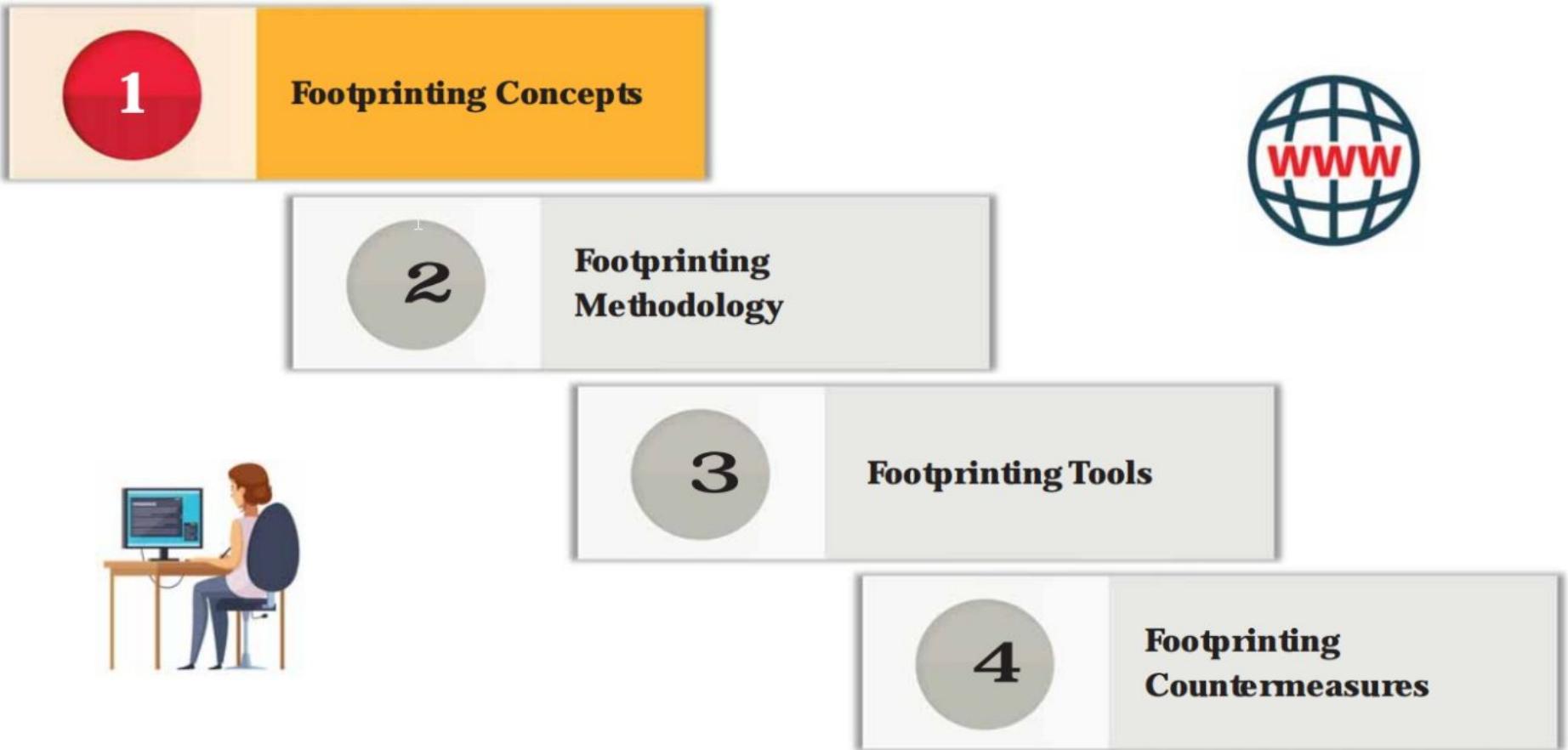


Footprinting and Reconnaissance





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

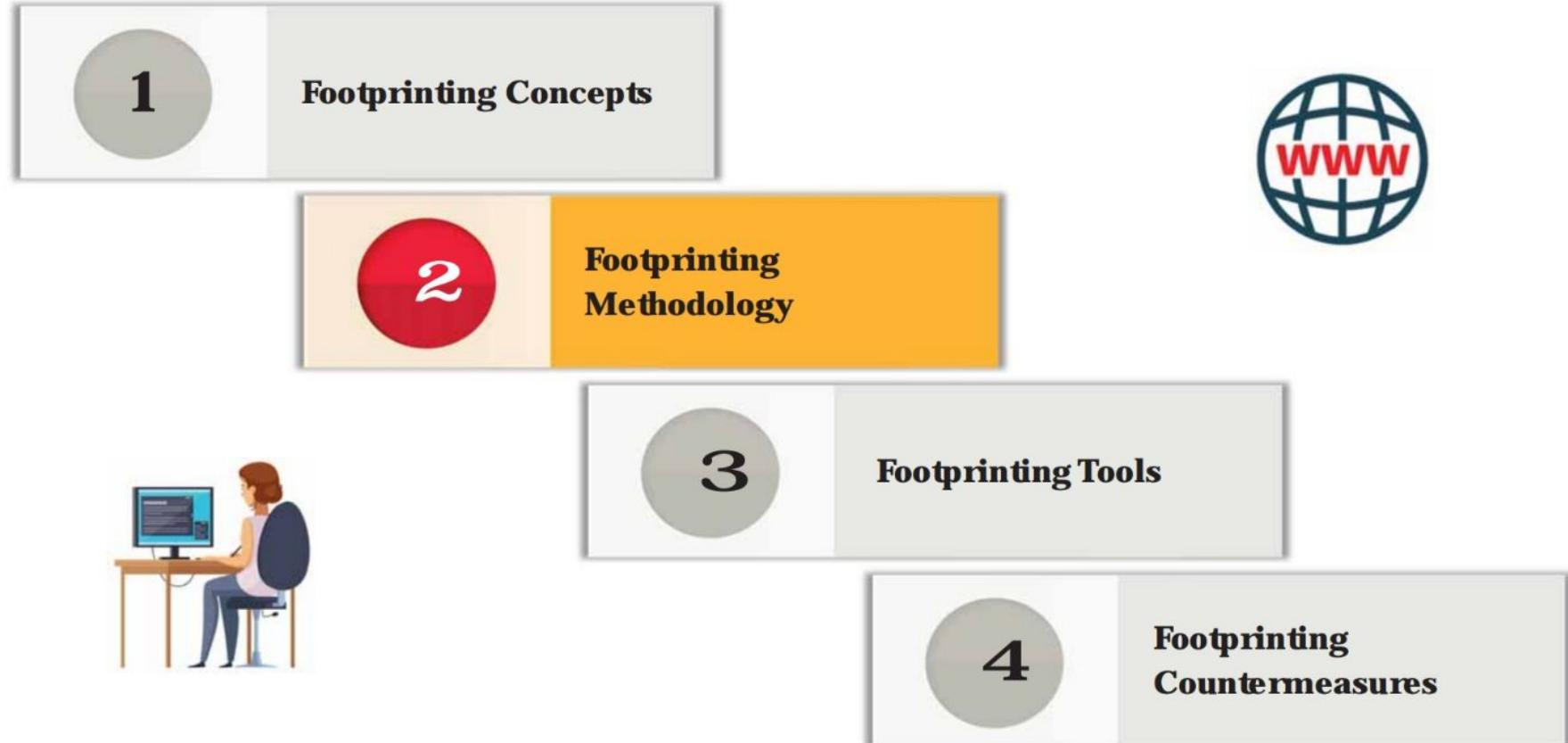
- OS and location of web servers, users and passwords, etc.

