EC-Council

CEH
Certified Ethical Hacker

Module 02

Footprinting and Reconnaissance

Module Flow

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

What is Footprinting?

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

Types of Footprinting

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

Information Obtained in Footprinting

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

Objectives of Footprinting

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

Module Flow

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

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

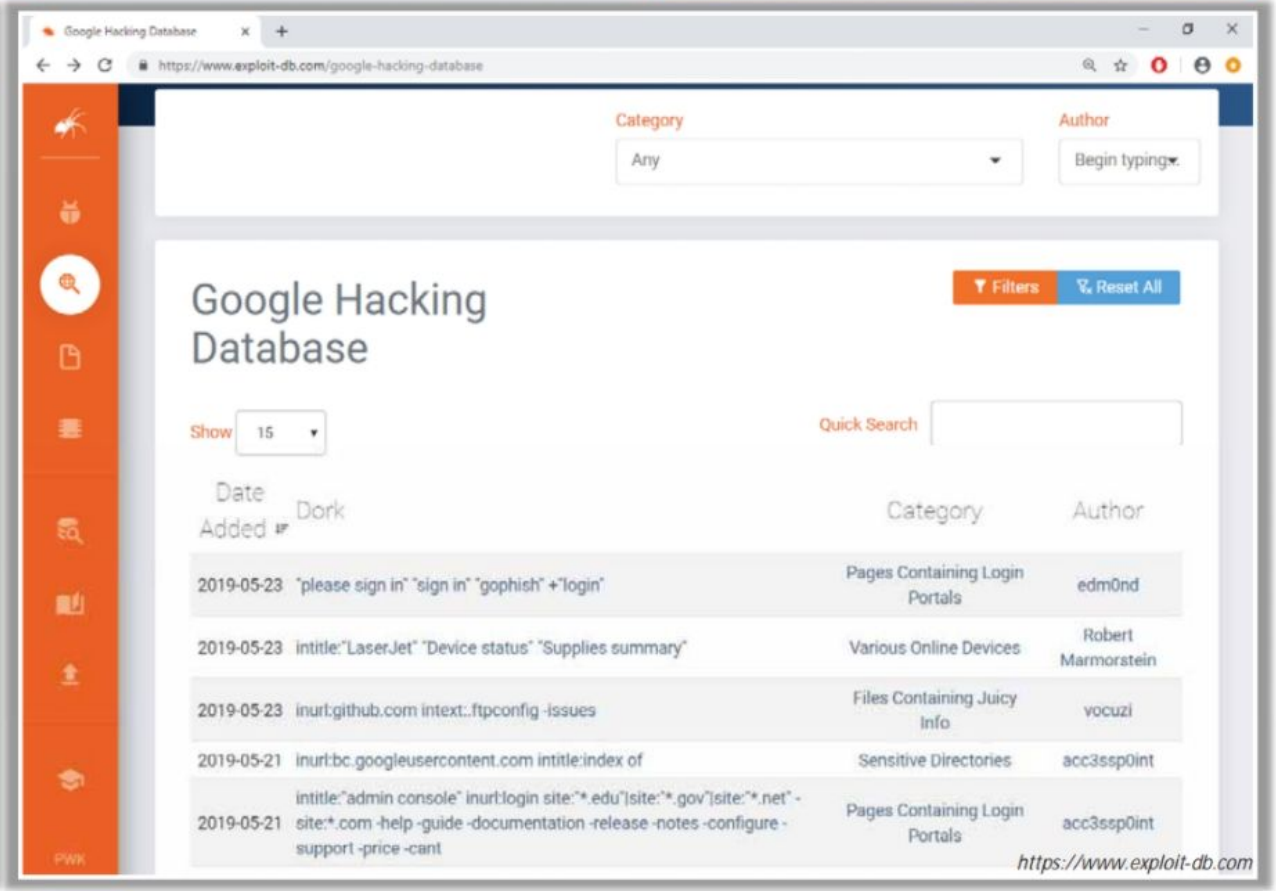
Popular Google advanced search operators

- [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

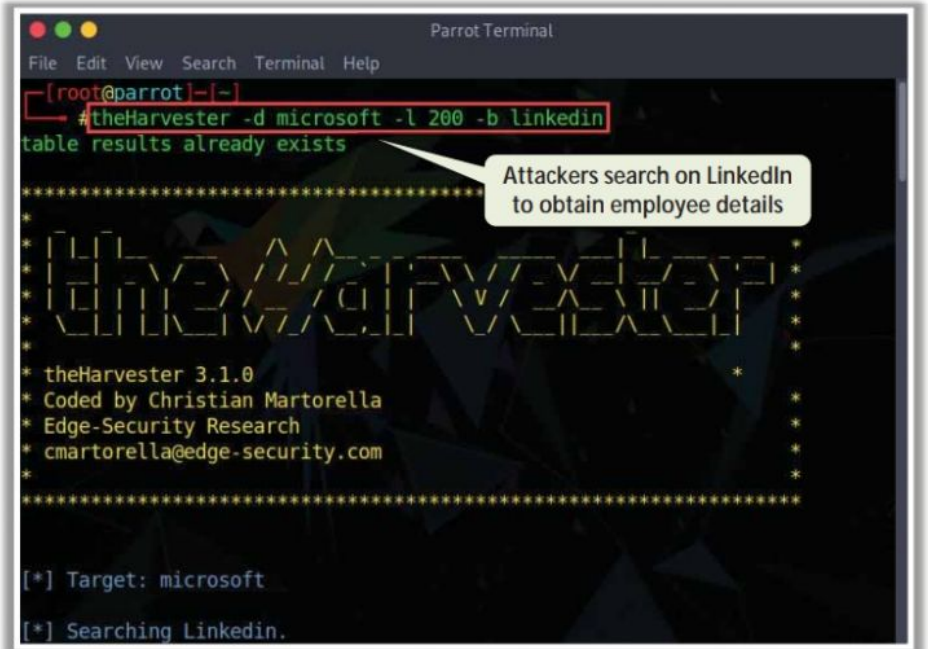
- The Google Hacking Database (GHDB) is an authoritative source for querying the ever-widening reach of the Google search engine
- Attackers use Google dorks in Google advanced search operators to extract sensitive information about their target, such as vulnerable servers, error messages, sensitive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

