Website Footprinting

Website Footprinting

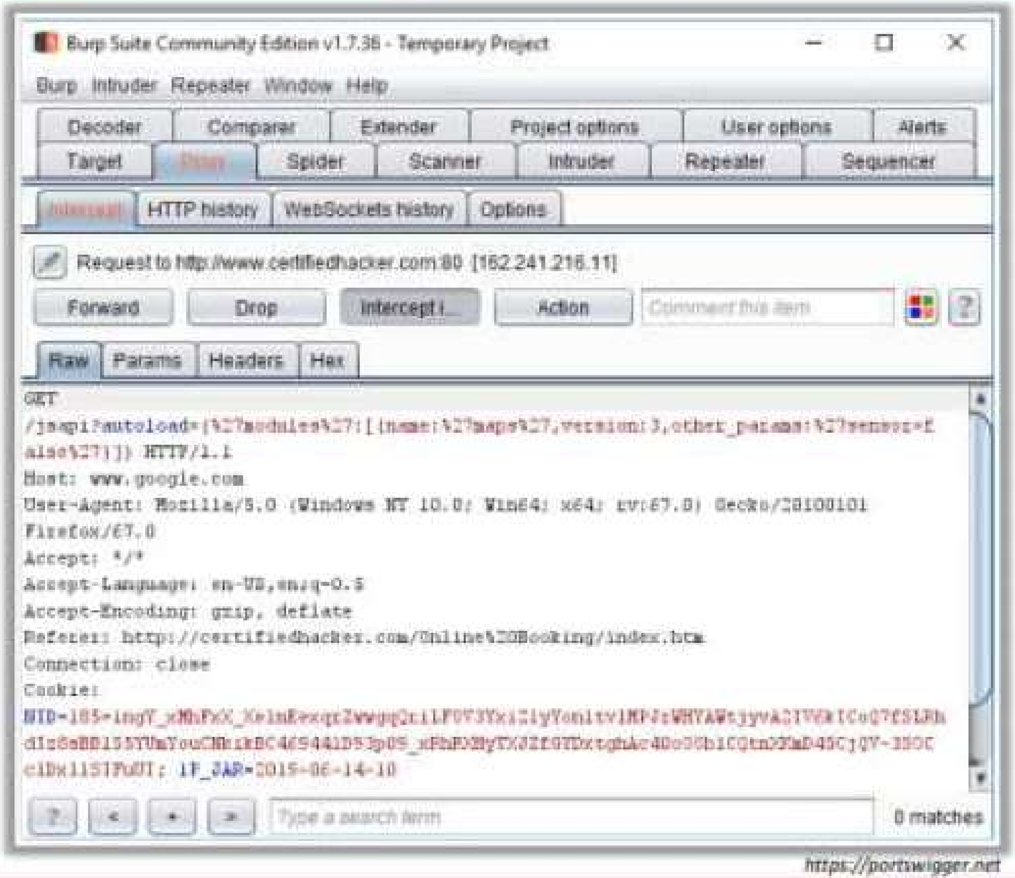
- Website footprinting refers to the **monitoring and analysis of the target organization's website** for information

Browsing the target website may provide the following information:

- Software used and its version
- Operating system used and its scripting platform
- Sub-directories and parameters
- Filename, path, database field name, or query
- Technologies used
- Contact and CMS details

Attackers use **Burp Suite**, **Zaproxy**, **Wappalyzer**, **Website Informer**, etc. to view headers that provide the following information:

- Connection status and content-type
- Accept-Ranges and Last-Modified
- X-Powered-By information
- Web server in use and its version



Request to http://www.certifiedhacker.com:80 [162.241.216.11]

```
GET
/jsapi?autoload={%27modules%27:[{name:%27maps%27,version:3,other_params:%27sensor=f
alse%27}]} HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101
Firefox/67.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://certifiedhacker.com/Online%20Booking/index.htm
Connection: close
Cookie:
NID=185=ingY_xMhFxX_KelnRexqzZwwpgQriLF0V3Yxi1lyYonltv1MPJzWHYAWtjyvA2IVkIC0Q7fSLRh
dIz6eBB155YUmYouCHkikBC4f9441D53p05_xPhFXHyTXJZf0YDxtghAc40o00b1CQtm0KmD45CjQV-350C
c1Dx115TFuUI; 1P_JAR=2015-06-14-10
```

https://portswigger.net

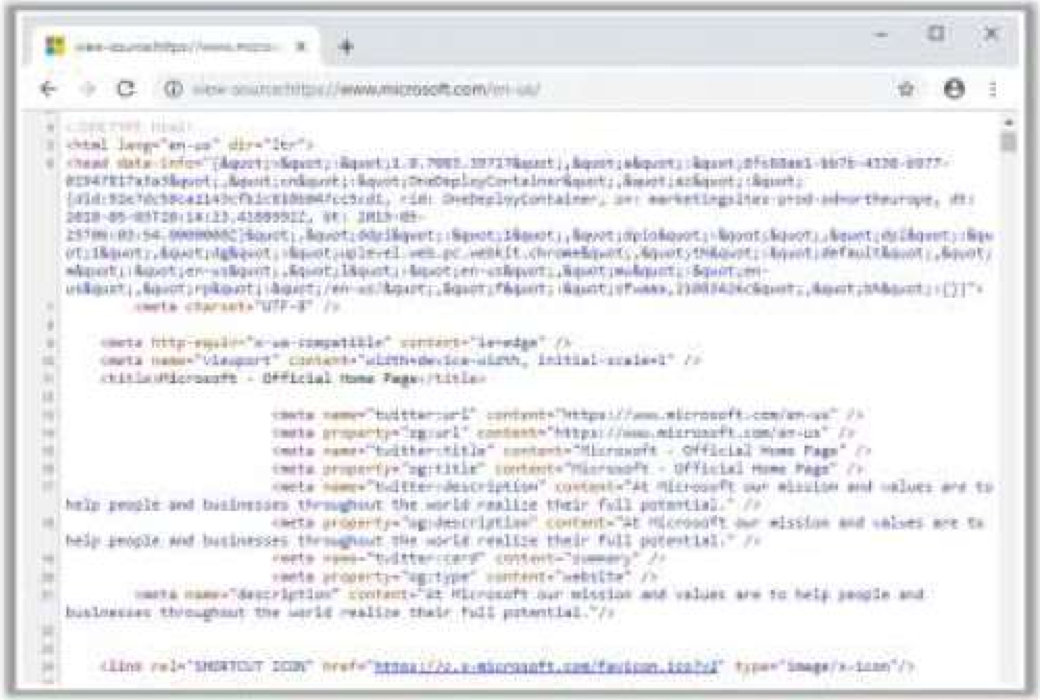
Website Footprinting (Cont'd)

Examining the HTML source code may provide

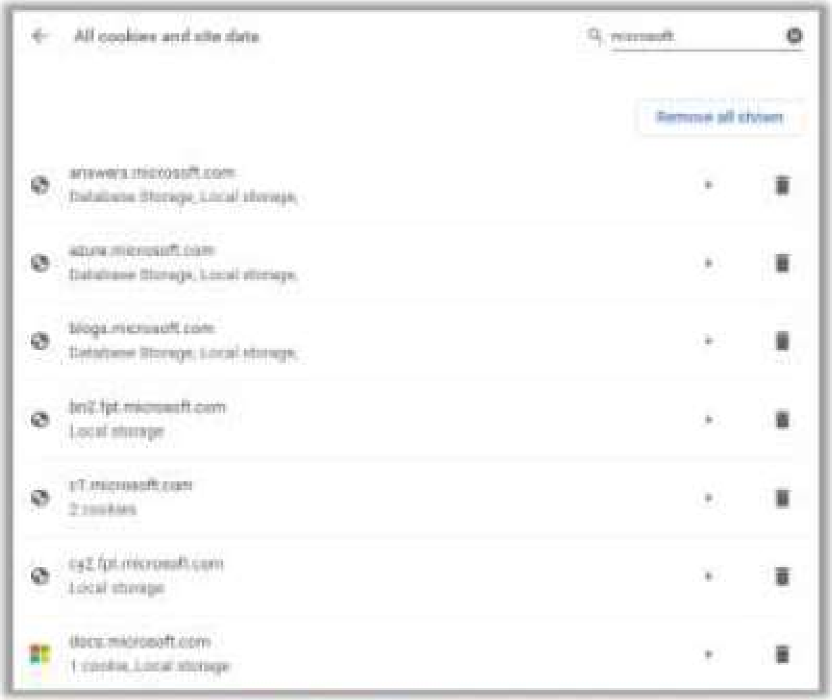
- Comments present in the source code
- Contact details of the web developer or admin
- File system structure and script type

Examining cookies may provide

- Software in use and its behavior
- Scripting platforms used



```
<!DOCTYPE html>
<html lang="en-us" dir="ltr">
<head data-info="{&quot;v&quot;:&quot;1.0.7083.35717&quot;,&quot;a&quot;:&quot;[illegible]
[illegible]
        <meta charset="UTF-8" />

    <meta http-equiv="x-ua-compatible" content="ie=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <title>Microsoft - Official Home Page</title>

                        <meta name="twitter:url" content="https://www.microsoft.com/en-us" />
                        <meta property="og:url" content="https://www.microsoft.com/en-us" />
                        <meta name="twitter:title" content="Microsoft - Official Home Page" />
                        <meta property="og:title" content="Microsoft - Official Home Page" />
                        <meta name="twitter:description" content="At Microsoft our mission and values are to
help people and businesses throughout the world realize their full potential." />
                        <meta property="og:description" content="At Microsoft our mission and values are to
help people and businesses throughout the world realize their full potential." />
                        <meta name="twitter:card" content="summary" />
                        <meta property="og:type" content="website" />
        <meta name="description" content="At Microsoft our mission and values are to help people and
businesses throughout the world realize their full potential."/>


    <link rel="SHORTCUT ICON" href="https://c.s-microsoft.com/favicon.ico?v2" type="image/x-icon"/>
```



answers.microsoft.com
Database Storage, Local storage,

azure.microsoft.com
Database Storage, Local storage,

blogs.microsoft.com
Database Storage, Local storage,

bn2.fpt.microsoft.com
Local storage

c1.microsoft.com
2 cookies

cy2.fpt.microsoft.com
Local storage

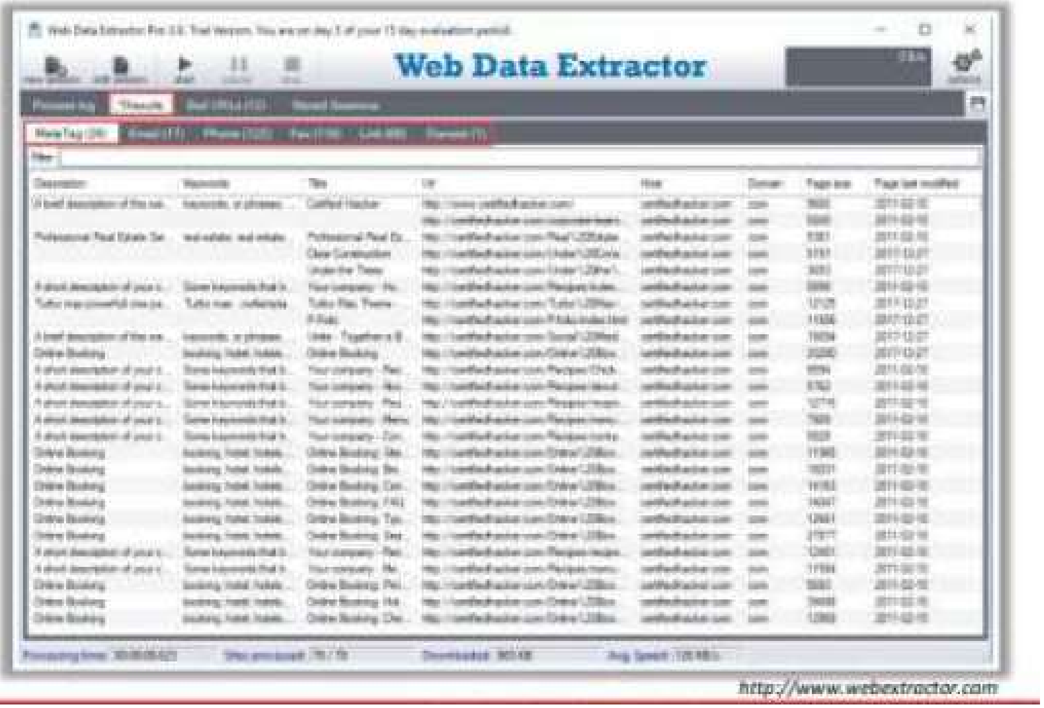
docs.microsoft.com
1 cookie, Local storage

Website Footprinting using Web Spiders

- Web spiders, such as **Web Data Extractor** and **ParseHub**, perform automated searches on the target website and collect specified information, such as **employee names** and **email addresses**
- Attackers use the collected information to perform **footprinting** and **social engineering attacks**

User-Directed Spidering

- Attackers use **standard web browsers** to walk through the target website functionalities
- The incoming and outgoing **traffic of the target website is monitored** and analyzed by tools that include features of both a web spider and an intercepting proxy
- Attackers use tools such as **Burp Suite** and **WebScarab** to perform user-directed spidering

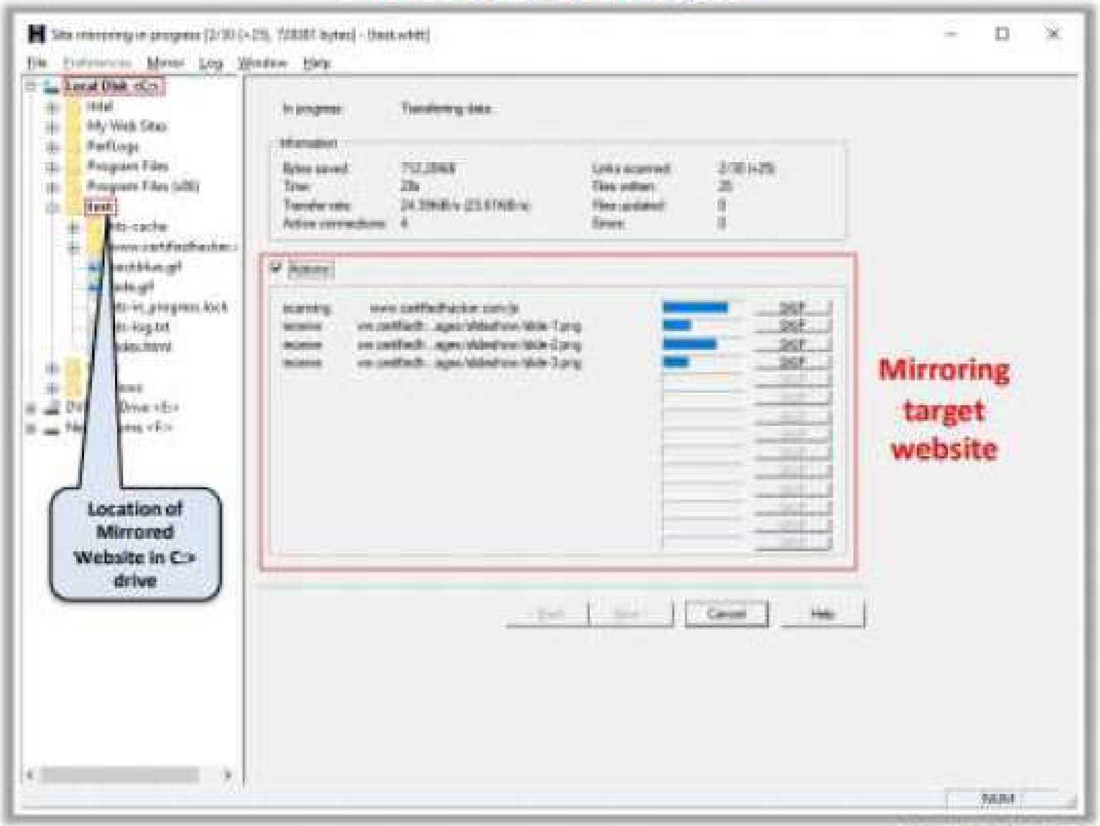


http://www.webextractor.com

Mirroring Entire Website

- Mirroring an entire website onto a local system enables an attacker to browse website offline; it also assists in finding **directory structure** and other valuable information from the mirrored copy without sending multiple requests to web server
- Web mirroring tools, such as HTTrack Web Site Copier, and NCollector Studio, allow you to **download a website to a local directory**, recursively building all directories, HTML, images, flash, videos, and other files from the server to your computer

