Chapter 2: Footprinting & Reconnaissance

Technology Brief

Footprinting phase allows the attacker to gather the information regarding internal and external security architecture; he has to face a target. Collection of information also helps to identify the vulnerabilities within a system, which exploits, to gain access. Getting deep information about target reduces the focus area & bring attacker closer to the target. The attacker focuses the target by mean of the range of IP address he has to go through, to hack target or regarding domain information or else.

Footprinting Concepts

The first step to ethical hacking is Footprinting. Footprinting is the collection of every possible information regarding the target and target network. This collection of information helps in identifying different possible ways to enter into the target network. This collection of information may have gathered through publicly- available personal information and sensitive information from any secret source. Typically, footprinting & reconnaissance is performing social engineering attacks, system or network attack, or through any other technique. Active and passive methods of reconnaissance are also popular for gaining information of target directly or indirectly. The overall purpose of this phase is to keep interaction with the target to gain information without any detection or alerting.

Pseudonymous Footprinting

Pseudonymous footprinting includes footprinting through online sources. In Pseudonymous footprinting, information about a target is shared by posting with an assumed name. This type information is shared with the real credential to avoid trace to an actual source of information.

Internet Footprinting

Internet Footprinting includes the Footprinting and reconnaissance methods for gaining information through the internet. In Internet Footprinting, processes such as Google Hacking, Google Search, Google Application including search engines other than Google as well.

Objectives of Footprinting

The major objectives of Footprinting are: -

1. To know security posture
2. To reduce focus area
3. Identify vulnerabilities

4. Draw network map

Footprinting Methodology

It is not a big deal to get information regarding anyone as the internet, social media, official websites and other resources have much information about their users which are not sensitive, but a collection of information may fulfill the requirements of an attacker and attacker can gather enough information by a little effort. Below are more often techniques used by hackers: -

- Footprinting through Search Engines
- Footprinting through Advance Google Hacking Techniques
- Footprinting through Social Networking Sites
- Footprinting through Websites
- Footprinting through Email
- Footprinting through Competitive Intelligence
- Footprinting through WHOIS
- Footprinting through DNS
- Footprinting through Network
- Footprinting through Social Engineering

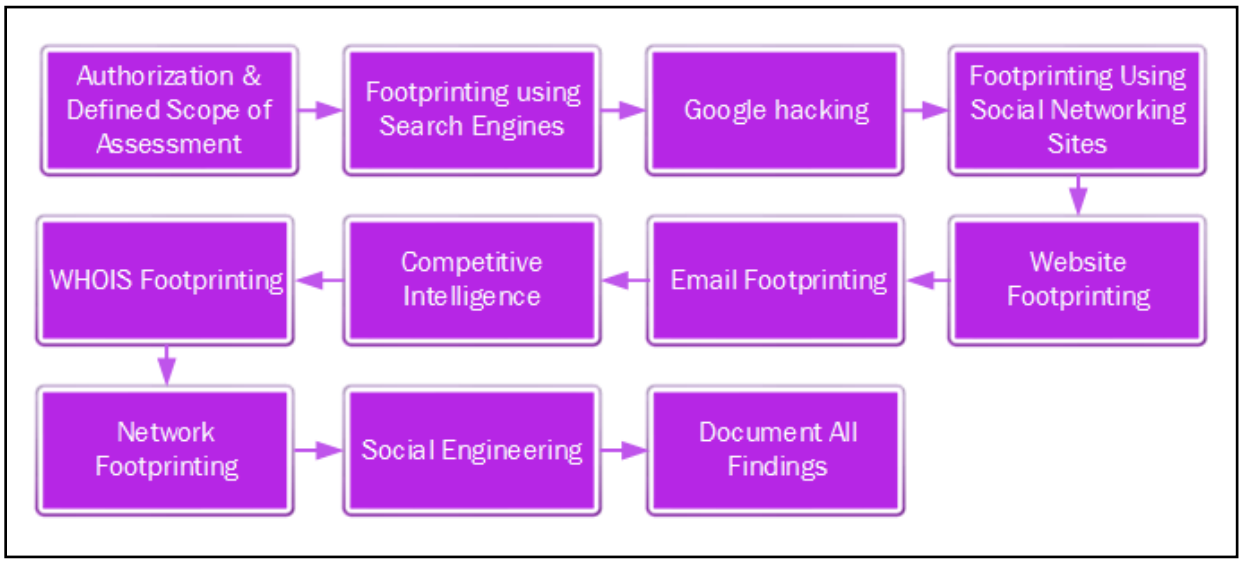


Figure 2-01 Footprinting Methodology

Footprinting through Search Engines

The most basic option that is very responsive as well is Footprinting through search engines. Search engines extract the information about an entity you have searched for from internet. You can open a web browser and through any search engine like Google or Bing, search for any organization. The result collects every available information on the internet.

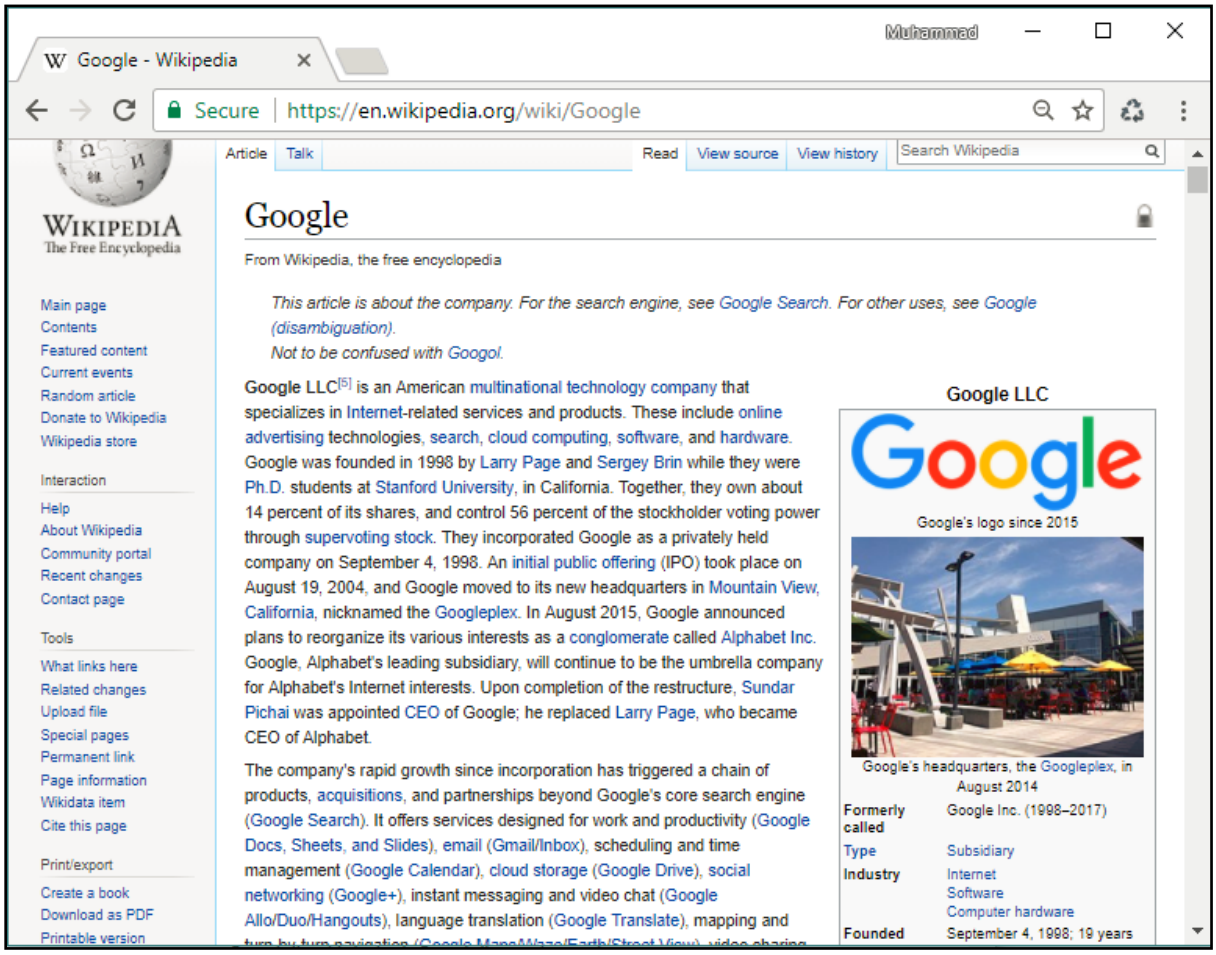


Figure 2-02 Footprinting

For example, Search for google shows the information about the world's most popular search engine itself. This information includes headquartering location, the date on which the organization founded, names of founders, number of employees, parent organization, and its official website. You can scroll to its official website to get more information or any other websites to get information about it.

Apart from this publically available information, websites and search engines caches can also serve the information that is not available, updated or modified on the official website.

Finding Company's Public and Restricted Websites

During the collection of information, the attacker also collects organization's official Website information including its public and restricted URLs. Official Website can search through a search engine like Google, Bing, and others. To find restricted URL of an organization, using trial and error method, using different services which can fetch the information from Web sites such as www.netcraft.com.

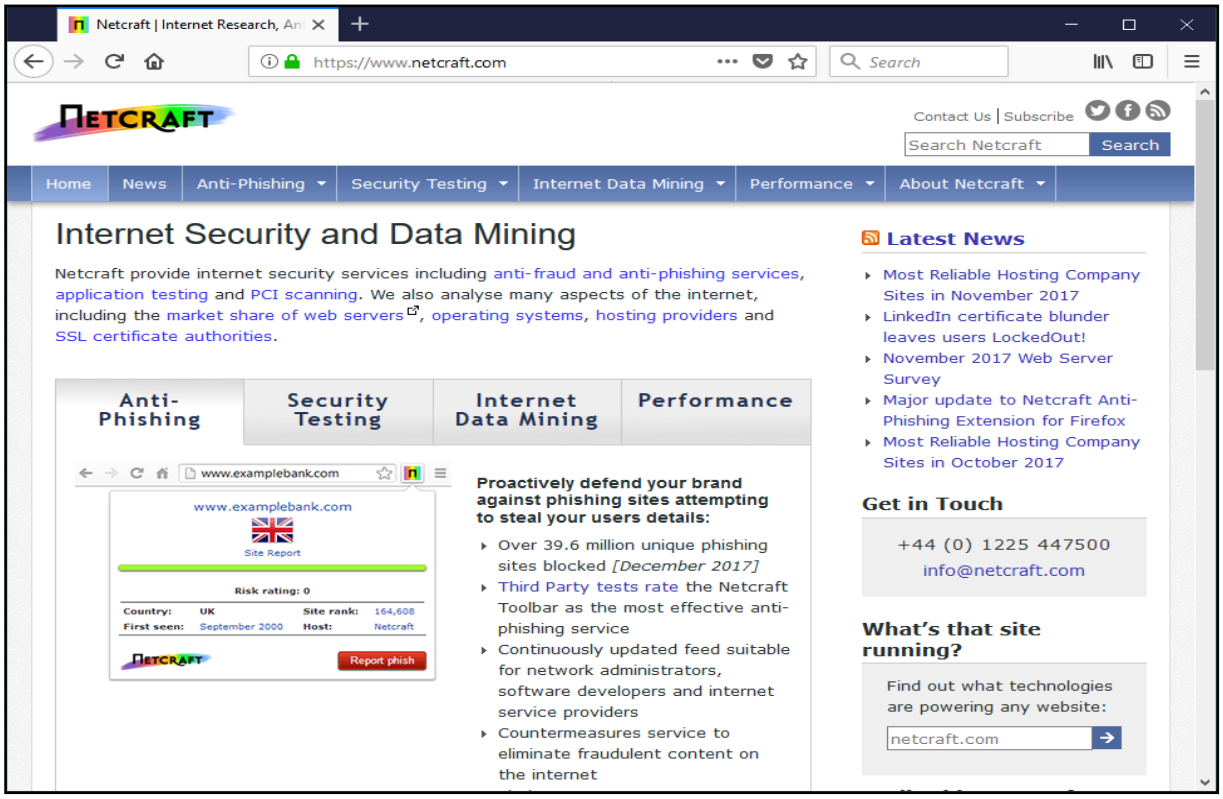


Figure 2-03 Netcraft Webpage

Collect Location Information

After collection of basic information through search engines and different services like Netcraft and Shodan. You can collect local information like the physical location of headquarters with the surrounding, the location of branch offices and other related information from online location and map services.

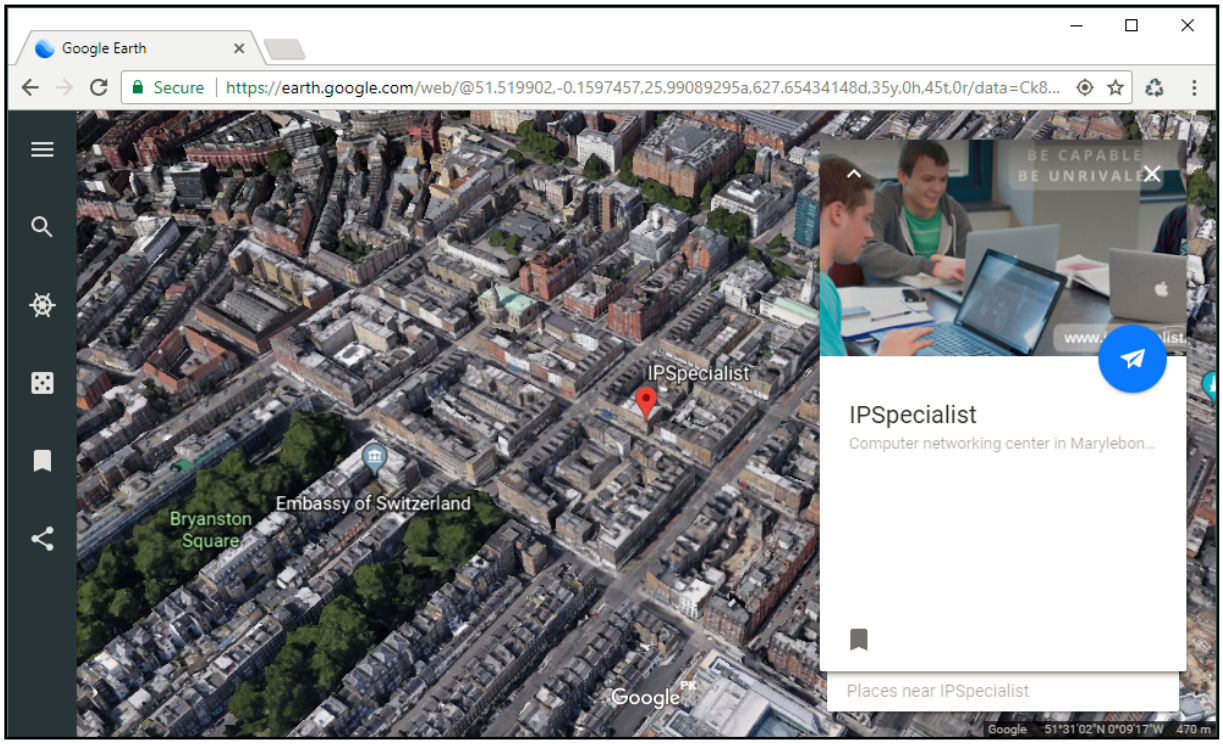


Figure 2-04 Collection of Location Information

Some of these most popular online services are: -

- Google Earth
- Google Map
- Bing Map
- Wikimapia
- Yahoo Map
- Other Map and Location services

People Search Online Services

There are some online services, popularly used to identify the Phones numbers, Addresses, and People.