Objectives of Footprinting

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



Module Flow



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:

Google

Bing

YAHOO!

Ask.com

Aol.

Baidu 百度



DuckDuckGo

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

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

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

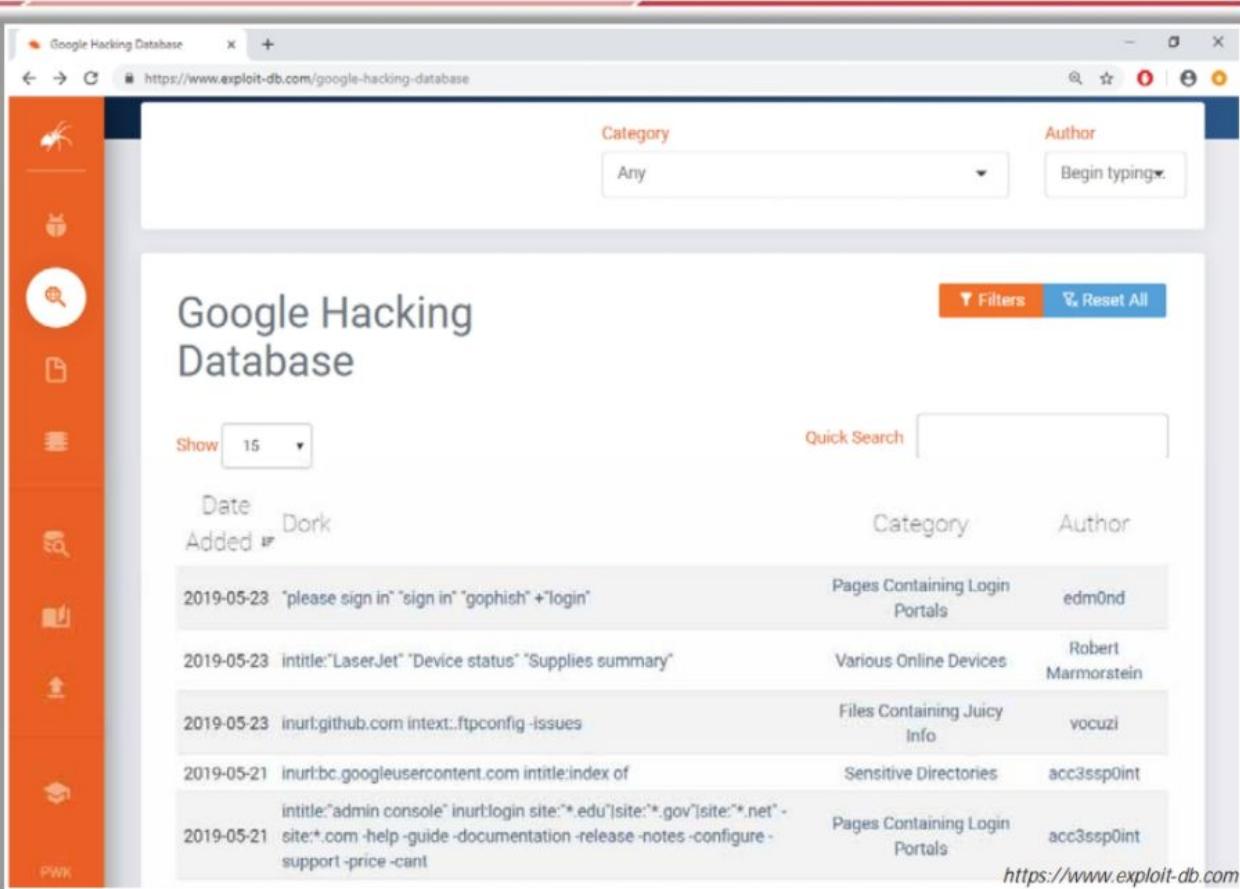
[inurl:] Restricts the results to documents containing the search keyword in the URL

[location:] Finds information for a specific location

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



The screenshot shows the GHDB interface on a web browser. The left sidebar has orange icons for various search types: spider (all), file type (pdf), search (dork), document (doc), code (js), image (img), and link (link). Below these is a 'PWN' button. The main page title is 'Google Hacking Database'. It features a search bar at the top right with dropdowns for 'Category' (set to 'Any') and 'Author' (placeholder 'Begin typing...'). Buttons for 'Filters' and 'Reset All' are also there. A 'Show 15' dropdown is set to 15 results. A 'Quick Search' input field is present. The main content area lists search results with columns for Date Added, Dork, Category, and Author. The results are:

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 -cant	Pages Containing Login Portals	acc3ssp0int

At the bottom right is the URL <https://www.exploit-db.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

```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot] ~
#theHarvester -d microsoft -l 200 -b linkedin
[*] Users found: 80
-----
Amrita Shanbhag - Software Engineer II - Microsoft
Andrew Wilson - Chief Digital Officer - Microsoft
Arun Rajappa - Director of Product Management - Microsoft
Ashis Roy - Group Development Manager - Microsoft
Ashish Shah - Director Of Engineering - Microsoft
Brad Smith - President - Microsoft
Brendan Burns - Corporate Vice President - Microsoft
Brian Holt - Senior Program Manager - Microsoft
Charles Lamanna - Corporate Vice President - Microsoft
Charu Srinivasan - Microsoft
Chetan Parulekar - Partner Group Manager - Microsoft
Chris L. - Senior Director Software Partnerships - Microsoft
Dalan Mendonca - Product Manager - Microsoft
David Cattanach - Azure Technical Trainer - Microsoft
David Fowler - Partner Software Architect - Microsoft
David Maltz - Distinguished Engineer - Microsoft
Deepak Menon - Partner Director - Microsoft
Dharma Shukla - Technical Fellow - Microsoft
Dominic Williamson - Senior Program Manager - Microsoft
Doug Burger - Technical Fellow - Microsoft
```

Attackers search on LinkedIn to obtain employee details

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

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=*	Looks for profile configuration files (.pcf), which contain user VPN profiles
ext:pcf 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

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

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

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

NETCRAFT

Hostnames matching *.microsoft.com

► Search with another pattern?