HTTrack Web Site Copier



Site mirroring in progress [2/30 (+25), 728387 bytes] - [test.whtt]

In progress: Transferring data

Information

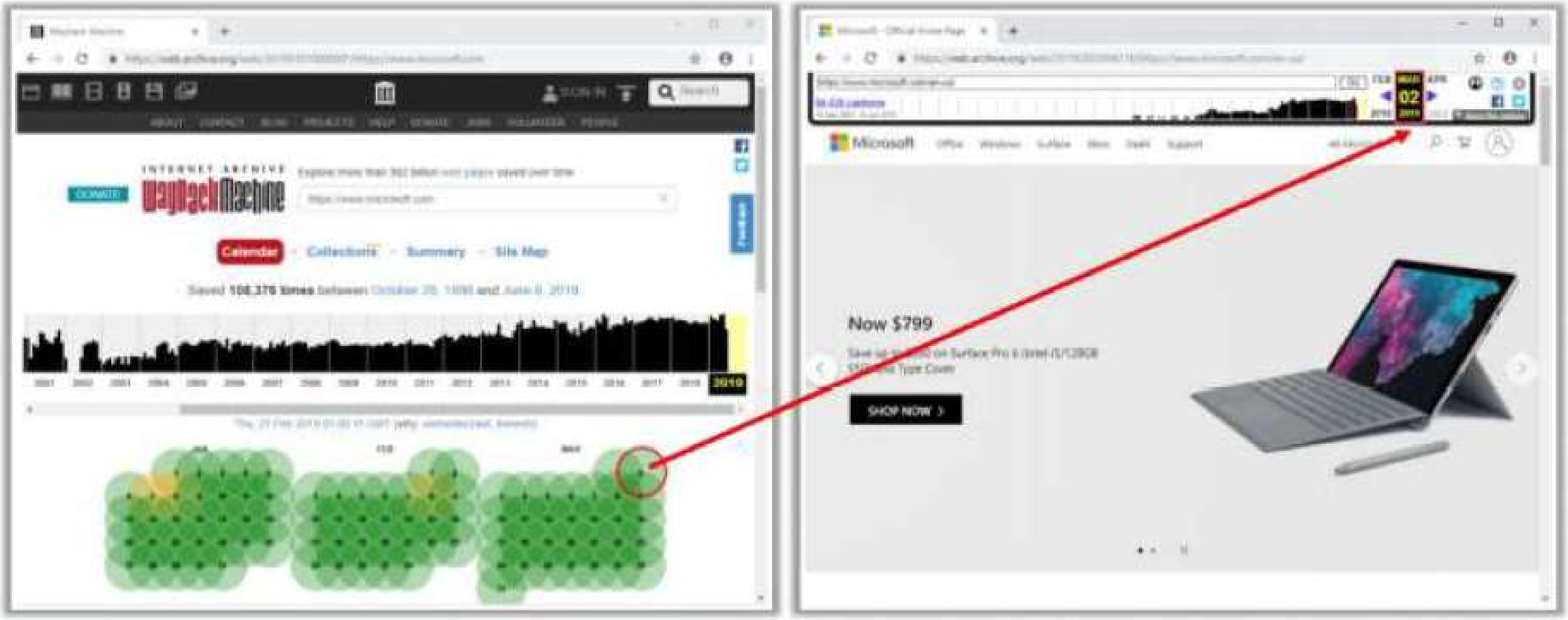
Bytes saved: 712,26KiB Links scanned: 2/30 (+25)
Time: 23s Files written: 25
Transfer rate: 24,39KiB/s (23,67KiB/s) Files updated: 0
Active connections: 4 Errors: 0

scanning www.certifiedhacker.com/js
receive ww.certifiedh...ages/slideshow/slide-1.png
receive ww.certifiedh...ages/slideshow/slide-2.png
receive ww.certifiedh...ages/slideshow/slide-3.png

http://www.httrack.com

Extracting Website Information from https://archive.org

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



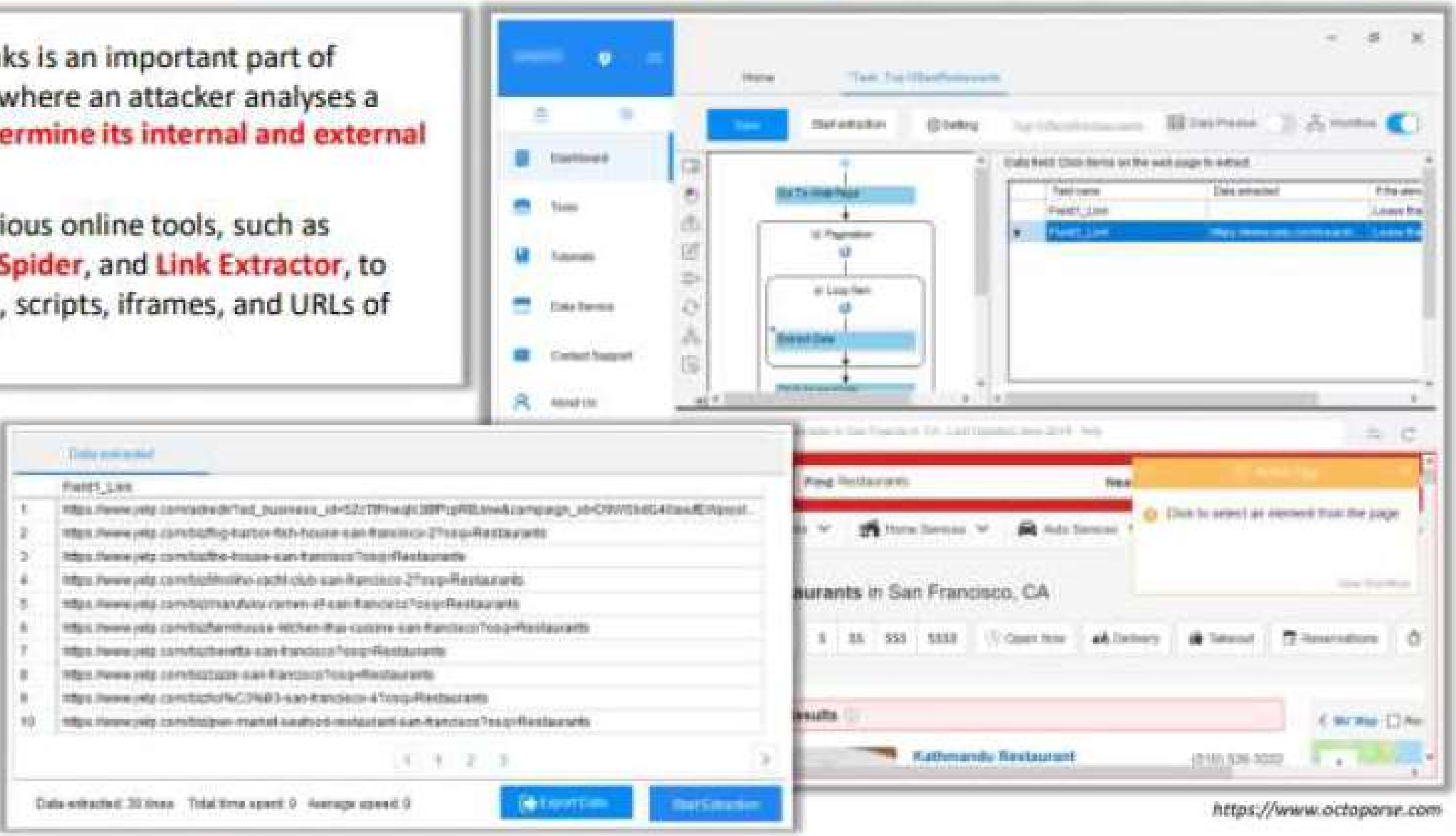
Saved 108,376 times between October 20, 1996 and June 8, 2019

Extracting Website Links

- Extracting website links is an important part of website footprinting where an attacker analyses a target website to **determine its internal and external links**
- Attackers can use various online tools, such as **Octoparse**, **Netpeak Spider**, and **Link Extractor**, to extract linked images, scripts, iframes, and URLs of the target website

Octoparse

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



Data extracted

	Field1_Link
1	https://www.yelp.com/adredir?ad_business_id=[illegible]&campaign_id=[illegible]
2	https://www.yelp.com/biz/fog-harbor-fish-house-san-francisco-2?osq=Restaurants
3	https://www.yelp.com/biz/the-house-san-francisco?osq=Restaurants
4	https://www.yelp.com/biz/[illegible]-yacht-club-san-francisco-2?osq=Restaurants
5	https://www.yelp.com/biz/marufuku-ramen-sf-san-francisco?osq=Restaurants
6	https://www.yelp.com/biz/farmhouse-kitchen-thai-cuisine-san-francisco?osq=Restaurants
7	https://www.yelp.com/biz/beretta-san-francisco?osq=Restaurants
8	https://www.yelp.com/biz/zazie-san-francisco?osq=Restaurants
9	https://www.yelp.com/biz/[illegible]%C3%[illegible]-san-francisco-4?osq=Restaurants
10	https://www.yelp.com/biz/pier-market-seafood-restaurant-san-francisco?osq=Restaurants

‹ 1 2 3 ›

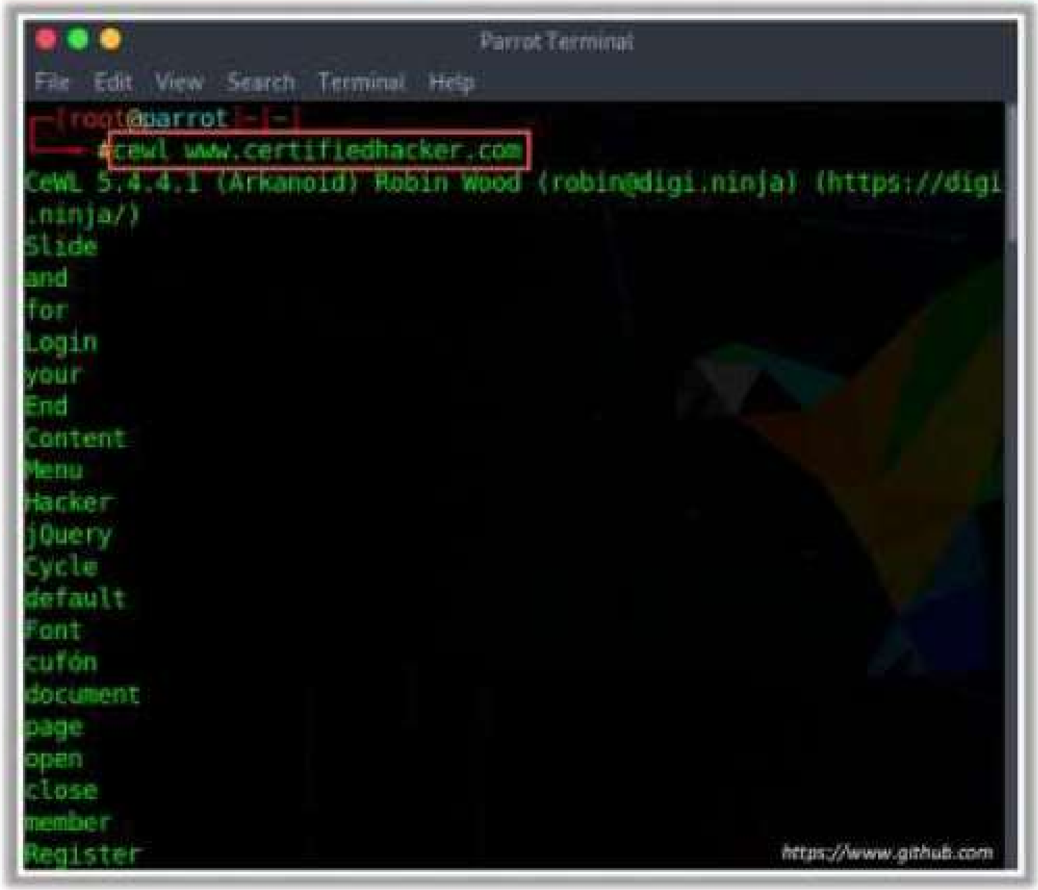
Data extracted: 30 lines Total time spent: 0 Average speed: 0

Export Data Start Extraction

https://www.octoparse.com

Gathering Wordlist from the Target Website

- Attackers **gather a list of words available on the target website** to brute-force the email addresses gathered through search engines, social networking sites, web spidering, etc.
- Attackers use **CeWL** tool to gather a list of words from the target website
- Use the following command to extract all the words available on the target website:
  - `cewl www.certifiedhacker.com`



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

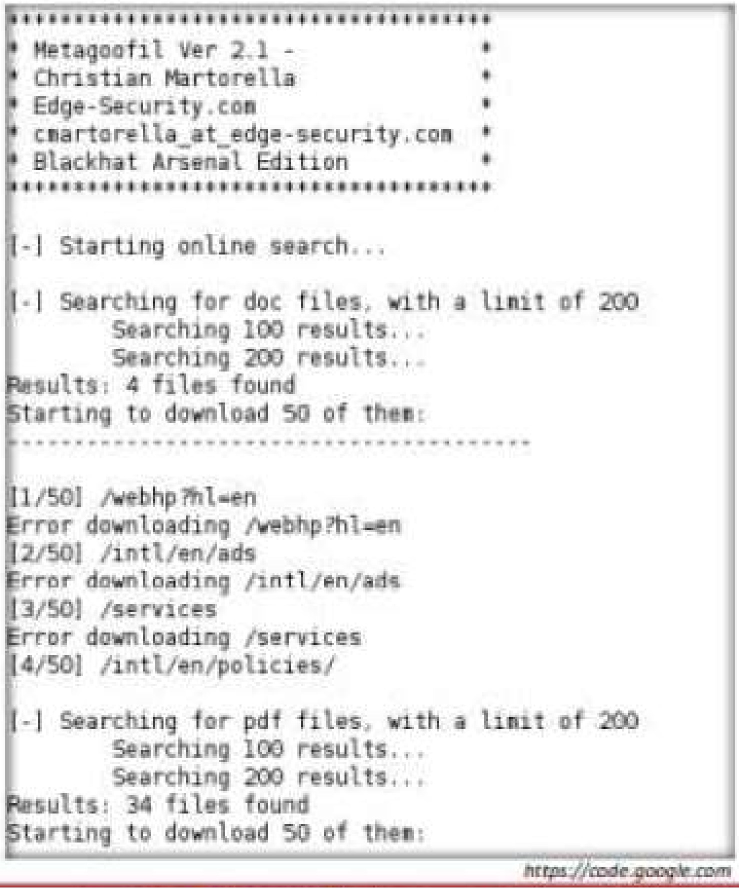
https://www.github.com

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

Other Techniques for Website Footprinting

Monitoring Web Pages for Updates and Changes

- Attackers use web updates monitoring tools, such as **WebSite-Watcher** and **VisualPing**, to detect changes or updates in a target website, and they analyze the gathered information to detect underlying vulnerabilities in the target website