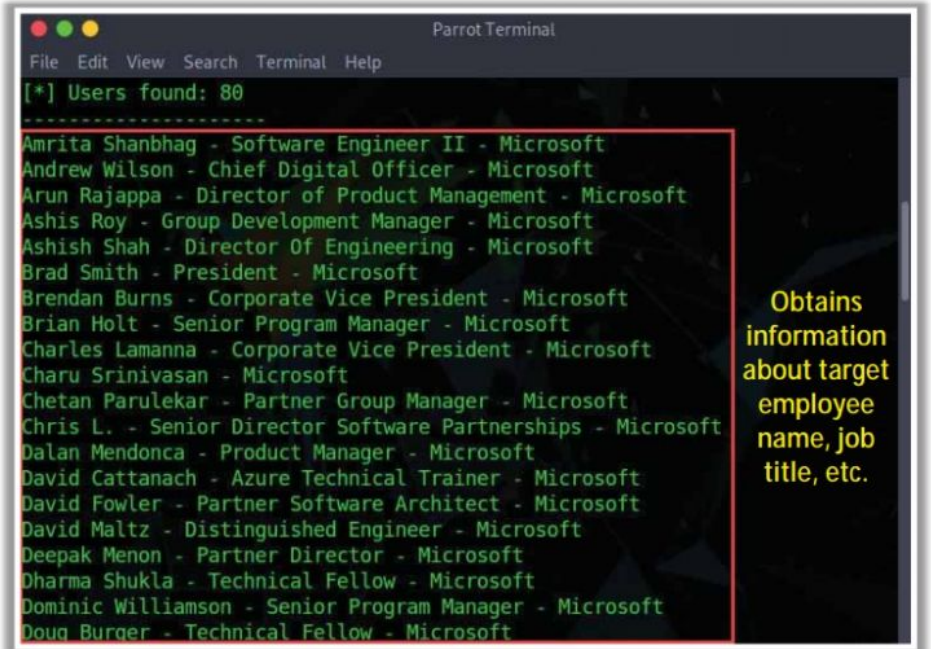
EXPLOIT DATABASE



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





VoIP and VPN Footprinting through Google Hacking Database

Google search queries forVoIP 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 forVPN footprinting

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

https://www.exploit-db.com

Other Techniques for Footprinting through Search Engines (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

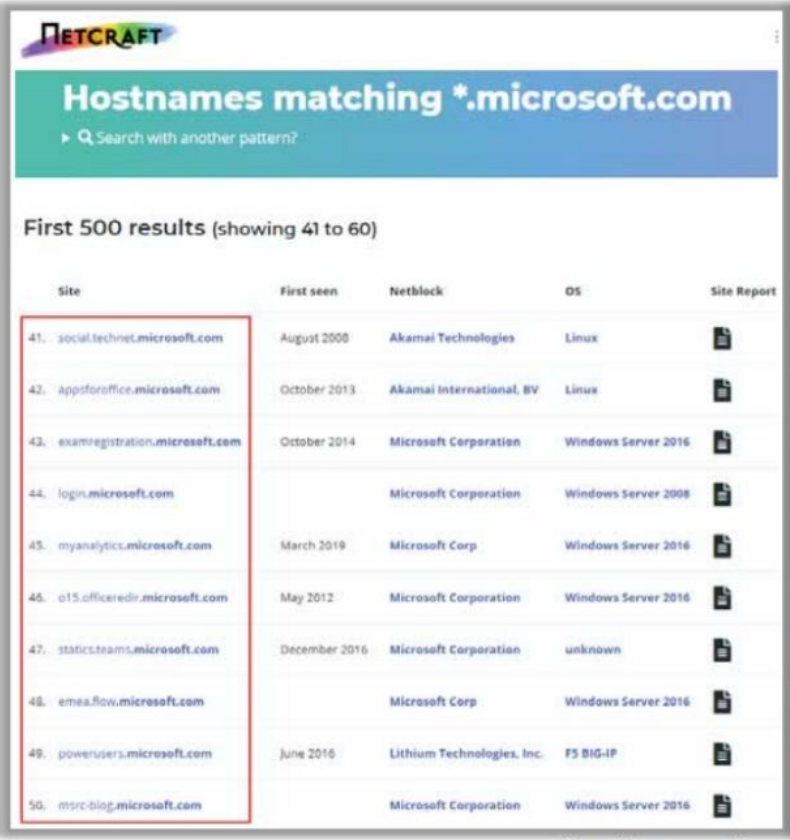
- FTP search engines are used to search for files located on the FTP servers
- Attackers use FTP search engines, such as NAPALM FTP Indexer and Global FTP Search Engine, to retrieve critical files and directories about the target that reveal valuable information, such as business strategy, tax documents,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