First 500 results (showing 41 to 60)

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

<https://www.netcraft.com>

Parrot Terminal

```
-[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.1.google.com
client.1.google.com
clients.1.google.com
gmail-smtp-mas.1.google.com
misc-anycast.1.google.com
31.google.com
360suite.google.com
clients-2.google.com
Mw1.google.com
aboutme.google.com
```

<https://github.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

```
[+] 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.DouceurJonHowellBryanParnojohnndo
howellparno@microsoft.com
quarantine@messaging.microsoft.com
hicwhql@microsoft.com
ctcwhql@microsoft.com
age3support@microsoft.com
...STOR.WW.00.EN.MSF.RMD.TS.T15.SPT.00.EM@css.one.microsoft.com
pexdata@microsoft.com
brohrer@microsoft.com
rightlicense@microsoft.com
```

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

The screenshot shows the TOR Browser interface. The address bar displays 'https://duckduckgo.com/?ia=web'. The search query 'microsoft' is entered in the search bar. The results page for Microsoft shows the official home page and recent news articles. A sidebar on the right provides detailed information about Microsoft, including its logo, website, description as an American multinational technology company, and links to Wikipedia and financial information. The bottom of the page includes social media icons and a feedback link.

microsoft at DuckDuckGo

microsoft

Web Images Videos News

Microsoft - Official Home Page

Microsoft Corporation is an American multinational technology company with headquarters in Redmond, Washington. It develops, manufactures, licenses, supports and sells computer software, consumer electronics, personal computers, and services. [Wikipedia](#)

Type: Public

Traded as: NASDAQ: msft MSFT, NASDAQ 100 component, DJIA component, S&P 100 component, S&P 500 component

Industry: Computer software, Computer hardware, Consumer electronics, Social networking service, Cloud computing, Video games, Internet, Corporate venture capital

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

The screenshot shows the Shodan search interface with the query "microsoft.com". The results page displays various network services found on the Microsoft website. Key sections include:

- TOTAL RESULTS:** 4,048
- TOP COUNTRIES:** United States (4,222), Brazil (484), China (312), Japan (253), Netherlands (224)
- TOP SERVICES:** SSH (1,541), HTTPS (844), HTTP (434), DNS (388), SMTP (42)
- TOP ORGANIZATIONS:** Microsoft Azure (783), Vivo (315), Verizon Wireless (168), Telmex (74), Amazon.com (68)
- TOP OPERATING SYSTEMS:** Windows 7 or 8 (25)

Below the main results, there is a detailed breakdown of the Microsoft homepage service, including its SSL certificate information and supported SSL versions.

<https://www.shodan.io>

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

The screenshot shows the Censys search interface with the IP address "192.99.7.58" entered. The results page displays the following information:

- Basic Information:** OS: CentOS, Network: OVH (FR), Routing: 192.99.0.0/16 via AS16276, Protocols: 80/HTTP, 22/SSH, 3306/MYSQL.
- 80/HTTP:** A detailed view of the Microsoft homepage service, showing the Apache httpd 2.4.6 server, status 200 OK, and the GET / request.
- 22/SSH:** A detailed view of the SSH service, showing the OpenSSH 7.4 server and banner SSH-2.0-OpenSSH_7.4.

On the right side, there is a map showing the location of the IP address (Montreal, Quebec, Canada) and a sidebar for geographic location settings.

<https://censys.io>

VoIP and VPN Footprinting through SHODAN

SHODAN | VoIP | Explore | Pricing | Enterprise Access

TOTAL RESULTS 385,782

TOP COUNTRIES

Country	Count
Italy	367,499
Germany	5,277
Taiwan	3,671
United States	2,458
Korea, Republic of	652

TOP SERVICES

Service	Count
SIP	568,858
SNMP	4,379
NAS Web Interfaces	3,267
Telnet + SSL	2,329
Telnet	1,374

TOP ORGANIZATIONS

Organization	Count
Wind Telecommunications	211,040
WIND	19,665
Wind Telecommunications SpA	14,544
Infrastrada Italia	7,162
H3G Italy	6,942

TOP OPERATING SYSTEMS

OS	Count
Unix	35
Linux 2.x	12
Linux 2.6.x	9
Windows 8.1	3
Linux 2.4.x	2

TOP PRODUCTS

Product	Count
VoIP	368

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

151.53.38.214
Wind Telecommunications
Added on 2014-05-01 12:10:28 GMT
Italy, Catania

```
 SIP/2.0 404 Not Found
From: <sip:mrnbn@tag>root
To: <sip:mrnbn@tag>tag=115e0-97352d8f-13c4-5586-d8112-5fcad241-d8112
Call-ID: 30000
CSeq: 42 OPTIONS
User-Agent: DLink VoIP Stack
Supported: replaces,timer,100rel
Via: SIP/2.0/UDP nn:replaced+4+,1.189.52.190:20810;branch=foo
Content-Length:...
```

151.55.180.80
Wind Telecommunications
Added on 2014-05-01 12:33:12 GMT
Italy, Cassigrande

```
 SIP/2.0 404 Not Found
From: <sip:mrnbn@tag>root
To: <sip:mrnbn@tag>tag=10e6768-5d841797-13c4-5506-837aa-3f610283-837aa
Call-ID: 30000
CSeq: 42 OPTIONS
User-Agent: DLink VoIP Stack
Supported: replaces,timer,100rel
Via: SIP/2.0/UDP nn:replaced+4+,182.137.190.190:20810;branch=foo
Content-Length:...
```

151.29.5.31
Wind Telecommunications
Added on 2014-05-01 12:37:52 GMT
Italy, Rome

```
 SIP/2.0 404 Not Found
From: <sip:mrnbn@tag>root
To: <sip:mrnbn@tag>tag=55575b-1f251d97-13c4-5506-71542b-2021a335-71542b
Call-ID: 30000
CSeq: 42 OPTIONS
User-Agent: DLink VoIP Stack
Supported: replaces,timer,100rel
Via: SIP/2.0/UDP nn:replaced+4+,182.137.190.190:20810;branch=foo
Content-Length:...
```

