435,026

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

79.234.197.39

VPN (IKE)

Flags:
Encryption: False
Commit: False
Authentication: False

104.238.174.237

VPN (IKE)

182.71.72.94

153.178.212.203

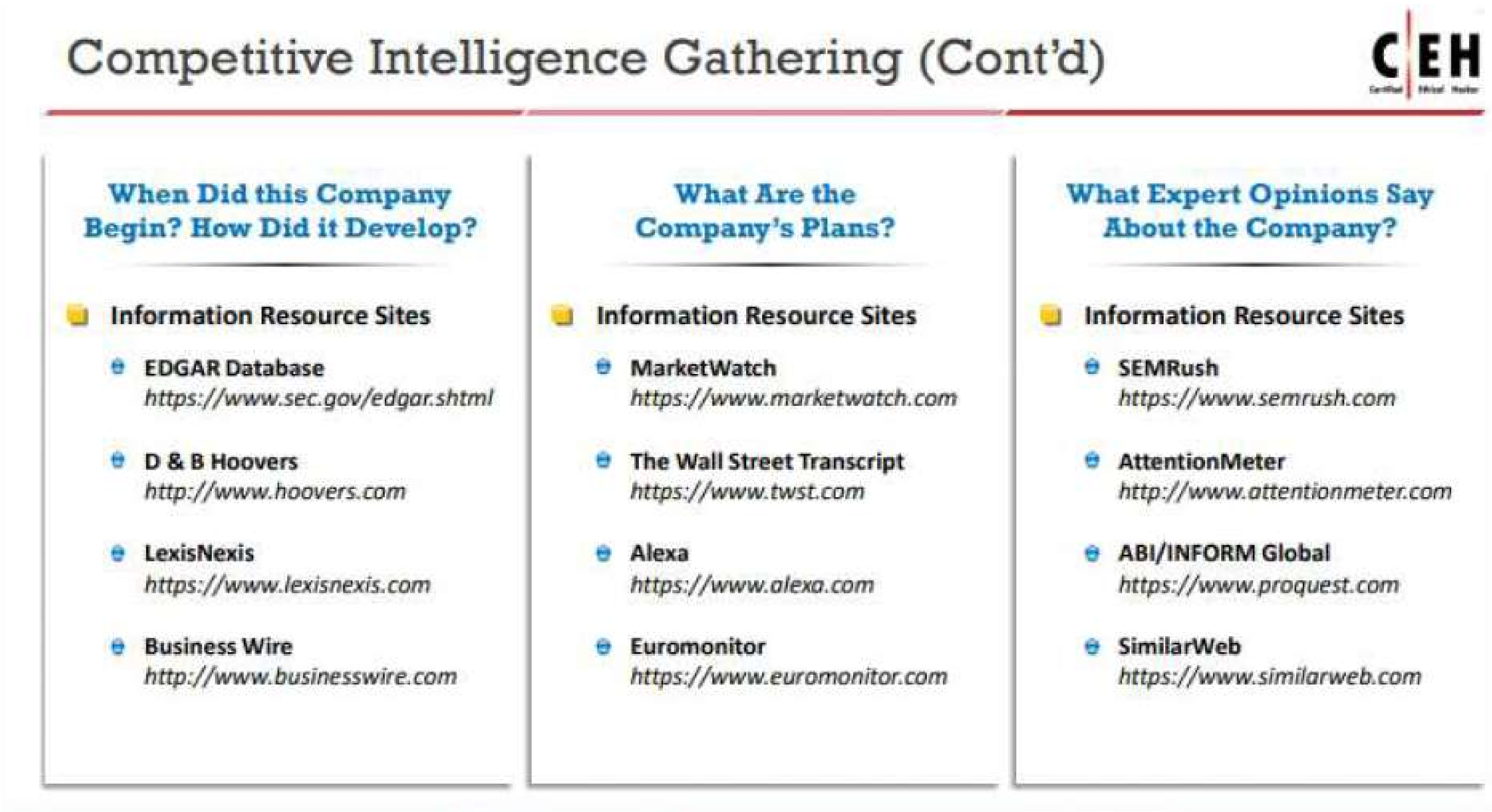
https://www.shodan.io

Competitive Intelligence Gathering

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

Sources of Competitive Intelligence

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



Competitive Intelligence Gathering (Cont'd)

When Did this Company Begin? How Did it Develop?