Searching for Contact Information, Email Addresses, and Telephone Numbers from Company Website

- Attackers can search the target company's website to **obtain crucial information** about the company, such as the company's contact details, location, partner information, news, and links to other sites

Searching for Web Pages Posting Patterns and Revision Numbers

- Attackers can search for **copyright notices** and revision numbers on the web and can use these details to perform deep analyses on the target organization

Monitoring Website Traffic of Target Company

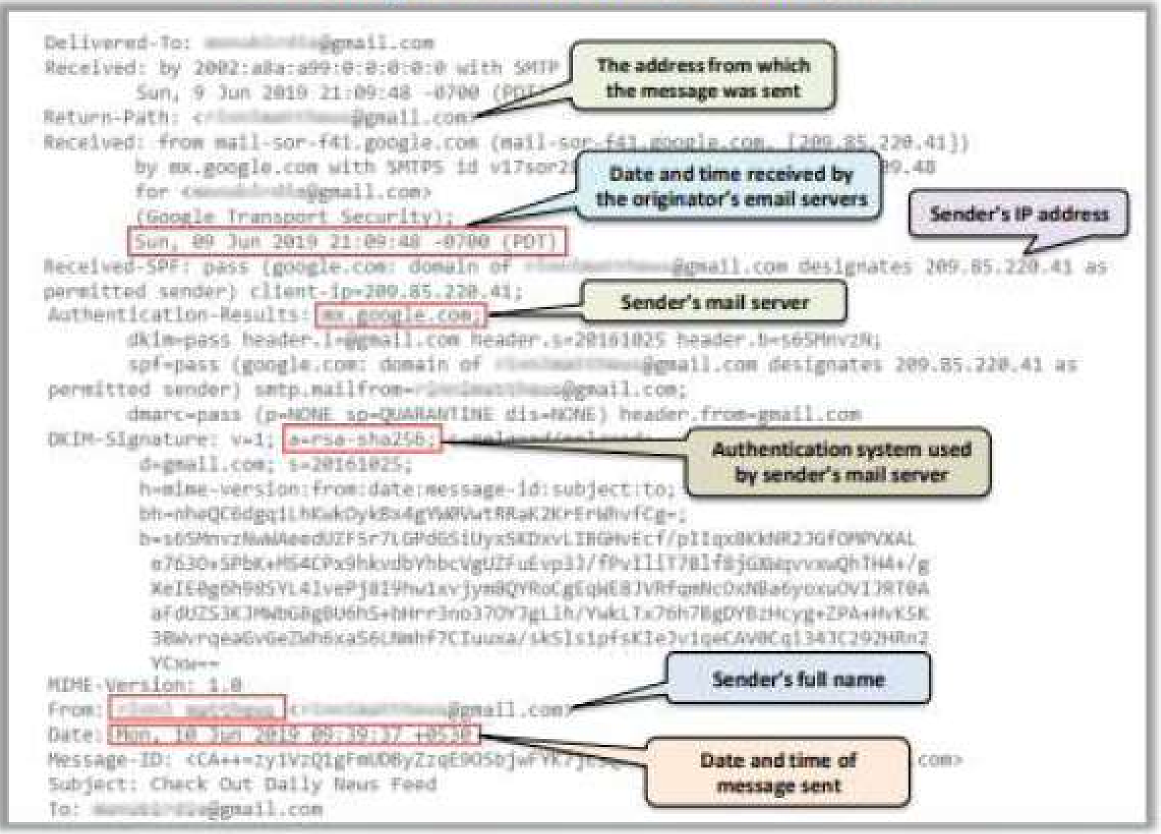
- Attackers use website traffic monitoring tools, such as **Web-Stat**, **Alexa**, and **Monitis**, to collect information about the target company's website, such as total visitors, page views, bounce rate, and site ranking

Email Footprinting

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

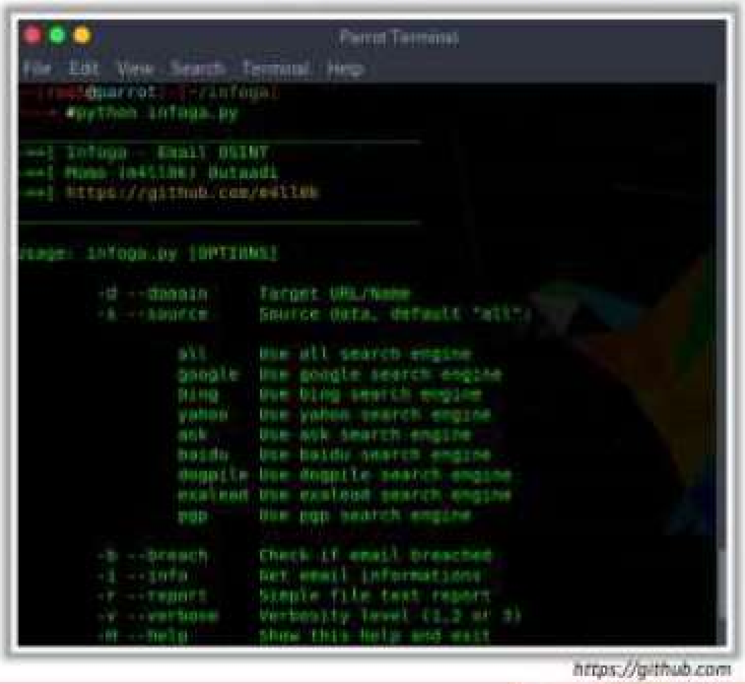


```
Delivered-To: [redacted]@gmail.com
Received: by 2002:a8a:a99:0:0:0:0:0 with SMTP
        Sun, 9 Jun 2019 21:09:48 -0700 (PDT)
Return-Path: <[redacted]@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id v17sor2                              9.48
        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=s65MnvzN;
       spf=pass (google.com: domain of [redacted]@gmail.com designates 209.85.220.41 as
permitted sender) smtp.mailfrom=[redacted]@gmail.com;
       dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20161025;
        h=mime-version:from:date:message-id:subject:to;
        bh=nheQC6dgq1LhKwkOyk8x4gYWRVwtRRaK2KrErWhvfCg=;
        b=s65MnvzNwWAeedUZF5r7LGPdGS1UyxSKDxvLIBGHvEcf/pIIqxBKkNR2JGfOMPVXAL
         e7630+5PbK+M54CPx9hkvdbYhbcVgUZFuEvp3J/fPvIlIT78lf8jGXWqvvxwQhTH4+/g
         XeIE0g6h9SYL4lvePj8I9hw1xvjym8QYRoCgEqWE8JVRfqmNcOxNBa6yoxuOVIJRT0A
         afdUZS3KJMWbG8g8U6hS+bHrr3no37OV7gLih/YwkLTx76h7BgDYBzHcyg+ZPA+HvKSK
         3BWvrqeaGvGeZWh6xaS6UWmhF7CIuuxa/skSlsipfsKIeJv1qeCAV8Cq1343C292HRn2
         YCxw==
MIME-Version: 1.0
From: [redacted] <[redacted]@gmail.com>
Date: Mon, 10 Jun 2019 09:39:37 +0530
Message-ID: <CA++=zy1VzQ1gFmUD8yZzqE9O5bjwFYk7je                                .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

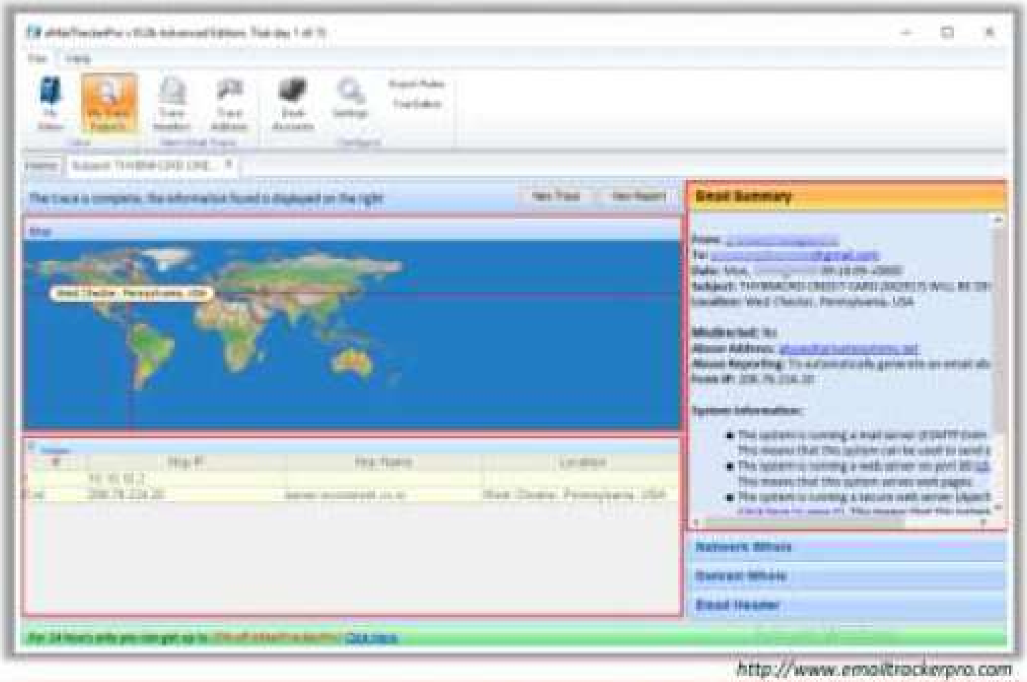
Email Tracking Tools

- Email tracking tools, such as eMailTrackerPro, Infoga, Mailtrack, and PoliteMail, allow an attacker to **track an email and extract information**, such as sender identity, mail server, sender's IP address, and location
- eMailTrackerPro analyzes email headers and reveals information, such as **sender's geographical location** and IP address



```
-[root@parrot]-[~/infoga]
--- #python infoga.py
-----------------------------------------------
--[ Infoga - Email OSINT
--[ Momo (m4ll0k) Outaadi
--[ https://github.com/m4ll0k
-----------------------------------------------
Usage: infoga.py [OPTIONS]

        -d --domain     Target URL/Name
        -s --source     Source data, default "all":

                all     Use all search engine
                google  Use google search engine
                bing    Use bing search engine
                yahoo   Use yahoo search engine
                ask     Use ask search engine
                baidu   Use baidu search engine
                dogpile Use dogpile search engine
                exalead Use exalead search engine
                pgp     Use pgp search engine

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

https://github.com



http://www.emailtrackerpro.com

Whois Footprinting

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

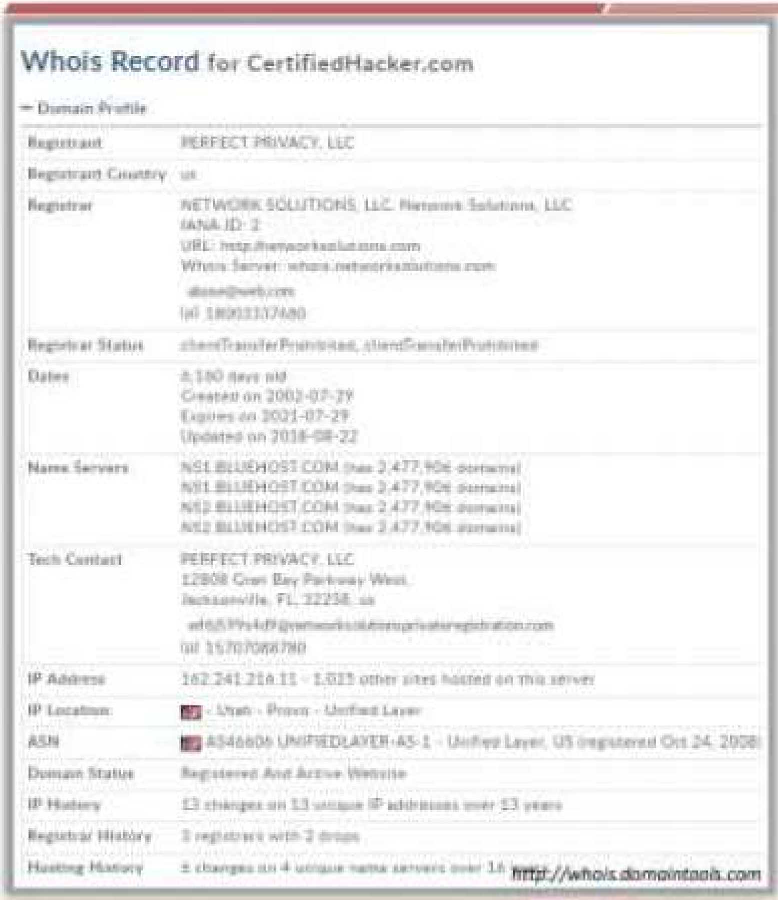
AFRINIC

RIPE NCC

lacnic

APNIC

Whois Lookup (Cont'd)