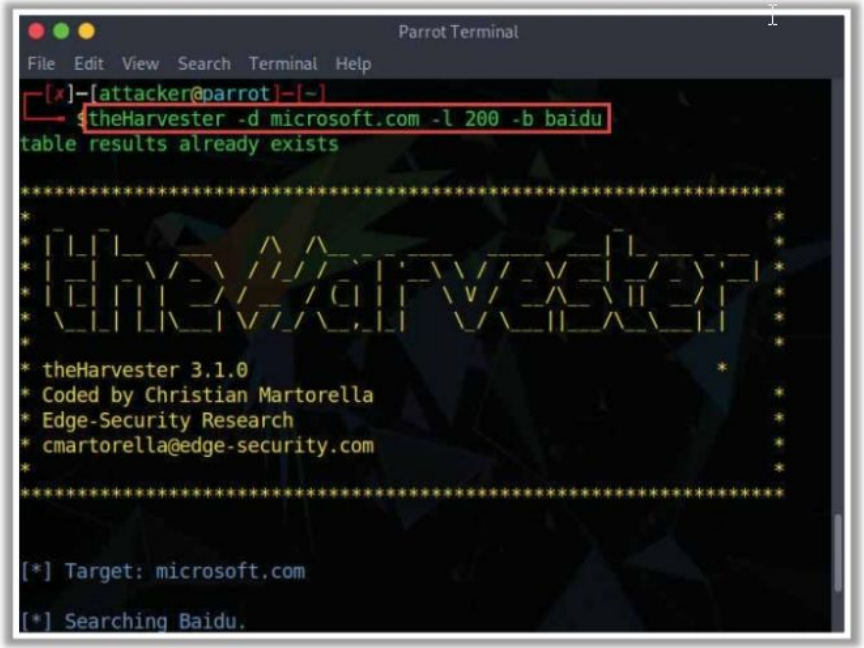


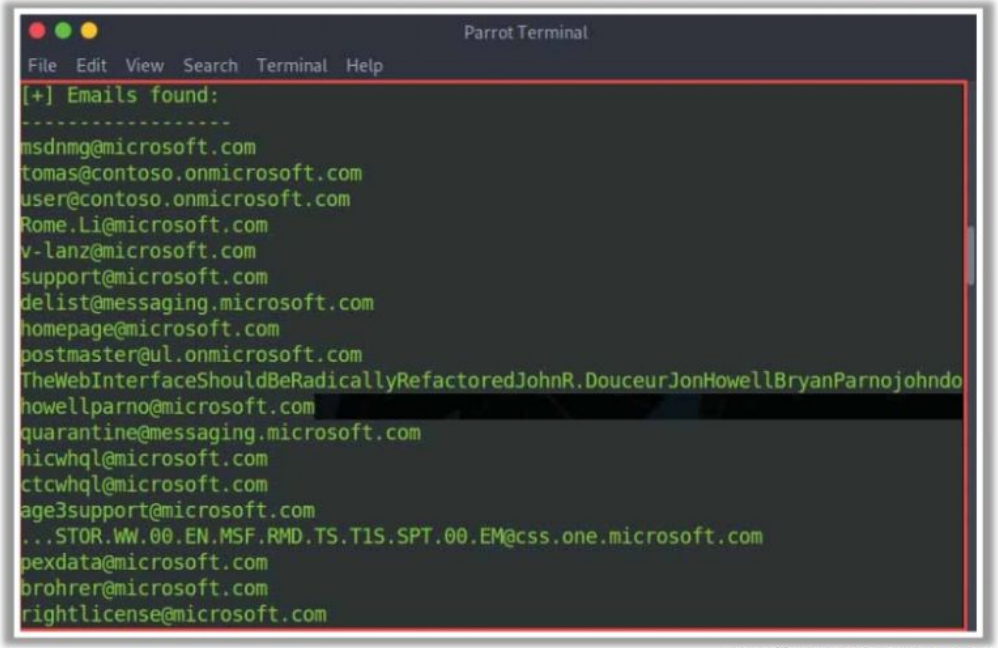
https://www.netcraft.com

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





Deep and Dark Web Footprinting

Deep web

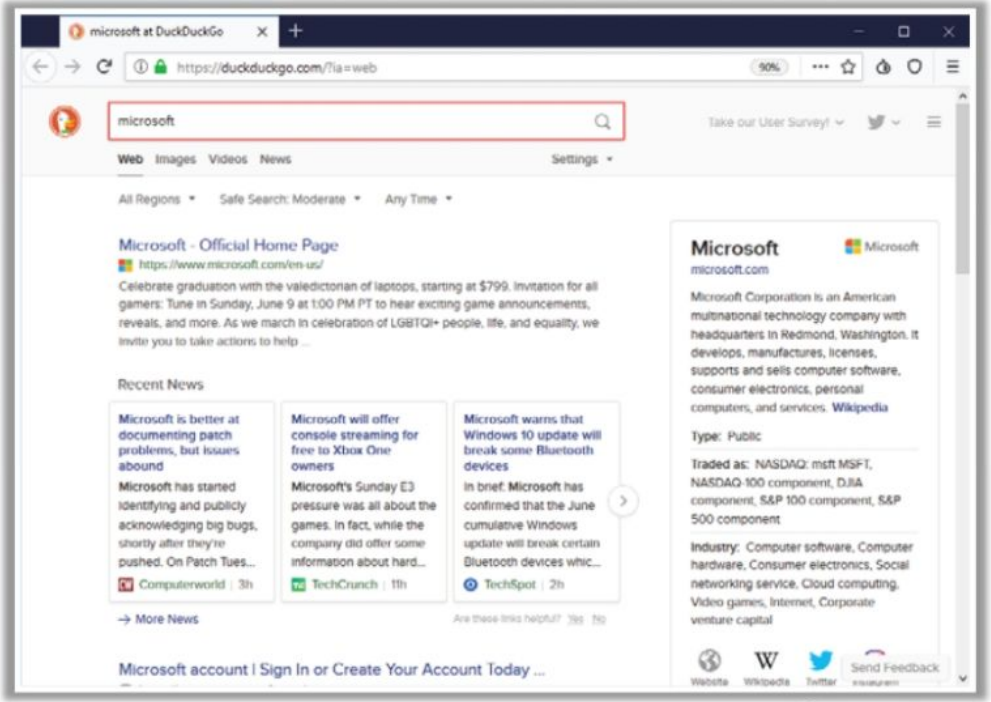
- It consists of web pages and contents that are hidden and unindexed and cannot be located using traditional web browsers and search engines
- It can be accessed by search engines like Tor Browser and The WWW Virtual Library

Dark web or Darknet

- It is the subset of the deep web that enables anyone to navigate anonymously without being traced
- It can be accessed by browsers, such as TOR Browser, Freenet, GNUnet, I2P, and Retroshare

- Attackers use deep and dark web searching tools, such as Tor Browser and ExoneraTor, to gather confidential information about the target, including credit card details, passport information, identification card details, medical records, social media accounts, Social Security Numbers (SSNs), etc.