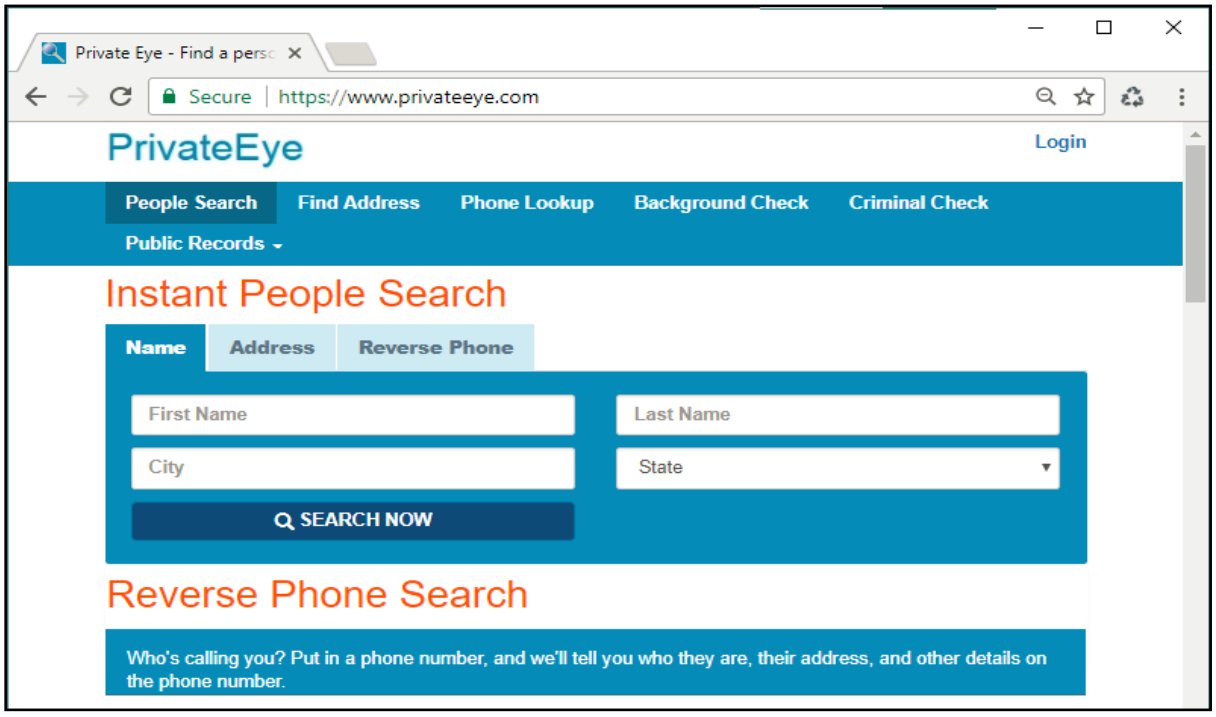


Figure 2-05 Online People Search Service

Some of these websites include: -

- www.privateeye.com
- www.peoplesearchnow.com
- www.publicbackgroundchecks.com
- www.anywho.com
- www.intelius.com
- www.4111.com
- www.peoplefinders.com

Gather Information from Financial Services

There are some Financial Services powered by different search engines which provide financial information of International known organizations. By just searching for your targeted organization, you can get financial information of these organizations. Google and Yahoo are the most popular Online Financial Services.

- www.google.com/finance
- finance.yahoo.com

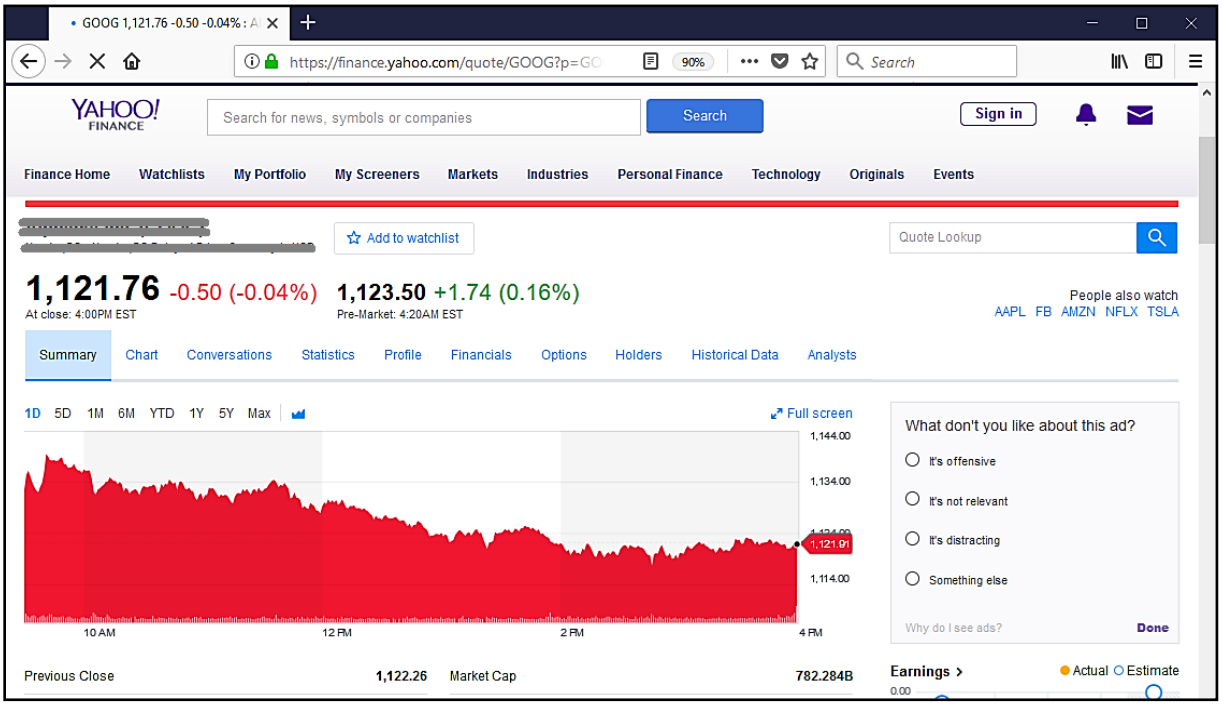


Figure 2-06 Financial Services

Footprinting through Job Sites

In Job Sites, Company's offering the vacancies to people provide their organization's information and portfolio as well is job post. This information includes Company location, Industry information, Contact Information, number of employees, Job requirement, hardware, and software information. Similarly, on these job sites, by a fake job posting, personal information can be collected from a targeted individual. Some of the popular job sites are: -

- www.linkedIn.com
- www.monster.com
- www.indeed.com
- www.careerbuilder.com

Monitoring Target Using Alerts

Google, Yahoo, and other Alert services offer Content monitoring services with an alert feature that notifies the subscriber with the latest and up-to-date information related to the subscribed topic.

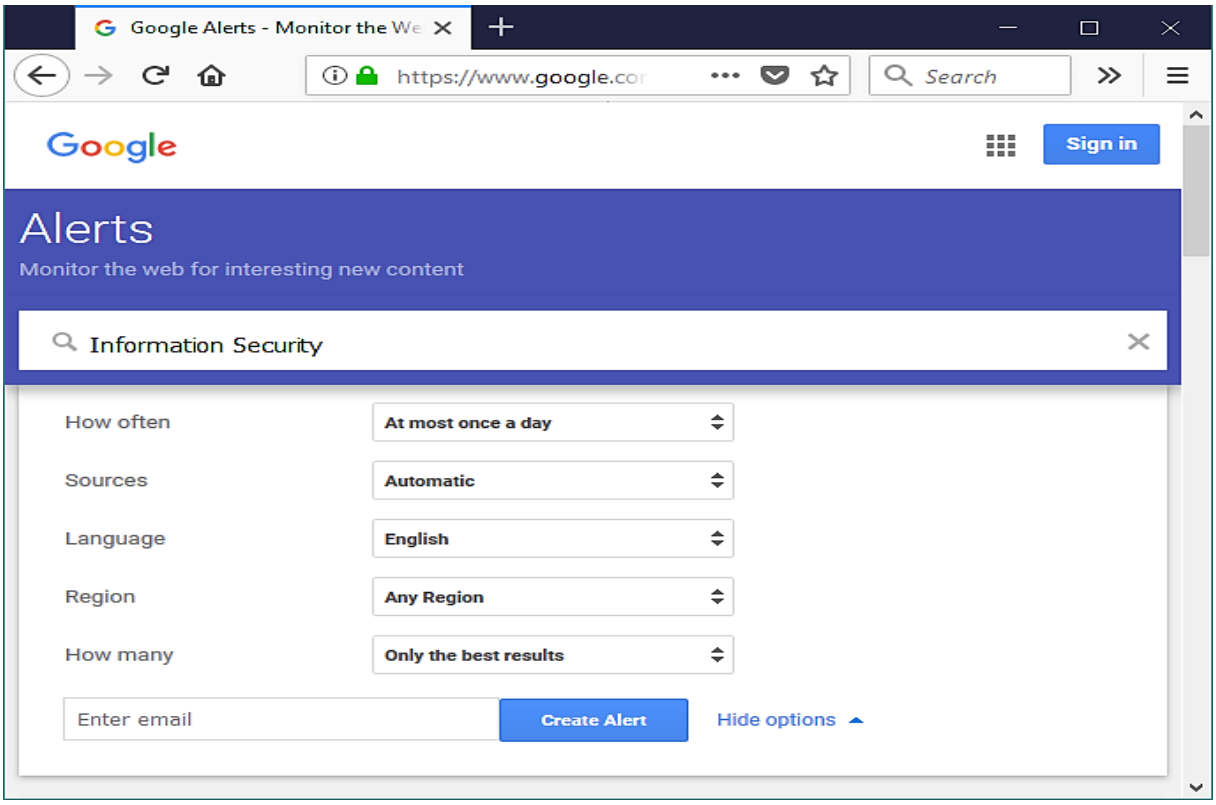


Figure 2-07 Alert Service by Google

Information Gathering Using Groups, Forums, and Blogs

Groups, Forums, Blogs, and Communities can be a great source of sensitive information. Joining with fake ID on these platforms and reaching closest to the target organization's group is not a big deal for anyone. Any official and non-official group can leak sensitive information.

Footprinting using Advanced Google Hacking Techniques

Google Advanced Search Operators

Some advanced options can be used to search for a specific topic using search engines. These Advance search operators made the searching more appropriate and focused on a certain topic. Advanced search operators by google are: -

Advanced Search Operators	Description
site :	Search for the result in the given domain
related :	Search for Similar web pages
cache :	Display the web pages stored in Cache
link :	List the websites having a link to a specific web page
allintext :	Search for websites containing a specific keyword
intext :	Search for documents containing a specific keyword

allintitle :	Search for websites containing a specific keyword in the title
intitle :	Search for documents containing a specific keyword in the title
allinurl :	Search for websites containing a specific keyword in URL
inurl :	Search for documents containing a specific keyword in URL

Table 2-01 Google Advanced Search Operators

For Google Advanced Search, you can also go to the following URL:

https://www.google.com/advanced_search

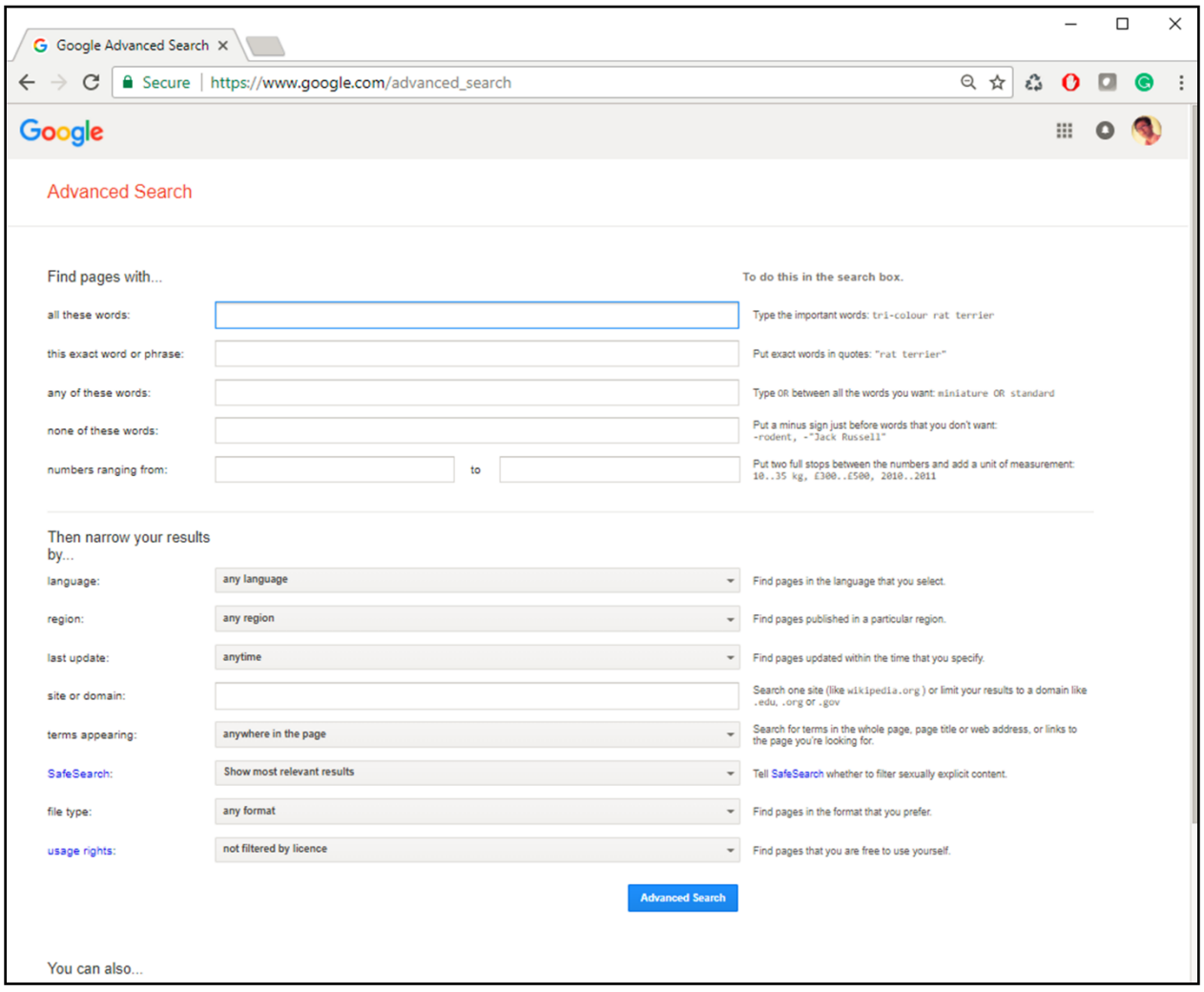


Figure 2-08 Footprinting with Google Advanced Search

Google Hacking Database (GHDB)

Google hacking, Google Dorking is a combination of computer hacking techniques that find the security holes within an organization's network and systems using Google search and other applications powered by Google. Google Hacking popularized by Johnny Long. He categorized the queries in a database known as Google Hacking Database (GHDB).