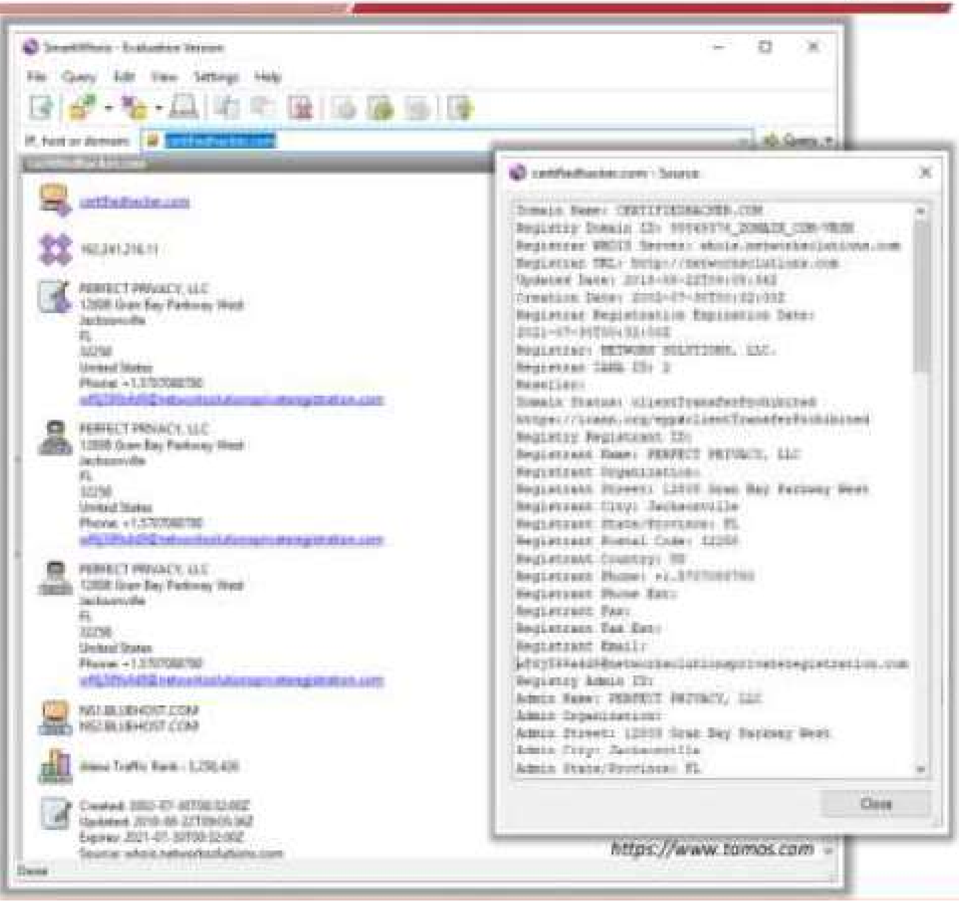


Whois Record for CertifiedHacker.com

− 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	6,180 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 wf6j539s4d9@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	4 changes on 4 unique name servers over 16

http://whois.domaintools.com



certifiedhacker.com

162.241.216.11

PERFECT PRIVACY, LLC
12808 Gran Bay Parkway West
Jacksonville
FL
32258
United States
Phone: +1.5707088780
wf6j539s4d9@networksolutionsprivateregistration.com

PERFECT PRIVACY, LLC
12808 Gran Bay Parkway West
Jacksonville
FL
32258
United States
Phone: +1.5707088780
wf6j539s4d9@networksolutionsprivateregistration.com

PERFECT PRIVACY, LLC
12808 Gran Bay Parkway West
Jacksonville
FL
32258
United States
Phone: +1.5707088780
wf6j539s4d9@networksolutionsprivateregistration.com

NS1.BLUEHOST.COM
NS2.BLUEHOST.COM

Alexa Traffic Rank - 1,250,430

Created: 2002-07-30T00:32:00Z
Updated: 2018-08-22T09:05:34Z
Expires: 2021-07-30T00:32:00Z
Source: whois.networksolutions.com

Done

certifiedhacker.com - Source

```
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 99749774_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2018-08-22T09:05:34Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date:
2021-07-30T04:32:00Z
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:
wf6j539s4d9@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
```

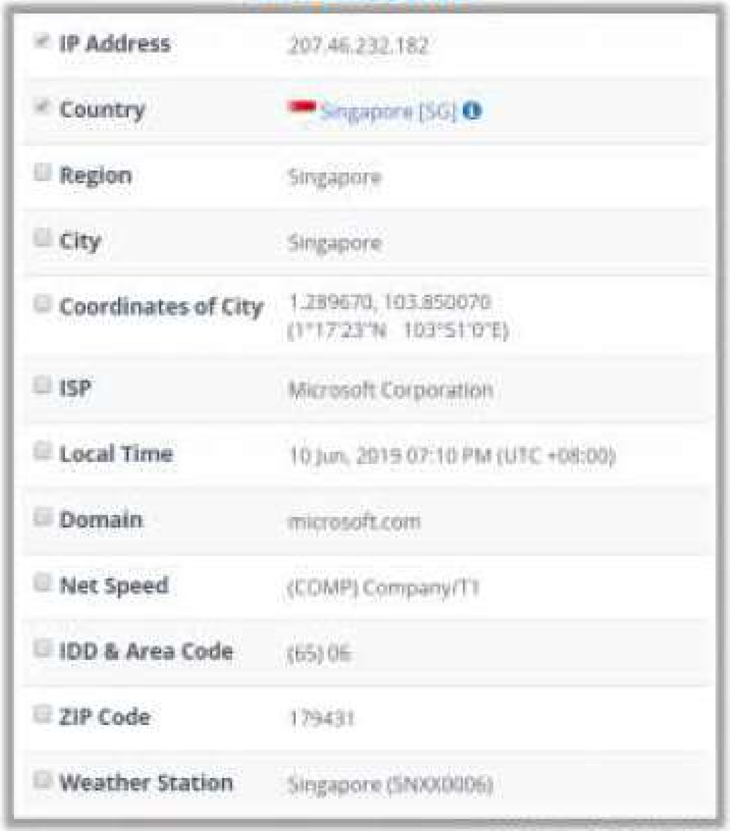
https://www.tamos.com

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

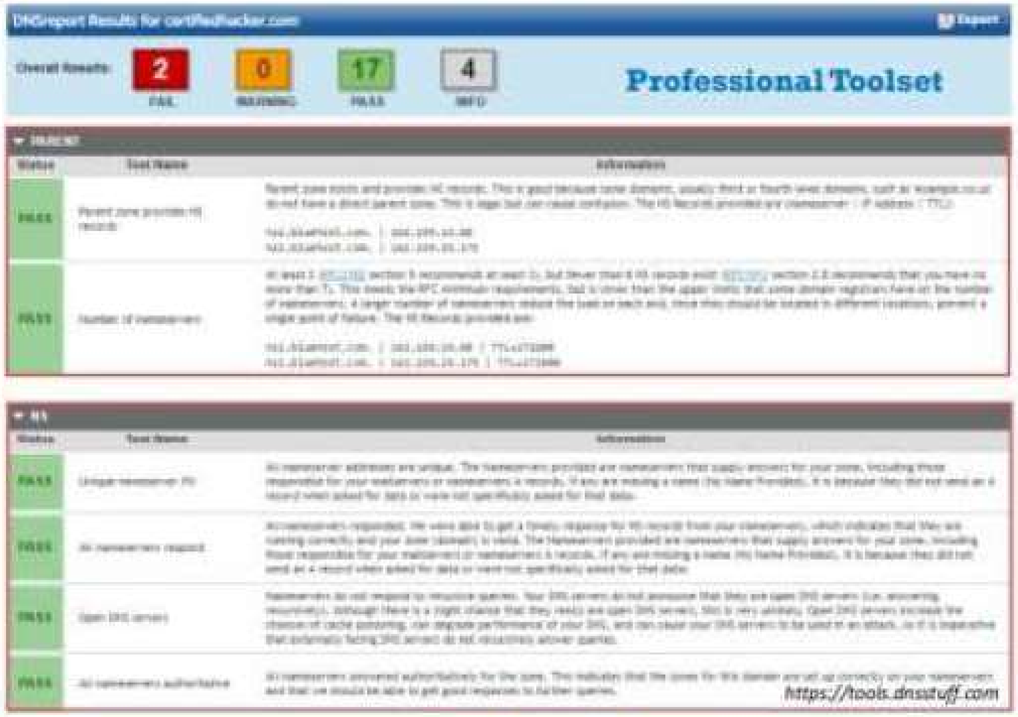
DNS Footprinting

Extracting DNS Information

- DNS records provide important information about the **location and types of servers**
- Attackers can gather DNS information to **determine key hosts in the network** and can perform social engineering attacks

Record Type	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for a domain
SRV	Service records
PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

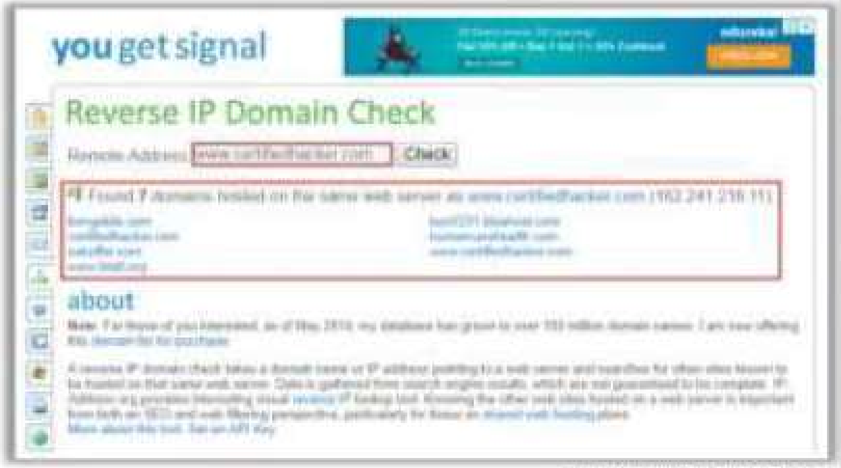
- Attackers query DNS servers using DNS interrogation tools, such as Professional Toolset and DNS Records, to **retrieve the record structure** that contains information about the target DNS



https://tools.dnsstuff.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**



Reverse IP Domain Check

Remote Address: www.certifiedhacker.com Check

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

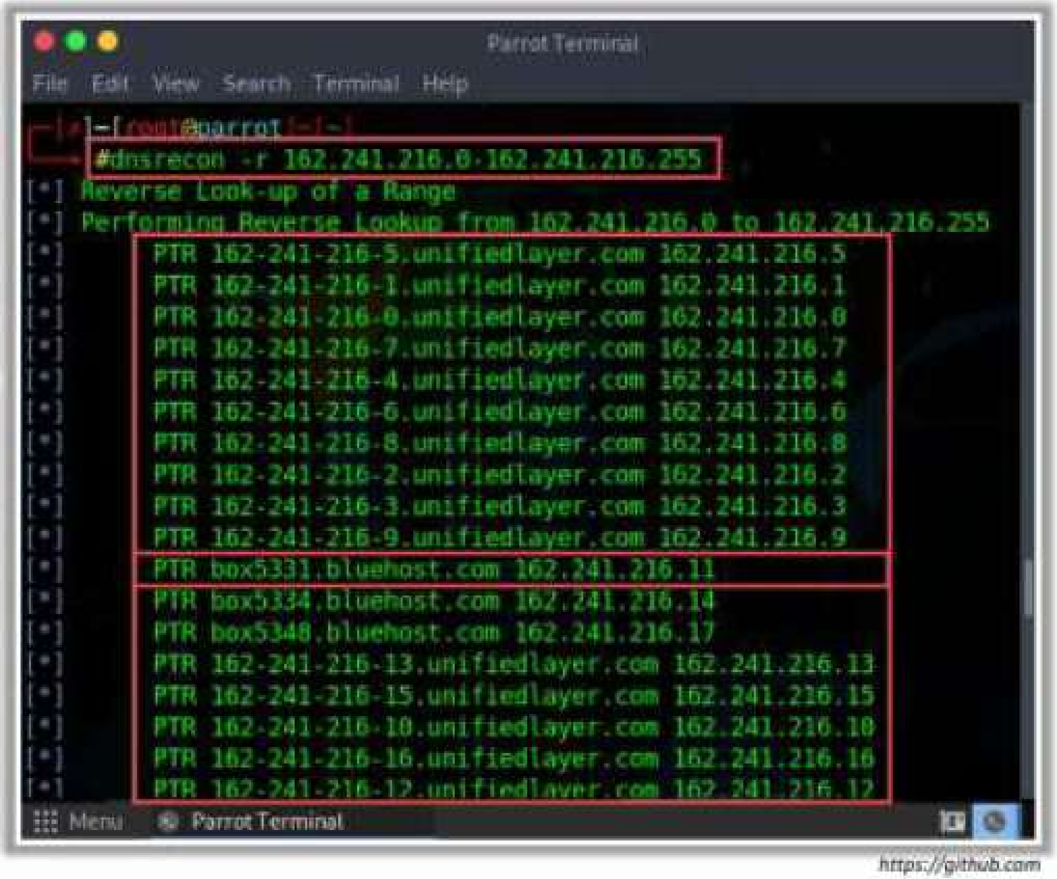
[illegible].com
certifiedhacker.com
[illegible]
www.[illegible].org
box5331.bluehost.com
[illegible].com
www.certifiedhacker.com

about

Note: For those of you interested, as of May 2016, my database has grown to over 100 million domain names. I am now offering this domain list for purchase.