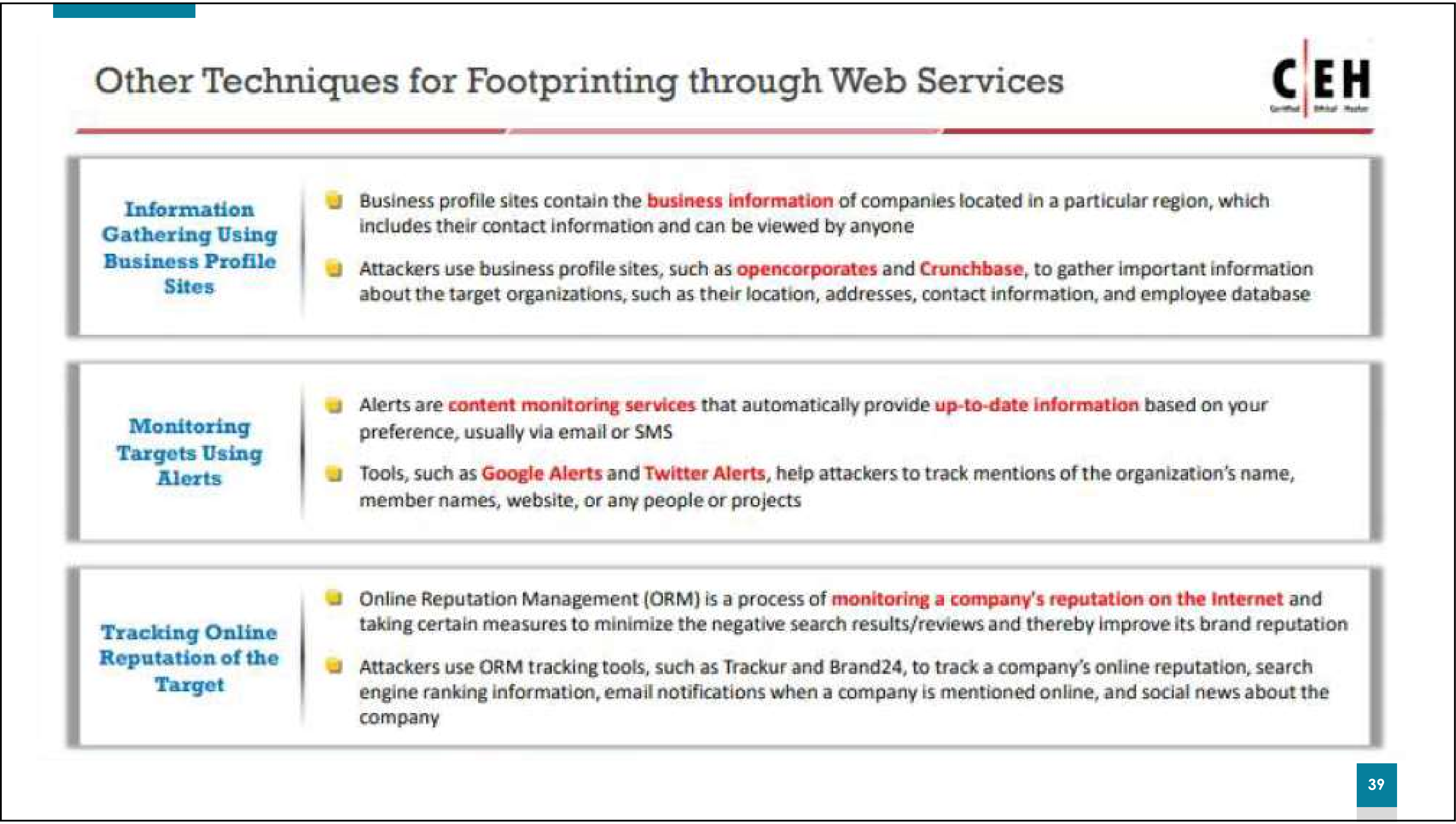
- Information Resource Sites
  - **EDGAR Database**
    https://www.sec.gov/edgar.shtml
  - **D & B Hoovers**
    http://www.hoovers.com
  - **LexisNexis**
    https://www.lexisnexis.com
  - **Business Wire**
    http://www.businesswire.com