This categorized database of queries is designed to uncover the information. This information might be sensitive and not publically available. Google hacking is used to speed up searches. As shown in the figure, through www.exploit-db.com, you can search GHDB or browse the category of GHDB. Similarly, www.hackersforcharity.org is also an online platform for GHDB.

Enter the following URL:

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

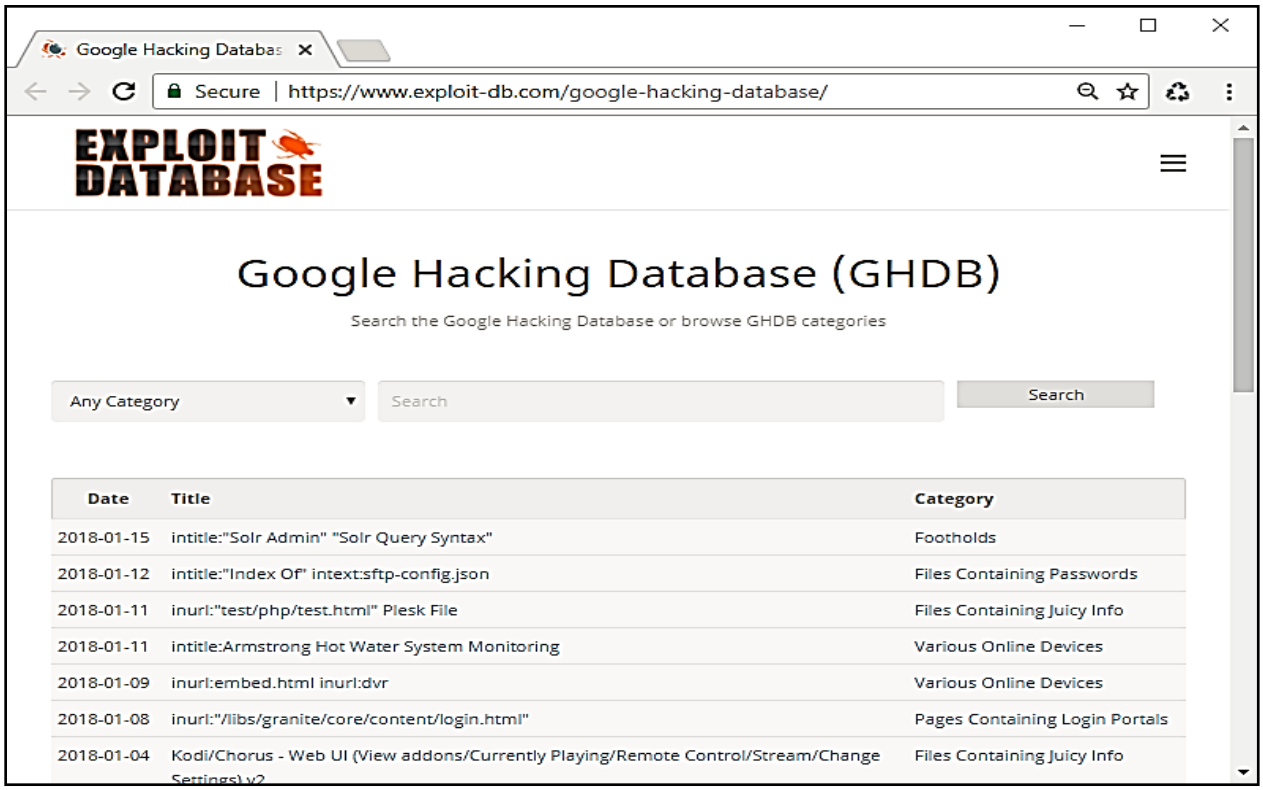


Figure 2-09 Google Hacking Database

Google hacking database provide the updated information that is useful for exploitation such as footholds, sensitive directories, vulnerable files, error messages and much more.

Footprinting through Social Networking Sites

Social Engineering

Social Engineering in Information Security refers to the technique of psychological manipulation. This trick is used to gather information from different social networking and other platforms from people for fraud, hacking and getting information for being close to the target.

Footprinting using Social Engineering on Social Networking Sites

Social Networking is one of the best information sources among other sources. Different popular and most widely used social networking site has made quite easy to find

someone, get to know about someone, including its basic personal information as well as some sensitive information as well. Advanced features on these social networking sites also provide up-to-date information. An Example of footprinting through social networking sites can be finding someone on Facebook, Twitter, LinkedIn, Instagram and much more.

Figure 2-10 Social Networking Sites

Social Networking is not only a source of joy, but it also connects people personally, professionally and traditionally. Social Networking platform can provide sufficient information of an individual by searching the target. Searching for Social Networking for People or an organization brings much information such as Photo of the target, personal information and contact details, etc.

What Users Do	Information	What attacker gets
People maintain their profile	• Photo of the target • Contact numbers • Email Addresses • Date of birth • Location • Work details	• Personal Information about a target including personal information, photo, etc. • Social engineering
People updates their status	• Most recent personal information • Most recent location • Family & Friends information • Activities & Interest • Technology related information • Upcoming events information	• Platform & Technology related information. • Target Location. • List of Employees / Friends / Family. • Nature of business

Table 2-02 Social Engineering

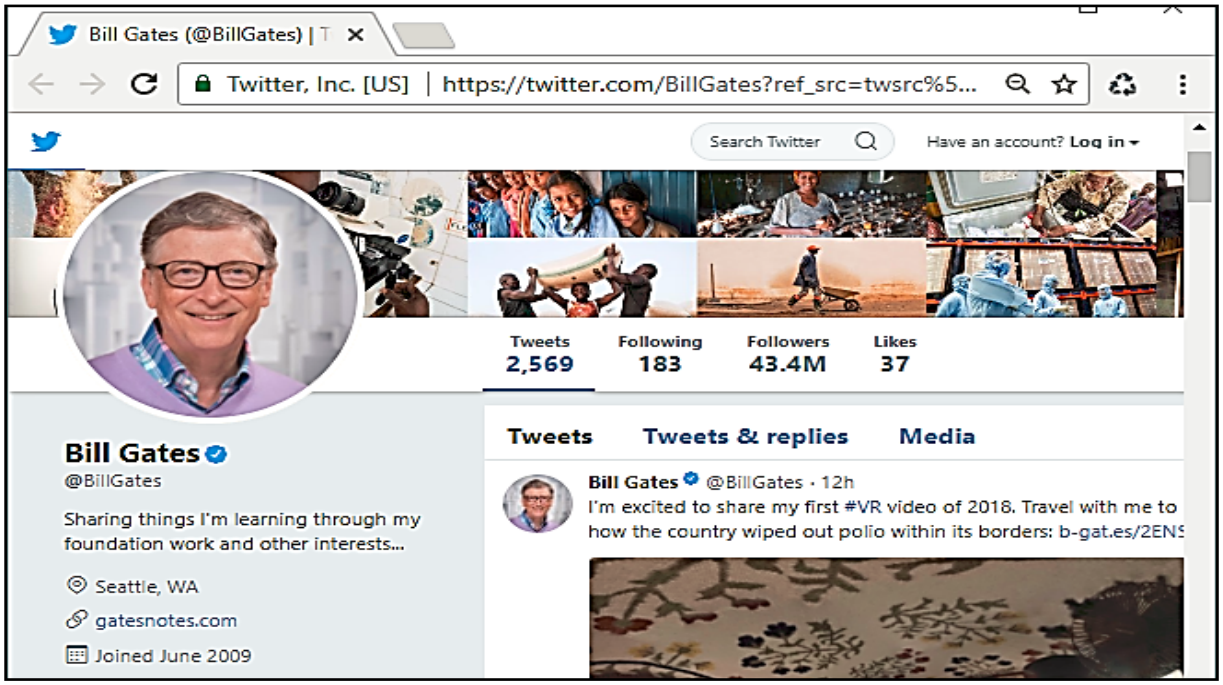
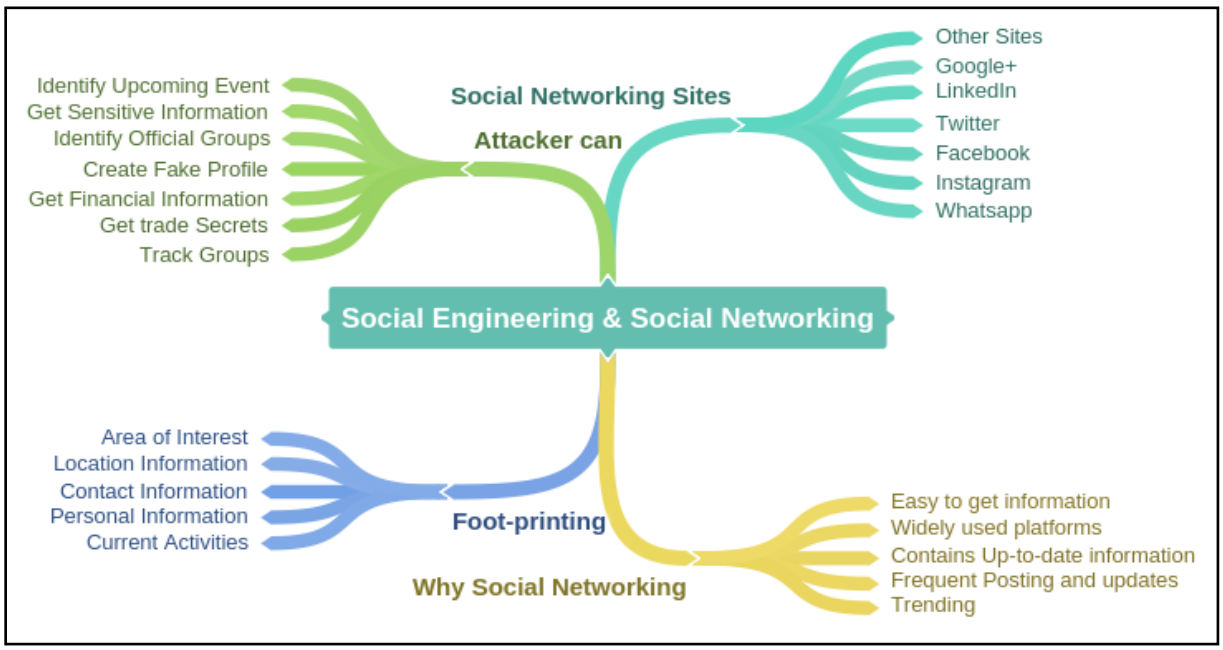


Figure 2-11 Collection of Information from Social Networking

Profile picture can identify the target; the profile can gather personal information. By using this personal information, an attacker can create a fake profile with the same information. Posts have location links, pictures and other location information helps to identify target location. Timelines and stories can also reveal sensitive information. By gathering information of interest and activities, an attacker can join several groups and forums for more footprinting. Furthermore, skills, employment history, current employment and much more. These are the information that can be gathered to easily and used for determining the type of business of an organization, technology, and platforms used by an organization. In the posts, people are posting on these platforms, never think that what they are posting. Their post may contain enough information for an attacker, or a piece of required information for an attacker to gain access to their systems.

Mind Map



Website Footprinting

Website Footprinting includes monitoring and investigating about the target organization's official website for gaining information such as Software running, versions of these software's, operating systems, Sub-directories, database, scripting information, and other details. This information can be gathered by online service as defined earlier like netcraft.com or by using software such as Burp Suite, Zaproxy, Website Informer, Firebug, and others. These tools can bring information like connection type and status and last modification information. By getting these type of information, an attacker can examine source code, developer's details, file system structure and scripting.

Determining the Operating System

Using websites such as Netcraft.com can also help in searching for Operating systems that are in use by the targeted organizations. Go to the website www.netcraft.com and enter the target organization's official URL. Results in the figure below are hidden to avoid legal issues.

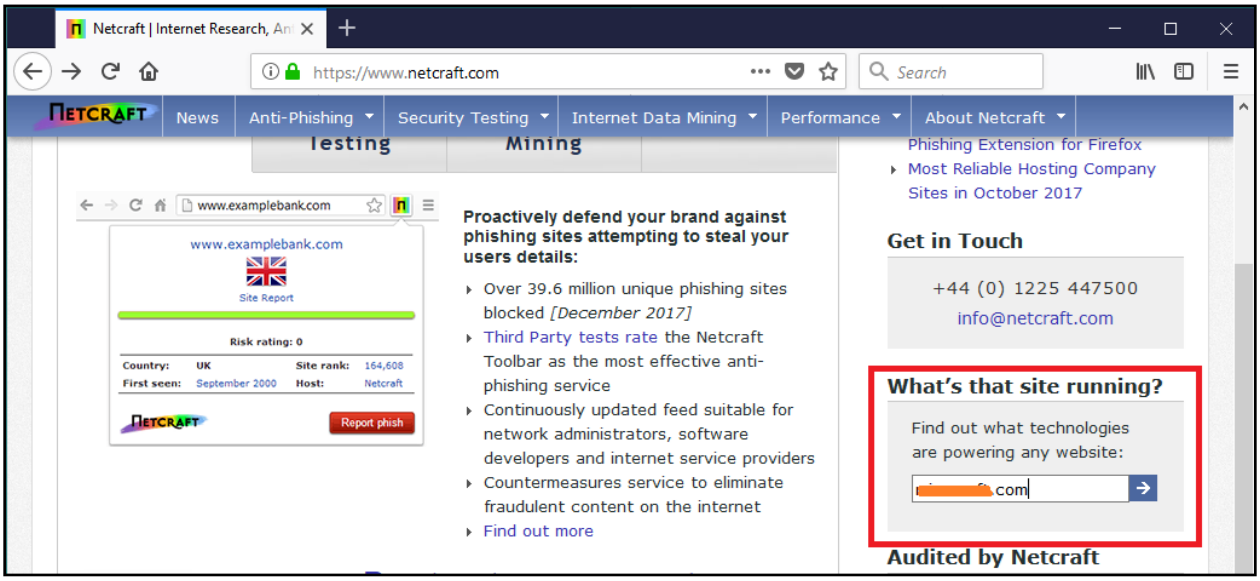


Figure 2-12 Determination of Website Information

The result brings all websites related to the domain of that organization including operating system information and other information. If you enter a complete URL, it shows the in-depth detail of that particular website.