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

https://www.yougetsignal.com



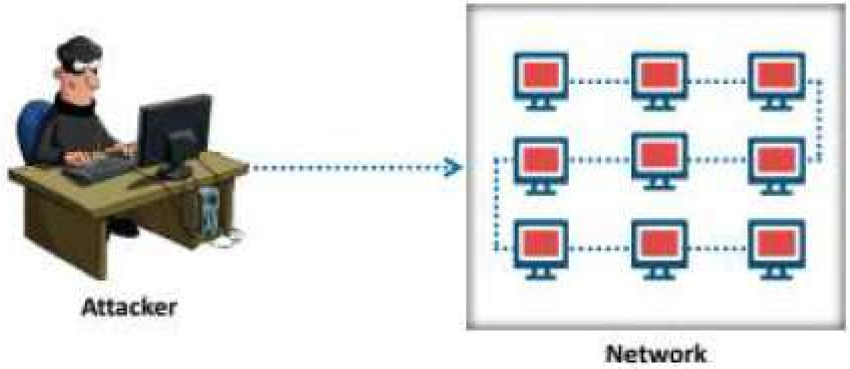
```
┌─[✗]─[root@parrot]─[~]
└──╼ #dnsrecon -r 162.241.216.0-162.241.216.255
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 162.241.216.0 to 162.241.216.255
[*]      PTR 162-241-216-5.unifiedlayer.com 162.241.216.5
[*]      PTR 162-241-216-1.unifiedlayer.com 162.241.216.1
[*]      PTR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

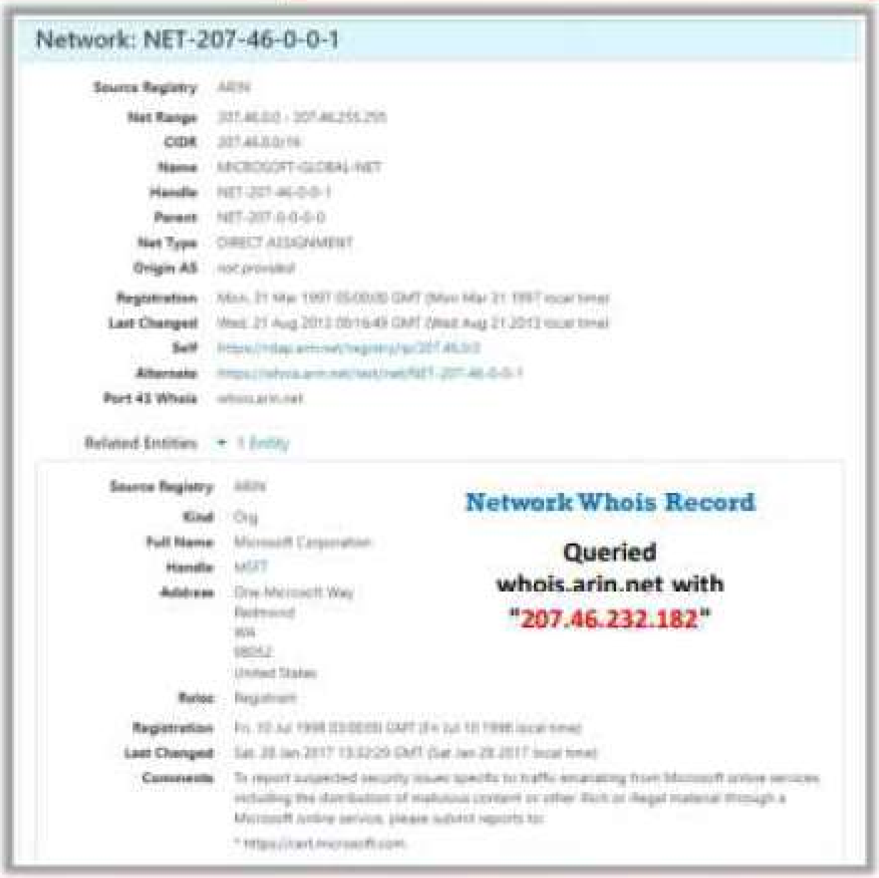
https://github.com

Network Footprinting

Locate the Network Range

- Network range information assists attackers in creating a **map of the target network**
- One can find the **range of IP addresses** using **ARIN whois database search** tool
- One can also find the range of IP addresses and the subnet mask used by the target organization from **Regional Internet Registry (RIR)**





Network: NET-207-46-0-0-1

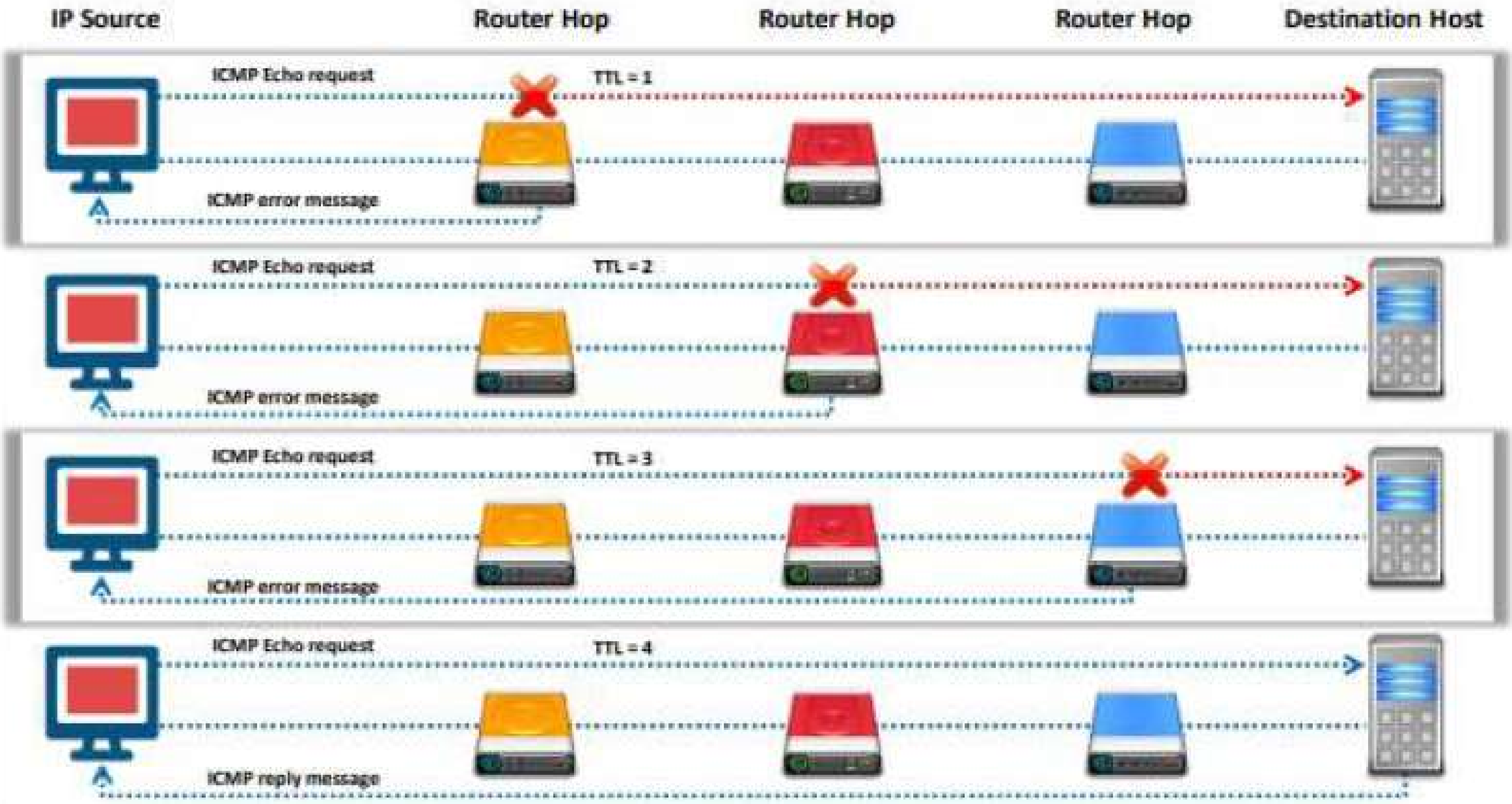
```
   Source Registry  ARIN
         Net Range  207.46.0.0 - 207.46.255.255
              CIDR  207.46.0.0/16
              Name  MICROSOFT-GLOBAL-NET
            Handle  NET-207-46-0-0-1
            Parent  NET-207-0-0-0-0
          Net Type  DIRECT ASSIGNMENT
         Origin AS  not provided
      Registration  Mon, 31 Mar 1997 05:00:00 GMT (Mon Mar 31 1997 local time)
      Last Changed  Wed, 21 Aug 2013 05:16:49 GMT (Wed Aug 21 2013 local time)
              Self  https://rdap.arin.net/registry/ip/207.46.0.0
         Alternate  https://whois.arin.net/rest/net/NET-207-46-0-0-1
     Port 43 Whois  whois.arin.net

  Related Entities  ▾ 1 Entity

   Source Registry  ARIN
              Kind  Org
         Full Name  Microsoft Corporation
            Handle  MSFT
           Address  One Microsoft Way
                    Redmond
                    WA
                    98052
                    United States
             Roles  Registrant
      Registration  Fri, 10 Jul 1998 03:00:00 GMT (Fri Jul 10 1998 local time)
      Last Changed  Sat, 28 Jan 2017 13:32:29 GMT (Sat Jan 28 2017 local time)
          Comments  To report suspected security issues specific to traffic emanating from Microsoft online services
                    including the distribution of malicious content or other illicit or illegal material through a
                    Microsoft online service, please submit reports to:
                    * https://cert.microsoft.com
```

Network Whois Record

Queried whois.arin.net with "207.46.232.182"

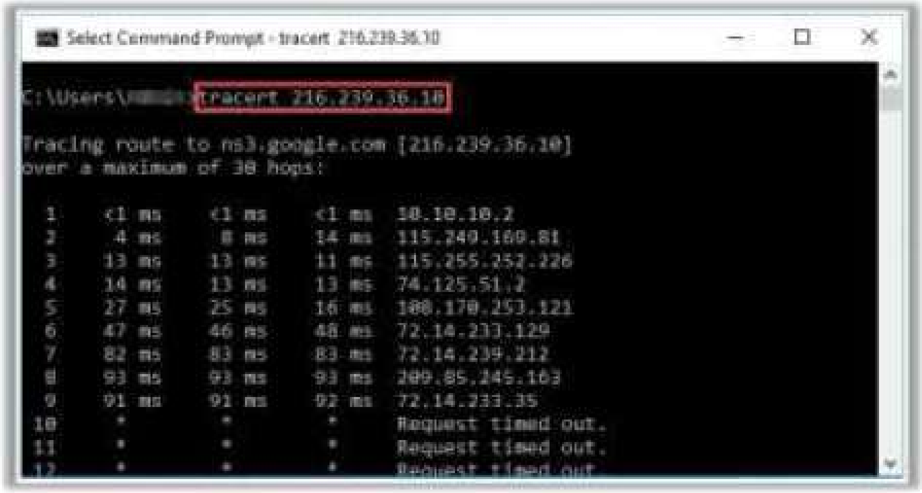
Traceroute

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



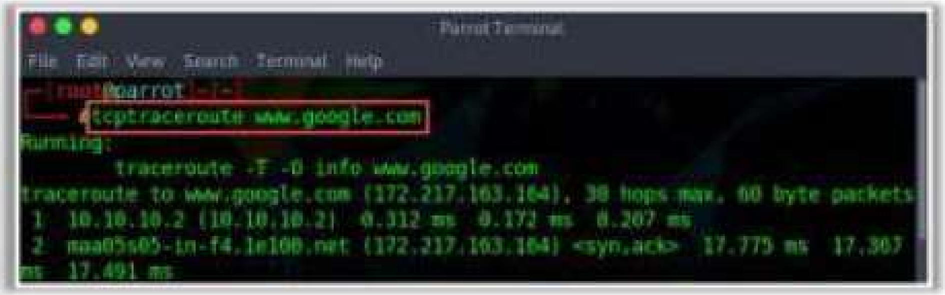
Traceroute (Cont'd)

IMCP Traceroute



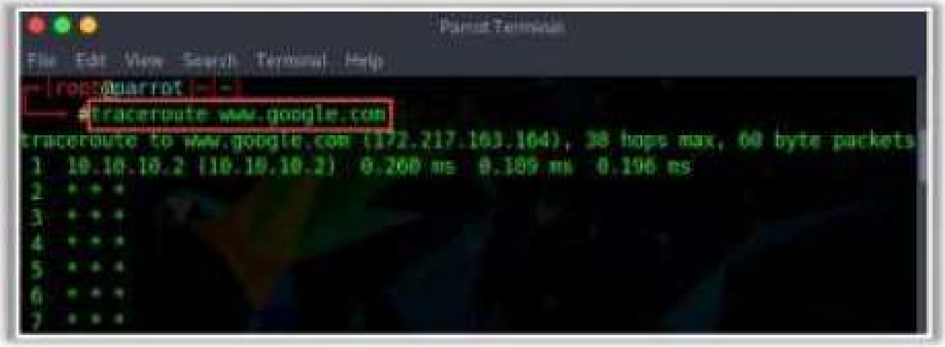
```
C:\Users\[redacted]>tracert 216.239.36.10

Tracing route to ns3.google.com [216.239.36.10]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.10.10.2
  2     4 ms     8 ms    14 ms  115.249.169.81
  3    13 ms    13 ms    11 ms  115.255.252.226
  4    14 ms    13 ms    13 ms  74.125.51.2
  5    27 ms    25 ms    16 ms  108.170.253.121
  6    47 ms    46 ms    48 ms  72.14.233.129
  7    82 ms    83 ms    83 ms  72.14.239.212
  8    93 ms    93 ms    93 ms  209.85.245.163
  9    91 ms    91 ms    92 ms  72.14.233.35
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
```

TCP Traceroute