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



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

Other Techniques for Footprinting through Web Services (Cont'd)

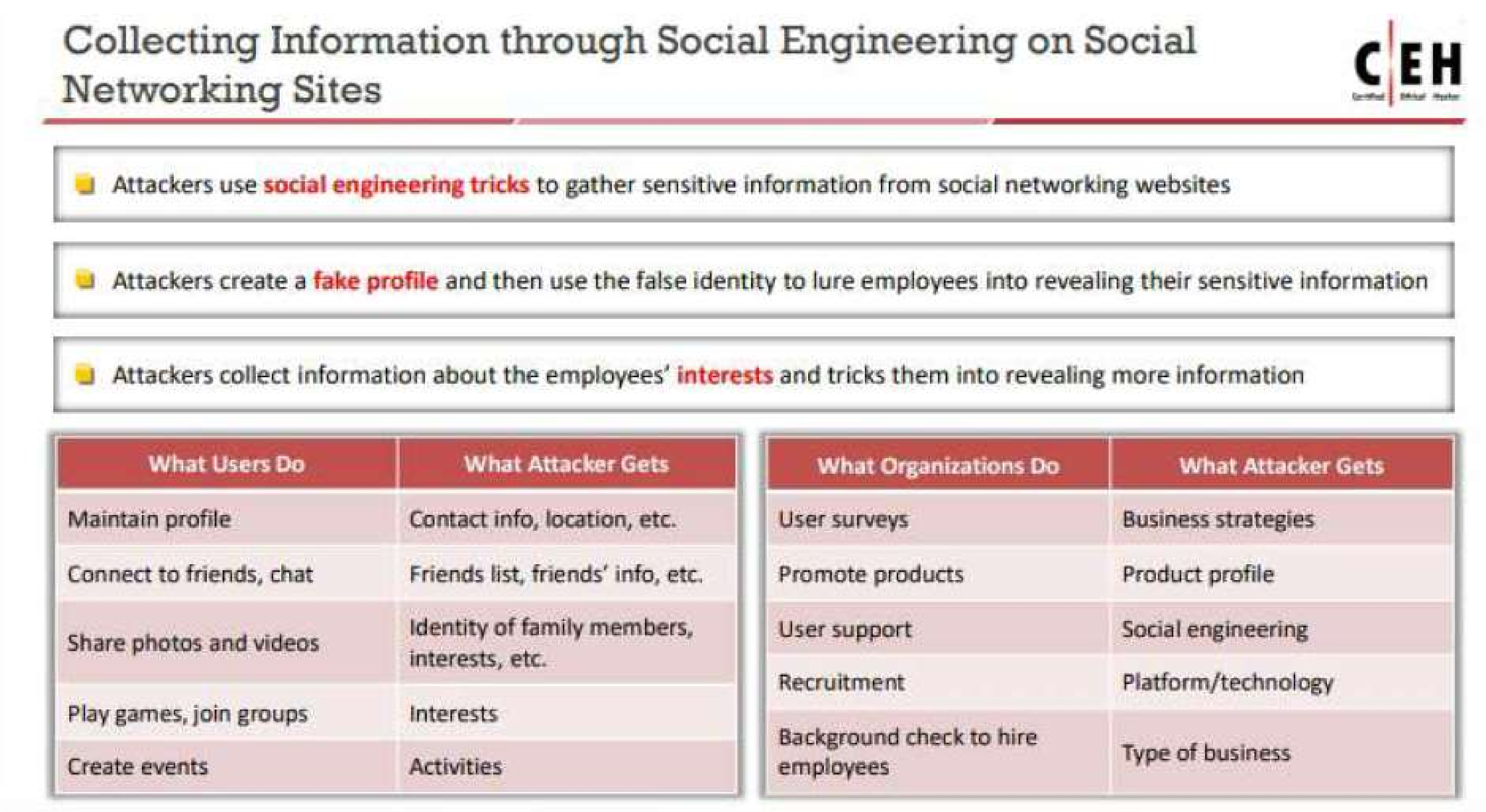
Information Gathering Using Groups, Forums, and Blogs