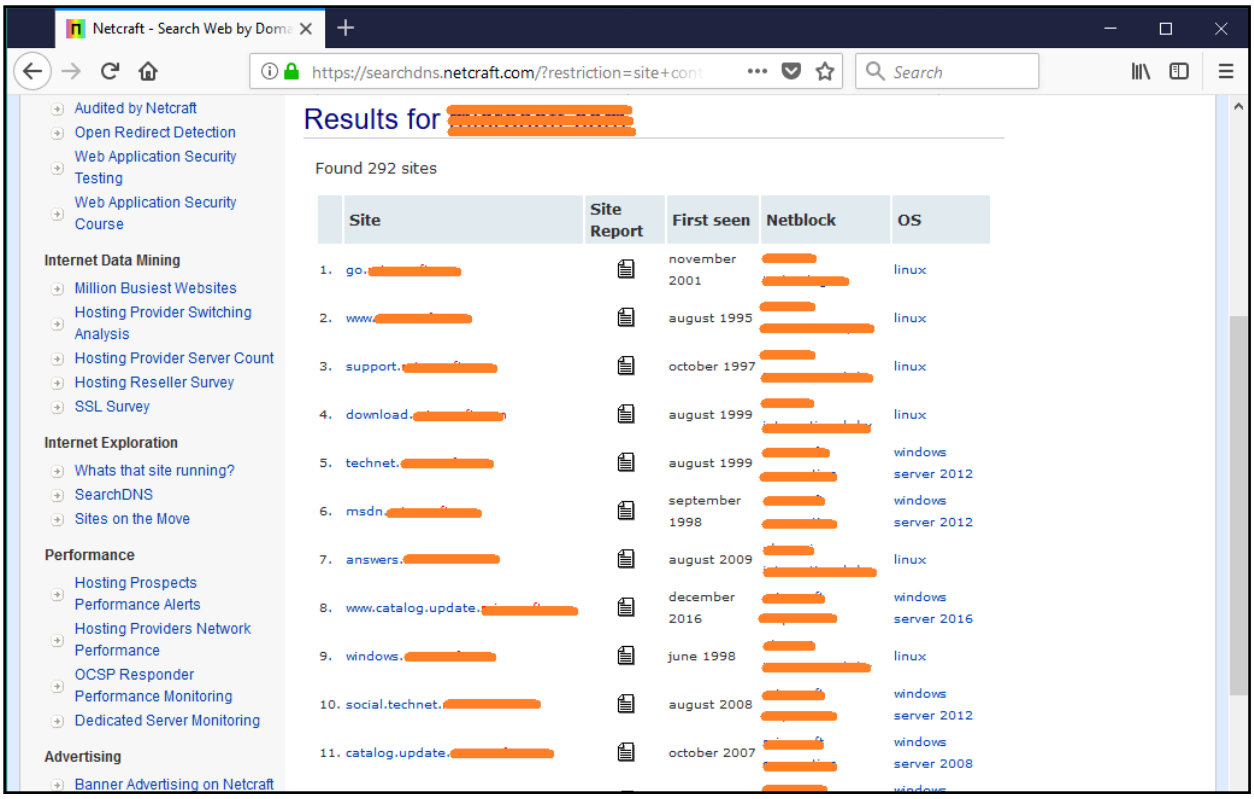


Figure 2-13 Determination of Operating System information

Another popular website for searching the detailed information regarding websites is Shodan, i.e. www.shodan.io. SHODAN search engine lets you find connected devices such as router, servers, IoT & other devices by using a variety of filters.

Go to the following URL

www.shodan.io

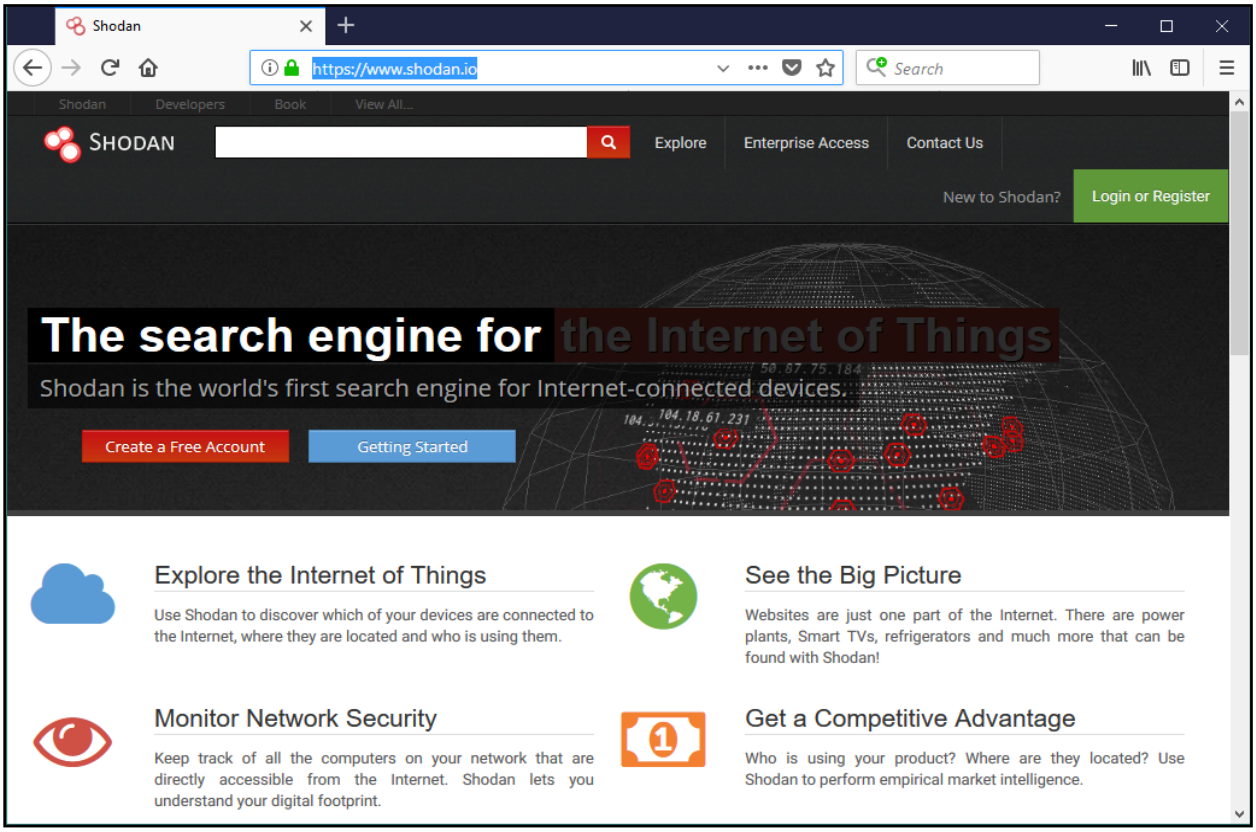


Figure 2-14 Determination of Website information

Now, a search of any device such as CSR1000v as shown in the figure next page:

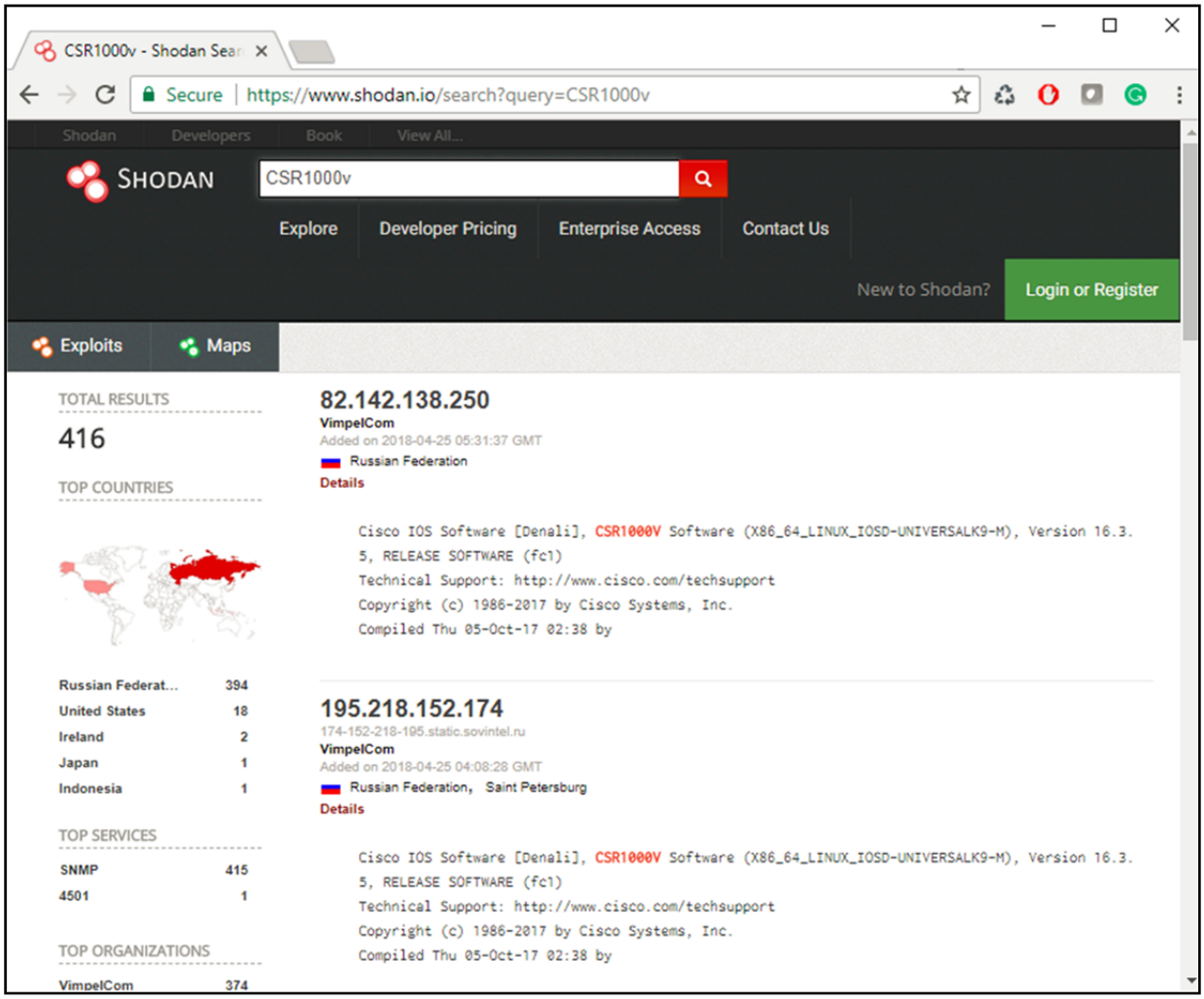


Figure 2-15 Shodan Search Engine

A search of the CSR1000v device brings 416 results along with IP addresses, Cisco IOS software version information, location information and others details.

Website Footprinting using Web Spiders

Web Spiders or Web Crawlers are the internet bots that are used to perform systematic, automated browsing on World Wide Web. This browsing is targeted to a website to gather specific information such as names, email addresses.

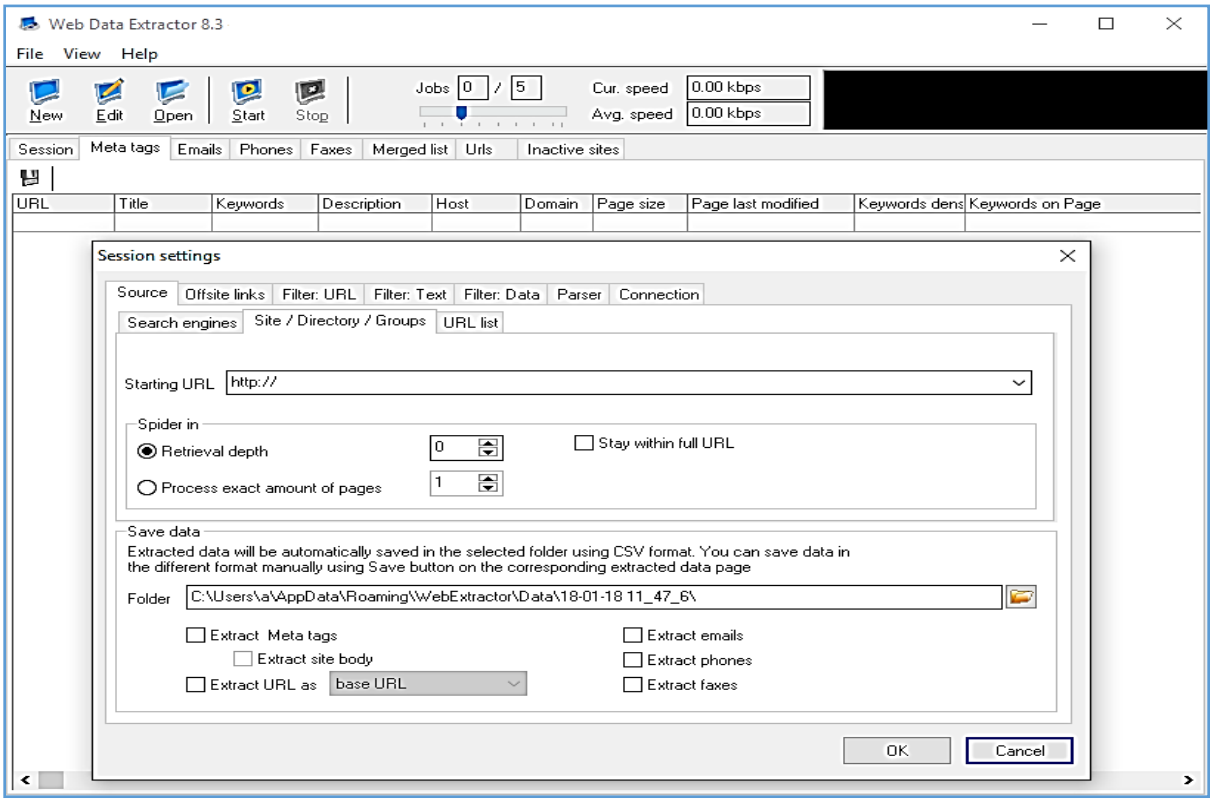


Figure 2-16 Web Data Extractor Application (Web Spider)

Mirroring Entire Website

Mirroring a website is the process to mirror the entire website in the local system. Downloading entire website onto the system enables the attacker to use, inspect the website, directories, structure and to find other vulnerabilities from this downloaded mirrored website copy in an offline environment. Instead of sending multiple copies to a web server, this is a way to find vulnerabilities on a website. Mirroring tools are available which can download a website. Additionally, they are capable of building all directories, HTML and other files from the server to a local directory.