```
┌─[root@parrot]─[~]
└──╼ #tcptraceroute www.google.com
Running:
        traceroute -T -O info www.google.com
traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
 1  10.10.10.2 (10.10.10.2)  0.312 ms  0.172 ms  0.207 ms
 2  maa05s05-in-f4.1e100.net (172.217.163.164) <syn,ack>  17.775 ms  17.307
ms  17.491 ms
```

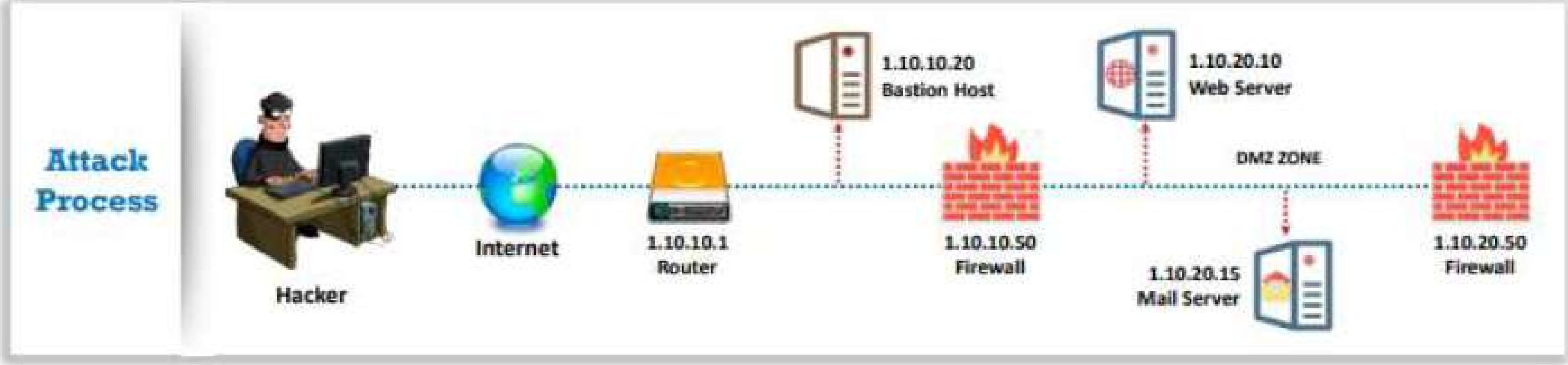
UDP Traceroute



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

Traceroute Analysis

- Attackers conduct traceroute to extract information about **network topology**, **trusted routers**, and **firewall locations**
- For example, after running several **traceroutes**, an attacker might obtain the following information:
  - traceroute 1.10.10.20, second to last hop is 1.10.10.1
  - traceroute 1.10.20.10, third to last hop is 1.10.10.1
  - traceroute 1.10.20.10, second to last hop is 1.10.10.50
  - traceroute 1.10.20.15, third to last hop is 1.10.10.1
  - traceroute 1.10.20.15, second to last hop is 1.10.10.50
- By putting this information together, attackers can draw the **network diagram**



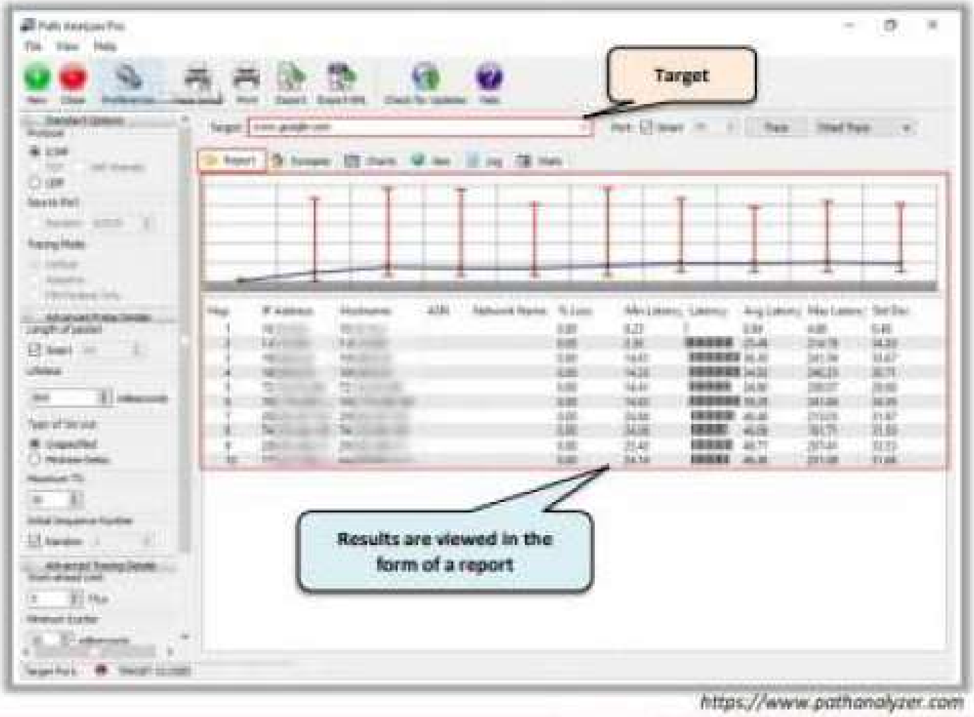
Traceroute Tools

Path Analyzer Pro

It **delivers network route tracing** with performance tests, DNS, Whois, and network resolution to investigate network issues

VisualRoute

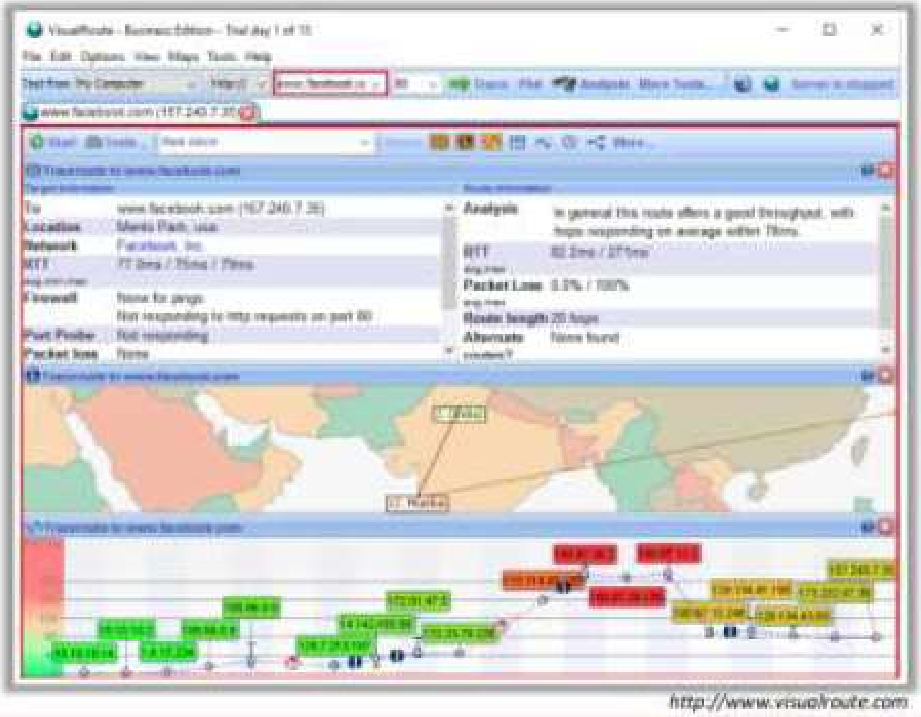
It is a traceroute and network diagnostic tool that **identifies the geographical location of routers**, servers, and other IP devices



Target

Results are viewed in the form of a report

https://www.pathanalyzer.com



http://www.visualroute.com

Footprinting through Social Engineering

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

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

Module Flow

1 Footprinting Concepts

2 Footprinting Methodology

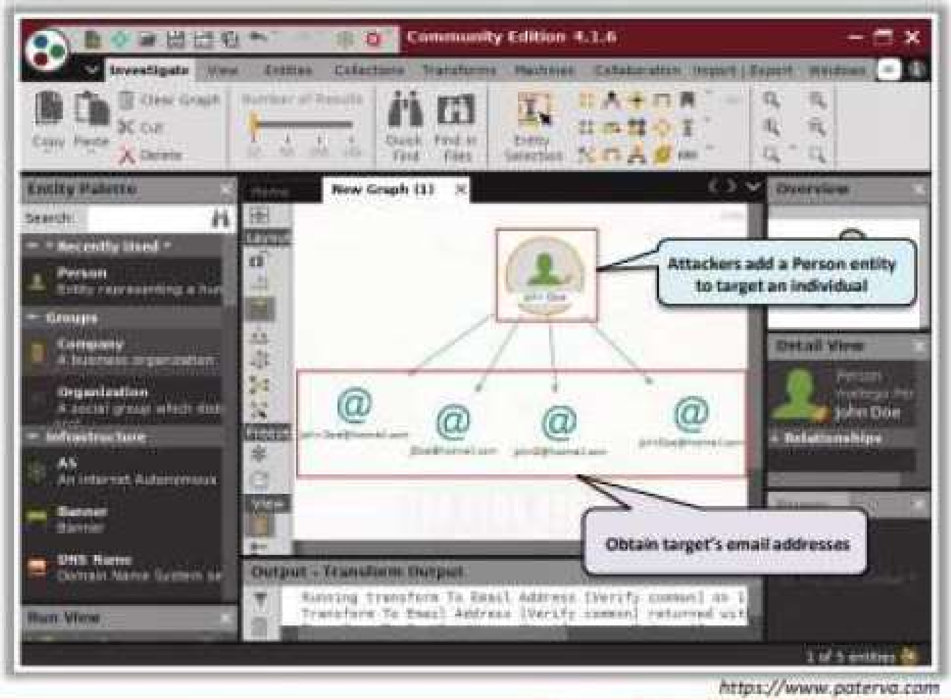
3 Footprinting Tools

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.

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

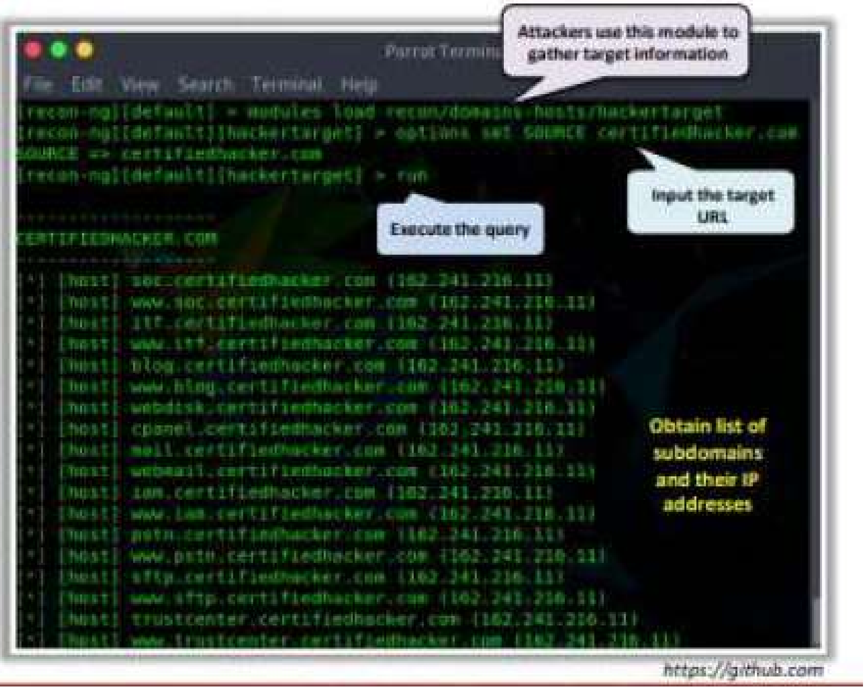


```
Running transform To Email Address [Verify common] on 1
Transform To Email Address [Verify common] returned wit
```

Attackers add a Person entity to target an individual

Obtain target's email addresses

https://www.paterva.com



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

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

Attackers use this module to gather target information

Input the target URL

Execute the query

Obtain list of subdomains and their IP addresses

https://github.com

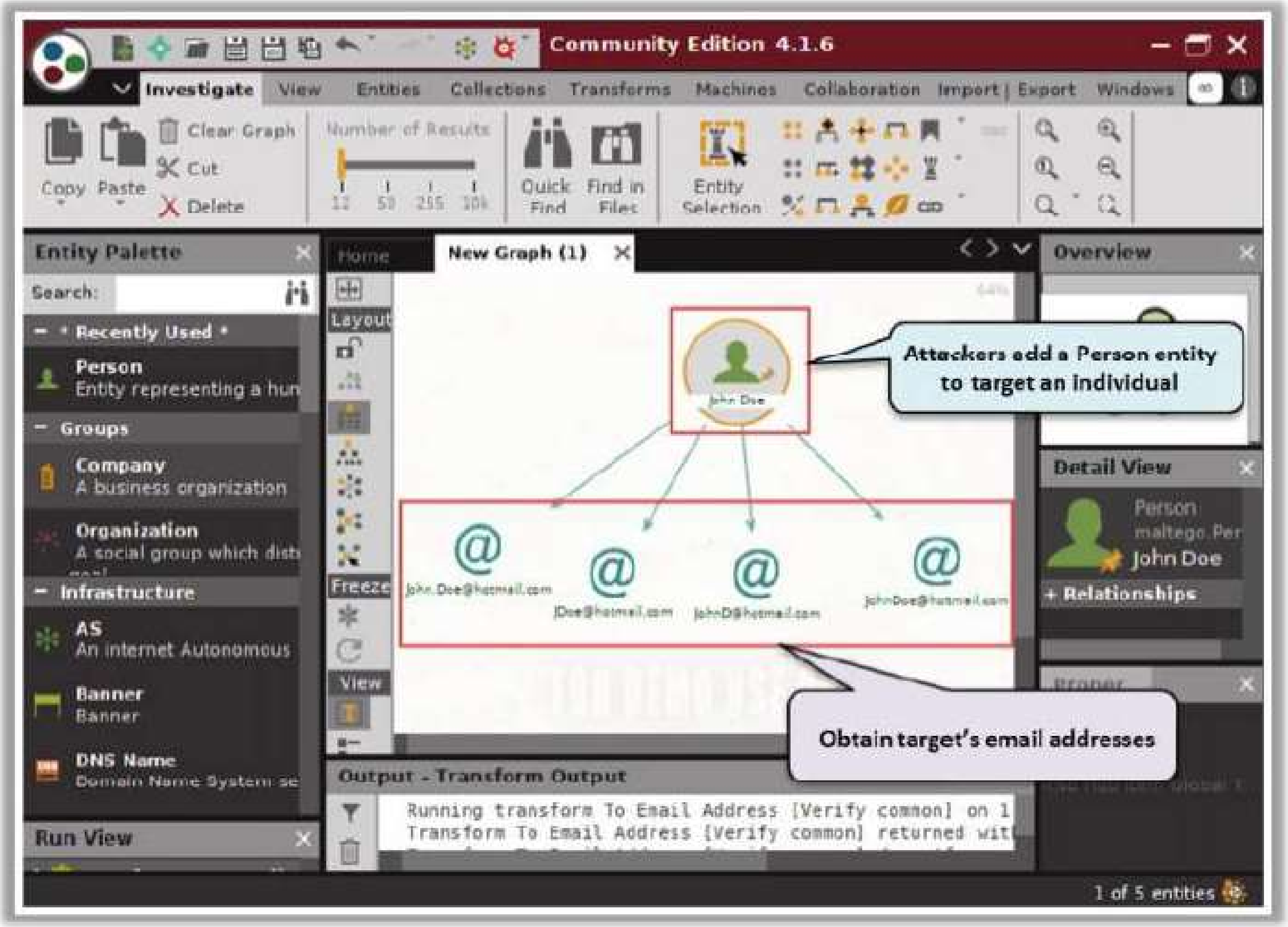
Maltego

Source: *https://www.paterva.com*

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

Attackers can use different entities available in the tool to obtain information such as email addresses, a list of phone numbers, and a target's Internet infrastructure (domains, DNS names, Netblocks, IP addresses information).

As shown in the screenshot, attackers add a `Person entity`, rename it with the target's name, and obtain the email addresses associated with the target.



Attackers add a Person entity to target an individual

Obtain target's email addresses

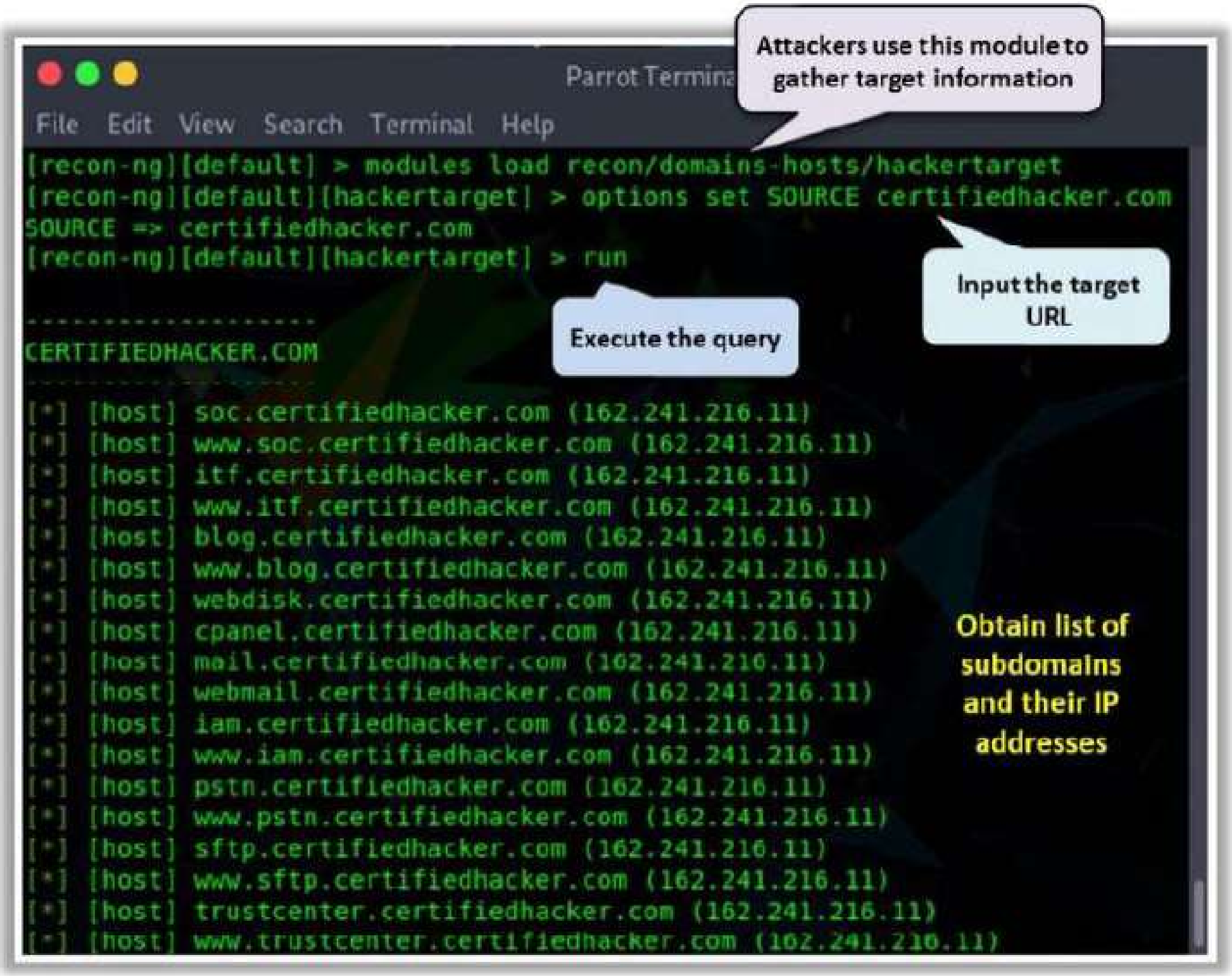
```
Running transform To Email Address [Verify common] on 1
Transform To Email Address [Verify common] returned wit
```

Recon-ng

Source: *https://github.com*

Recon-ng is a web reconnaissance framework with independent modules for database interaction that provides an environment in which open-source web-based reconnaissance can be conducted.

As shown in the screenshot, attackers use the module **`recon/domains-hosts/hackertarget`** to extract a list of subdomains and IP addresses associated with the target URL.



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

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

Attackers use this module to gather target information

Input the target URL

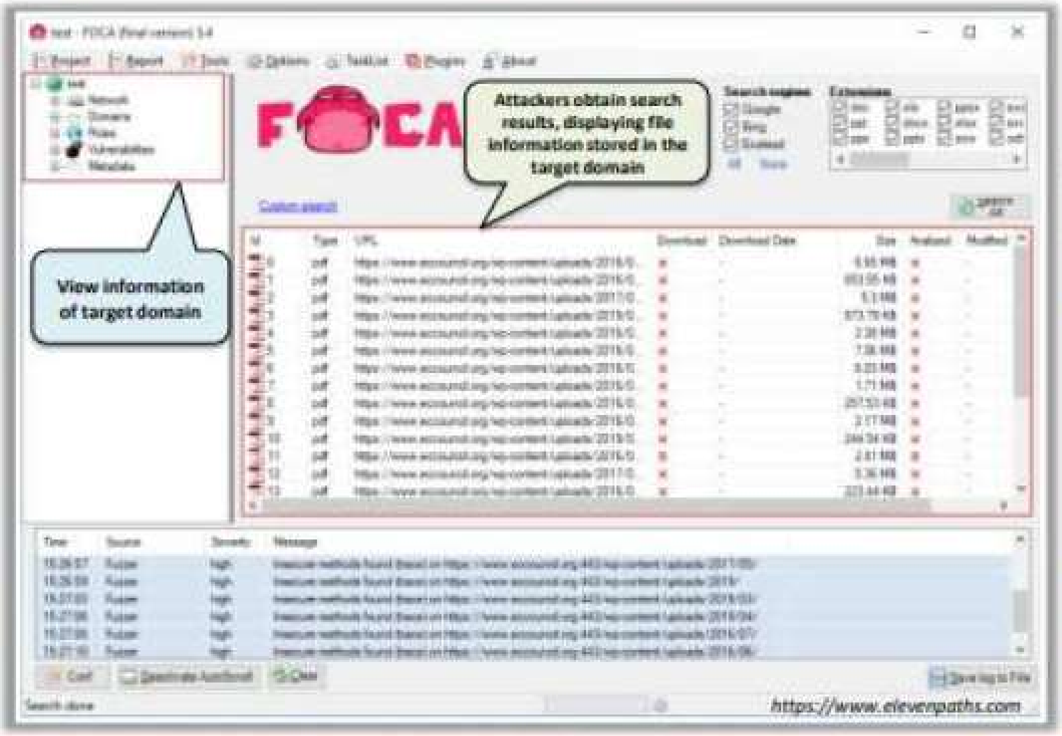
Execute the query

Obtain list of subdomains and their IP addresses

Footprinting Tools: FOCA and OSRFramework

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

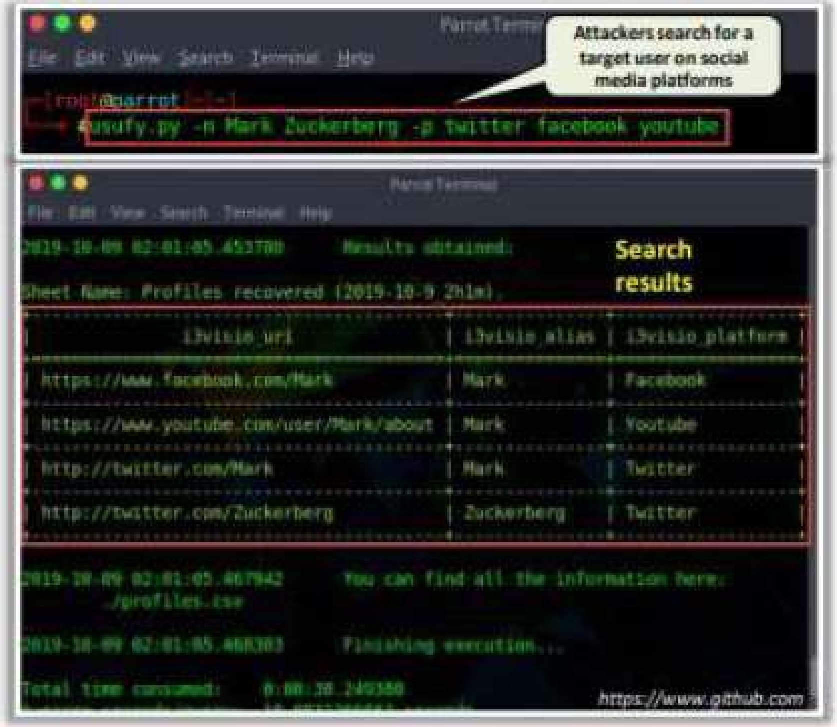
OSRFramework includes applications related to username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction, etc.



Attackers obtain search results, displaying file information stored in the target domain

View information of target domain

https://www.elevenpaths.com



Attackers search for a target user on social media platforms

