

Module 02

Footprinting and Reconnaissance

Learning Objectives

- 01 Explain Footprinting Concepts
- 02 Demonstrate Footprinting through Search Engines
- 03 Demonstrate Footprinting through Internet Research Services
- 04 Demonstrate Footprinting through Social Networking Sites
- 05 Use Different Techniques for Whois Footprinting
- 06 Use Different Techniques for DNS Footprinting
- 07 Use Different Techniques for Network and Email Footprinting
- 08 Demonstrate Footprinting through Social Engineering
- 09 Automate Footprinting Tasks using Advanced Tools and AI
- 10 Explain Footprinting Countermeasures

Objective 01

Explain Footprinting Concepts

Reconnaissance

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

Types of Reconnaissance

Passive

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

It involves:

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

Active

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

It involves:

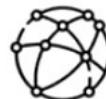
- DNS interrogation
- Social engineering
- Network/port scanning
- User and service enumeration

Information Obtained in Footprinting



Organization information

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



Network information

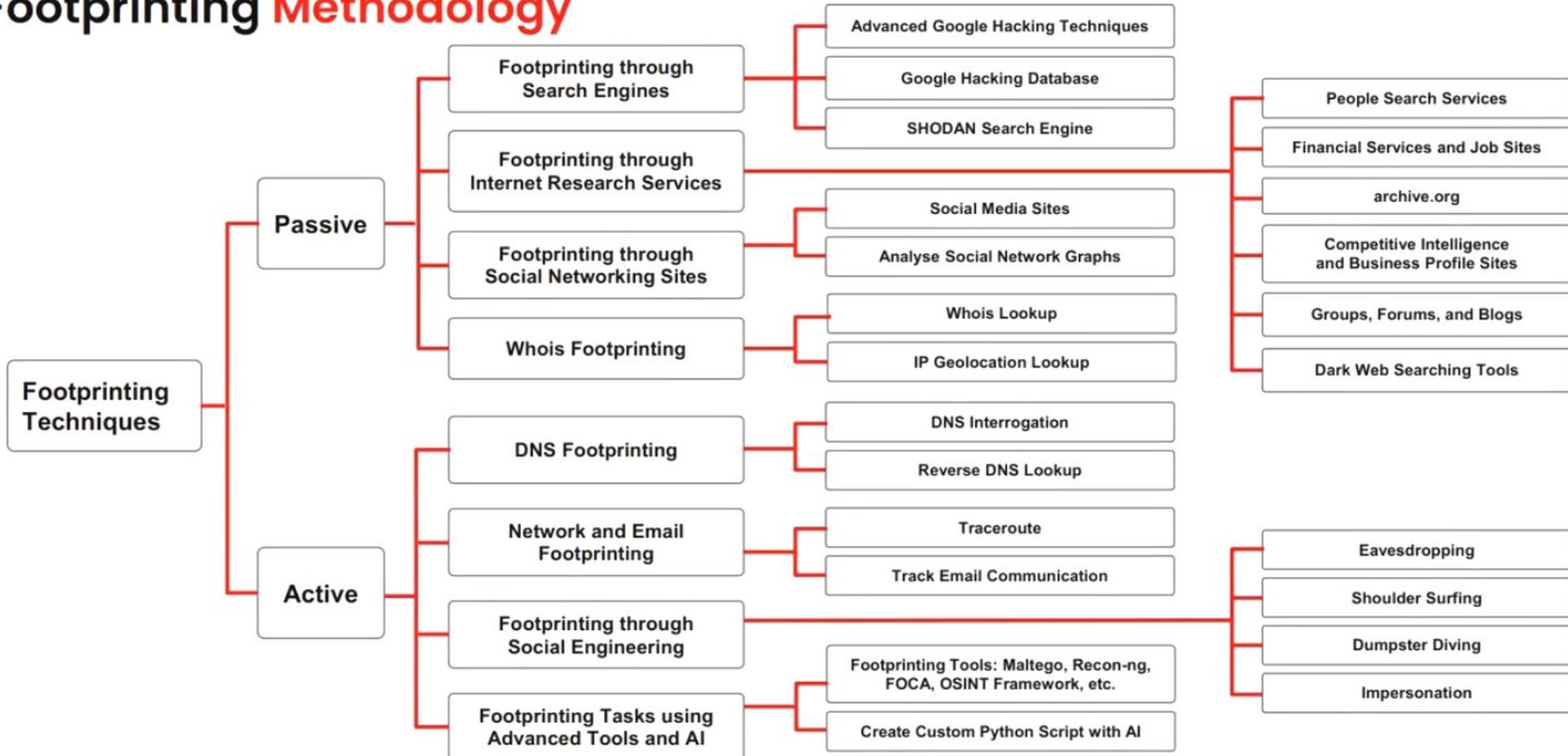
- Domain and sub-domains
- Network blocks
- Network topology, trusted routers, and firewalls
- IP addresses of the reachable systems
- Whois records
- DNS records



System information

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

Footprinting Methodology



Objective **02**

Demonstrate Footprinting through Search Engines

Passive Reconnaissance

Footprinting Using Advanced Google Hacking Techniques

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

Popular Google advanced search operators

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

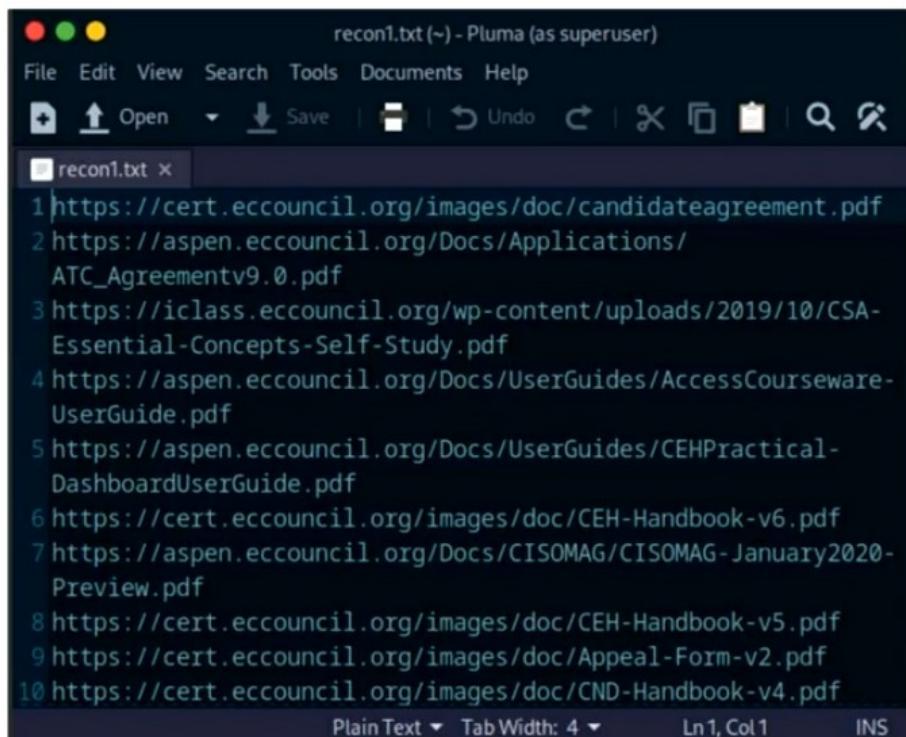
Search Operator	Purpose
[allintitle:]	Restricts the results to those websites containing all the search keywords in the title
[intitle:]	Restricts the results to documents containing the search keyword in the title
[allinurl:]	Restricts the results to those containing all the search keywords in the URL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

Footprinting Using Advanced Google Hacking Techniques **with AI**

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

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

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



Google Hacking Database

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

A screenshot of a web browser displaying the Exploit Database's Google Hacking Database. The page has a dark blue header with the "EXPLOIT DATABASE" logo. Below the header is a search bar and a "Google Hacking Database" title. On the left, there is a vertical orange sidebar with various icons. The main content area shows a table of search results with columns for Date, Dork, Category, and Author. The results are listed in descending order of date added.