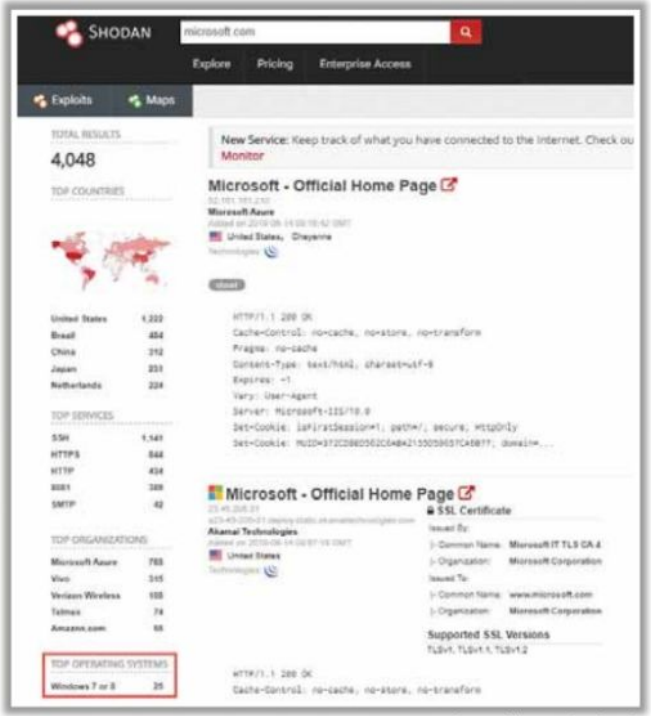
TOR Browser | It is used to access the deep and dark web where it acts as a default VPN for the user and bounces the network IP address through several servers before interacting with the web