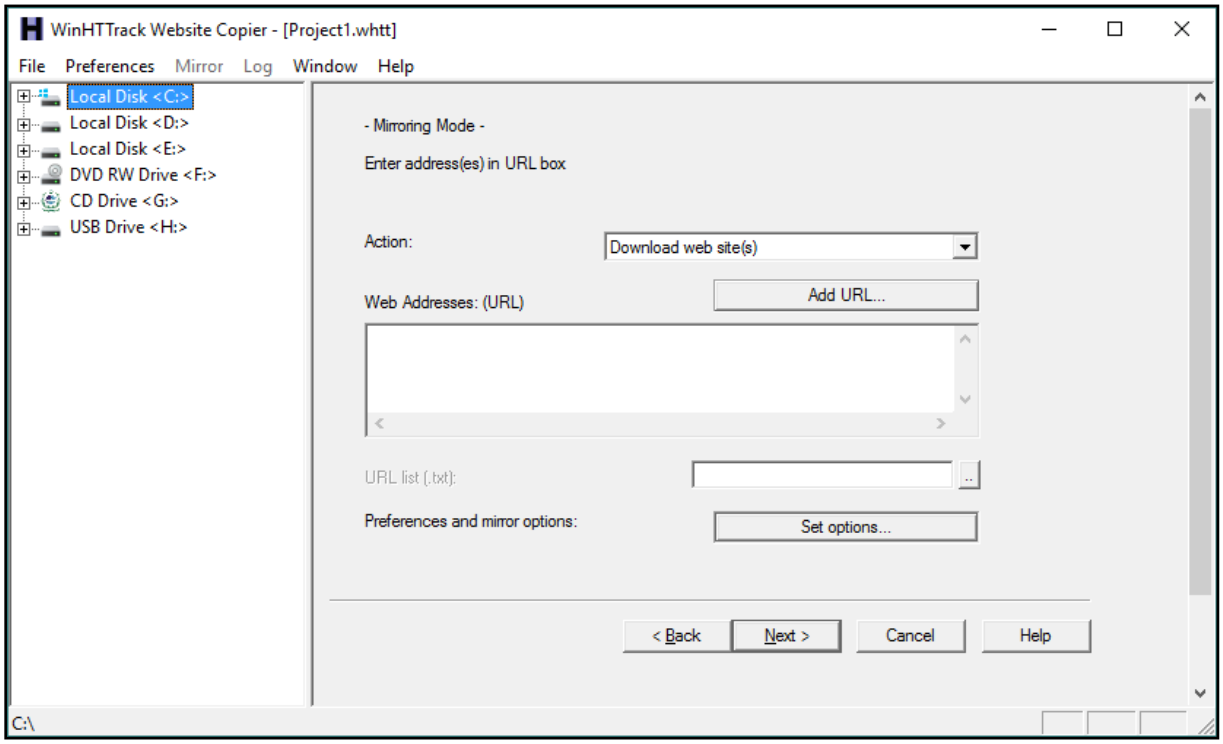


Figure 2-17 WinHTTrack Website Copier

Website Mirroring Tools

Website mirroring tools includes some applications that offer Website mirroring. Some of these tools include: -

Software	Websites
Win HTTrack Website Copier	https://www.httrack.com/page/2/
Surf offline Professional	http://www.surfoffline.com/
Black Widow	http://softbytelabs.com
NCollector Studio	http://www.calluna-software.com
Website Ripper Copier	http://www.tensons.com
Teleport Pro	http://www.tenmax.com
Portable Offline Browser	http://www.metaproducts.com
PageNest	http://www.pagenest.com
Backstreet Browser	http://www.spadixbd.com
Offline Explorer Enterprise	http://www.metaproducts.com
GNU Wget	http://www.gnu.org.com
Hooeey Webprint	http://www.hooeeywebprint.com

Table 2-03 Website Mirroring Tools

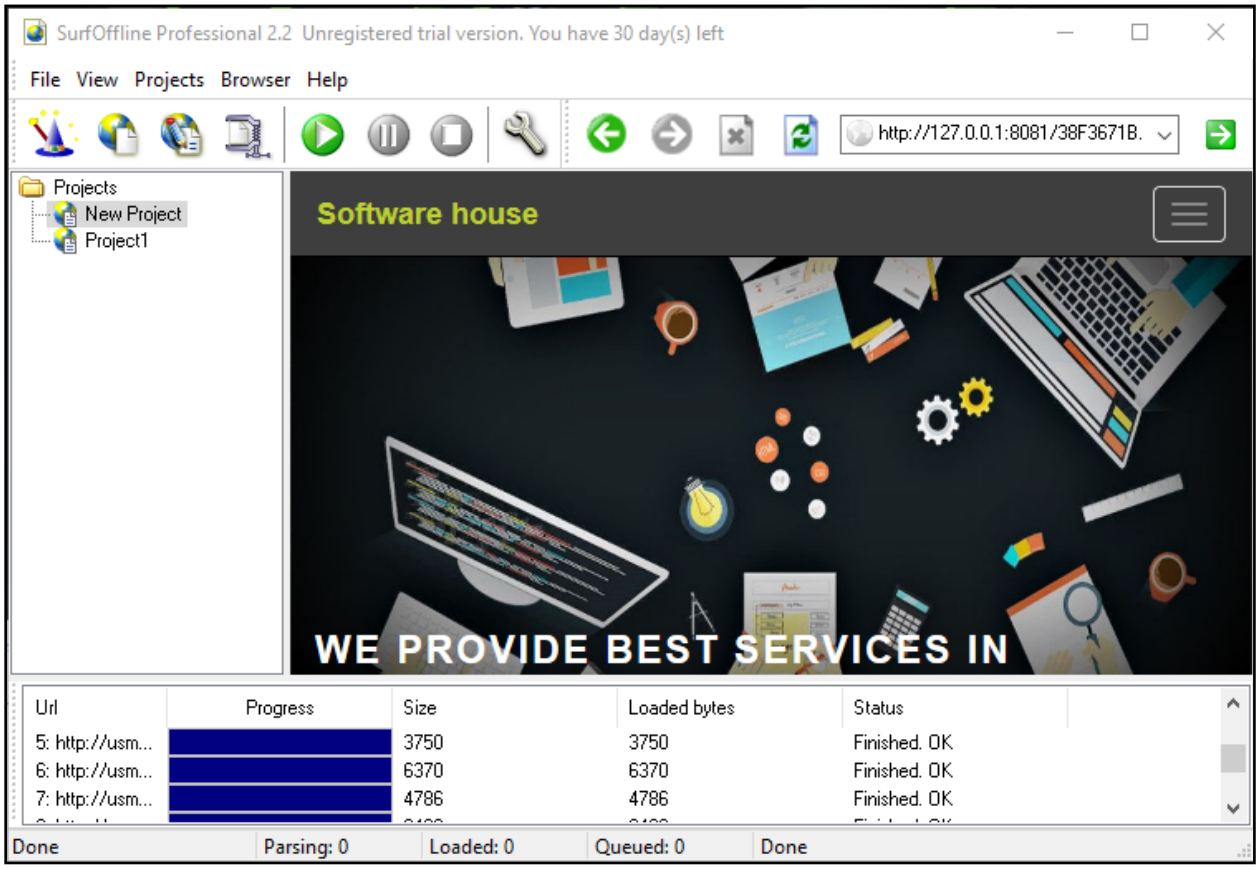


Figure 2-18 Surf Offline Professional Application

Extract Website Information

Archive.com is an online service that provides an archived version of websites. The result consists of a summary of the website including Summary on MIME-type Count, Summary for TLD/HOST/Domain, a sitemap of website and dates, Calendar view and other information.

Extracting Information using the Wayback machine
1. Go to the following URL: **https://web.archive.org** 2. Search for a target website. 3. Select Year from the calendar.