```
┌─[root@parrot]─[~]
└──╼ #usufy.py -n Mark Zuckerberg -p twitter facebook youtube
```

Search results

```
2019-10-09 02:01:05.453780      Results obtained:

Sheet Name: Profiles recovered (2019-10-9 2h1m).
+-----------------------------------------+---------------+-----------------+
|              i3visio_uri                | i3visio_alias | i3visio_platform |
+=========================================+===============+=================+
| https://www.facebook.com/Mark           | Mark          | Facebook        |
+-----------------------------------------+---------------+-----------------+
| https://www.youtube.com/user/Mark/about | Mark          | Youtube         |
+-----------------------------------------+---------------+-----------------+
| http://twitter.com/Mark                 | Mark          | Twitter         |
+-----------------------------------------+---------------+-----------------+
| http://twitter.com/Zuckerberg           | Zuckerberg    | Twitter         |
+-----------------------------------------+---------------+-----------------+

2019-10-09 02:01:05.467942      You can find all the information here:
        ./profiles.csv

2019-10-09 02:01:05.468303      Finishing execution...

Total time consumed:    0:00:30.249380
```

https://www.github.com

FOCA

Source: *https://www.elevenpaths.com*

Fingerprinting Organizations with Collected Archives (FOCA) is a tool used mainly to find metadata and hidden information in the documents that its scans. FOCA is capable of scanning and analyzing a wide variety of documents, with the most common ones being Microsoft Office, Open Office, or PDF files.

Features:

- **Web Search** - Searches for hosts and domain names through URLs associated with the main domain. Each link is analyzed to extract information from its new host and domain names.
- **DNS Search** - Checks each domain to ascertain the host names configured in NS, MX, and SPF servers to discover the new host and domain names.
- **IP Resolution** - Resolves each host name by comparison with the DNS to obtain the IP address associated with this server name. To perform this task accurately, the tool performs analysis against the organization's internal DNS.
- **PTR Scanning** - Finds more servers in the same segment of a determined address; IP FOCA executes a PTR log scan.
- **Bing IP** - Launches FOCA, which is a search process for new domain names associated with that IP address for each IP address discovered.
- **Common Names** - Perform dictionary attacks against the DNS.

As shown in the screenshot, attackers search the target domain and obtain the file information stored in it. The extracted files can be viewed on the web browser. Further, the attackers can view additional information such as network domains, roles, vulnerabilities, and metadata of the target domain.

OSRFramework

Source: *https://github.com*

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

The tools included in the OSRFramework package that attackers can use to gather information on the target are listed below:

○ **`usufy.py`** - Checks for a user profile on up to 290 different platforms

○ **`mailfy.py`** - Check for the existence of a given email

○ **`searchfy.py`** - Performs a query on the platforms in OSRFramework

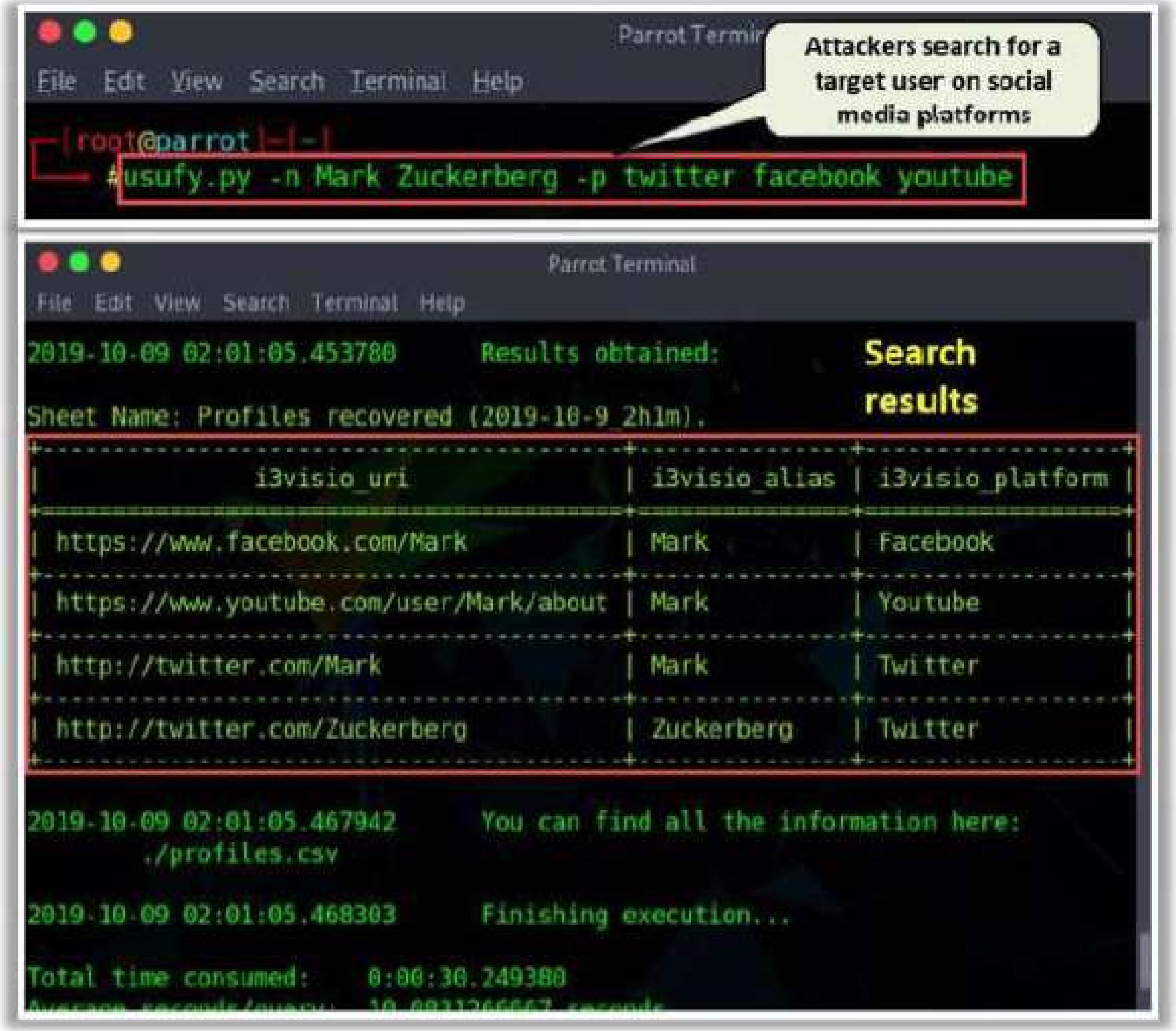
○ **`domainfy.py`** - Checks for the existence of domains

○ **`phonefy.py`** - Checks for the existence of a given series of phones

○ **`entify.py`** - Uses regular expressions to extract entities

As shown in the screenshot, attackers use the following command to search for a target user on social media platforms,

```
usufy.py -n Mark Zuckerberg -p twitter facebook youtube
```



Parrot Terminal
File Edit View Search Terminal Help

```
┌─[root@parrot]─[~]
└──╼ #usufy.py -n Mark Zuckerberg -p twitter facebook youtube
```

Attackers search for a target user on social media platforms

Parrot Terminal
File Edit View Search Terminal Help

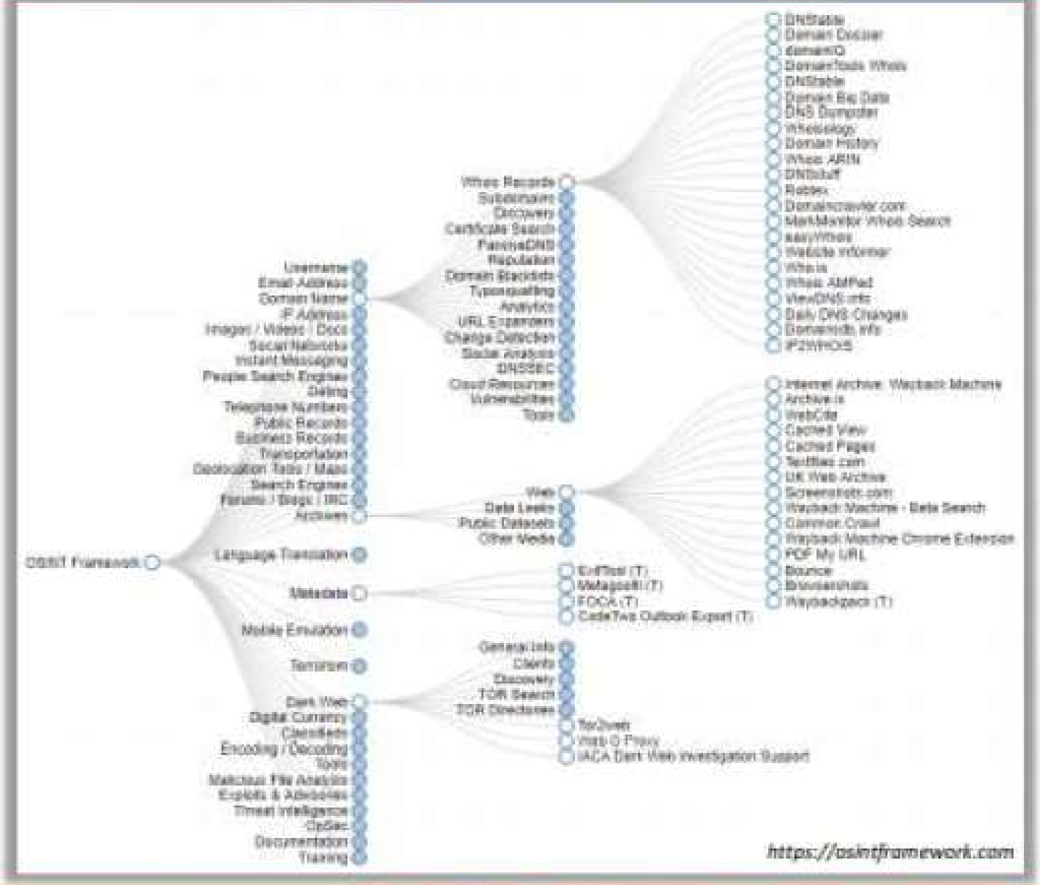
```
2019-10-09 02:01:05.453780      Results obtained:

Sheet Name: Profiles recovered (2019-10-9_2h1m).
+-------------------------------------------+-----------------+--------------------+
|                i3visio_uri                | i3visio_alias   | i3visio_platform   |
+===========================================+=================+====================+
| https://www.facebook.com/Mark             | Mark            | Facebook           |
+-------------------------------------------+-----------------+--------------------+
| https://www.youtube.com/user/Mark/about   | Mark            | Youtube            |
+-------------------------------------------+-----------------+--------------------+
| http://twitter.com/Mark                   | Mark            | Twitter            |
+-------------------------------------------+-----------------+--------------------+
| http://twitter.com/Zuckerberg             | Zuckerberg      | Twitter            |
+-------------------------------------------+-----------------+--------------------+

2019-10-09 02:01:05.467942      You can find all the information here:
        ./profiles.csv

2019-10-09 02:01:05.468303      Finishing execution...