https://www.torproject.org

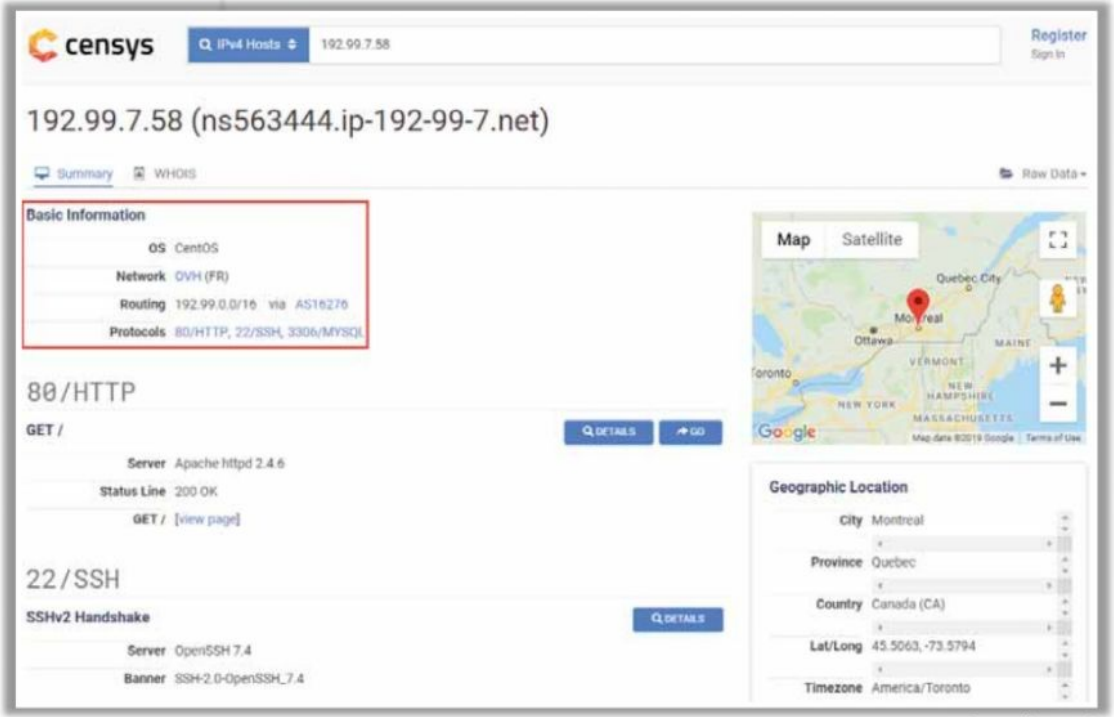
Determining the Operating System

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



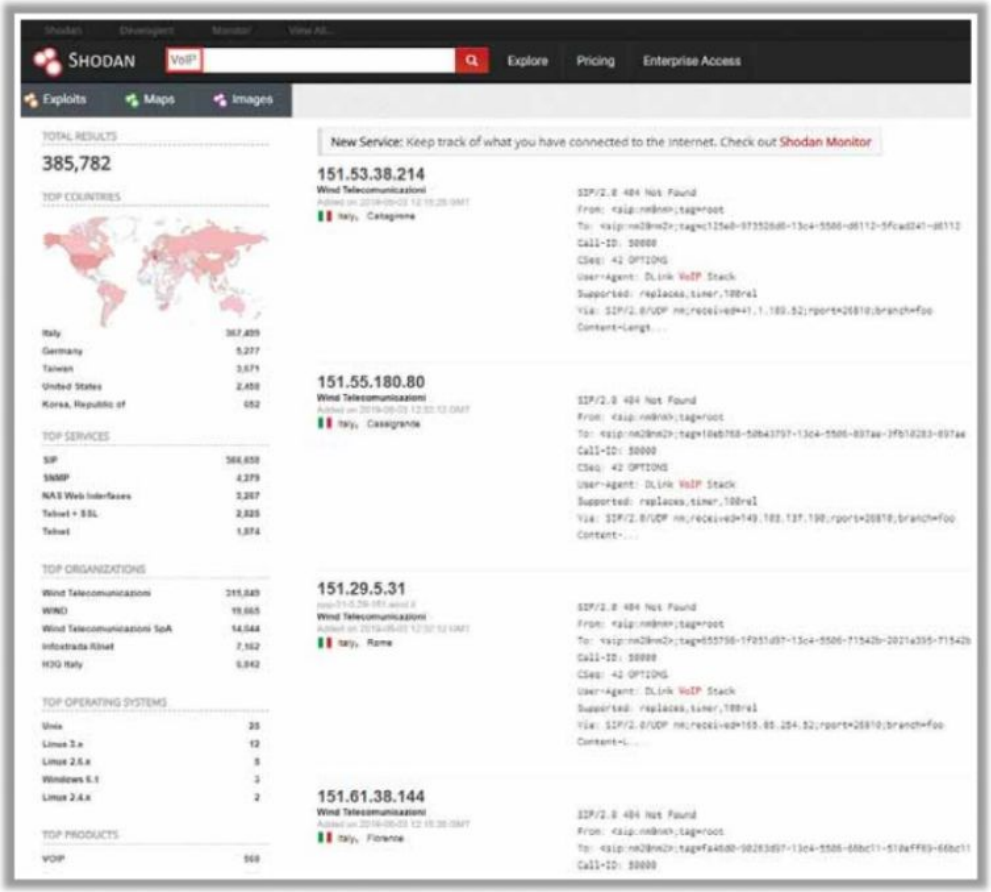
https://www.shodan.io

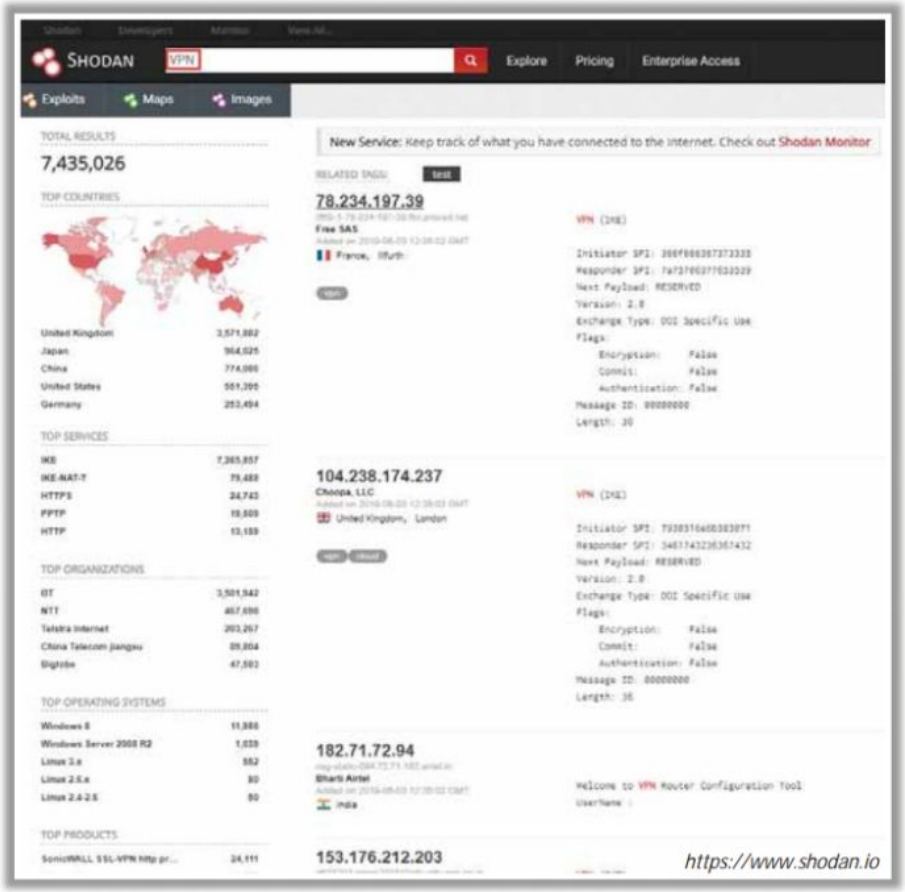
- Censys search engine provides a full view of every server and device exposed to the Internet