151.61.38.144
Wind Telecommunications
Added on 2014-05-01 12:19:00 GMT
Italy, Florence

```
 SIP/2.0 404 Not Found
From: <sip:mrnbn@tag>root
To: <sip:mrnbn@tag>tag=f4608-98283d97-13c4-5586-68bc1-519aFF09-66bc1
Call-ID: 30000
```

SHODAN | VoIP | Explore | Pricing | Enterprise Access

TOTAL RESULTS 7,435,026

RELATED TAGS [VoIP](#)

TOP COUNTRIES

Country	Count
United Kingdom	3,571,862
Japan	364,025
China	774,098
United States	561,700
Germany	253,494

TOP SERVICES

Service	Count
ICP	7,385,857
ICN-NAT-T	79,488
HTTP2	24,743
PPTP	19,809
HTTP	13,159

TOP ORGANIZATIONS

Organization	Count
Chinapac, LLC	104,238,174,237
United Kingdom, London	...

TOP OPERATING SYSTEMS

OS	Count
Windows 8	11,388
Windows Server 2008 R2	1,033
Linux 3.x	852
Linux 2.6.x	80
Linux 2.4-2.6	80

TOP PRODUCTS

Product	Count
Shans Antif	182,717,294
Shans Antif	...
SonicWALL SSL VPN Appliance	153,176,212,203

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

78.234.197.39
Initiator SPI: 7872760377523229
Responder SPI: 7a72760377523229
Next Payload: RESERVED
Version: 2.0
Exchange Type: DOI Specific Use
Flags
Encryption: False
Commit: False
Authentication: False
Message ID: 00000000
Length: 30

VPN (IKE)

Initiator SPI: 206F0003037373333
Responder SPI: 7a72760377523229
Next Payload: RESERVED
Version: 2.0
Exchange Type: DOI Specific Use
Flags
Encryption: False
Commit: False
Authentication: False
Message ID: 00000000
Length: 30

VPN (IKE)

Initiator SPI: T9303164003830771
Responder SPI: 34E174322E367432
Next Payload: RESERVED
Version: 2.0
Exchange Type: DOI Specific Use
Flags
Encryption: False
Commit: False
Authentication: False
Message ID: 00000000
Length: 36

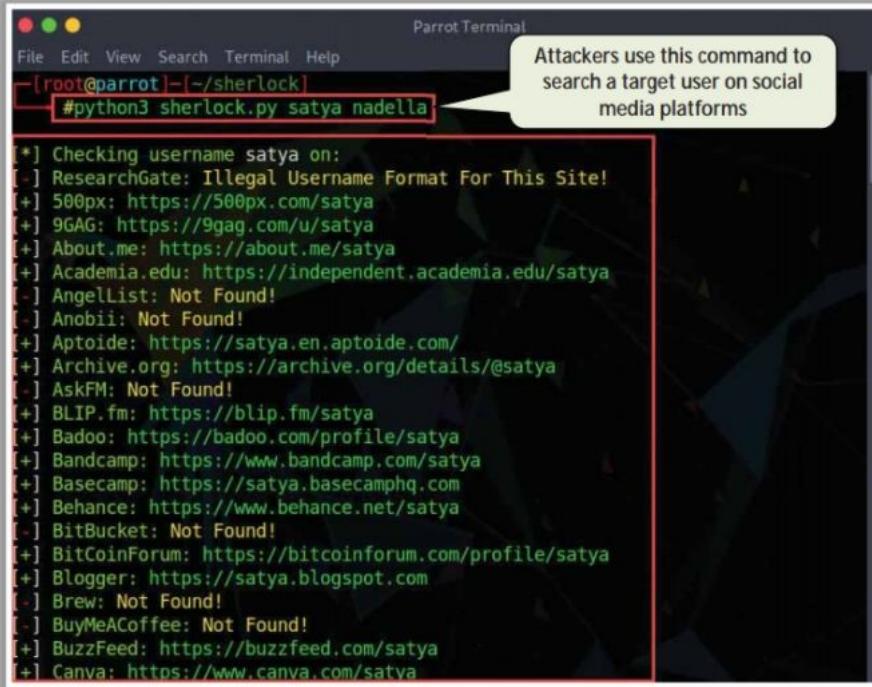
Welcome to VPN Router Configuration Tool
Username: ...

<https://www.shodan.io>

Tools for Footprinting through Social Networking Sites

Sherlock

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



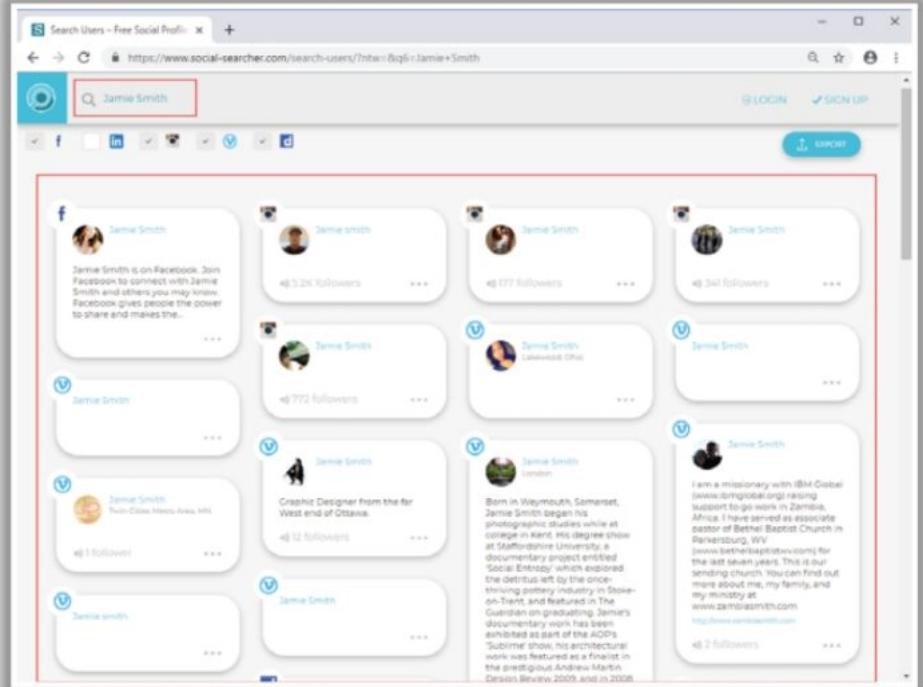
```
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot -]~/sherlock]
#python3 sherlock.py satya nadella

[*] 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
```