- 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 through Social Networking Sites



Collecting Information through Social Engineering on Social Networking Sites

- Attackers use **social engineering tricks** to gather sensitive information from social networking websites

- Attackers create a **fake profile** and then use the false identity to lure employees into revealing their sensitive information

- Attackers collect information about the employees' **interests** and tricks them into revealing more information

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

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

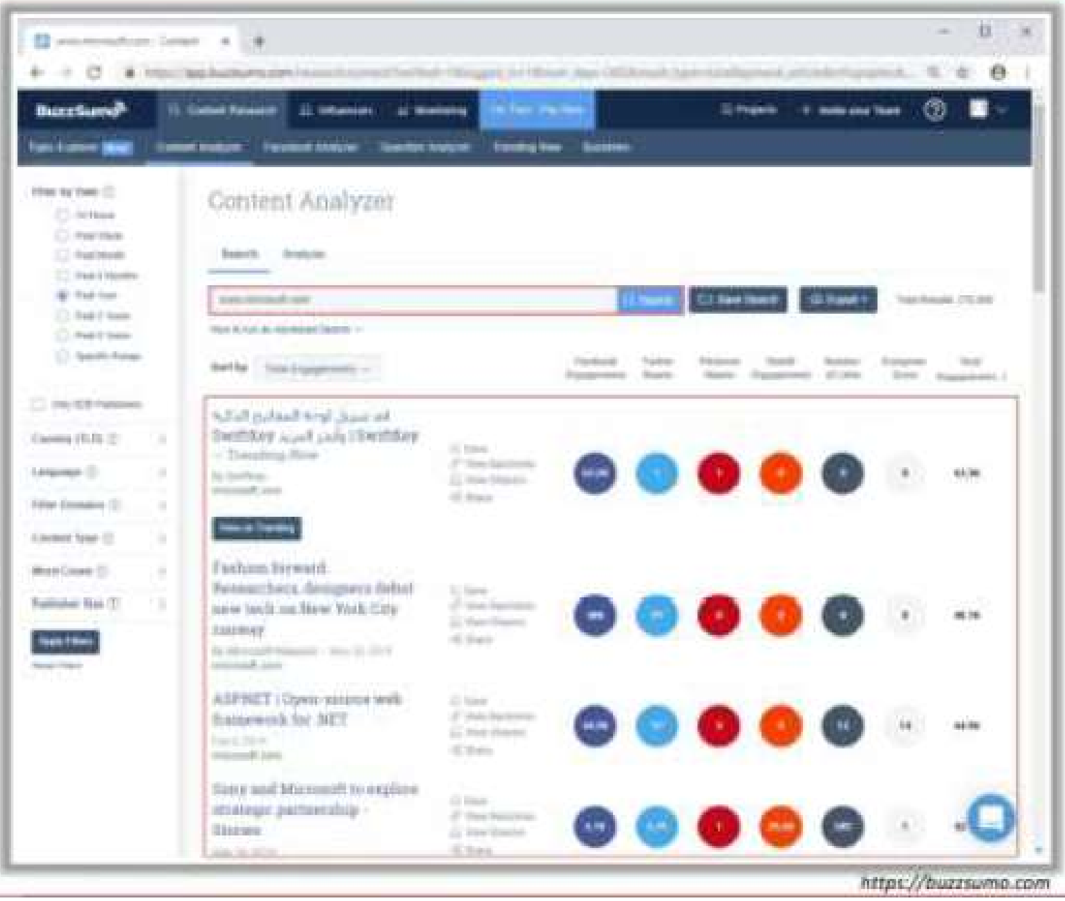
General Resources for Locating Information from Social Media Sites