https://censys.io

VoIP and VPN Footprinting through SHODAN

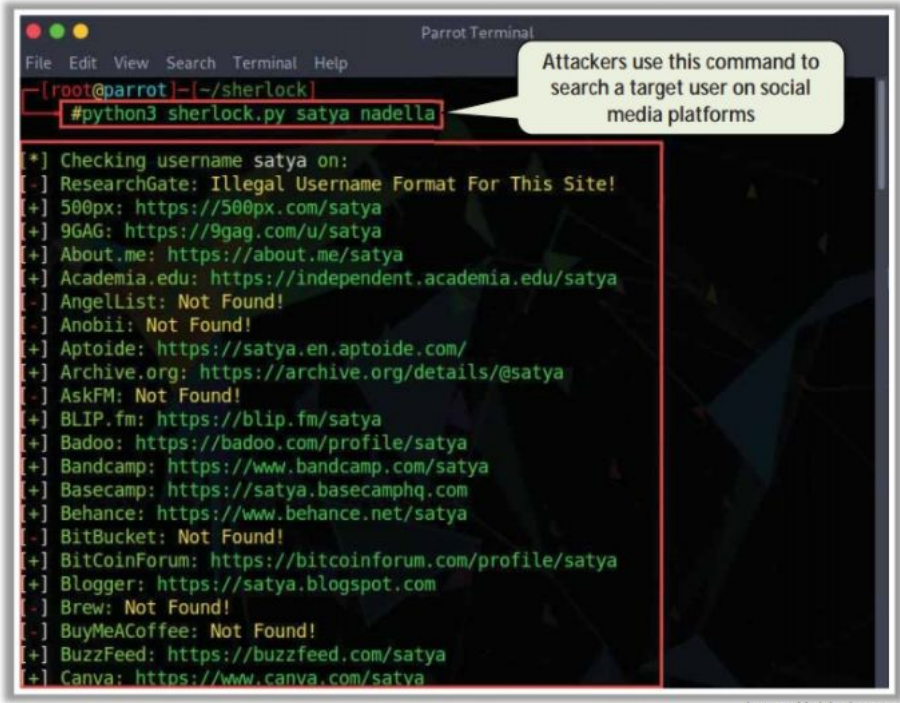




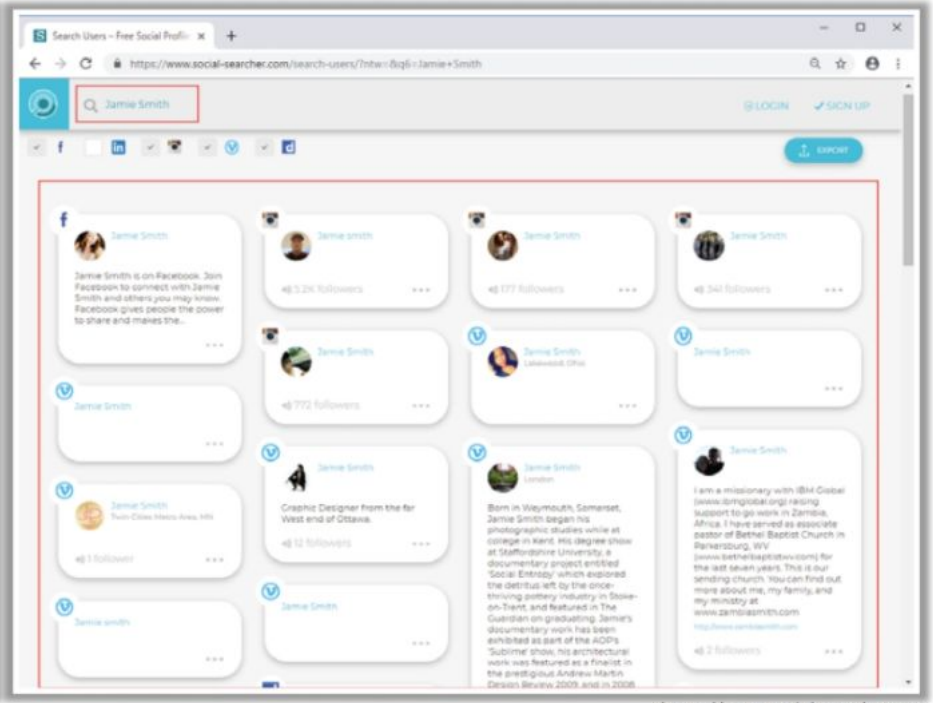
https://www.shodan.io

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



https://github.com



https://www.social-searcher.com

Extracting Metadata of Public Documents

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

Metagoofil

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

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

[-] Starting online search...

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

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

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

https://code.google.com

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

The address from which the message was sent

Date and time received by the originator's email servers

Sender's IP address

Sender's mail server

Authentication system used by sender's mail server

Sender's full name

Date and time of message sent

Whois Lookup

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

Whois query returns

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

Information obtained from Whois database assists an attacker to

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

Regional Internet Registries (RIRs)

ARIN

AFRINIC

RIPE NCC

lacnic

APNIC

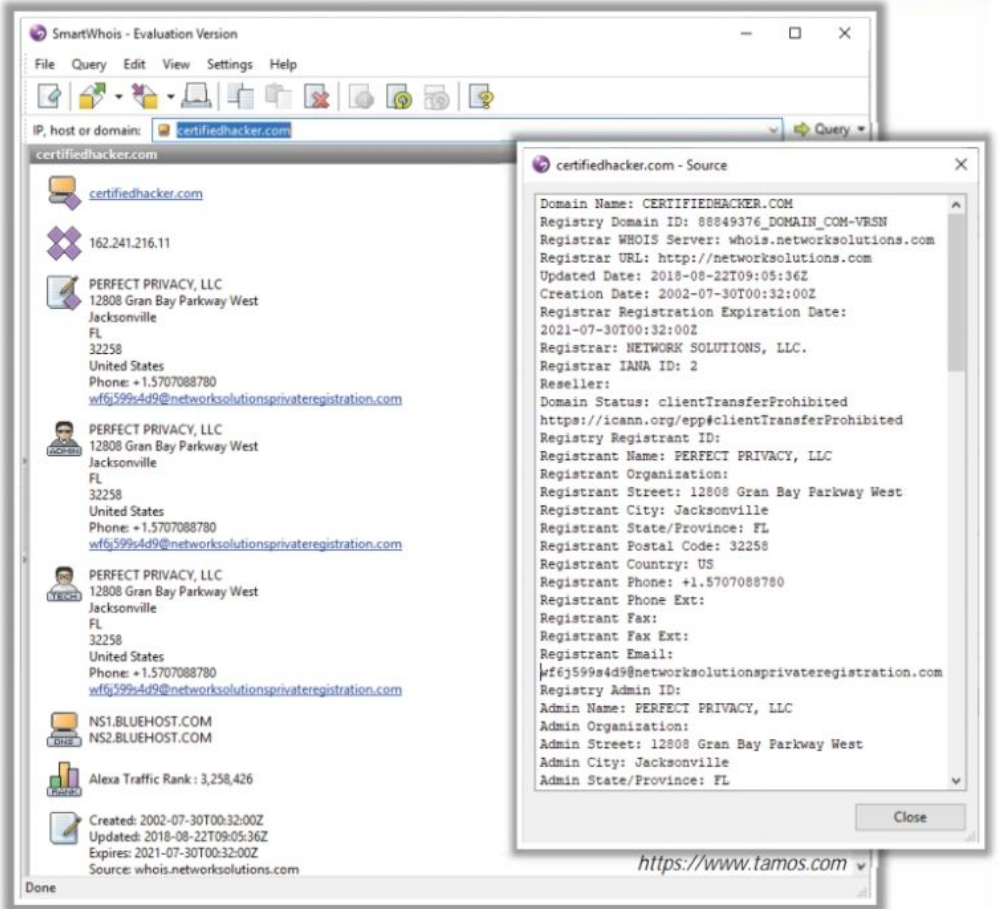
Whois Lookup (Cont'd)