<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 a web browser window titled "Search Users - Free Social Profile" with the URL <https://www.social-searcher.com/search-users/?name=&qfli=Jamie+Smith>. The search bar contains "Jamie Smith". Below the search bar, there are icons for different social media platforms: Facebook, LinkedIn, Twitter, YouTube, and others. The main area displays a grid of search results for "Jamie Smith" from various sources. Each result card includes a small profile picture, the name "Jamie Smith", and a brief description. For example, one card says "Jamie Smith is on Facebook. Join Facebook to connect with Jamie Smith and others you may know. Facebook gives people the power to share and makes the..." Another card says "Born in Weymouth, Somerset, Jamie Smith began his photographic studies while at college in Kent. His degree show at Taunton School was a documentary project entitled 'Social Entropy' which explored the structures left by the once-thriving community of Gloucester Town and featured in The Gloucester Guardian on graduating. Jamie's documentary work has been exhibited as part of the AOTS's 'Surreal' exhibition in 2009, and some of his work was featured as a finalist in the prestigious Andrew Martin Design Review 2009, and in 2008..." At the bottom right of the grid, there is a button labeled "EXPORT".

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

Extracting Metadata of Public Documents

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



Metagoofil

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

```
*****
* Metagoofil Ver 2.1 - *
* Christian Martorella   *
* Edge-Security.com      *
* cmartorella_at_edge-security.com *
* Blackhat Arsenal Edition   *
*****  
[-] Starting online search...  
[-] Searching for doc files, with a limit of 200  
      Searching 100 results...  
      Searching 200 results...  
Results: 4 files found  
Starting to download 50 of them:  
-----  
[1/50] /webhp?hl=en  
Error downloading /webhp?hl=en  
[2/50] /intl/en/ads  
Error downloading /intl/en/ads  
[3/50] /services  
Error downloading /services  
[4/50] /intl/en/policies/  
[-] Searching for pdf files, with a limit of 200  
      Searching 100 results...  
      Searching 200 results...  
Results: 34 files found  
Starting to download 50 of them:
```

Tracking Email Communications

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



Collecting Information from Email Header

Delivered-To: [REDACTED]@gmail.com
Received: by 2002:a8a:a99:0:0:0:0:0 with SMTP
Sun, 9 Jun 2019 21:09:48 -0700 (PDT)
Return-Path: <[REDACTED]@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
by mx.google.com with SMTPS id v17sor28
for <[REDACTED]@gmail.com>
(Google Transport Security);
Sun, 09 Jun 2019 21:09:48 -0700 (PDT)
Received-SPF: pass (google.com: domain of [REDACTED]@gmail.com designates 209.85.220.41 as
permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
dkim=pass header.i=@gmail.com header.s=20161025 header.b=s6SMnvzN;
spf=pass (google.com: domain of [REDACTED]@gmail.com designates 209.85.220.41 as
permitted sender) smtp.mailfrom=[REDACTED]@gmail.com;
dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
DKIM-Signature: v=1; a=rsa-sha256; c=nolay/nolay;
d=gmail.com; s=20161025;
h=mime-version:from:date:message-id:subject:to;
bh=nheQC6dgq1LhKwkOykBx4gYw0VwtRRaK2KrErWhvfCg=;
b=s6SMnvzNwAeedUZF5r7LGPdGSiUyxSKDxvLIBGhvEc/pIIqx8KkNR2JGFOMPvxAL
e7630+SPbK+M54CPx9hkvdbYhbCvgUZFuEvp3J/fPvIliT7Blf8jGXWqvvxwQhTH4+/g
XeIE0g6h98SYL4lvePj8I9hw1xvjym8QYRoCgEqWE8JVRfqmNcOxBa6yoxxuOVIJRT0A
aFdUZ53KJMlbG8gBU6hS+bHrr3no370YJgLlh/YwkLTx76h7BgDYBzHcyg+ZPA+HvK5K
3BhvrqeavGeZh6xa56Lnmh7CIuuxa/skSls1pfsK1qeCAV0Cq134JC292HRn2
YCXw==
MIME-Version: 1.0
From: [REDACTED] <[REDACTED]@gmail.com>
Date: Mon, 10 Jun 2019 09:39:37 +0530
Message-ID: <CA++=zy1VzQ1gFmUDByZzqE90SbjwFYk/jc...>
Subject: Check Out Daily News Feed
To: [REDACTED]@gmail.com

The address from which the message was sent

Date and time received by the originator's email servers

Sender's IP address

Sender's mail server

Authentication system used by sender's mail server

Sender's full name

Date and time of message sent

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

Registrant	PERFECT PRIVACY, LLC
Registrant Country	us
Registrar	NETWORK SOLUTIONS, LLC. Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com abuse@web.com (p) 18003337680
Registrar Status	clientTransferProhibited, clientTransferProhibited
Dates	6,160 days old Created on 2002-07-29 Expires on 2021-07-29 Updated on 2018-08-22
Name Servers	NS1.BLUEHOST.COM (has 2,477,906 domains) NS1.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains)
Tech Contact	PERFECT PRIVACY, LLC 12808 Gran Bay Parkway West, Jacksonville, FL, 32258, us wf6599s4d9@networksolutionsprivateregistration.com (p) 15707088780
IP Address	162.241.216.11 - 1,025 other sites hosted on this server
IP Location	■ - Utah - Provo - Unified Layer
ASN	■ AS46606 UNIFIEDLAYER-AS-1 - Unified Layer, US (registered Oct 24, 2008)
Domain Status	Registered And Active Website
IP History	13 changes on 13 unique IP addresses over 13 years
Registrar History	3 registrars with 2 drops
Hosting History	6 changes on 4 unique name servers over 16 years
	http://whois.domaintools.com

SmartWhois - Evaluation Version

File Query Edit View Settings Help

IP, host or domain: certifiedhacker.com

certifiedhacker.com

certifiedhacker.com

162.241.216.11

PERFECT PRIVACY, LLC
12808 Gran Bay Parkway West
Jacksonville
FL
32258
United States
Phone: +1.5707088780
wf6599s4d9@networksolutionsprivateregistration.com