Date Added	Dork	Category	Author
2024-05-13	"START test_database" ext:log	Files Containing Usernames	Nadir Boulacheb (RubX)
2024-05-13	"Header for logs at time" ext:log	Files Containing Usernames	Nadir Boulacheb (RubX)
2024-05-01	intitle:"GlobalProtect Portal"	Files Containing Juicy Info	Javier Bernardo
2024-05-01	intext:"dhcpd user" "index of"	Files Containing Juicy Info	Prathamesh Waidande
2024-05-01	intitle:index of /etc/openldap	Files Containing Juicy Info	Joel Indra
2024-05-01	intitle:"zircote/swagger-ph"	Files Containing Juicy Info	Anirudh Kumar Kushwaha
2024-05-01	site:preprod.* * inturl:login	Files Containing Juicy Info	Jagdish Rathod
2024-05-01	inttitle:"index of" setting.php	Files Containing Juicy Info	saurabh kode
2024-05-01	"PHP Fatal error" ext:log OR ext:txt	Files Containing Juicy Info	Nadir Boulacheb (RubX)
2024-05-01	site:uat.* * inturl:login	Files Containing Juicy Info	Jagdish Rathod
2024-04-19	"rbac.yaml" "role.yaml" "rolebinding.yaml" "rbac.yaml" inttitle:"index of"	Files Containing Juicy Info	vinit asher

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

Footprinting through SHODAN Search Engine

Shodan | Maps | Images | Monitor | Developer | More

 SHODAN Explore Pricing ⚡ VoIP VoIP 🔍 Login

TOTAL RESULTS 204,560

TOP COUNTRIES



204,560

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

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

151.48.235.161 2024-03-07T09:48:07.031500

addr=151.48.235.161
proto=tcp
port=443
country=US
state=California
city=San Francisco
org=WIND TRE S.p.A.
lat=37.775
lon=-122.423
time=2024-03-07T09:48:07.031500Z
http://151.48.235.161/favicon.ico
User-Agent: DLINK_VoIP_Stack
Supported: replaces,timer,100rel
Via: SIP/2.0/UDP nn,received=224.189.132.67,port=20810,branch=400
Content-Length: 0

Italy 190,048

Taiwan 4,700

Germany 2,300

United States 1,178

South Africa 842

[More...](#)

TOP PORTS

5060	191,807
9000	2,889
9001	1,780
992	1,370
161	617
More...	

TOP ORGANIZATIONS

WIND TRE... 137,590
WIND Tele... 10,987
Wind telecom... 7,831

151.21.16.67 2024-03-07T09:47:22.190985

addr=151.21.16.67
proto=tcp
port=21
country=US
state=Texas
city=Houston
org=WIND TRE S.p.A.
lat=29.760
lon=-95.373
time=2024-03-07T09:47:22.190985Z
http://151.21.16.67/favicon.ico
User-Agent: DLINK_VoIP_Stack
Supported: replaces,timer,100rel
Via: SIP/2.0/UDP nn,received=224.252.135.87,port=20810,branch=400
Content-Length: 0

37.101.203.236 2024-03-07T09:46:54.401800

addr=37.101.203.236
proto=tcp
port=443
country=IT
state=Lombardy
city=Milano
org=WIND TRE S.p.A.
lat=41.902
lon=12.496
time=2024-03-07T09:46:54.401800Z
http://37.101.203.236/favicon.ico
User-Agent: DLINK_VoIP_Stack
Supported: replaces,timer,100rel
Via: SIP/2.0/UDP nn,received=224.44.78.245,port=20810,branch=400
Content-Length: 0

Shodan Maps Images Monitor Developer More

SHODAN Explore Pricing & VPN Search Login

TOTAL RESULTS: 2,761,685

TOP COUNTRIES:



Japan 523,731
China 420,963
United States 372,254
Australia 227,820
Germany 156,397
[More...](#)

TOP PORTS:

500	2,626,109
4500	63,944
443	20,694
1723	9,825
80	7,271

[More...](#)

TOP ORGANIZATIONS:

Telstra	102,252
Open Com...	100,346
Telstra Inter...	91,926

View Report | Browse Images | View on Map

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

218.41.232.62 2024-03-07T10:05:14.474Z01

proto:https://:443
method:GET
path:/
headers:

- Host: Service
- Content-Type: application/json
- Accept: */*
- User-Agent: curl/7.64.0
- Accept-Encoding: gzip, deflate
- Connection: close

body:

```
{
  "id": "218.41.232.62.443.1",
  "version": "1.0",
  "type": "Informational",
  "payload": "Hello, World!",
  "flags": {
    "Encryption": false,
    "Compressed": false,
    "Authentication": false
  },
  "message_id": "00000000000000000000000000000000",
  "length": 40
}
```

178.32.89.193 2024-03-07T10:05:07.807Z22

proto:https://:443
method:POST
path:/
headers:

- Host: Service
- Content-Type: application/json
- Accept: */*
- User-Agent: curl/7.64.0
- Accept-Encoding: gzip, deflate
- Connection: close

body:

```
{
  "id": "178.32.89.193.443.1",
  "version": "2.0",
  "type": "DOI Specific Data",
  "payload": "Hello, World!",
  "flags": {
    "Encryption": false,
    "Compressed": false,
    "Authentication": false
  },
  "message_id": "00000000000000000000000000000000",
  "length": 36
}
```

<https://www.shodan.io>

Objective **03**

Demonstrate Footprinting through Internet Research Services

Passive Reconnaissance

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

- Search for the target company's external URL in a search engine, such as **Google** and **Bing**
- Sub-domains **provide an insight** into different departments and business units in an organization
- You may find a company's sub-domains by **trial and error method** or using a service such as <https://www.netcraft.com>
- You can use the **DNSdumpster** tool, which can discover hosts related to a domain

netcraft

Hostnames matching *.microsoft.com

▶ Q Search with another pattern?

First 500 results (showing 1 to 20)

Rank	Site	First seen	Netblock	OS
35	ircm.microsoft.com [IC]	November 2010	Microsoft Corporation	Windows Server 2008
39	ircn.microsoft.com [IC]	July 2015	Akamai International, BV	unknown
66	support.microsoft.com [IC]	October 1997	Akamai Technologies	unknown
86	www.microsoft.com [IC]	August 1995	Akamai Technologies, Inc.	Linux
170	admin.microsoft.com [IC]	November 2017	Microsoft Corporation	Windows Server 2008
182	security.microsoft.com [IC]	December 2006	Microsoft Corporation	Windows Server 2008
204	answers.microsoft.com [IC]	August 2009	Akamai International, BV	unknown
403	account.microsoft.com [IC]	July 2006	Akamai Technologies, Inc.	Linux
427	admin.exchange.microsoft.com [IC]	September 2019	Microsoft Corporation	Windows Server 2008

<https://www.netcraft.com>

The screenshot shows a web browser window with the address bar containing "dnsdumpster.com". The main content area displays a table of discovered hosts for the domain "ecomail.org". The table includes columns for the host name, IP address (104.18.9.100), and status (HTTP: live/alive). The listed hosts include "orderd.ecomail.org", "backend-orderd.ecomail.org", "preload.ecomail.org", "greencycle.ecomail.org", "ware.ecomail.org", "store.ecomail.org", "sysopslab-enterprise.ecomail.org", "affiliate.ecomail.org", "marketing-education-institute.ecomail.org", "slacklineusabilityinstitute.ecomail.org", "cryptobrief.ecomail.org", "planning.ecomail.org", and "staging.ecomail.org".

Host	IP	Status
orderd.ecomail.org	104.18.9.100	HTTP: live/alive
backend-orderd.ecomail.org	104.18.9.100	HTTP: live/alive
preload.ecomail.org	104.18.9.100	HTTP: live/alive
greencycle.ecomail.org	104.18.9.100	HTTP: live/alive
ware.ecomail.org	104.18.9.100	HTTP: live/alive
store.ecomail.org	104.18.9.100	HTTP: live/alive
sysopslab-enterprise.ecomail.org	104.18.9.100	HTTP: live/alive
affiliate.ecomail.org	104.18.9.100	HTTP: live/alive
marketing-education-institute.ecomail.org	104.18.9.100	HTTP: live/alive
slacklineusabilityinstitute.ecomail.org	104.18.9.100	HTTP: live/alive
cryptobrief.ecomail.org	104.18.9.100	HTTP: live/alive
planning.ecomail.org	104.18.9.100	HTTP: live/alive
staging.ecomail.org	104.18.9.100	HTTP: live/alive