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 wf6j599s4d9@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



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

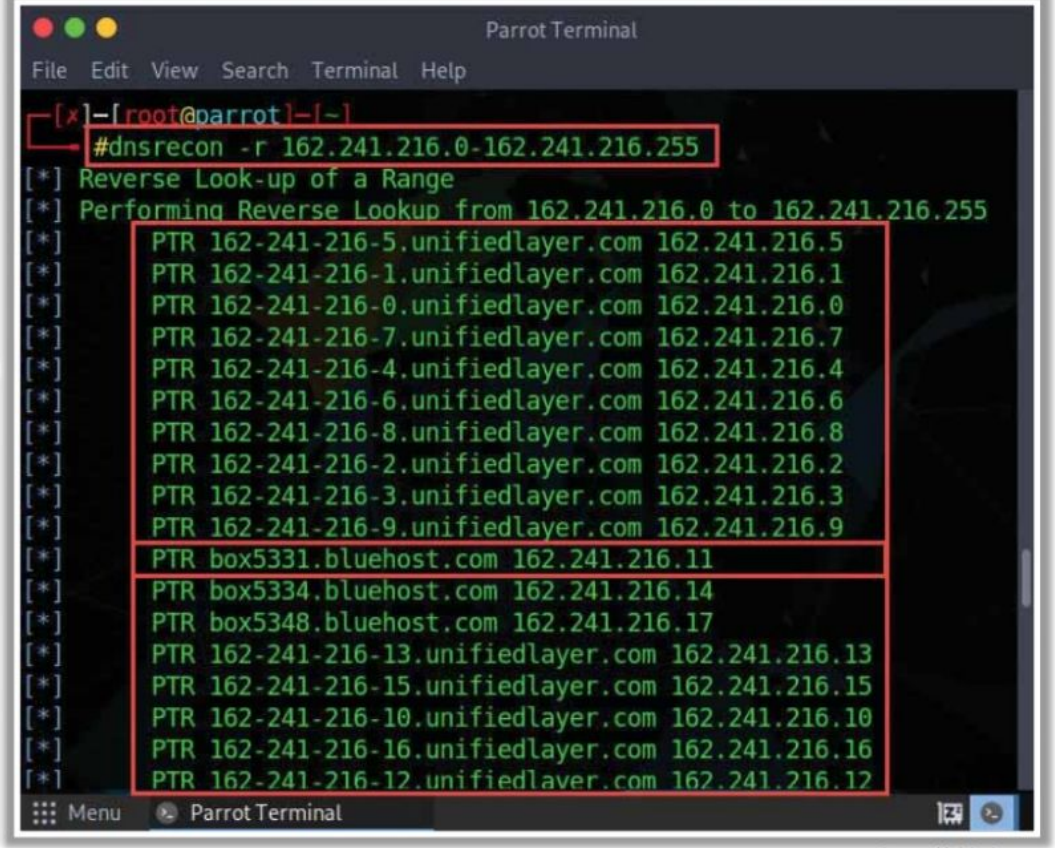
IP Address	207.46.232.182
Country	Singapore [SG]
Region	Singapore
City	Singapore
Coordinates of City	1.289670, 103.850070 (1°17'23"N 103°51'0"E)
ISP	Microsoft Corporation
Local Time	10 Jun, 2019 07:10 PM (UTC +08:00)
Domain	microsoft.com
Net Speed	(COMP) Company/T1
IDD & Area Code	(65) 06
ZIP Code	179431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