PERFECT PRIVACY, LLC
12808 Gran Bay Parkway West
Jacksonville
FL
32258
United States
Phone: +1.5707088780
wf6599s4d9@networksolutionsprivateregistration.com

NS1.BLUEHOST.COM
NS2.BLUEHOST.COM

Alexa Traffic Rank: 3,258,426

Created: 2002-07-30T00:32:00Z
Updated: 2018-08-22T09:05:36Z
Expires: 2021-07-30T00:32:00Z
Source: whois.networksolutions.com

Done

certifiedhacker.com - Source

Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2018-08-22T09:05:36Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date: 2021-07-30T00:32:00Z
Registrar: NETWORK SOLUTIONS, LLC.
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited
<https://icann.org/epp#clientTransferProhibited>
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 12808 Gran Bay Parkway West
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32258
Registrant Country: US
Registrant Phone: +1.5707088780
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email:
wf6599s4d9@networksolutionsprivateregistration.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
Admin Organization:
Admin Street: 12808 Gran Bay Parkway West
Admin City: Jacksonville
Admin State/Province: FL

Close

<https://www.tamos.com>

Finding IP Geolocation Information

- IP geolocation helps to identify information, such as country, region/state, city, ZIP/postal code, time zone, **connection speed, ISP (hosting company)**, domain name, IDD country code, area code, mobile carrier, and elevation

- IP geolocation **lookup tools**, such as **IP2Location** and **IP Location Finder**, help to collect IP geolocation information about the target, which in turn helps attackers in **launching social engineering attacks**, such as spamming and phishing



IP2Location

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

Reverse DNS Lookup

- Attackers perform a reverse DNS lookup on IP ranges in an attempt to **locate a DNS PTR record** for those IP addresses
- Attackers use various tools, such as **DNSRecon**, to perform the reverse DNS lookup on the target host
- Attackers can also find the other domains that share the same web server, using tools such as **Reverse IP Domain Check**

The screenshot shows a web-based tool for reverse IP domain checking. At the top, there's a banner for 'you get signal' with a deal about 3X learning and cashback. Below it, the main interface has a header 'Reverse IP Domain Check'. A form asks for a 'Remote Address' (input: www.certifiedhacker.com) and a 'Check' button. The results section displays a green success message: 'Found 7 domains hosted on the same web server as www.certifiedhacker.com (162.241.216.11)'. It lists the following domains:

- bongekile.com
- certifiedhacker.com
- oakoffer.com
- www.liststl.org
- box5331.bluehost.com
- humancarehealth.com
- www.certifiedhacker.com

A sidebar on the left contains links for 'about', 'Note' (mentioning over 100 million domain names), and 'A reverse IP domain check...'. At the bottom, there's a note about shared hosting and a link to 'More about this tool. Set an API Key.'

The terminal window is titled 'Parrot Terminal'. The command entered is '#dnsrecon -r 162.241.216.0-162.241.216.255'. The output shows the results of the reverse DNS lookup for the specified IP range, listing PTR records for various domains:

- PTR 162-241-216-5.unifiedlayer.com 162.241.216.5
- PTR 162-241-216-1.unifiedlayer.com 162.241.216.1
- PTR 162-241-216-0.unifiedlayer.com 162.241.216.0
- PTR 162-241-216-7.unifiedlayer.com 162.241.216.7
- PTR 162-241-216-4.unifiedlayer.com 162.241.216.4
- PTR 162-241-216-6.unifiedlayer.com 162.241.216.6
- PTR 162-241-216-8.unifiedlayer.com 162.241.216.8
- PTR 162-241-216-2.unifiedlayer.com 162.241.216.2
- PTR 162-241-216-3.unifiedlayer.com 162.241.216.3
- PTR 162-241-216-9.unifiedlayer.com 162.241.216.9
- PTR box5331.bluehost.com 162.241.216.11
- PTR box5334.bluehost.com 162.241.216.14
- PTR box5348.bluehost.com 162.241.216.17
- PTR 162-241-216-13.unifiedlayer.com 162.241.216.13
- PTR 162-241-216-15.unifiedlayer.com 162.241.216.15
- PTR 162-241-216-10.unifiedlayer.com 162.241.216.10
- PTR 162-241-216-16.unifiedlayer.com 162.241.216.16
- PTR 162-241-216-12.unifiedlayer.com 162.241.216.12

Footprinting through Social Engineering

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



Social engineers attempt to gather

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



Social engineering techniques include

- Eavesdropping
- Shoulder surfing
- Dumpster diving
- Impersonation



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



DumpsterDiving

- 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.