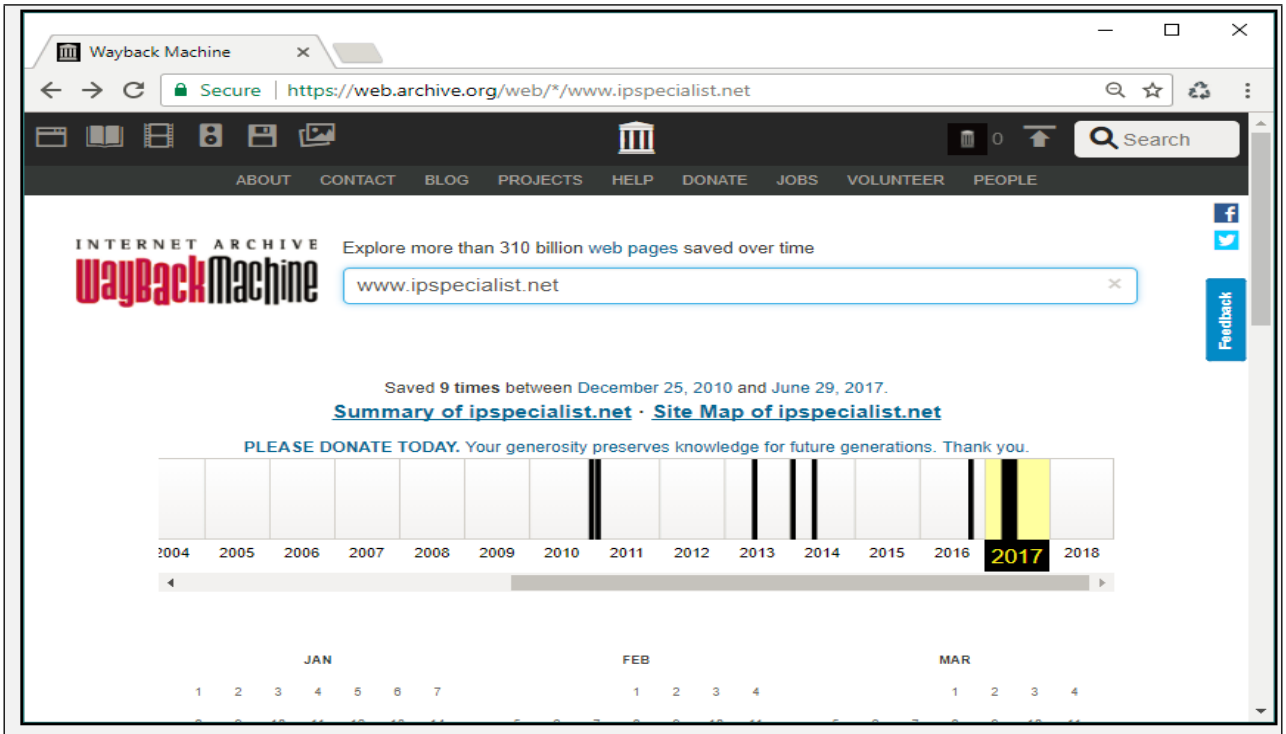


Figure 2-19 Archive.com Wayback Machine

4. Select date from the highlighted dates.

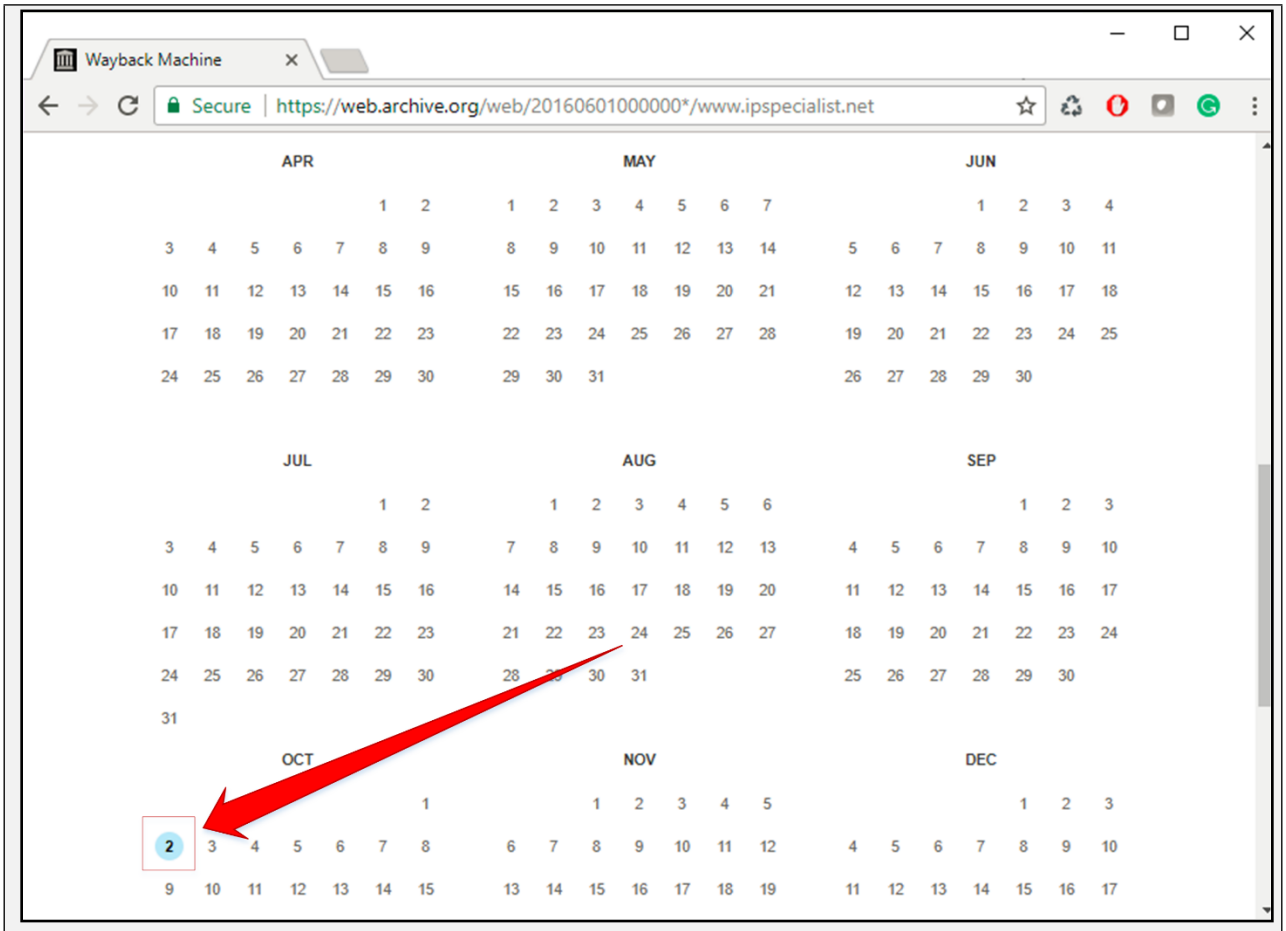


Figure 2-20 Select Date

5. The following is the snapshot of the website on 2nd October 2016.

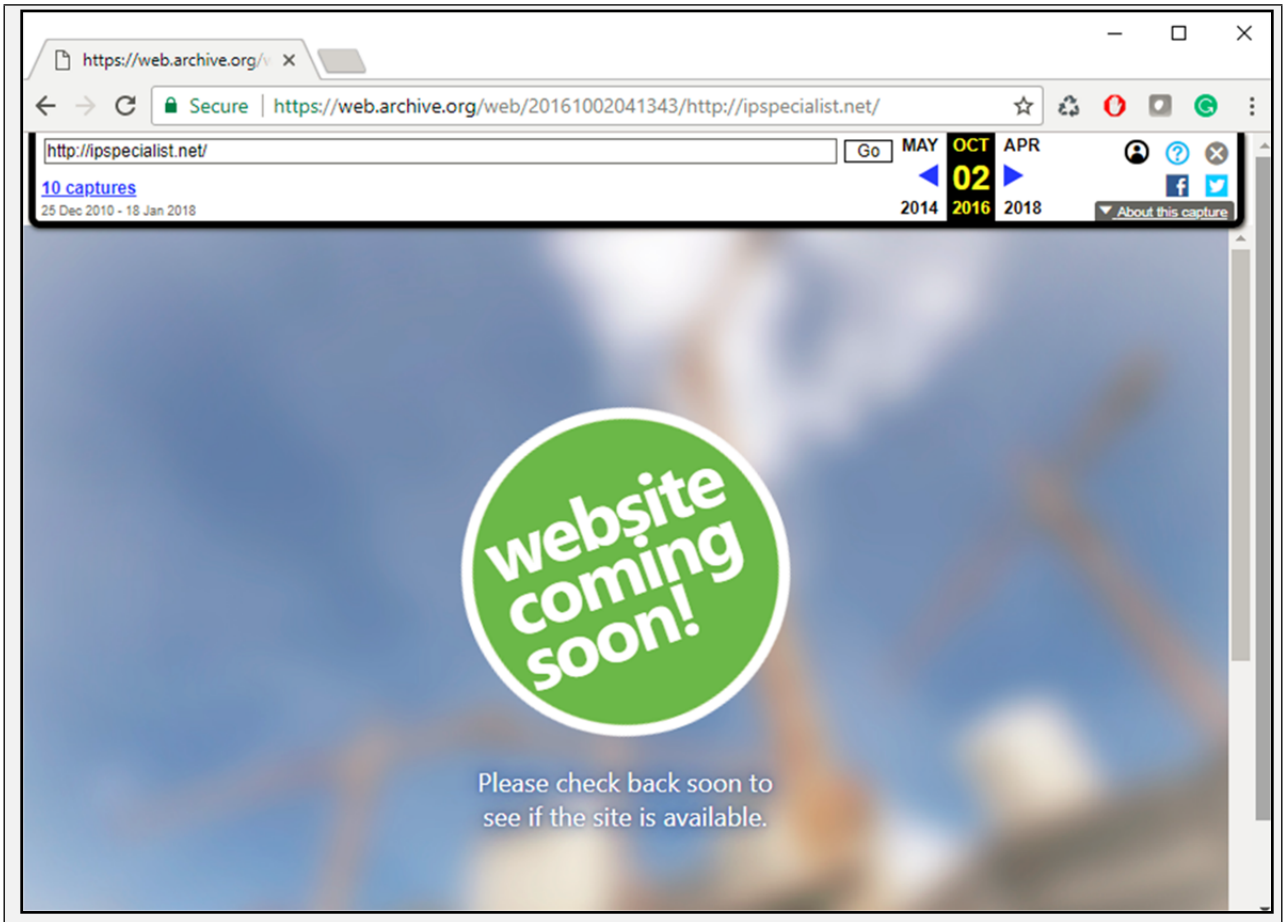


Figure 2-21 Archived Snapshot of Website

Monitoring Web Updates

Website-Watcher and other available tools offer website monitoring. These tools automatically check for updates and changes made to target websites.

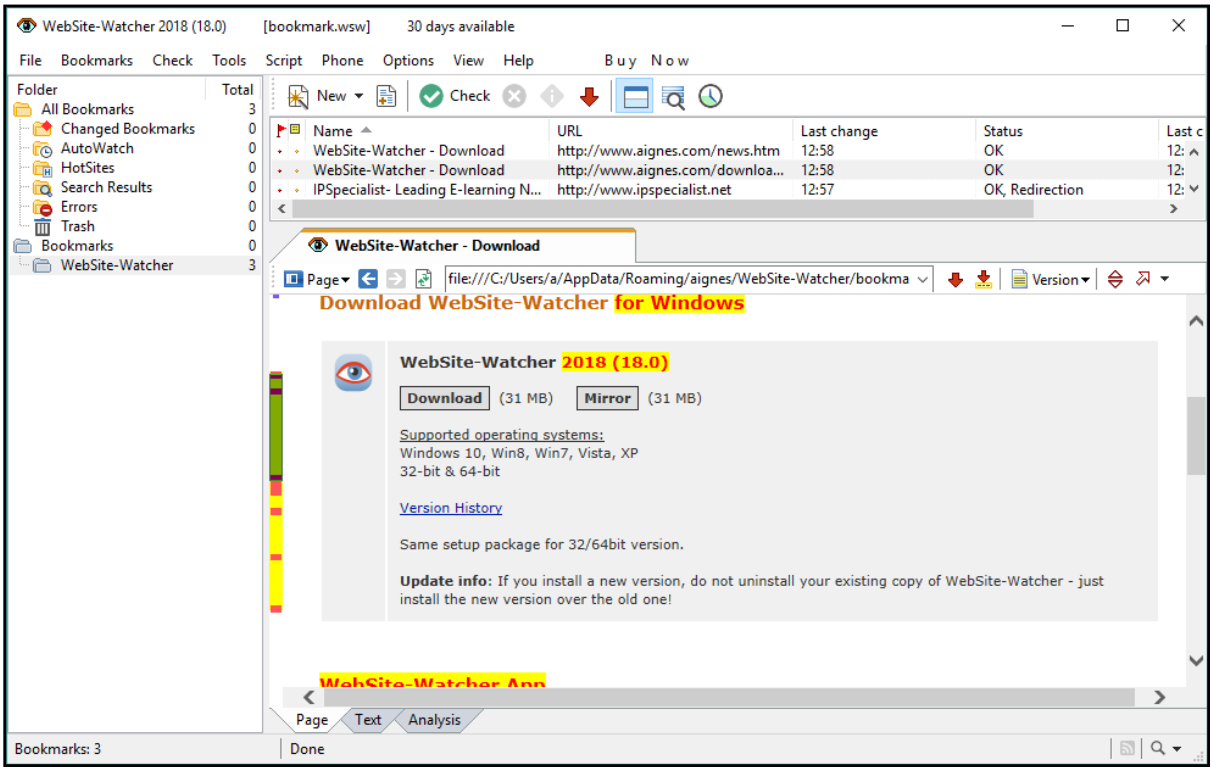


Figure 2-22 Website-Watcher Application

Some other Website Monitoring Tools are: -

Monitoring Tools	Websites
Change Detection	http://www.changedetection.com
Follow That Page	http://www.followthatpage.com
Page2RSS	http://page2rss.com
Watch That Page	http://www.watchthatpage.com
Check4Change	https://addons.mozilla.org
OnWebChange	http://onwebchange.com
Infominder	http://www.infominder.com
TrackedContent	http://trackedcontent.com
Websnitcher	https://websnitcher.com
Update Scanner	https://addons.mozilla.org

Table 2-04 Website Monitoring Tools

Email Footprinting

Email plays an important role in running an organization's business. Email is one of the most popular, widely used professional ways of communication which is used by every organization. Communicating with the partners, employees, competitor, contractors and other types of people which are involved in running an organization. Content or body of Email is hence important, extremely valuable to attackers. This content may include

hardware and software information, user credentials, network and security devices information, financial information which is valuable for penetration testers and attackers. Polite Mail is a very useful tool for Email footprinting. Polite Mail tracks email communication with Microsoft Outlook. Using this tool, with a list of email addresses of a targeted organization, the malicious link can be sent and trace the individual event. Tracing an email using email header can reveal the following information:

- Destination address
- Sender's IP address
- Sender's Mail server
- Time & Date information
- Authentication system information of sender's mail server

Tracking Email from Email Header

Tracing Email from Email header offer hop by hop trace of an email along with IP addresses, Hop Name, and location. Several online and software applications offer Email header tracing. Email Tracker Pro is one of the popular tools.

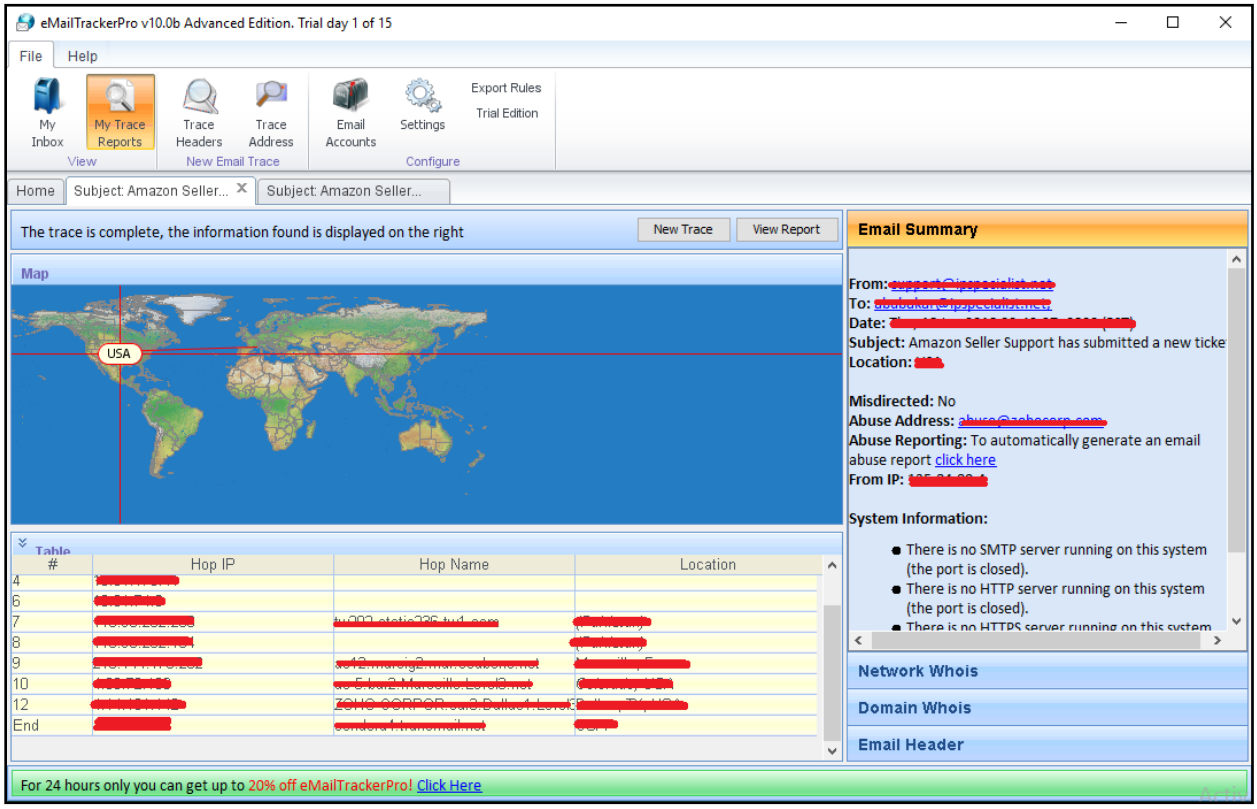


Figure 2-23 Email Tracker Pro

Email Tracking Tools

Popular Email Tracking tools are as follows:

- Polite Mail

- Email Tracker Pro
- Email Lookup
- Yesware
- Who Read Me
- Contact Monkey
- Read Notify
- Did They Read It
- Get Notify
- Point of Mail
- Trace Email
- G-Lock Analytics

Competitive Intelligence

Competitive Intelligence gathering is a method of collecting information, analyzing and gathering statistics regarding the competitors. Competitive Intelligence gathering process is non-interfering as it is the process of collection of information through the different resources. Some basic sources of competitive intelligence are:

- Official Websites
- Job Advertisements
- Press releases
- Annual reports
- Product catalogs
- Analysis reports
- Regulatory reports
- Agents, distributors & Suppliers

Competitive Intelligence Gathering

To get competitive information, you should visit websites like EDGAR, LexisNexis, Business Wire & CNBC. These websites gather information and reports of companies including legal news, press releases, financial information, analysis reports, and upcoming projects and plans as well. For more information, visit these websites: -

Websites	URL
EDGAR	https://www.sec.gov/edgar.shtml
LexisNexis	https://risk.lexisnexis.com
Business Wire	www.businesswire.com/portal/site/home/
CNBC	www.cnbc.com
Hoovers	www.hoovers.com

Table 2-05 Competitive Intelligence Sources

Gathering information from these resources, Penetration testers and attacker can identify: -

- When did the company begin?
- Evolution of the company
- Authority of the company
- Background of an organization
- Strategies and planning
- Financial Statistics
- Other information

Monitoring Website Traffic of Target Company

There are some website monitoring tools, which are being widely used by developers, attackers, and penetration tester to check the statistics of websites. These tools include Web-stat & Alexa and other tools showing information of ranking of the targeted website, geographical view to the user from all over the world, number of worldwide users, users from different countries, daily pages viewed, Daily time on site, the total number of the site linked, and much more.

Website Traffic Monitoring Tools

Tools	URL
Monitis	http://www.monitis.com/
Web-stat	https://www.web-stat.com/
Alexa	https://www.alexa.com/

Table 2-06 Website Traffic Monitoring Tools

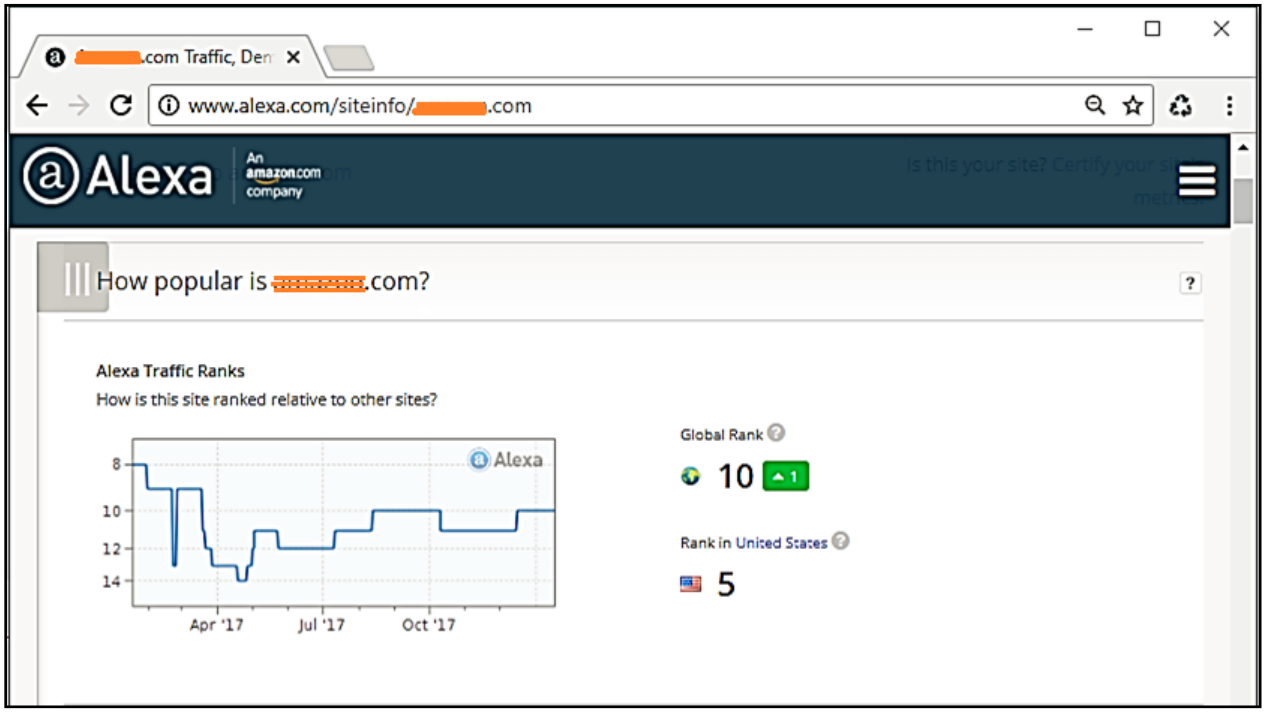


Figure 2-24 Website Statistics using Alexa

In the figure above, the most popular site, Amazon.com is searching by Alexa. The result shows Alexa Traffic Ranking, Global Rank of Website, Rank in the United States. Scrolling down the page shows further results such as a Geographical view of the audience, percentage, and ranking in every country and much more.