https://www.ip2location.com

Reverse DNS Lookup

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

https://www.yougetsignal.com



https://github.com

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

C|EH Certified Ethical Hacker

Eavesdropping

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

ShoulderSurfing

- 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

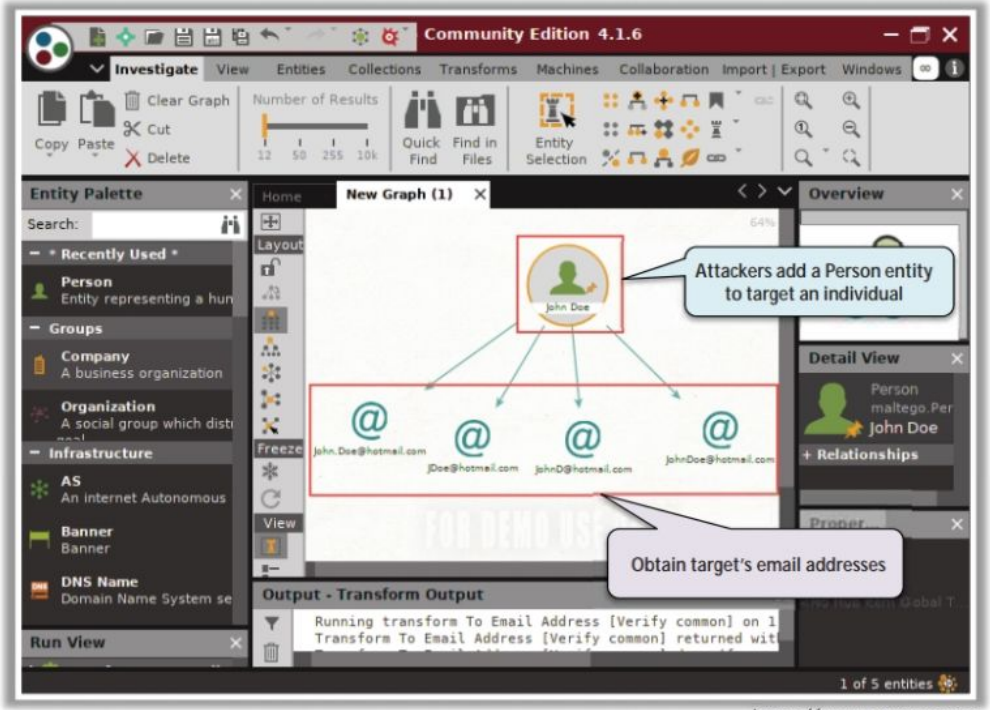
Module Flow

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

Footprinting Tools: Maltego and Recon-ng

Maltego

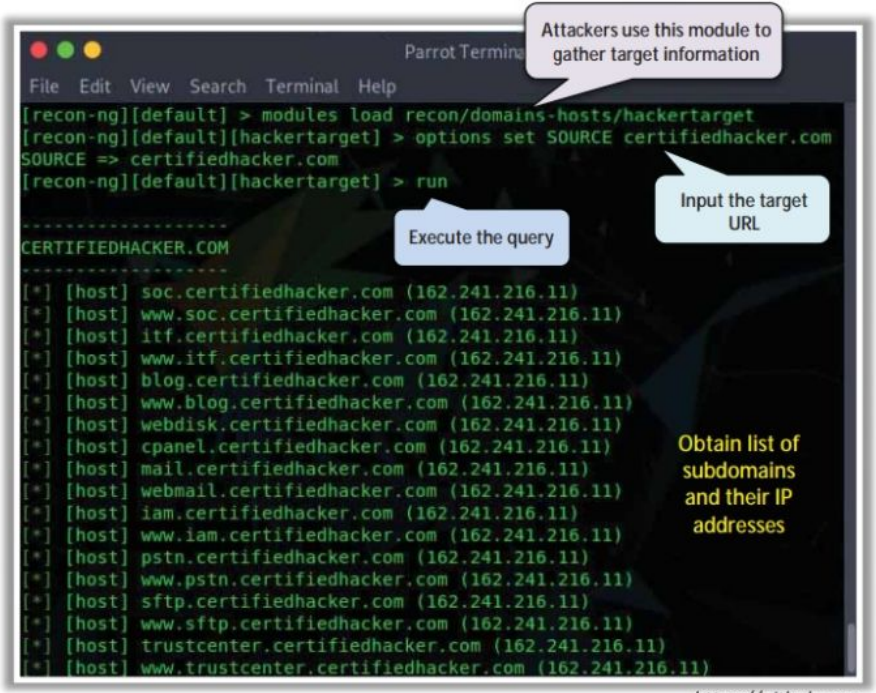
Maltego can be used to determine the relationships and real world links between people, groups of people, organizations, websites, Internet infrastructure, documents, etc.



https://www.paterva.com

Recon-ng

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

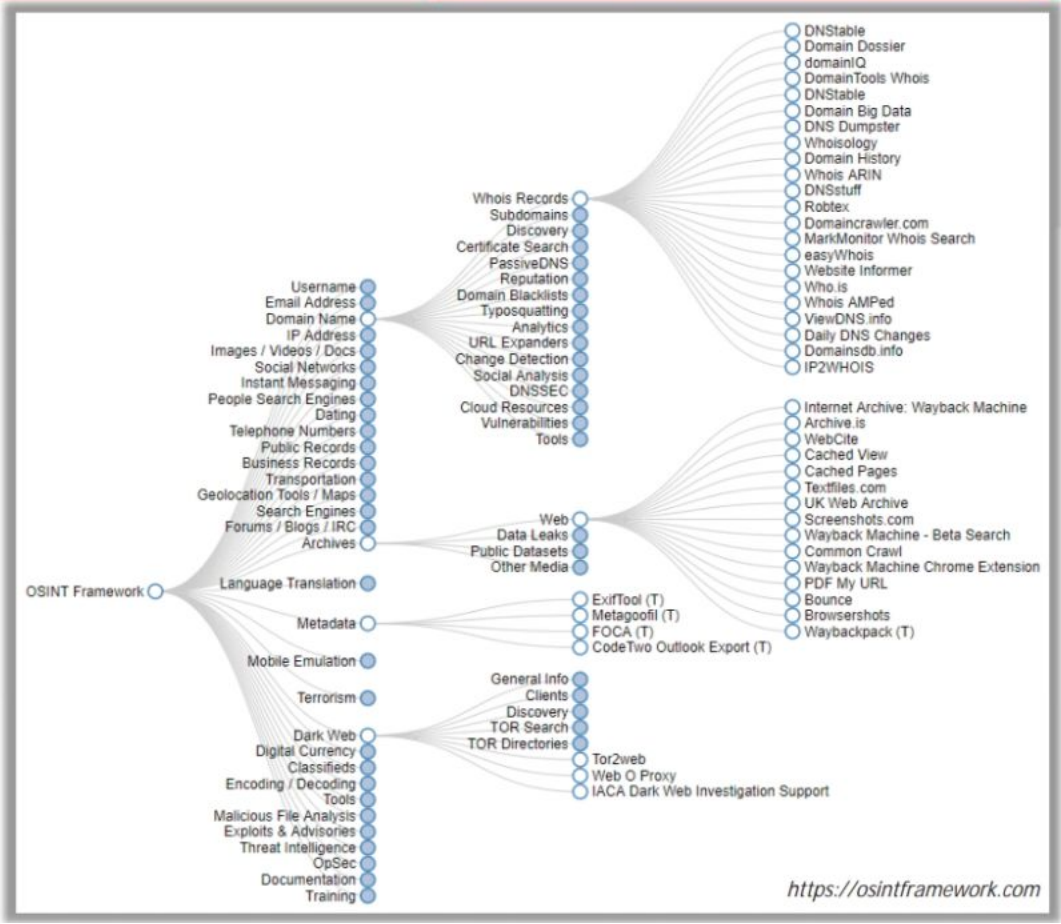


https://github.com

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

https://www.github.com

BillCipher

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

https://github.com

- **theHarvester** — http://www.edge-security.com
- **Th3Inspector** — https://github.com
- **Raccoon** — https://github.com
- **Orb** — https://github.com
- **PENTMENU** — https://github.com

Module Flow

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

Footprinting Countermeasures

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

Configure web servers to avoid information leakage

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

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

Limit the amount of information published on the website/Internet

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

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