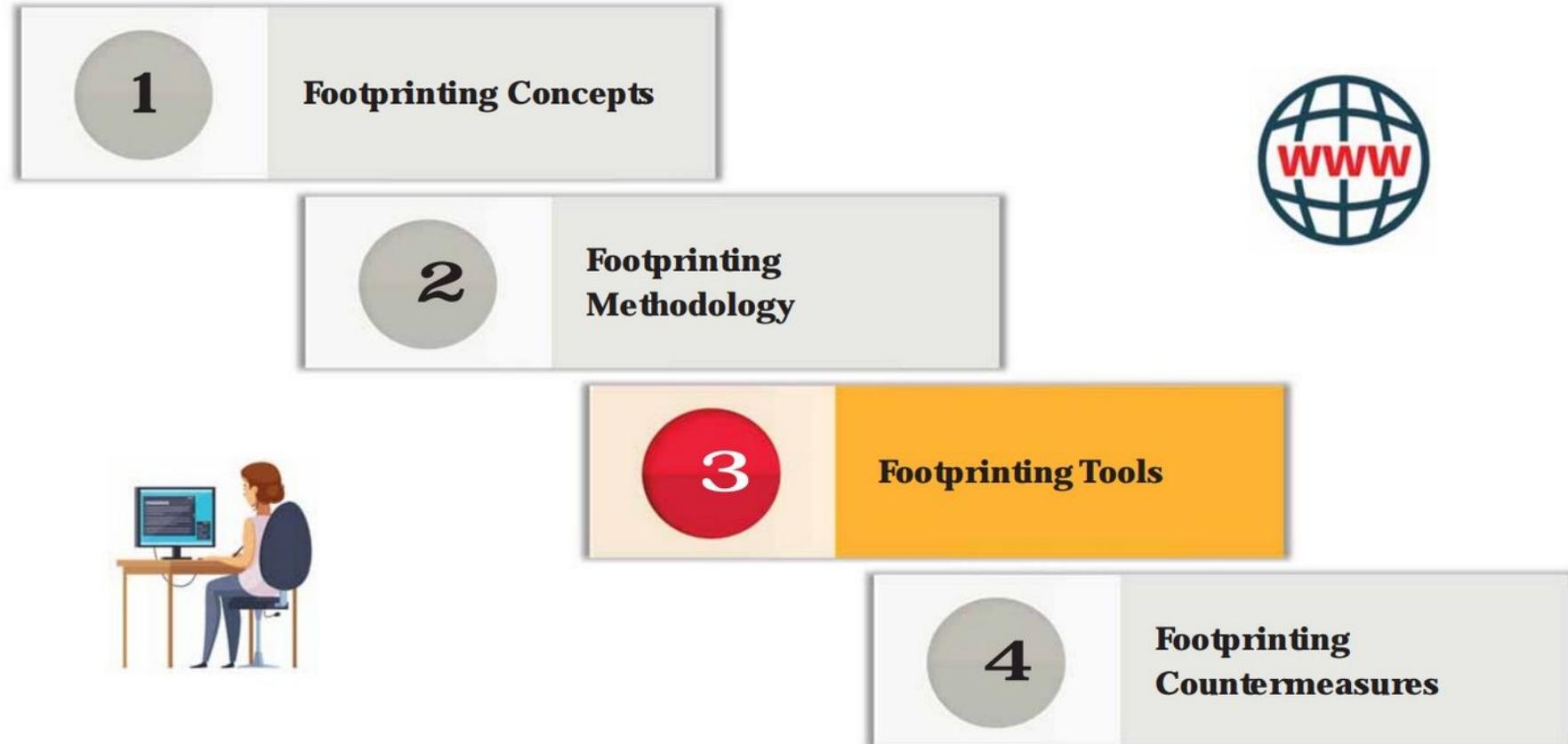


Impersonation

- 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



Module Flow



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.

Community Edition 4.1.6

Entity Palette

- Recently Used
- Person
- Groups
- Company
- Organization
- Infrastructure
- AS
- Banner
- DNS Name

Output - Transform Output

```
Running transform To Email Address [Verify common] on 1
Transform To Email Address [Verify common] returned with 4 entities
```