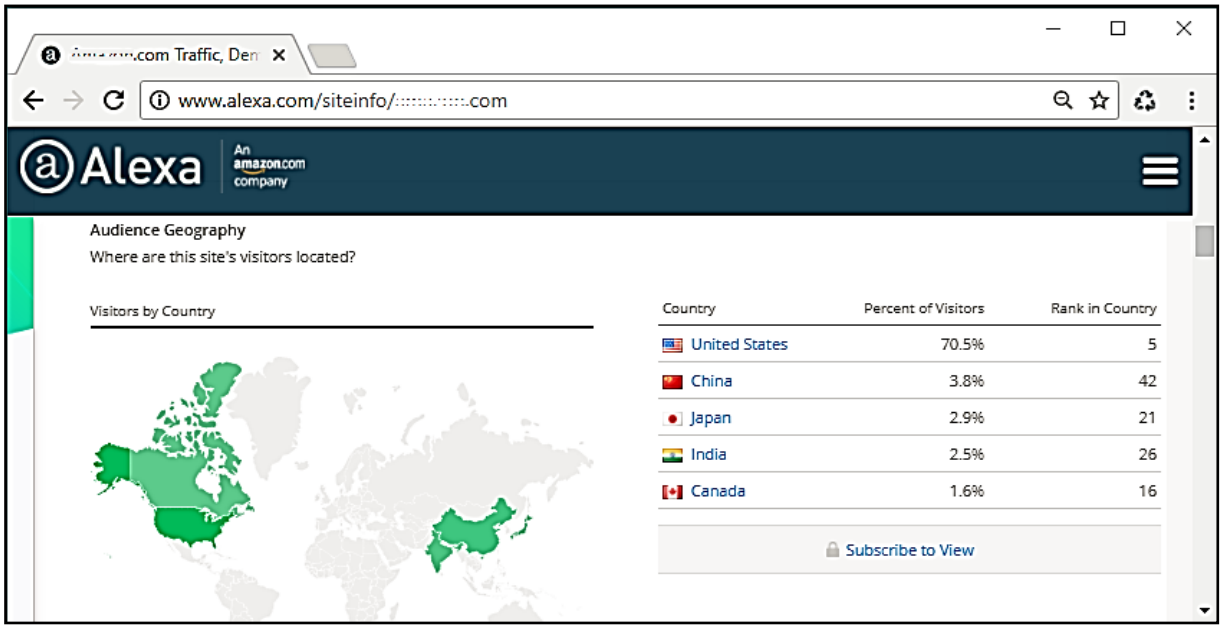


Figure 2-25 Website Statistics using Alexa

Similarly, another tool like Web-stat and Monitis monitor website traffic for collecting bounce rate, live visitors map, and other information.

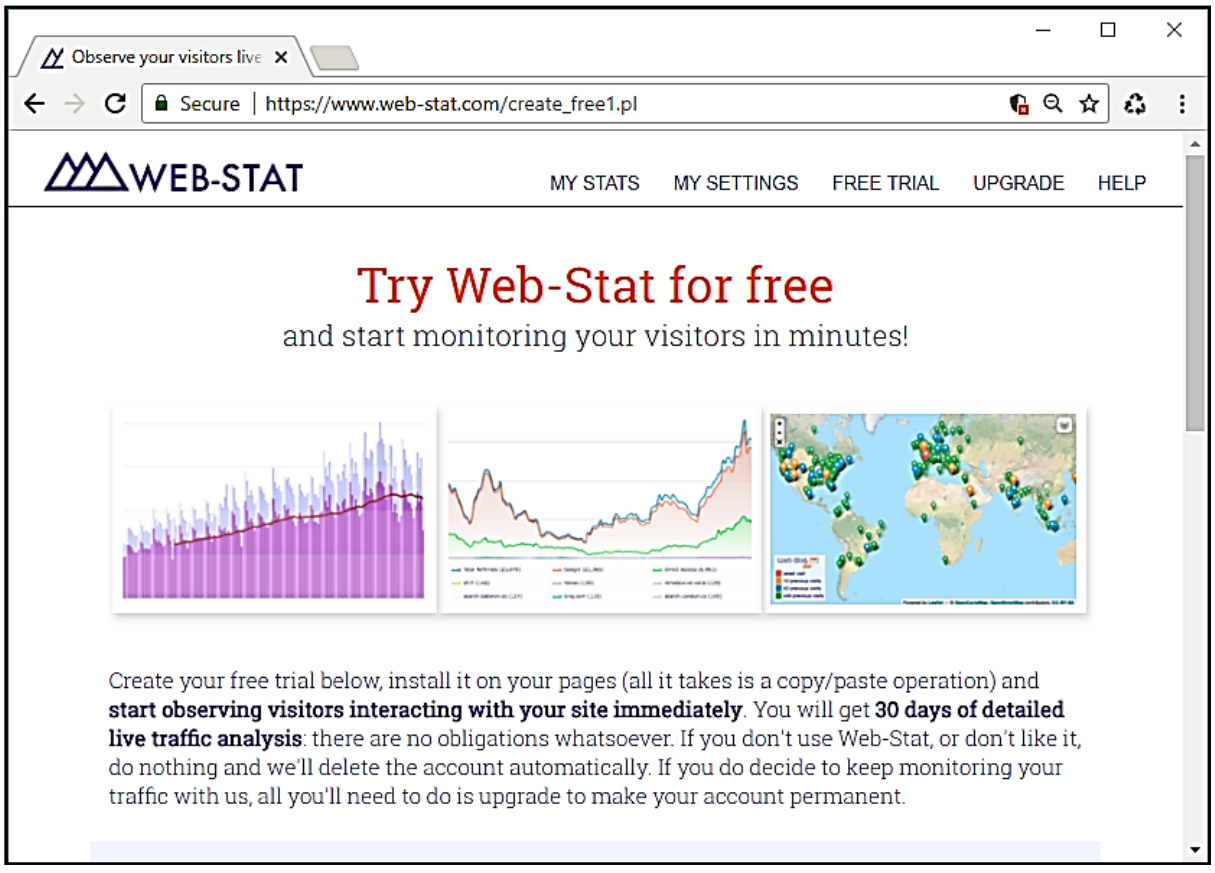


Figure 2-26 Web-stat (Website Monitoring Tool)

Tracking Online Reputation of the Target

The reputation of an organization can be monitored as well through online services. Online Reputation Management (ORM) offers to monitor an organization's reputation. These tools are used to track the reputation, ranking, setting up a notification when an organization known over the internet and much more.

Tools for Tracking Online Reputation

Tool	URL
Google Alerts	https://www.google.com
WhosTalkin	http://www.whostalkin.com
Rankur	http://rankur.com
PR Software	http://www.cision.com
Social Mention	http://www.socialmention.com
Reputation Defender	https://www.reputation.com

Table 2-07 Reputation Monitoring Tools

One of the popular monitoring tools is Trackur (www.trackur.com). Here you can search any keyword such as those shown in the figure showing the result for Microsoft. Their icons separate results from different sources; you can review the result by selecting an entry.

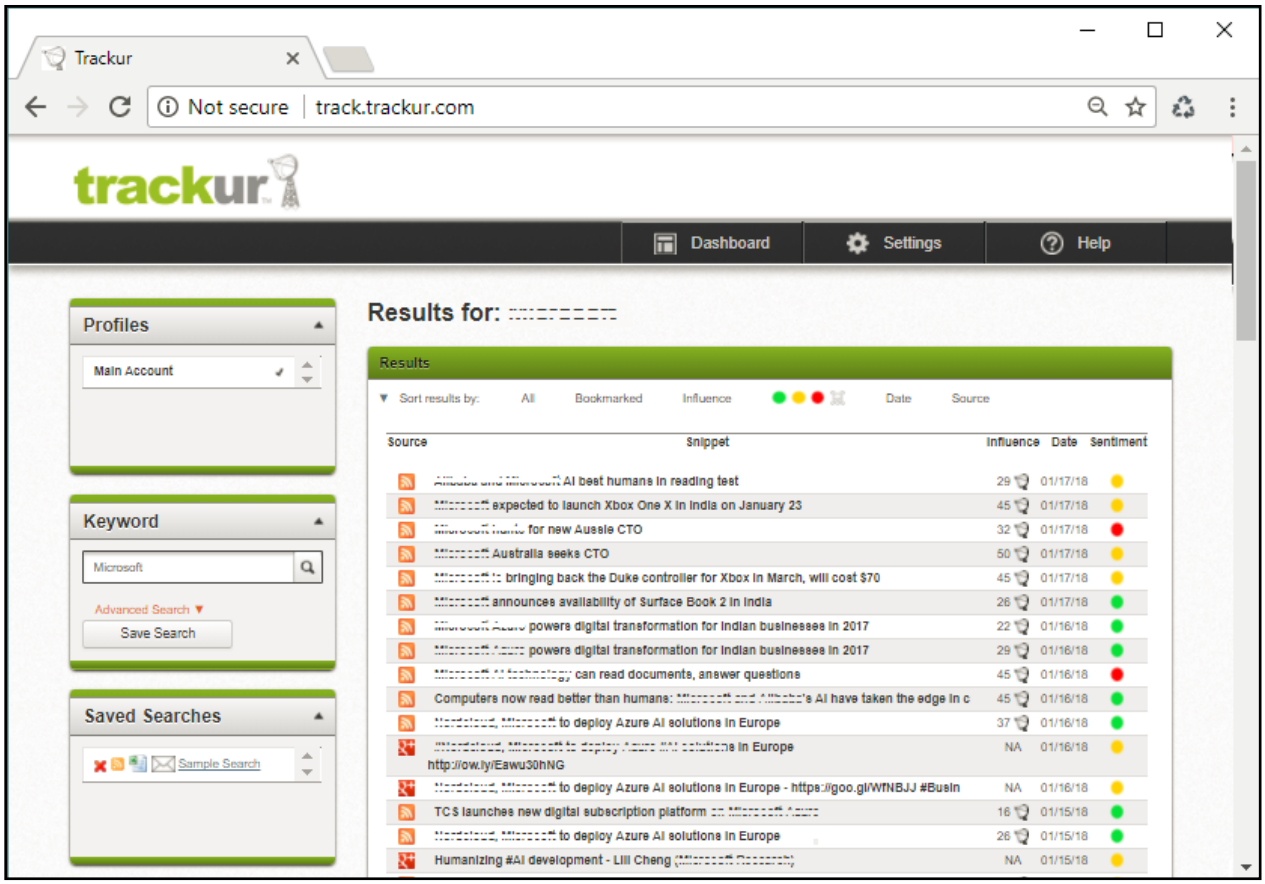


Figure 2-27 Trackur (Reputation Monitoring Tool)

WHOIS Footprinting

WHOIS Lookup

"WHOIS" helps to gain information regarding domain name, ownership information. IP Address, Netblock data, Domain Name Servers and other information's. Regional Internet Registries (RIR) maintain WHOIS database. WHOIS lookup helps to find out who is behind the target domain name.

The Regional Internet Registry system evolved, eventually dividing the world into five RIRs: -

RIRs	Acronym	Location
African Network Information Center	AFRINIC	Africa
American Registry for Internet Numbers	ARIN	United States, Canada, several parts of the Caribbean region, and Antarctica
Asia-Pacific Network Information Centre	APNIC	Asia, Australia, New Zealand, and neighboring countries
Latin America and Caribbean Network Information Centre	LACNIC	Latin America and parts of the Caribbean region
Réseaux IP Européens Network Coordination Centre	RIPE NCC	Europe, Russia, the Middle East, and Central Asia

Table 2-08 Regional Internet Registry System

Performing WHOIS Footprinting

1. Go to the URL **https://www.whois.com/**

Figure 2-28 WHOIS Footprinting Engine

2. A search of Target Domain

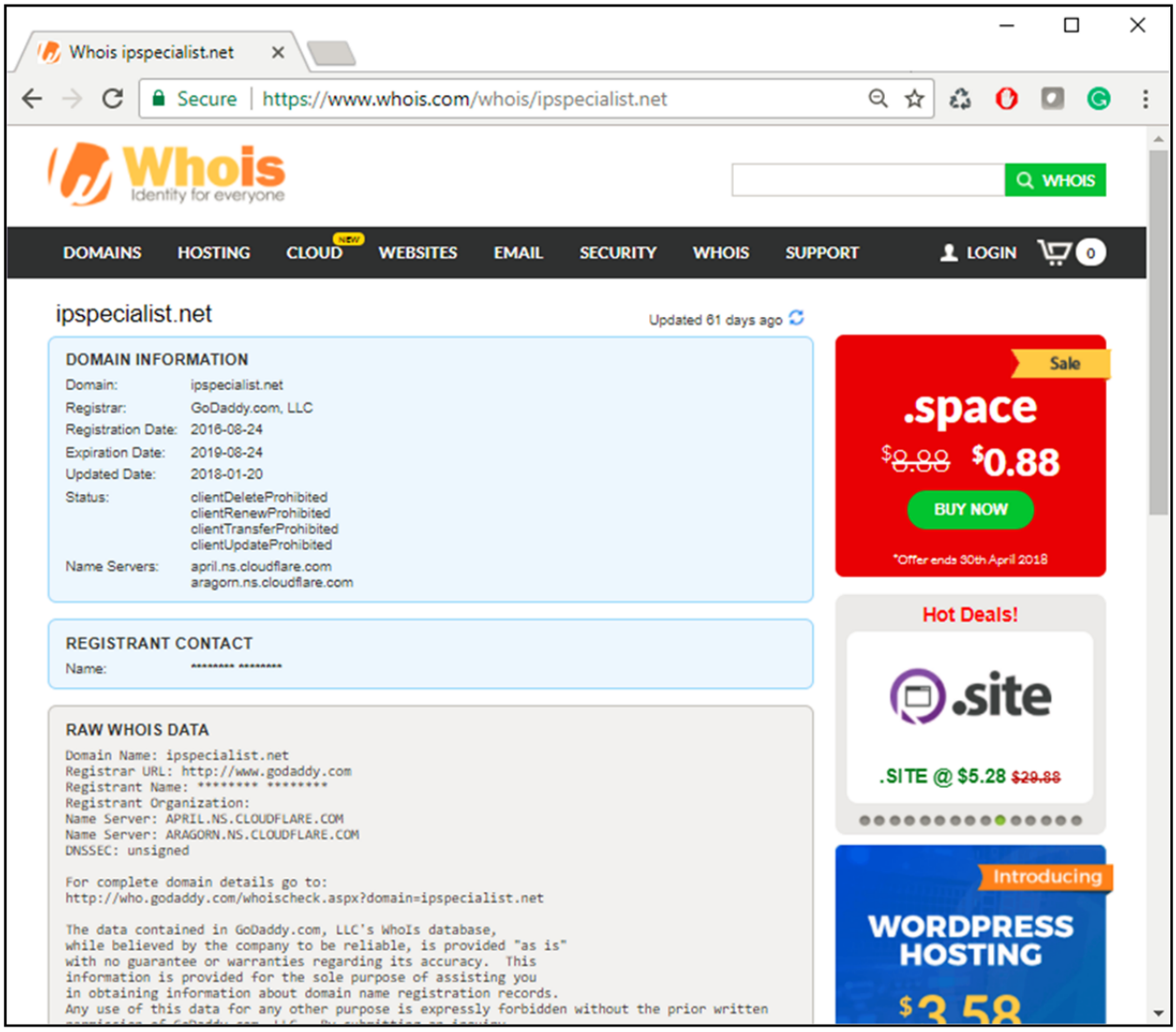


Figure 2-29 WHOIS Footprinting

WHOIS Lookup Result Analysis

Lookup Result shows complete domain profile, including

- Registrant information
- Registrant Organization
- Registrant Country
- Domain name server information
- IP Address
- IP location
- ASN
- Domain Status
- WHOIS history
- IP history,

- Registrar history,
- Hosting history

It also includes other information such as Email and postal address of registrar & admin along with contact details. You can go to ***https://whois.domaintools.com*** can enter the targeted URL for whois lookup information.