<https://dnsdumpster.com>

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

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

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

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

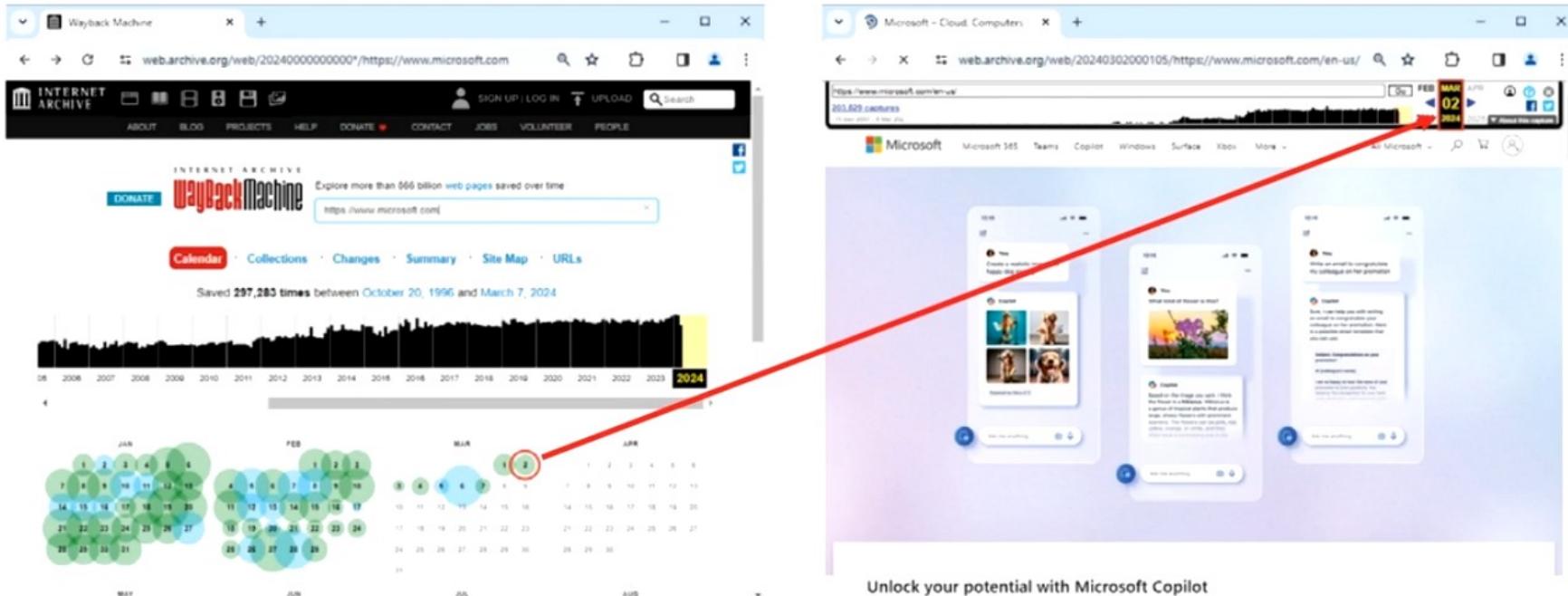
sgpt --chat footprint --shell "Use Sublist3r to gather a list of subdomains of the target organization"
File Edit View Search Terminal Help
(E)execute, (D)escribe, (A)bort: E

# Code By Ahmed Aboul-Ela - #aboullila

[] Enumerating subdomains now for ecouncil.org
[+] 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 VirusShare.
[+] Searching now in ThreatCrowd.
```

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

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



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

Footprinting through People Search Services and Job Sites

- People search services, such as **Spokeo**, **Intelius**, and **pipl** can provide critical **information about a person or an organization**, including location, emails, websites, blogs, contacts, important dates, address, etc.
- Job sites such as Dice, LinkedIn, and Glassdoor can reveal details about a **company's infrastructure**, potentially aiding attackers in **identifying vulnerabilities within the target's IT environment**

The screenshot shows the Spokeo search interface. At the top, there is a map of the United States with numerous orange dots representing search results. Below the map, the search bar contains "John Furner". To the right of the search bar are links for "ABOUT", "LOGIN", and "SIGN UP". The main search results are displayed in a grid format. The first result is highlighted with a red border and shows "John Furner" with a checkmark, indicating 26 people found. It also mentions locations like New York, Virginia, and 10 other states. Below this, there are three more results for "John Albert Furner" (81), "John Martin Furner" (61), and another "John Albert Furner" (81). Each result card includes the person's name, age, residence, and a "SEE RESULTS" button. On the left side of the page, there is a sidebar titled "BROWSE LOCATIONS" with dropdown menus for "Alabama", "Arizona", "Arkansas", "California", "Colorado", "District of Columbia", "Florida", and "Georgia".

<https://www.spokeo.com>

The screenshot shows a job listing on Glassdoor for a "Junior Network Administrator / Assistant" position in Dallas, TX. The job title is at the top, followed by the location "Dallas, TX". The job description includes sections for "Qualifications and Experience" and "Cybersecurity experience and skills". The "Qualifications and Experience" section lists requirements such as an engineering degree, 2+ years of experience maintaining complex IP networks, and knowledge of network segmentation. The "Cybersecurity experience and skills" section lists tasks like maintaining image hub functions, handling tickets through Jira, and working in fast-paced teams. At the bottom, there is a section for "Essential Functions & Day to Day Activities" which includes supporting network admins, managing cybersecurity tasks, and maintaining firewalls. Below the job description, there is a "SEE RESULTS" button. The URL "glassdoor.co.i..." is visible in the browser's address bar.

<https://www.glassdoor.com>

Dark Web Footprinting

Dark web or Darknet

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



TOR Browser

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

<https://www.torproject.org>

Competitive Intelligence Gathering

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

Sources of Competitive Intelligence

- | | |
|---|---------------------------------------|
| ① Company websites and employment ads | 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 |

Other Techniques for Footprinting through Internet Research Services

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

Objective **04**

Demonstrate Footprinting through Social Networking Sites

Passive Reconnaissance

Gathering Information from LinkedIn

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

```
theHarvester -d eccouncil -l 200 -b linkedin - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot] ~
# theHarvester -d eccouncil -l 200 -b linkedin
*****
* [!] Target: eccouncil
* [!] LinkedIn Users found: 197
* [!] Software Engineer
* [!] Vice President
* [!] Cyber Security Training Coordinator
* [!] Vice President Finance
* [!] Manager Masterclass
* [!] Manager - Partner Outreach
* [!] Operations Manager
* [!] Software Engineer
* [!] EC-Council
* [!] Manager Business Development
* [!] Account Executive
* [!] Assistant Manager International Sales
* [!] Security Consultant
* [!] Researcher
* [!] IT security hobbyist
* [!] Senior Operations Executive
* [!] Research Specialist
* [!] SVP and Head of Americas
```

Attackers search on LinkedIn to obtain employee details

```
theHarvester -d eccouncil -l 200 -b linkedin - Parrot Terminal
File Edit View Search Terminal Help
[*] Target: eccouncil
[*] Searching 100 results.
[*] Searching 200 results.
[*] Searching LinkedIn.
[*] LinkedIn Users found: 197
.....
- Software Engineer
- Vice President
- Cyber Security Training Coordinator
- Vice President Finance
- Manager Masterclass
- Manager - Partner Outreach
- Operations Manager
- Software Engineer
- EC-Council
- Manager Business Development
- Account Executive
- Assistant Manager International Sales
- Security Consultant
- Researcher
- IT security hobbyist
- Senior Operations Executive
- Research Specialist
- SVP and Head of Americas
```

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

<https://github.com>

Harvesting Email Lists with AI

- Attackers use automated tools such as **theHarvester** and **Email Spider** to collect publicly available email addresses of the target organization that helps them perform social engineering and brute-force attacks
- An attacker can also leverage AI-powered ChatGPT or other generative AI technology to perform this task by using an appropriate prompt such as
"Use theHarvester to gather email accounts associated with microsoft.com, limiting results to 200, and leveraging 'baidu' as a data source"

```

theHarvester -d microsoft.com -l 200 -b baidu -Parrot Terminal
File Edit View Search Terminal Help
attacker@parrot:~$ 
attacker@parrot:~$ sudo su
[sudo] password for attacker:
root@parrot:~# /home/attacker/
root@parrot:~# cd
root@parrot:~# ./theHarvester -d microsoft.com -l 200 -b baidu
[*] Target: microsoft.com
[*] Searching Baidu
[*] No IPs found
[*] Emails found: 1
edge_ef@microsoft.com
[*] Hosts found: 5
windowsupdate.microsoft.com
docs.microsoft.com
msdn.microsoft.com
technet.microsoft.com
testconnectivity.microsoft.com

```

<https://github.com>

```

attacker@parrot:~$ 
$sgpt --chat fp --shell 'Use theHarvester to gather email accounts associated with microsoft.com, limiting results to 200, and leveraging "baidu" as a data source'
theHarvester -d microsoft.com -l 200 -b baidu -f microsoft_emails.xml
[E]execute, [D]escribe, [A]bort: E
[*] Target: microsoft.com
[*] Searching Baidu
[*] No IPs found.
[*] Emails found: 8
edge_ef@microsoft.com
contactopencode@microsoft.com
edge_ef@microsoft.com
emailopencode@microsoft.com
msatp@microsoft.com
mscnappsfeedback@microsoft.com
opensource@microsoft.com
xxx@microsoft.com
[*] Hosts found: 33
update.microsoft.com
windowsupdate.microsoft.com
JFdevblogs.microsoft.com
JFdocs.microsoft.com