- 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

Conducting Location Search on Social Media Sites

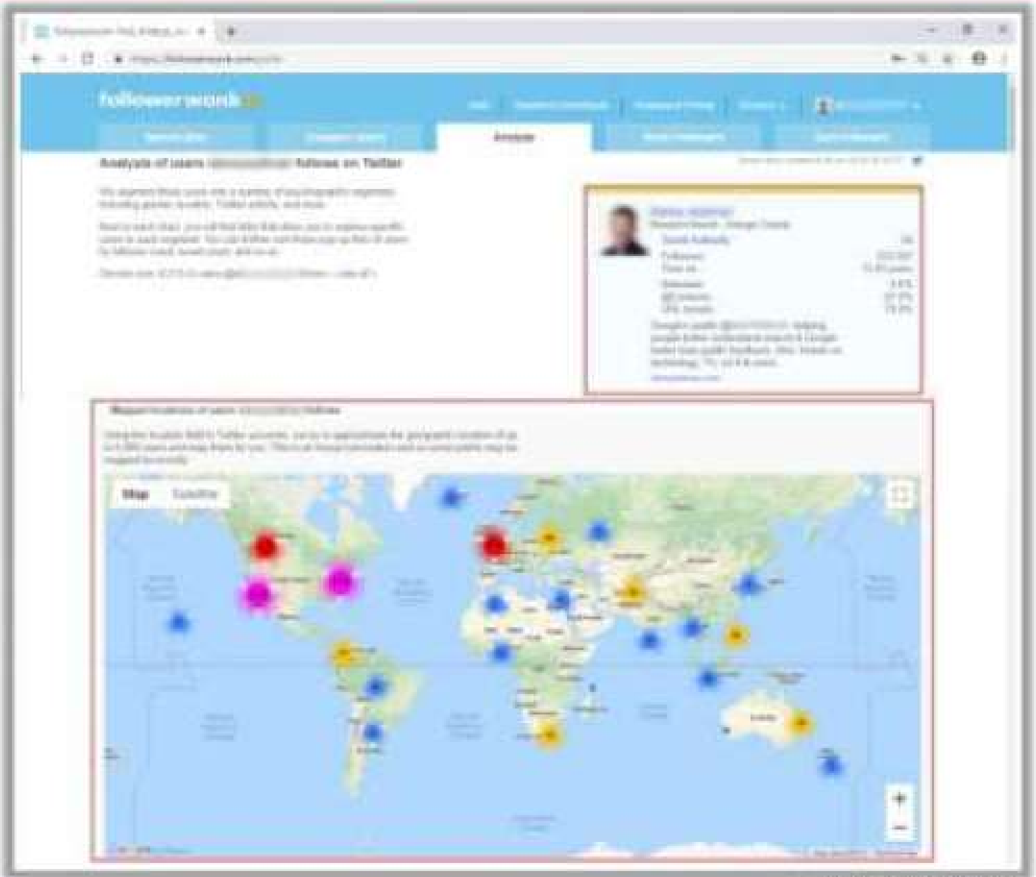
- Conducting location search on social media sites, such as Twitter, Instagram, and Facebook, helps attackers in **detecting the geolocation of the target**