Total time consumed:    0:00:30.249380
Average seconds/query:  10.0831266667 seconds
```

Search results

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



https://osintframework.com

OSINT Framework

Source: *https://osintframework.com*

OSINT Framework is an open source intelligence gathering framework that helps security professionals in performing automated footprinting and reconnaissance, OSINT research, and intelligence gathering. It is focused on gathering information from free tools or resources. This framework includes a simple web interface that lists various OSINT tools arranged by category, and it is shown as an OSINT tree structure on the web interface.

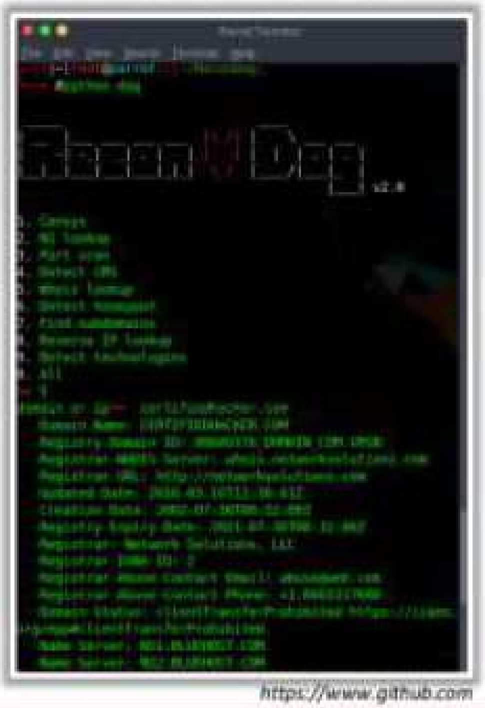
As shown in the screenshot, the tools listed include the following indicators:

- (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

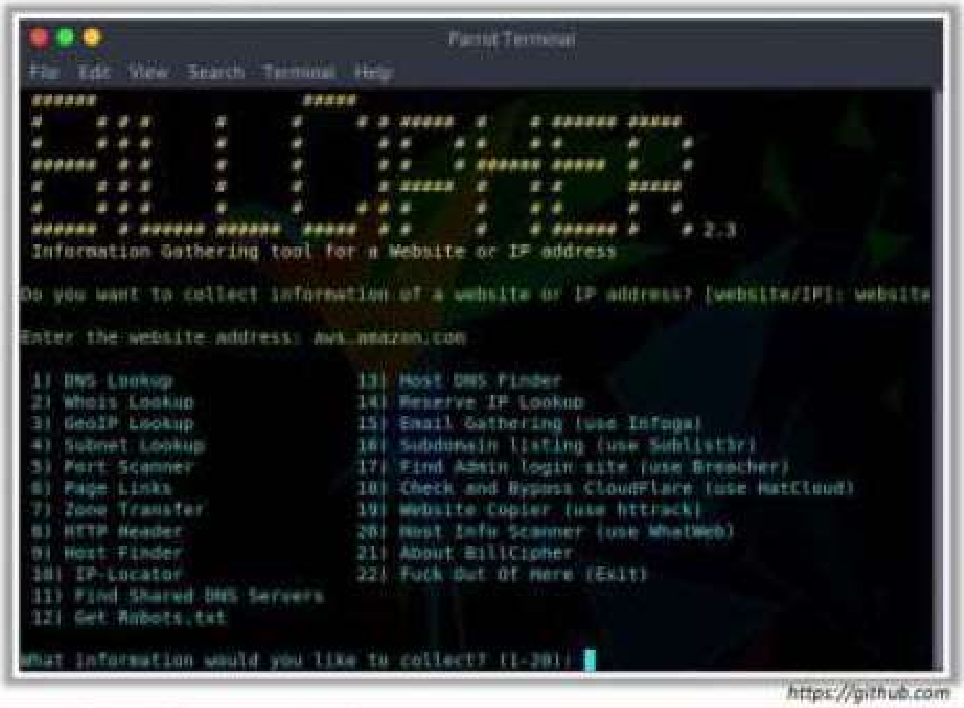


```
1. Censys
2. NS lookup
3. Port scan
4. Detect CMS
5. Whois lookup
6. Detect honeypot
7. Find subdomains
8. Reverse IP lookup
9. Detect technologies
0. All
   Domain Name: [illegible]
   Registry Domain ID: [illegible]
   Registrar WHOIS Server: whois.networksolutions.com
   Registrar URL: http://networksolutions.com
   Updated Date: [illegible]
   Creation Date: [illegible]
   Registry Expiry Date: [illegible]
   Registrar: Network Solutions, LLC
   Registrar IANA ID: 2
   Registrar Abuse Contact Email: [illegible]
   Registrar Abuse Contact Phone: [illegible]
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.BLUEHOST.COM
   Name Server: NS2.BLUEHOST.COM
```

https://www.github.com

BillCipher

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



```
                                                            # 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

Features:

- **Censys**: Uses censys.io to gather a massive amount of information about an IP address.
- **NS lookup**: Performs name server lookup
- **Port scan**: Scans most common TCP ports
- **Detect CMS**: Can detect 400+ content management systems
- **Whois lookup**: Performs a Whois lookup
- **Detect honeypot**: Uses shodan.io to check if the target is a honeypot
- **Find subdomains**: Uses findsubdomains.com to find subdomains
- **Reverse IP lookup**: Performs a reverse IP lookup to find domains associated with an IP address
- **Detect technologies**: Uses wappalyzer.com to detect 1000+ technologies
- **All**: Runs all utilities against the target

BillCipher

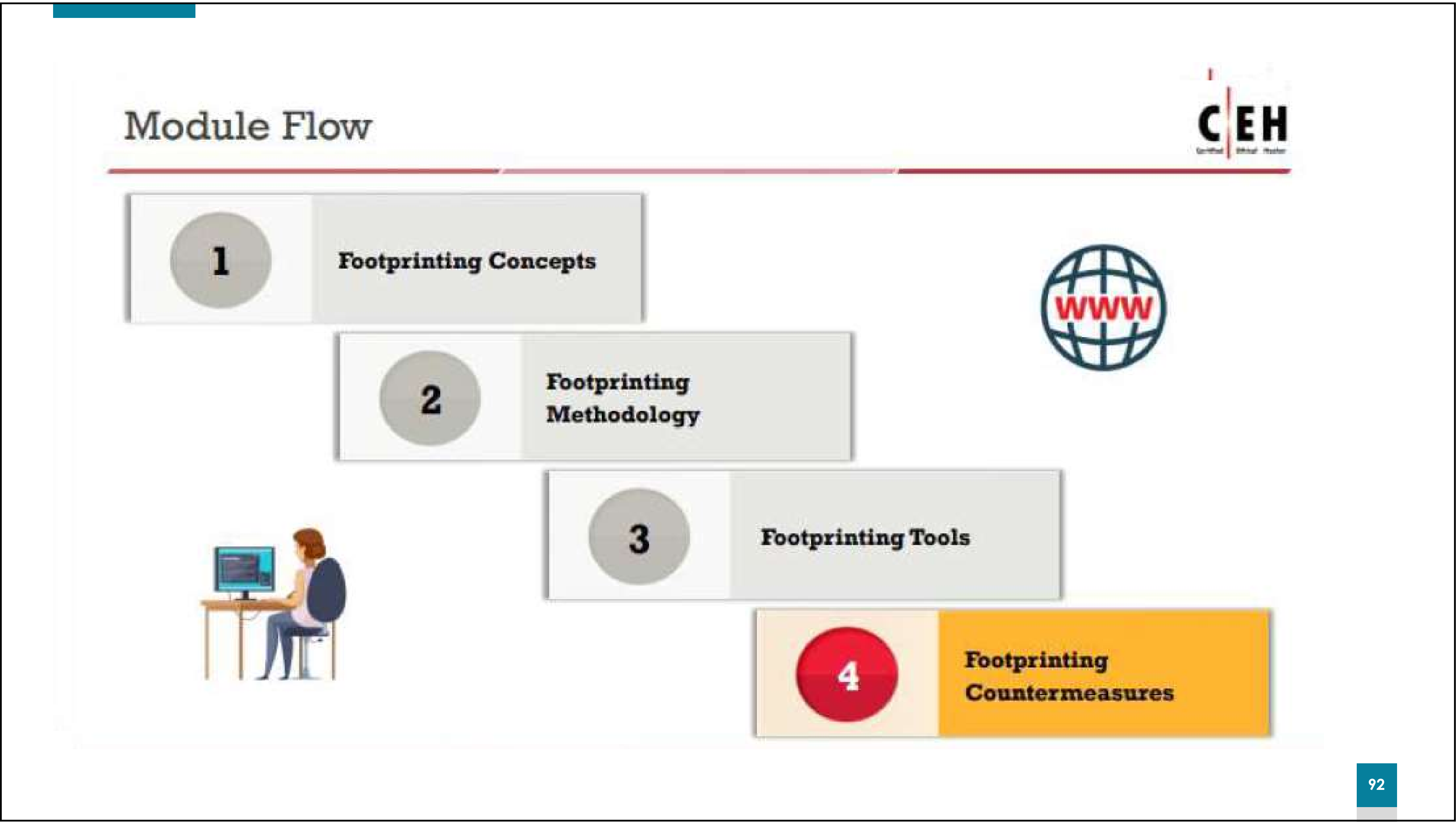
Source: *https://www.github.com*

BillCipher is an information gathering tool for a website or IP address. It can work on any operating system that supports Python 2, Python 3, and Ruby. This tool includes various options such as DNS lookup, Whois lookup, port scanning, zone transfer, host finder, and reverse IP lookup, which help to gather critical information.

Recon-Dog

Source: *https://www.github.com*

Recon-Dog is an all-in-one tool for all basic information gathering needs. It uses APIs to collect information about the target system.



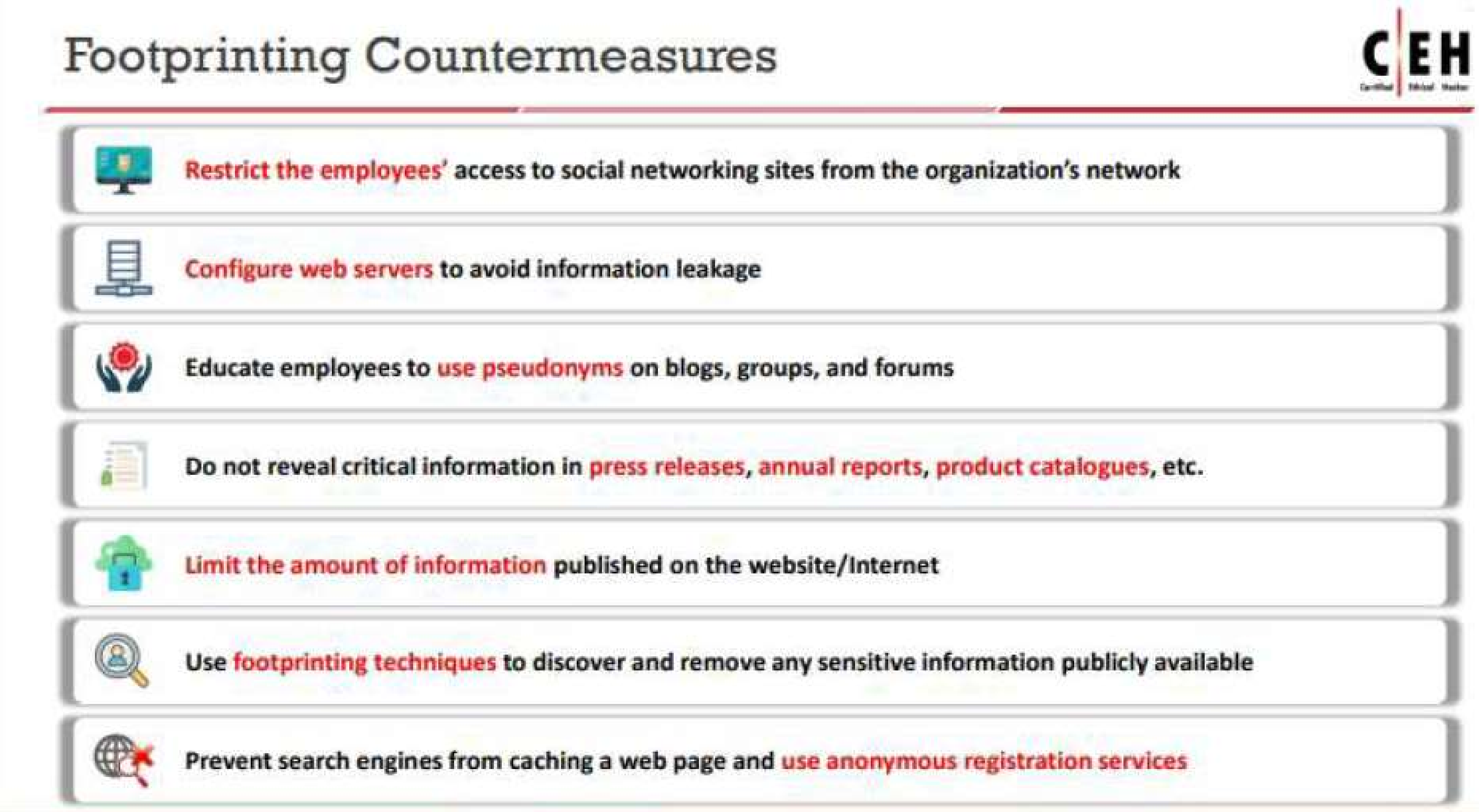
Module Flow

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
- 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 web servers
4. Conduct periodic security awareness training to educate employees about various **social engineering tricks and risks**
5. Opt for privacy services on **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 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

THANK YOU