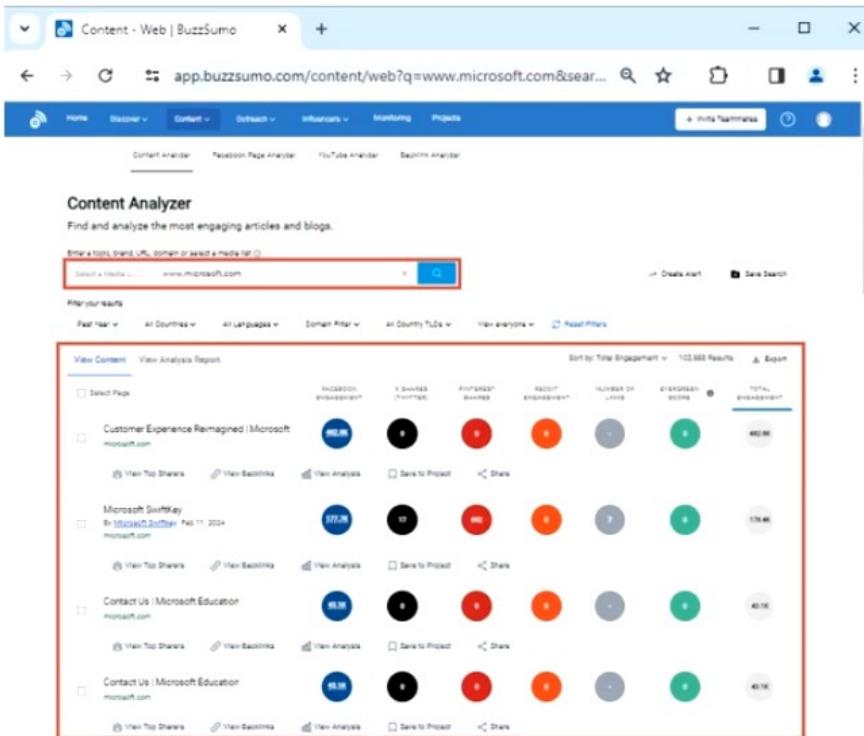
```

Analyzing Target Social Media Presence

- Attackers track social media sites using BuzzSumo, Google Trend, Hashatit, etc. to **discover most shared content** using hashtags or keywords, track accounts and URLs, email addresses, etc.
- Attackers use this information to perform **phishing, social engineering**, and other types of attacks

BuzzSumo

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

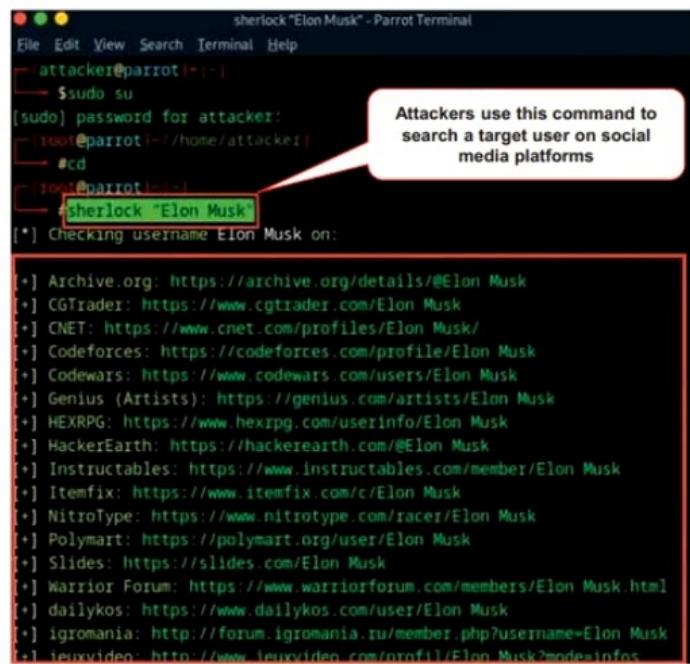


<https://buzzsumo.com>

Tools for Footprinting through Social Networking Sites

Sherlock

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



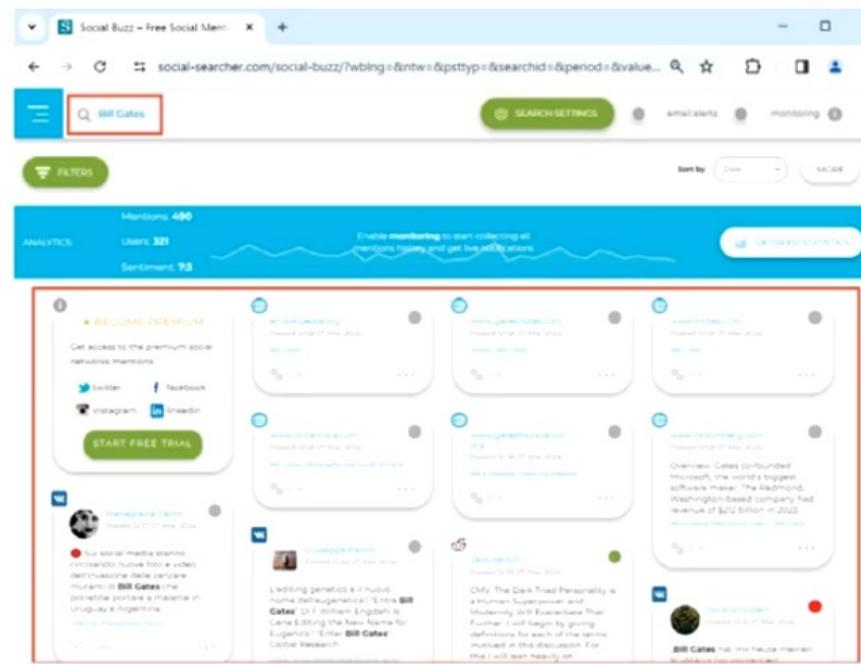
```
sherlock "Elon Musk" - Parrot Terminal
File Edit View Search Terminal Help
attacker@parrot:~$ sudo su
[sudo] password for attacker:
root@parrot:~# /home/attacker/z
root@parrot:~# cd
root@parrot:~# ./sherlock "Elon Musk"
[*] Checking username Elon Musk on:

+] Archive.org: https://archive.org/details/@Elon Musk
+] CGTrader: https://www.cgtrader.com/Elon Musk
+] CNET: https://www.cnet.com/profiles/Elon Musk/
+] Codeforces: https://codeforces.com/profile/Elon Musk
+] Codewars: https://www.codewars.com/users/Elon Musk
+] Genius (Artists): https://genius.com/artists/Elon Musk
+] HEXRPG: https://www.hextrpg.com/userinfo/Elon Musk
+] HackerEarth: https://hackerearth.com/@Elon Musk
+] Instructables: https://www.instructables.com/member/Elon Musk
+] Itemfix: https://www.itemfix.com/c/Elon Musk
+] NitroType: https://www.nitrotype.com/racer/Elon Musk
+] Polymart: https://polymart.org/user/Elon Musk
+] Slides: https://slides.com/Elon Musk
+] Warrior Forum: https://www.warriorforum.com/members/Elon Musk.html
+] dailykos: https://www.dailycos.com/user/Elon Musk
+] igromania: http://forum.igromania.ru/member.php?username=Elon Musk
+] ieuuxvideo: http://www.ieuuxvideo.com/profil/Elon.Musk?modeinfos
```

<https://github.com>

Social Searcher

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



The screenshot shows the Social Buzz interface from Social Searcher. A search bar at the top contains the query "Bill Gates". Below the search bar, there are sections for "Mentions: 460", "Users: 321", and "Sentiment: 93". A call-to-action button "Enable monitoring to start collecting all mentions history and get live notifications" is visible. The main area displays a grid of social media posts from various platforms like Twitter, Facebook, and LinkedIn. One post from "microsoft" (@Microsoft) is highlighted, showing a link to "https://www.microsoft.com". Another post from "Bill Gates" (@BillGates) discusses the company's revenue. The interface includes filters, search settings, and monitoring options.

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

Footprinting through Social Networking Sites with AI

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

"Use Sherlock to gather personal information about Sundar Pichai and save the result in recon2.txt"

```
sgpt --chat footprint --shell "Use Sherlock to gather personal information about Sundar Pichai and save the result in recon2.txt"
File Edit View Search Terminal Help
[root@parrot]~[~]
#sgpt --chat footprint --shell "Use Sherlock to gather personal
information about Sundar Pichai and save the result in recon2.txt"
sherlock SundarPichai output recon2
[E]xecute, [D]escribe, [A]bort: E
[*] Checking username SundarPichai on:

[+] About.me: https://about.me/SundarPichai
[+] Academia.edu: https://independent.academia.edu/SundarPichai
[+] Amino: https://aminoapps.com/u/SundarPichai
[+] Behance: https://www.behance.net/SundarPichai
[+] Blogger: https://SundarPichai.blogspot.com
[+] CGTrader: https://www.cgtrader.com/SundarPichai
[+] CNET: https://www.cnet.com/profiles/SundarPichai/
[+] Codecademy: https://www.codecademy.com/profiles/SundarPichai
[+] Codeforces: https://codeforces.com/profile/SundarPichai
[+] Coders Rank: https://profile.codersrank.io/user/SundarPichai/
```

```
recon2.txt (~) - Pluma (as superuser)
File Edit View Search Tools Documents Help
Open Save Undo C X
recon2.txt x
1 https://about.me/SundarPichai
2 https://independent.academia.edu/SundarPichai
3 https://aminoapps.com/u/SundarPichai
4 https://www.behance.net/SundarPichai
5 https://SundarPichai.blogspot.com
6 https://www.cgtrader.com/SundarPichai
7 https://www.cnet.com/profiles/SundarPichai/
8 https://www.codecademy.com/profiles/SundarPichai
9 https://codeforces.com/profile/SundarPichai
10 https://profile.codersrank.io/user/SundarPichai/
11 https://disqus.com/SundarPichai
12 https://www.duolingo.com/profile/SundarPichai
13 https://www.fiverr.com/SundarPichai
14 https://www.freelancer.com/u/SundarPichai
15 https://giphy.com/SundarPichai
Plain Text Tab Width: 4 Ln 9, Col 4 INS
```

Objective **05**

Use Different Techniques for Whois Footprinting

Passive Reconnaissance

Whois Lookup

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

Whois query returns

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

Information obtained from Whois database assists an attacker to

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

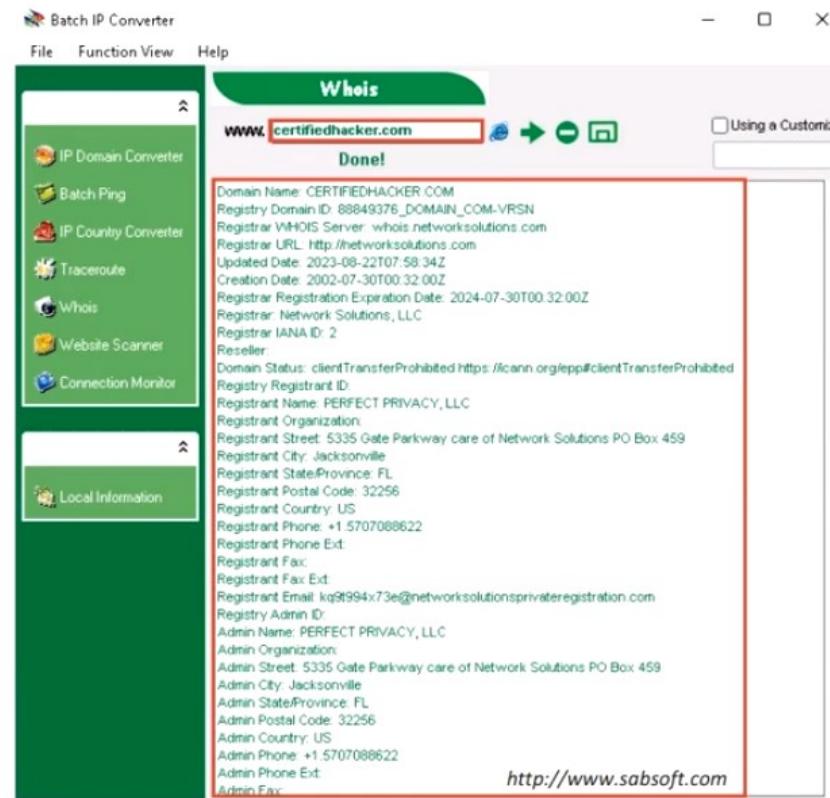
Regional Internet Registries (RIRs)



Whois Lookup (Cont'd)

Whois Record for CertifiedHacker.com

Domain Profile	
Registrar	Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com domain.operations@web.com (p) +1.8777228662
Registrar Status	clientTransferProhibited
Dates	7.097 days old Created on 2002-07-30 Expires on 2024-07-30 Updated on 2023-08-22
Name Servers	NS1.BLUEHOST.COM (has 2,349,716 domains) NS2.BLUEHOST.COM (has 2,349,716 domains)
IP Address	162.241.216.11 - 1,299 other sites hosted on this server
IP Location	Utah - Provo - Unified Layer
ASN	AS46606 UNIFIEDLAYER AS 1, US (registered Oct 24, 2008)
Domain Status	Registered And No Website
IP History	13 changes on 13 unique IP addresses over 10 years
Registrar History	3 registrars with 3 drops
Hosting History	6 changes on 4 unique name servers over 21 years
Whois Record (last updated on 2024-03-13)	
Domain Name: CERTIFIEDHACKER.COM Registry Domain ID: 88849376_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.networksolutions.com Registrar URL: http://networksolutions.com Updated Date: 2023-08-22T07:58:54Z Creation Date: 2002-07-30T00:32:00Z Registrar Registration Expiration Date: 2024-07-30T00:32:00Z Registrar: Network Solutions, LLC Registrar IANA ID: 2	



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

Geolocation Data

The geolocation data uses IP2Location DB26 geolocation database.

Permalink	https://www.ip2location.com/207.46.232.182
<input checked="" type="checkbox"/> IP Address	207.46.232.182
<input type="checkbox"/> Country	Singapore [SG]
<input type="checkbox"/> Region	Singapore
<input type="checkbox"/> City	Singapore
<input type="checkbox"/> Coordinates of City	1.289987, 103.850281 (1°17'24"N 103°51'1"E)
<input type="checkbox"/> ISP	Microsoft Corporation
<input type="checkbox"/> Local Time	08 Mar. 2024 06:25 PM (UTC +08:00)
<input type="checkbox"/> Domain	microsoft.com
<input type="checkbox"/> Net Speed	(T1) Data Center/Transit
<input type="checkbox"/> IDD & Area Code	(65) 06
<input type="checkbox"/> ZIP Code	178958
<input type="checkbox"/> Weather Station	Singapore (S0000006)
<input type="checkbox"/> Mobile Carrier	-
<input type="checkbox"/> Mobile Country Code	-
<input type="checkbox"/> Mobile Network Code	-
<input type="checkbox"/> Elevation	7m
<input type="checkbox"/> Usage Type	(DCH) Data Center/Web Hosting/Transit
<input type="checkbox"/> Address Type	Unicast
<input type="checkbox"/> Category	Data Centers
<input type="checkbox"/> District	-
<input type="checkbox"/> ASN	AS8075 Microsoft Corporation
Olson Time Zone	Asia/Singapore

<https://www.ip2location.com>

Objective 06

Use Different Techniques for DNS Footprinting

Active Reconnaissance

Extracting DNS Information

- DNS records provide important information about the **location and types of servers**
- Attackers can gather DNS information to **determine key hosts in the network** and can perform social engineering attacks
- Attackers query DNS servers using DNS interrogation tools, such as SecurityTrails, Fierce, DNSChecker, and zdns, to **retrieve the record structure** that contains information about the target DNS

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

The screenshot shows the SecurityTrails interface for the domain `microsoft.com`. The main content area is titled "microsoft.com DNS records as of Jun 7, 2024". It lists four categories of records:

- A records:** Microsoft Corporation (2023.10.10.3.3.16), 20.112.250.133, 20.231.239.248, 20.236.44.162, 20.70.246.20, 20.76.201.171
- AAAA records:** 2003.10.05.201.10.108, 2003.10.05.201.10.109, 2003.10.05.201.10.110, 2003.10.05.201.10.111, 2003.10.05.201.10.112
- MX records:** Microsoft Corporation, microsoft-com.mail.protection.outlook.com
- NS records:** Microsoft Corporation, ns1-39.azure-dns.net, ns2-39.azure-dns.org, ns3-39.azure-dns.net

At the bottom right, the URL <https://securitytrails.com> is visible.

DNS Lookup with AI

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

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

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

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

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

Reverse DNS Lookup

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

MX TOOLBOX®

Pricing Tools Delivery Center Monitoring

SuperTool Beta7

162.241.216.11 Reverse Lookup ▾

ptr:162.241.216.11 Find Problems

ptr

Type	IP Address	Domain Name	TTL
TypePTR	IP Address 162.241.216.11 Unknown (AS46606)	Domain Name box5331.bluehost.com	TTL 24 hrs

Test	Result
Status	NameDNS Record Published
	ResponseDNS Record found

smtp diag blacklist subnet tool dns propagation

Reported by ns2.unifiedlayer.com on 3/14/2024 at 3:10:51 AM (UTC -5). just for you Transcript

<https://mxtoolbox.com>