- 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

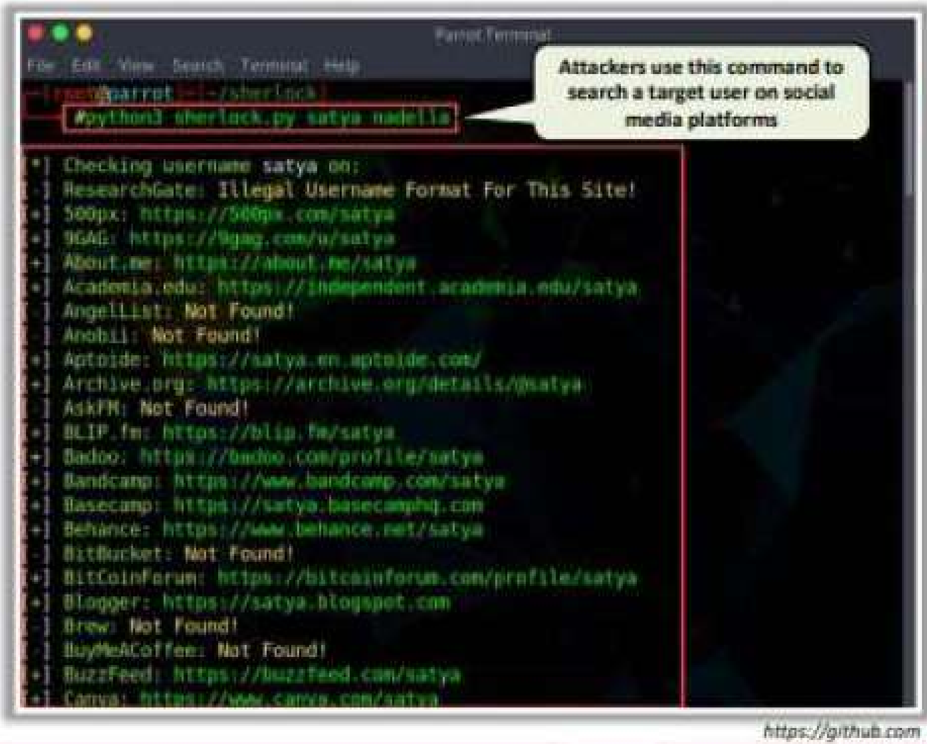


https://followerwonk.com

Tools for Footprinting through Social Networking Sites

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

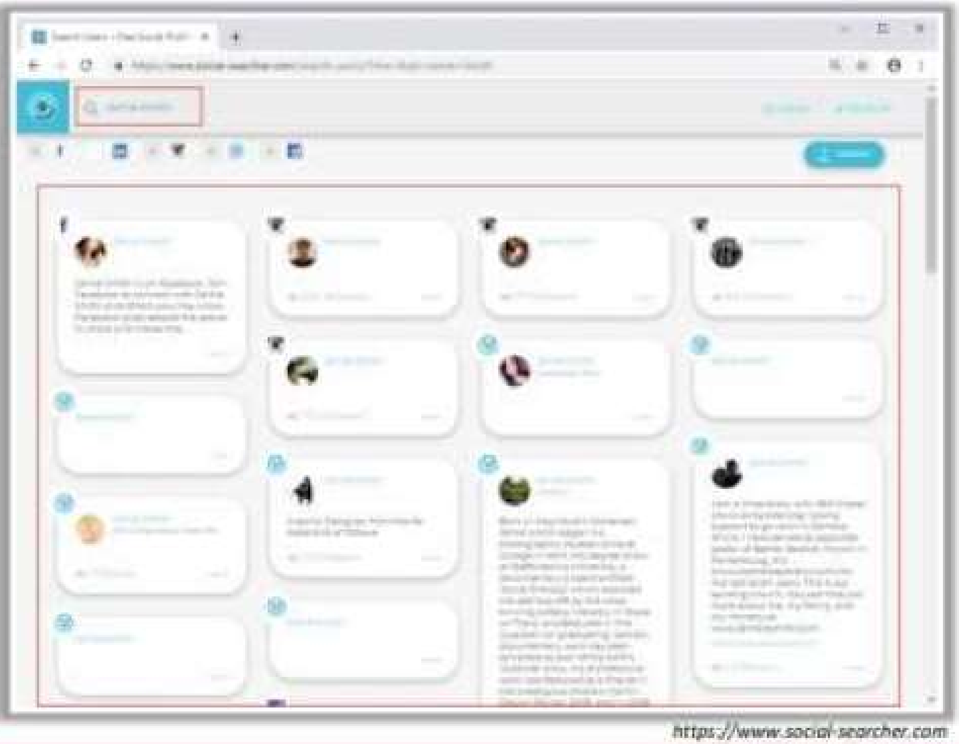
Social Searcher | Social Searcher allows you to search for content in social networks in real-time and provides deep analytics data



```
-[root@parrot]-[~/sherlock]
   #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
```

Attackers use this command to search a target user on social media platforms

https://github.com



https://www.social-searcher.com