1 of 5 entities

<https://www.paterva.com>

Recon-ng

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

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

CERTIFIEDHACKER.COM

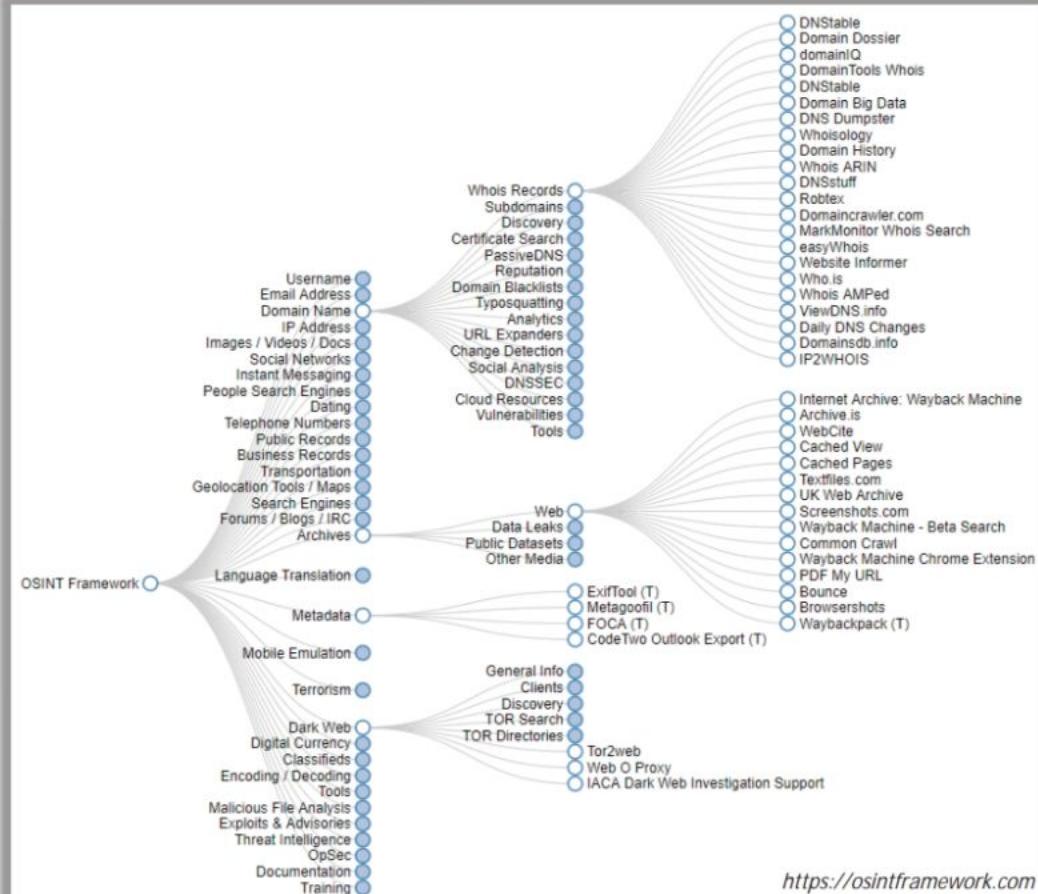
```
[*] [host] soc.certifiedhacker.com (162.241.216.11)
[*] [host] www.soc.certifiedhacker.com (162.241.216.11)
[*] [host] itf.certifiedhacker.com (162.241.216.11)
[*] [host] www.itf.certifiedhacker.com (162.241.216.11)
[*] [host] blog.certifiedhacker.com (162.241.216.11)
[*] [host] www.blog.certifiedhacker.com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

<https://github.com>

Footprinting Tools: OSINT Framework

OSINT Framework

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



Footprinting Tools (Cont'd)

Recon-Dog

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



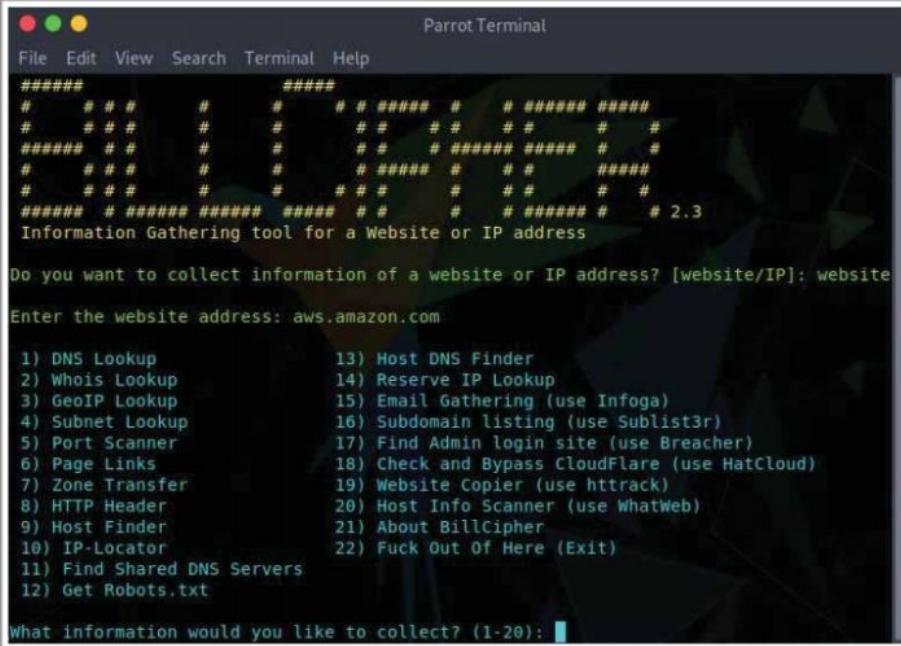
Parrot Terminal
File Edit View Search Terminal Help
root@parrot:~/jvneonblog# python dog

1. Censys
2. NS lookup
3. Port scan
4. Detect CMS
5. Whois lookup
6. Detect honeypot
7. Find subdomains
8. Reverse IP lookup
9. Detect technologies
0. All
#> 5
domain or ip> certifiedhacker.com
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376.DOMAIN.COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2016-03-16T12:30:41Z
Creation Date: 2002-07-30T00:32:00Z
Registry Expiry Date: 2021-07-30T00:32:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/eppClientTransferProhibited
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM

<https://www.github.com>

BillCipher

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



Parrot Terminal
File Edit View Search Terminal Help

2.3
Information Gathering tool for a Website or IP address

Do you want to collect information of a website or IP address? [website/IP]: website

Enter the website address: aws.amazon.com

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

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

<https://github.com>



theHarvester

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



Th3Inspector

<https://github.com>



Raccoon

<https://github.com>



Orb

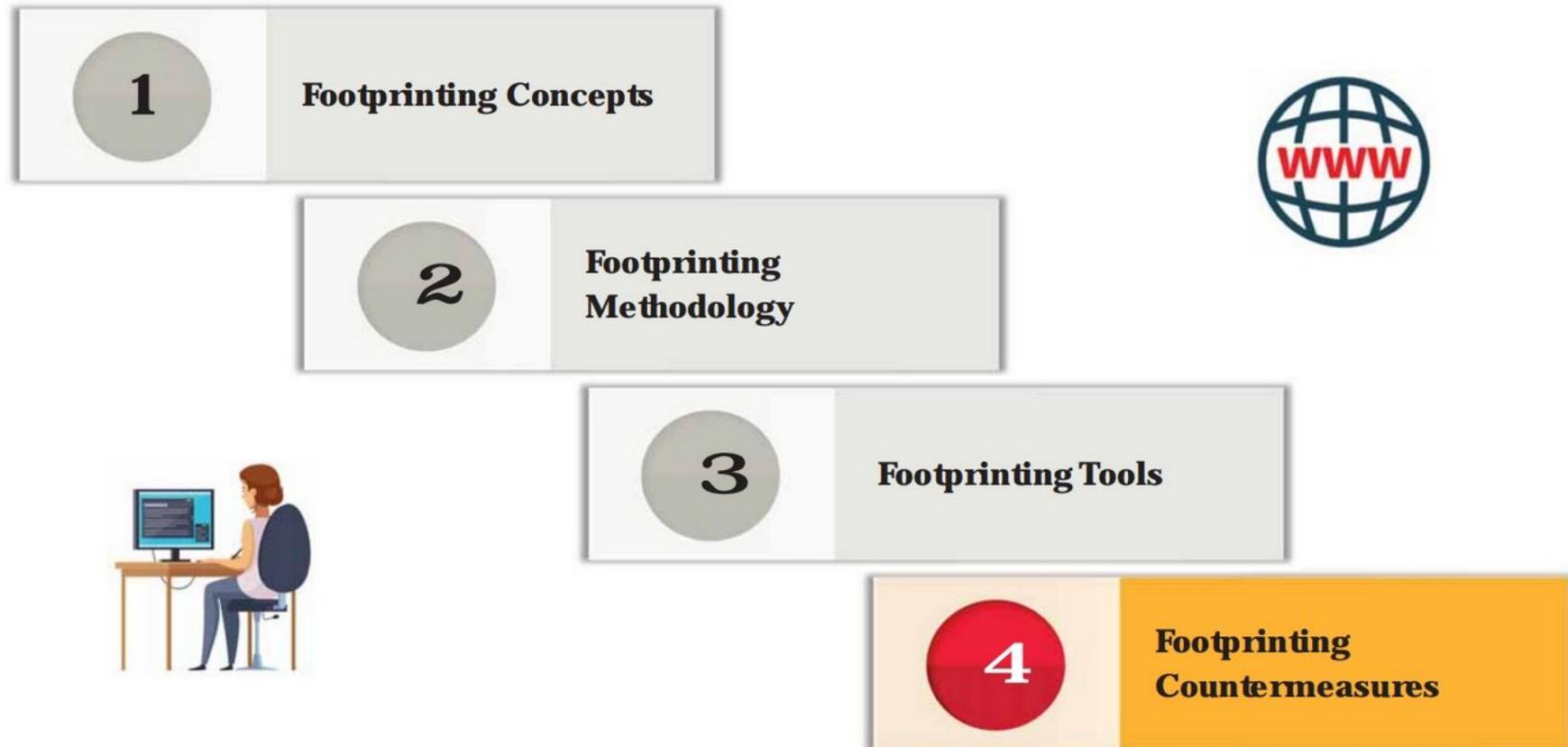
<https://github.com>



PENTMENU

<https://github.com>

Module Flow



Footprinting Countermeasures



Restrict the employees' access to social networking sites from the organization's network



Configure web servers to avoid information leakage



Educate employees to use pseudonyms on blogs, groups, and forums



Do not reveal critical information in press releases, annual reports, product catalogues, etc.



Limit the amount of information published on the website/Internet



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

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 web services, and footprinting through social networking sites
 - Website, email, Whois, and DNS 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