```
root@parrot:~/home/attacker$ dnsrecon -r 162.241.216.0-162.241.216.255
|:| Reverse Look-up of a Range
|:| Performing Reverse Look-up from 162.241.216.0 to 162.241.216.255
[+][{'type': 'PTR', 'name': '162-241-216-4.unifiedlayer.com', 'address': '162.241.216.4'}
[+][{'type': 'PTR', 'name': '162-241-216-2.unifiedlayer.com', 'address': '162.241.216.2'}
[+][{'type': 'PTR', 'name': '162-241-216-6.unifiedlayer.com', 'address': '162.241.216.6'}
[+][{'type': 'PTR', 'name': '162-241-216-8.unifiedlayer.com', 'address': '162.241.216.8'}
[+][{'type': 'PTR', 'name': '162-241-216-9.unifiedlayer.com', 'address': '162.241.216.9'}
[+][{'type': 'PTR', 'name': '5tIVGWP8ew0', 'address': '162.241.216.0'}
[+][{'type': 'PTR', 'name': '162-241-216-1.unifiedlayer.com', 'address': '162.241.216.1'}
[+][{'type': 'PTR', 'name': '162-241-216-12.unifiedlayer.com', 'address': '162.241.216.12'}
[+][{'type': 'PTR', 'name': 'box5331.bluehost.com', 'address': '162.241.216.11'}]
[+][{'type': 'PTR', 'name': '162-241-216-18.unifiedlayer.com', 'address': '162.241.216.10'}
[+][{'type': 'PTR', 'name': 'box5334.bluehost.com', 'address': '162.241.216.14'}
[+][{'type': 'PTR', 'name': '162-241-216-13.unifiedlayer.com', 'address': '162.241.216.13'}
[+][{'type': 'PTR', 'name': '162-241-216-5.unifiedlayer.com', 'address': '162.241.216.5'}
[+][{'type': 'PTR', 'name': '162-241-216-16.unifiedlayer.com', 'address': '162.241.216.16'}
[+][{'type': 'PTR', 'name': 'box5348.bluehost.com', 'address': '162.241.216.17'}
[+][{'type': 'PTR', 'name': '162-241-216-18.unifiedlayer.com', 'address': '162.241.216.18'}
[+][{'type': 'PTR', 'name': '162-241-216-7.unifiedlayer.com', 'address': '162.241.216.7'}
[+][{'type': 'PTR', 'name': 'box5350.bluehost.com', 'address': '162.241.216.20'}
[+][{'type': 'PTR', 'name': 'box5353.bluehost.com', 'address': '162.241.216.23'}
[+][{'type': 'PTR', 'name': '162-241-216-3.unifiedlayer.com', 'address': '162.241.216.3'}
[+][{'type': 'PTR', 'name': '162-241-216-24.unifiedlayer.com', 'address': '162.241.216.24'}
[+][{'type': 'PTR', 'name': 'box5354.bluehost.com', 'address': '162.241.216.26'}
[+][{'type': 'PTR', 'name': '162-241-216-15.unifiedlayer.com', 'address': '162.241.216.15'}
[+][{'type': 'PTR', 'name': '162-241-216-19.unifiedlayer.com', 'address': '162.241.216.19'}
[+][{'type': 'PTR', 'name': '162-241-216-21.unifiedlayer.com', 'address': '162.241.216.21'}
[+][{'type': 'PTR', 'name': '162-241-216-30.unifiedlayer.com', 'address': '162.241.216.30'}]
```

<https://github.com>

Objective **07**

Use Different Techniques for Network and Email Footprinting

Active Reconnaissance

Traceroute

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

ICMP Traceroute

```
C:\Users\Admin

```

TCP Traceroute

```
sudo tcptraceroute www.google.com - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot:~]$
[attacker@parrot:~]$ sudo tcptraceroute www.google.com
[sudo] password for attacker:
Running:
traceroute -T -0 info www.google.com
traceroute to www.google.com (142.251.111.104), 30 hops max, 60 byte packets
 1  10.10.1.2 (10.10.1.2)  0.458 ms  0.441 ms  0.430 ms
 2  172.18.0.1 (172.18.0.1)  0.803 ms  0.792 ms  0.782 ms
 3  192.168.0.1 (192.168.0.1)  0.947 ms  0.937 ms  0.925 ms
 4  103.186.82.26 (103.186.82.26)  1.305 ms  1.541 ms  0.911 ms
```

UDP Traceroute

```
traceroute www.google.com - Parrot Terminal
File Edit View Search Terminal Help
[attacker@parrot:~]$
[attacker@parrot:~]$ traceroute www.google.com
traceroute to www.google.com (142.251.33.100), 30 hops max, 60 byte packets
 1  10.10.1.2 (10.10.1.2)  0.276 ms  0.250 ms  0.230 ms
 2  172.18.0.1 (172.18.0.1)  0.340 ms  0.305 ms  0.284 ms
 3  192.168.0.29 (192.168.0.29)  0.325 ms  0.305 ms  0.286 ms
 4  163.47.101.133 (163.47.101.133)  0.789 ms  33.458 ms  33.438 ms
 5  pr01-ct-0-3-0-0.sea09.net.google.com (206.81.80.17)  11.341 ms  0.917 ms  0.847 ms
 6  192.178.105.129 (192.178.105.129)  1.348 ms  108.170.255.175 (108.170.255.175)  3.562 ms
 7  192.178.105.129 (192.178.105.129)  10.315 ms
 8  142.251.50.177 (142.251.50.177)  34.139 ms  28.801 ms  28.768 ms
 9  sea38s10-in-f4.1e100.net (142.251.33.100)  28.747 ms  1.101 ms  1.081 ms
```

Traceroute with AI

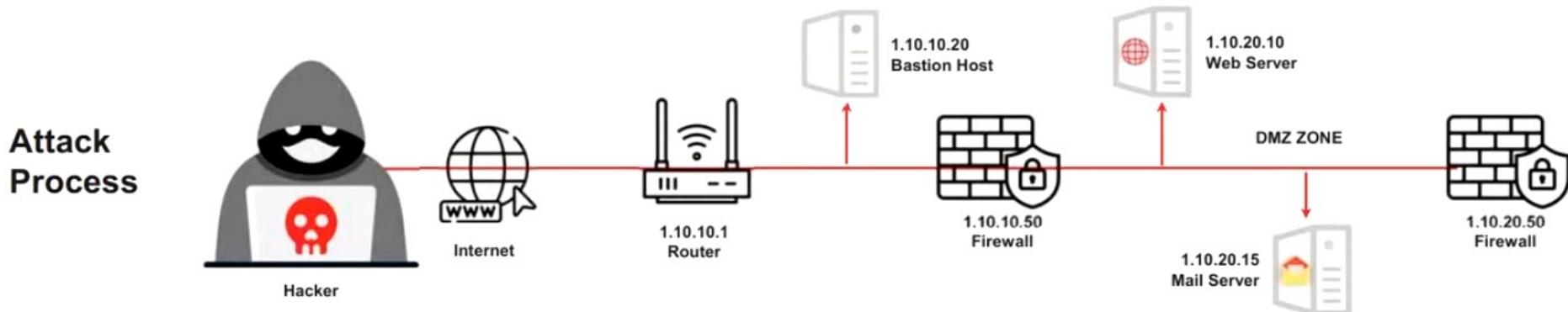
- An attacker can also leverage **AI-powered ChatGPT** or other generative AI technology to perform this task by using an appropriate prompt such as

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

```
● ● ● sgpt --chat footprint --shell "Perform network tracerouting to discover the routers on the path to a target host www.certifiedhacker.com"
File Edit View Search Terminal Help
[!root@parrot] ~
└─#sgpt --chat footprint --shell "Perform network tracerouting to discover the routers on the path to a target host www.certifiedhacker.com"
traceroute www.certifiedhacker.com
[X]ecute, [D]escribe, [A]bort: E
traceroute to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte
packets
 1 10.10.1.2 (10.10.1.2)  0.517 ms  0.494 ms  0.472 ms
 2 172.18.0.1 (172.18.0.1)  0.914 ms  0.894 ms  0.874 ms
 3 192.168.0.1 (192.168.0.1)  1.005 ms  0.985 ms  0.966 ms
 4 103.186.82.26 (103.186.82.26)  1.105 ms  1.420 ms  1.065 ms
 5 103.186.82.3 (103.186.82.3)  1.322 ms  1.360 ms  1.281 ms
 6  gi0-1-1-15.rcr21.iad01.atlas.cogentco.com (38.104.207.233)  1.741 ms  2.5
81 ms  2.221 ms
 7  be2956.ccr41.iad02.atlas.cogentco.com (154.54.30.193)  2.514 ms  2.180 ms
 2.224 ms
 8  telia.iad02.atlas.cogentco.com (154.54.12.62)  2.141 ms  1.752 ms  2.103
ms
 9  ash-bb2-link.ip.twelve99.net (62.115.123.124)  1.536 ms rest-bb1-link.ip.
twelve99.net (62.115.123.122)  2.380 ms 2.111 ms
10 nyk-bb1-link.ip.twelve99.net (62.115.141.245)  9.342 ms nyk-bb2-link.ip.t
welve99.net (62.115.136.200)  8.060 ms  8.385 ms
11 palo-b24-link.ip.twelve99.net (62.115.138.117)  76.917 ms palo-b24-link.ip.
twelve99.net (62.115.138.111)  76.381 ms palo-b24-link.ip.twelve99.net (62.
```

Traceroute Analysis

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



Tracking Email Communications

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



Delivered-To: [REDACTED]@gmail.com
 Received: by 2002: x50: 254b 0 b4 24x b984 0907 with SMTP id y11csp2051431ace;
 Thu, 7 Mar 2014 23:36:57 -0800 (PST)
 X-Google-Smtp-Source: ADH+TmC+nmPq1zxa/4qL/14w0uaasZmmBsgRe11ohvduzGhs/JN/RvYcpnMR8ms12GBMT5vrfDN
 X-Received: by 2002: x65: 673: b4 220: 67ba: c4a with SMTP id 119-
 2002b0d0f718893000d22058ax1am020842820ax; 14.1799883417230;
 Thu, 07 Mar 2014 23:36:57 -0800 (PST)
 ARC-Seal: i=1; v=rsha256; t=1799883417; cv=none;
 d-google.com, s=arc-28168816;
 p=2f21/85e820e48b41061giuuhv18t3j:u2k5RxpFVK3ee/eytD9t12dApndtu2Yk
 VC368y7Te/F05wvJ8Xk2N67Flir5hITvzrFG7/nfGmZlo/423860h+0Wt1308Rn
 wva:QG1pTEDCXdrK/BgCrU11Soud3>Dm6jgnwRlumenOpenCP1AosdFwmlp7V
 ECdnOpnFyf/099NQpewv02pV187213ka+onQf+e7mCQ+e3h31SHnx+F1Haklnv7V
 rvtDQ1vVubvYCksaJh#P<x57frrowab3xtRvC3le2F18kj79Lhpv0T1sdv5038o
 1a2o--
 ARC-Message-Signature: i=1; v=rsha256; c=relaxed/relaxed; d=google.com; s=arc-28168816;
 h=list-unsubscribe-post list-unsubscribe-feedback-id:sesame_open
 mime-version: subject: message-id:to:reply-to:from:date:sender
 :date-signature,
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w;
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor;
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 z=1mDwv81374wU1g7Tk6tJzz2n2k50001211tj5OK4mCkot7pV5DFw81MOPesD9
 w=d1BHtA1T0rZ1d41Rs7nbw1c7v31m1G4RgDnospel9uNttag7L8LCfZaLmGnD9
 rr=410K26Qm/D4cPF7Nmlh1mtdw+e1L
 95129WuGV1xrJTLi+kH6Li+8Gm6-
 Pw=--
 d=gmail.google.com
 ARC-Authentic-Result: i=1; m=gm
 dm=pass header:i=market.out
 sv=pass (google.com domain)
 svp=mailfrom (market.out)
 dmars=pas (p=QUARANTINE dis=NONE) header:From=market.out
 Return-Path: [REDACTED]@market.octoparse.com
 Received: From umail126.sendcloud.in ([REDACTED])
 by mail.google.com with ESRTPS id w69-1802ba3824800000005u7L1971194115075541pgd AB5-2014-03-07-23-36-54
 for [REDACTED] (version=TLS 1.2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
 Thu, 07 Mar 2014 23:36:57 -0800 (PST)
 Received-SPF: mail.google.com domain of umail126.sendcloud.in [REDACTED] as permitted sender
 (186.75.2.48);
 helo: [REDACTED]@market.octoparse.com
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1ZtJeqR0I-
 b=mAMNRC82I2gDy+uynbf/gu+2nDp77+1c3VjB3uGv//DDGtNgmaChP194.x0
 m=50MFYx0z41mlnd7aCv51H1GnfGf/VY1meevezEulor
 h=ARC-Signature: v=rsha256; c=relaxed/simple; d=market.octoparse.com; s=q-vde/1x5;
 m=5zbc26d6+DGtQuo3Ghmt21Tvs1jPym06c3w
 h=list-unsubscribe-post, m=11z/077pBaTnHQD75y5wvGbubU1Z

Objective 08

Demonstrate Footprinting through Social Engineering

Active Reconnaissance

Footprinting through Social Engineering

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

Social engineers attempt to gather

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

Social engineering techniques include

- Eavesdropping
- Shoulder surfing
- Dumpster diving
- Impersonation

Collecting Information through Social Engineering on Social Networking Sites

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

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

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

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

Eavesdropping

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



Shoulder Surfing

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



Dumpster Diving

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



Impersonation

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



Objective 09

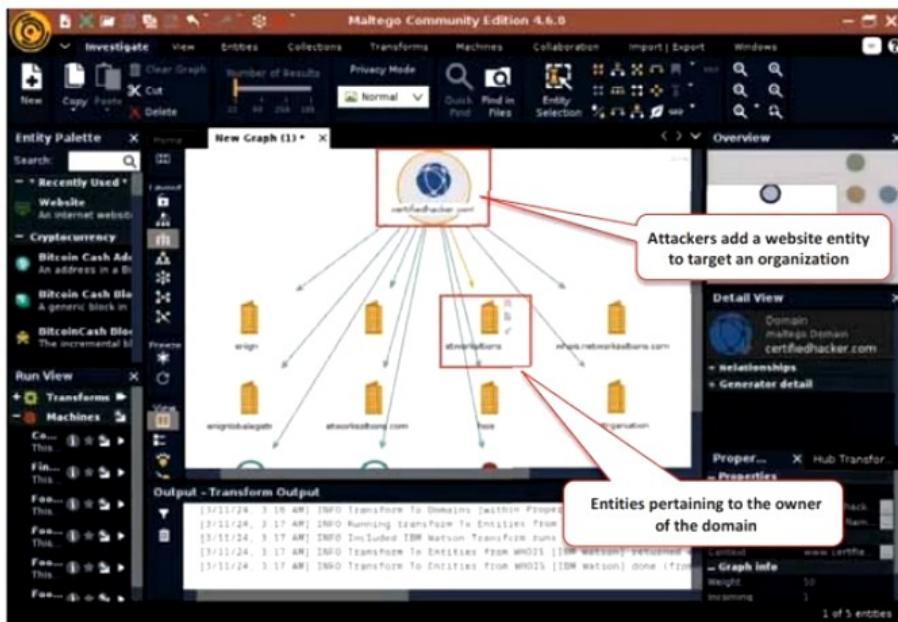
Automate Footprinting Tasks using Advanced Tools and AI

Active Reconnaissance

Footprinting Tools: Maltego and Recon-ng

Maltego

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



<https://www.maltego.com>

Recon-ng

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

```
recon-ng - Parrot Terminal
File Edit View Search Terminal Help
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts

[recon-ng][CEH] > modules load recon/domains-hosts/brute_hosts
[recon-ng][CEH][brute_hosts] > run
-----
CERTIFIEDHACKER.COM

No Wildcard DNS entry found.
02.certifiedhacker.com => No record found.
03.certifiedhacker.com => No record found.
1.certifiedhacker.com => No record found.
12.certifiedhacker.com => No record found.
13.certifiedhacker.com => No record found.
14.certifiedhacker.com => No record found.
0.certifiedhacker.com => No record found.
16.certifiedhacker.com => No record found.
17.certifiedhacker.com => No record found.
18.certifiedhacker.com => No record found.
15.certifiedhacker.com => No record found.
01.certifiedhacker.com => No record found.
3.certifiedhacker.com => No record found.
10.certifiedhacker.com => No record found

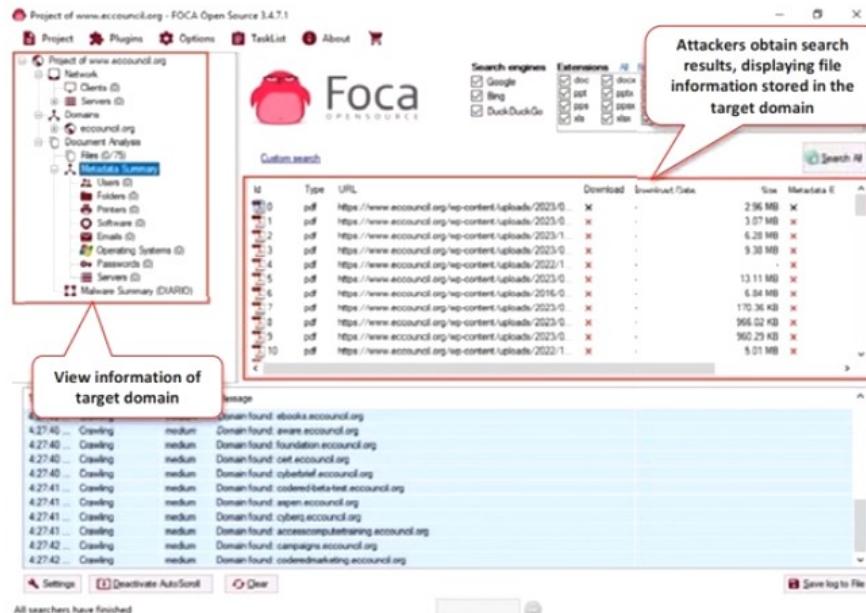
Attackers use this module to gather target hosts information
Execute the query
Harvests list of target hosts
```

<https://github.com>

Footprinting Tools: FOCA and subfinder

FOCA

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



<https://www.elevenpaths.com>

subfinder

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

```
subfinder -d certifiedhacker.com - ParrotTerminal
File Edit View Search Terminal Help
[root@parrot : /home/attacker]
└─$ subfinder -d certifiedhacker.com

____ _[ ]_ / ____ [ ]_ _[ ]_ [ ]_ _[ ]
(_-< [ ]_ [ ]_ \ [ ]_ [ ]_ \ / [ ]_ / [ ]_ ) [ ]
/ [ ]_ [ ]_ [ ]_ [ ]_ [ ]_ [ ]_ [ ]_ [ ]_ v2

projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using subfinder, you also agree to the terms of the APIs used.

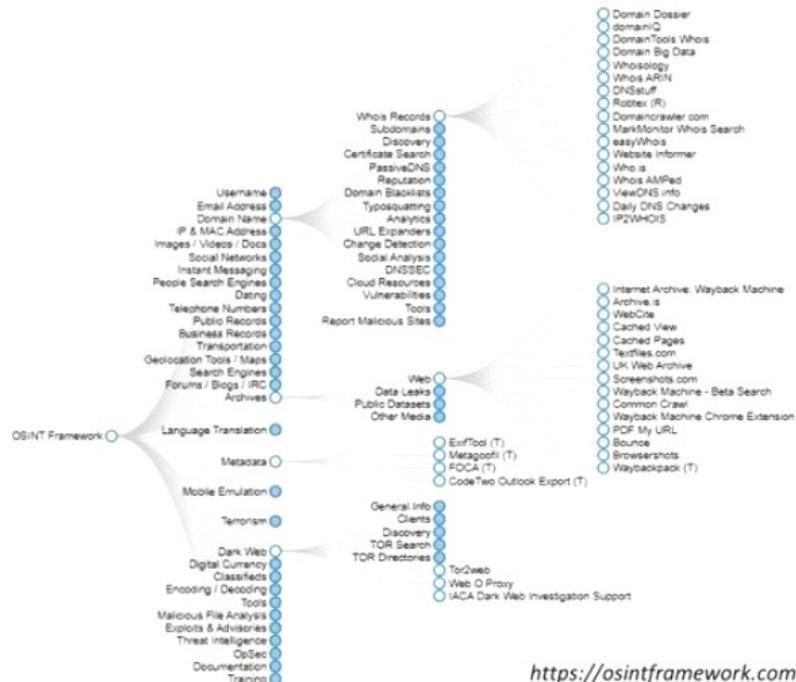
[!INF] Enumerating subdomains for certifiedhacker.com
www.certifiedhacker.com
autodiscover.certifiedhacker.com
blog.certifiedhacker.com
cpanel.certifiedhacker.com
cpcalendars.certifiedhacker.com
cpcontacts.certifiedhacker.com
demo.certifiedhacker.com
www.demo.certifiedhacker.com
autodiscover.demo.certifiedhacker.com
cpanel.demo.certifiedhacker.com
cpcalendars.demo.certifiedhacker.com

Attackers obtain
subdomains of the
target
```

<https://github.com>

Footprinting Tools: OSINT Framework

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



<https://osintframework.com>

Other Tools:

Sudomy
<https://github.com>

BillCipher
<https://github.com>

whatweb
<https://github.com>

Raccoon
<https://github.com>

Recon-Dog
<https://github.com>

Web Check
<https://web-check.xyz>

OSINT.SH
<https://osint.sh>

AI-Powered OSINT Tools

The screenshot shows the Taranis AI web interface. On the left is a sidebar with navigation links like Home, Recent, Search, and Filter. The main area displays several news articles in a grid format. One article is titled "Live Exploitation Undercores Urgency to Patch Critical WS-FTP Server Flaws" and another is "Lazarus Group Impersonates Recruiter from Meta to Target Spanish Aerospace Firms". Below the articles is a search bar with the URL <https://taranis.ai>.

The screenshot shows the GitHub Data Explorer interface. It features a search bar at the top with the placeholder "Questions about GitHub repos, users, orgs, languages...". Below it is a "Popular questions" section with a map of the world and a list of questions. One question is "How diverse is django's community (by coders' distribution)". At the bottom is a "Repository" section with a list of items like "Top 10 repos with the most contributions last month" and "Projects similar to @facebook/react". The URL <https://ossinsight.io> is visible at the bottom right.

Other Tools:

DorkGPT
<https://dorkgpt.com>

DorkGenius
<https://dorkgenius.com>

Google Word Sniper
<https://googlewordsniper.eu>

Cylect.io
<https://cylect.io>

ChatPDF
<https://chatpdf.com>

Taranis AI

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

OSS Insight

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

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

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

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

```
$sgpt --chat fp --shell " develop a python script which will accept domain name as www.microsoft.com as input and execute series of website footprinting commands, including DNS lookup, Whois records retrieval, email enumeration, and more, to gather information about target domain"
[at >> EOF > website_footprinting.py
import subprocess
def dns_lookup(domain):
    return subprocess.getoutput(f'dig
[E]xecute, [D]escribe, [A]bort: E
Performing DNS Lookup...
www.microsoft.com.      3125      IN
t.
Performing Whois Lookup...
No match for 'WWW.MICROSOFT.COM'.
>>> Last update of whois database: 2024
[*] Target: www.microsoft.com
[*] IPs found: 172
104.102.58.197
104.107.106.16
104.117.234.39
104.123.285.222
104.125.89.159
104.67.16.246
104.67.70.15
104.71.214.69
104.71.215.174
104.71.54.106
104.72.238.162
[*] Interesting URLs found: 64
https://www.microsoft.com/de-de/
https://www.microsoft.com/de-de/about
https://www.microsoft.com/de-de/al
https://www.microsoft.com/de-de/concern/scam?ttc=1
https://www.microsoft.com/de-de/d/Surface-Laptop-Go-3/Rpwmgj6c612
https://www.microsoft.com/de-de/d/Surface-Laptop-Studio-2/8rqz54k3
https://www.microsoft.com/de-de/d/surface-laptop-pro-9/93VQD8MP4FVK
https://www.microsoft.com/de-de/d/surface-studio-2plus/BVLFOC3597K
https://www.microsoft.com/de-de/download
https://www.microsoft.com/de-de/dynamics-365
https://www.microsoft.com/de-de/education
https://www.microsoft.com/de-de/education/devices/overview
https://www.microsoft.com/de-de/education/products/microsoft-365
https://www.microsoft.com/de-de/education/products/office
https://www.microsoft.com/de-de/education/products/teams
[*] Enumerating Emails...
theHarvester 4.4.3
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com
```

Objective 10

Explain Footprinting Countermeasures

Footprinting Countermeasures

-  Restrict the employees' access to social networking sites from the organization's network
-  Configure web servers to avoid information leakage
-  Educate employees to use pseudonyms on blogs, groups, and forums
-  Do not reveal critical information in press releases, annual reports, product catalogues, etc.
-  Limit the amount of information published on a website or the Internet
-  Use footprinting techniques to discover and remove any sensitive information that is publicly available
-  Prevent search engines from caching a web page and use anonymous registration services

Footprinting Countermeasures (Cont'd)

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

Module Summary



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