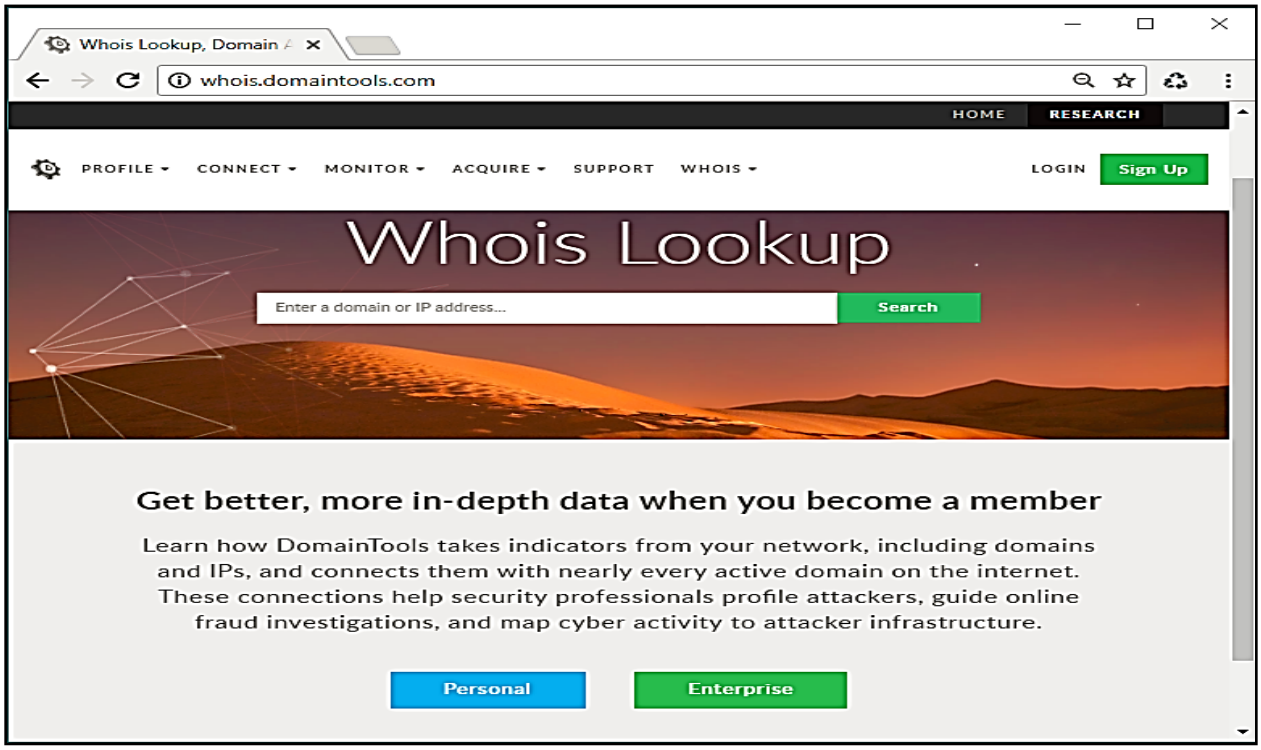


Figure 2-30 whois.domaintools.com

You can download software "***SmartWhois***" from ***www.tamos.com*** for Whois lookup as shown in the figure below: -

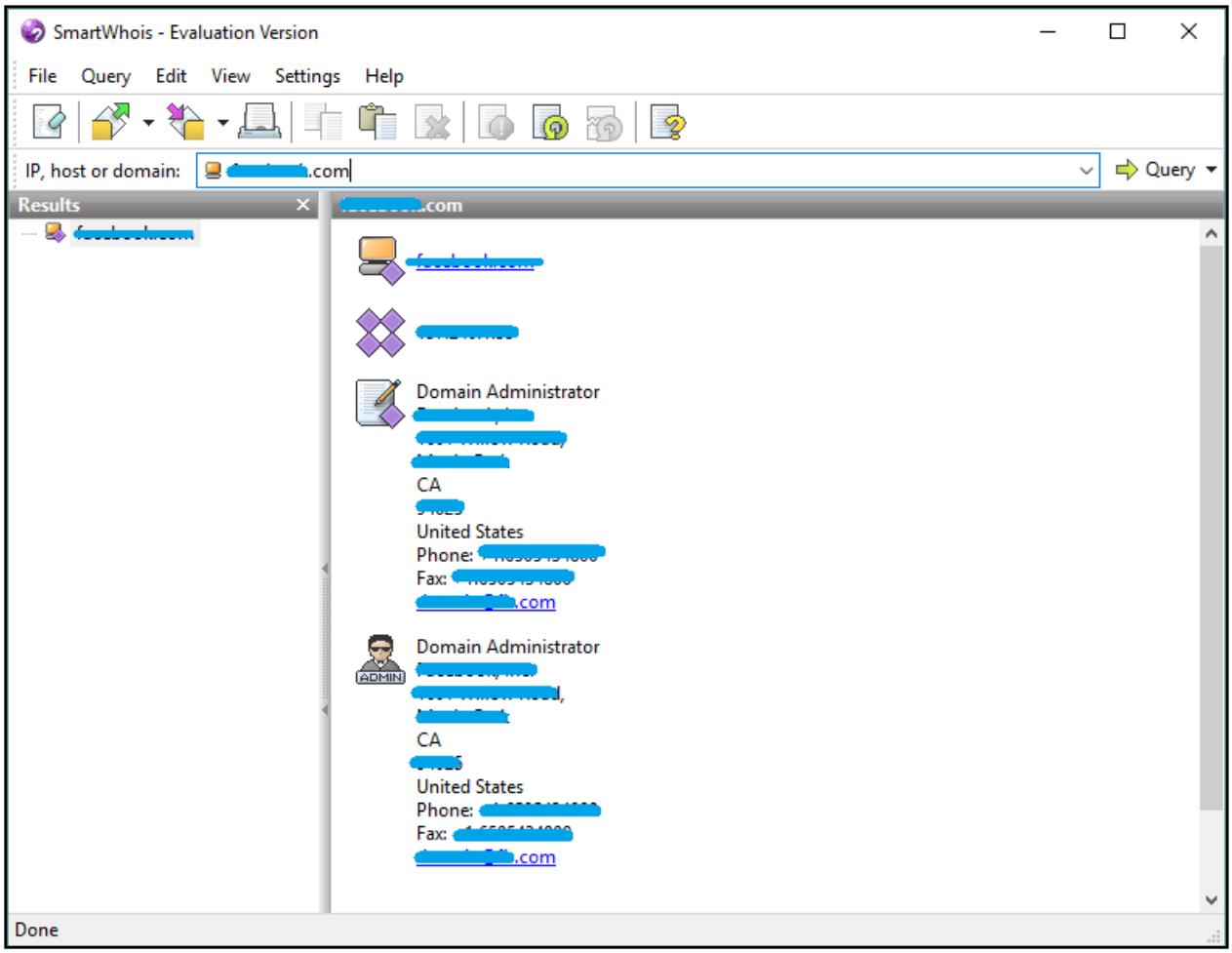


Figure 2-31 SmartWhois Lookup Application

WHOIS Lookup Tools

Tools powered by different developers on WHOIS lookup are listed below: -

- http://lantricks.com
- http://www.networkmost.com
- http://tialsoft.com
- http://www.johnru.com
- https://www.callerippro.com
- http://www.nirsoft.net
- http://www.sobolsoft.com
- http://www.softfuse.com

WHOIS Lookup Tools for Mobile

"DNS Tools" Application by www.dnssniffers.com is available on google play store. It includes other features as well including DNS Report, Blacklist Check, Email Validation, WHOIS, ping and reverses DNS.

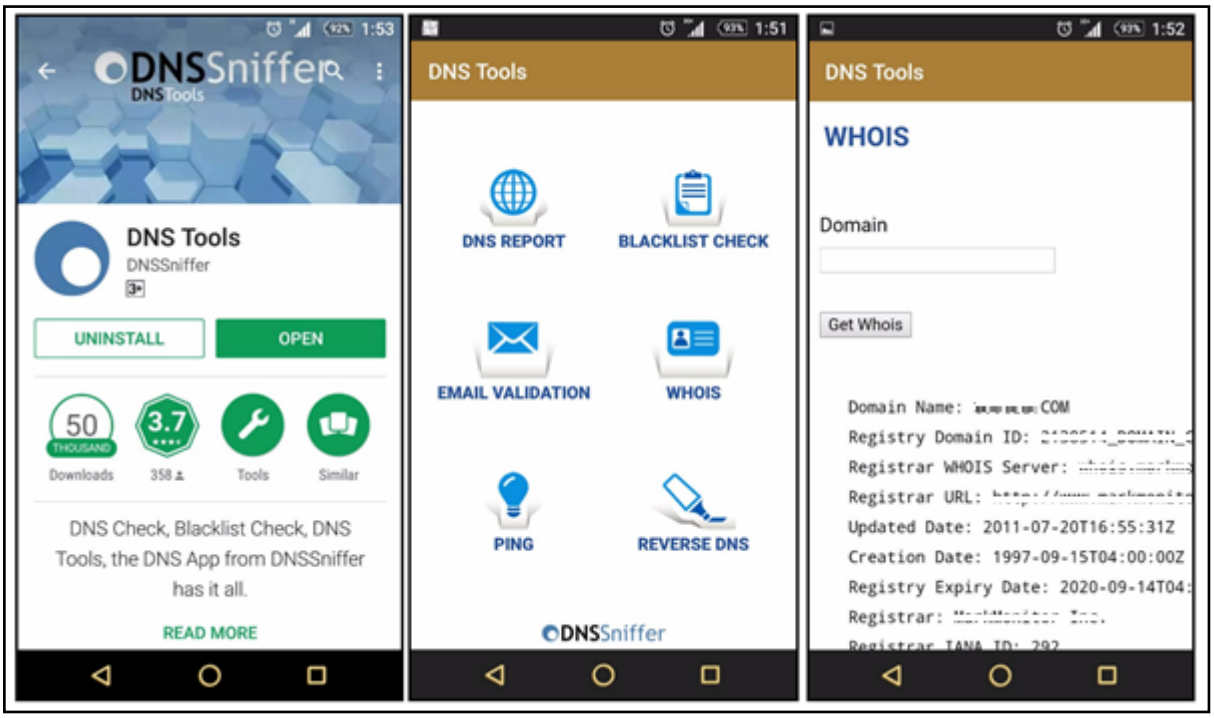


Figure 2-32 DNS tool Application

whois® by www.whois.com.au application on google play store for lookup. There are several lookup tools powered by www.whois.com.au such as: -

- WHOIS Lookup
- DNS Lookup
- RBL Lookup
- Traceroute
- IP Lookup
- API/Bulk Data Access

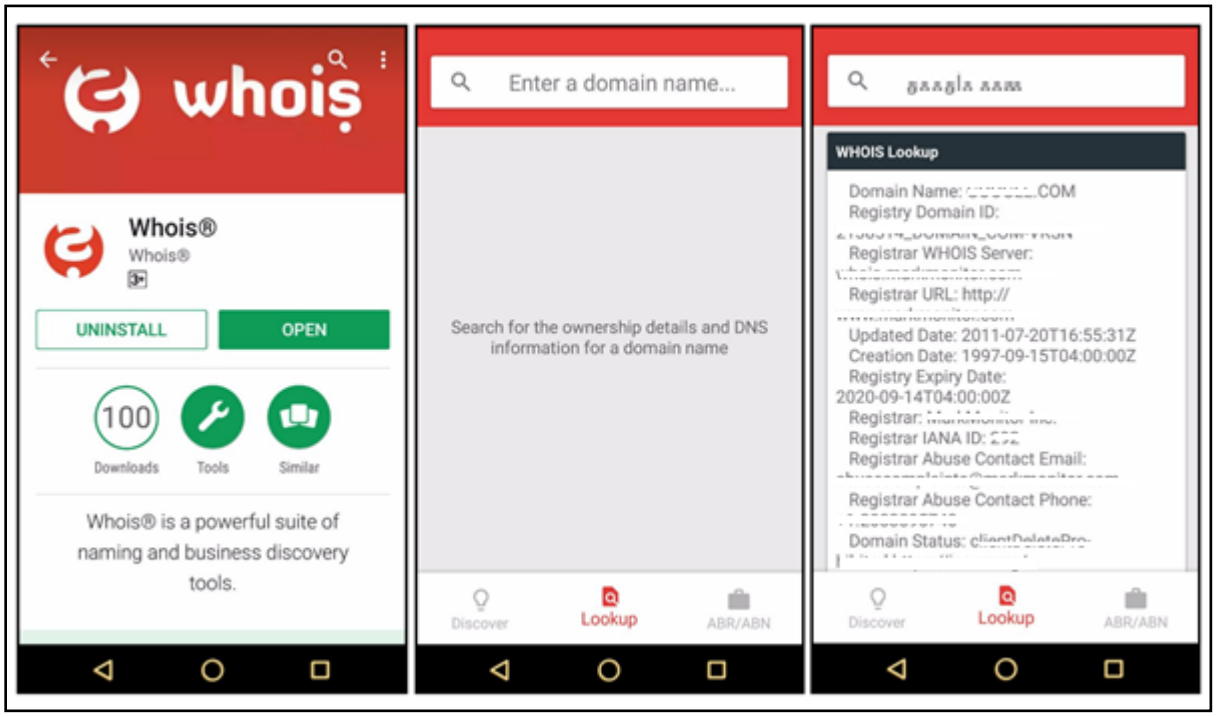


Figure 2-33 Whois Application

www.ultratools.com offers ultra Tools Mobile. This application offers multiple features like Domain health report, DNS Speed test, DNS lookup, Whois Lookup, ping, and other options.

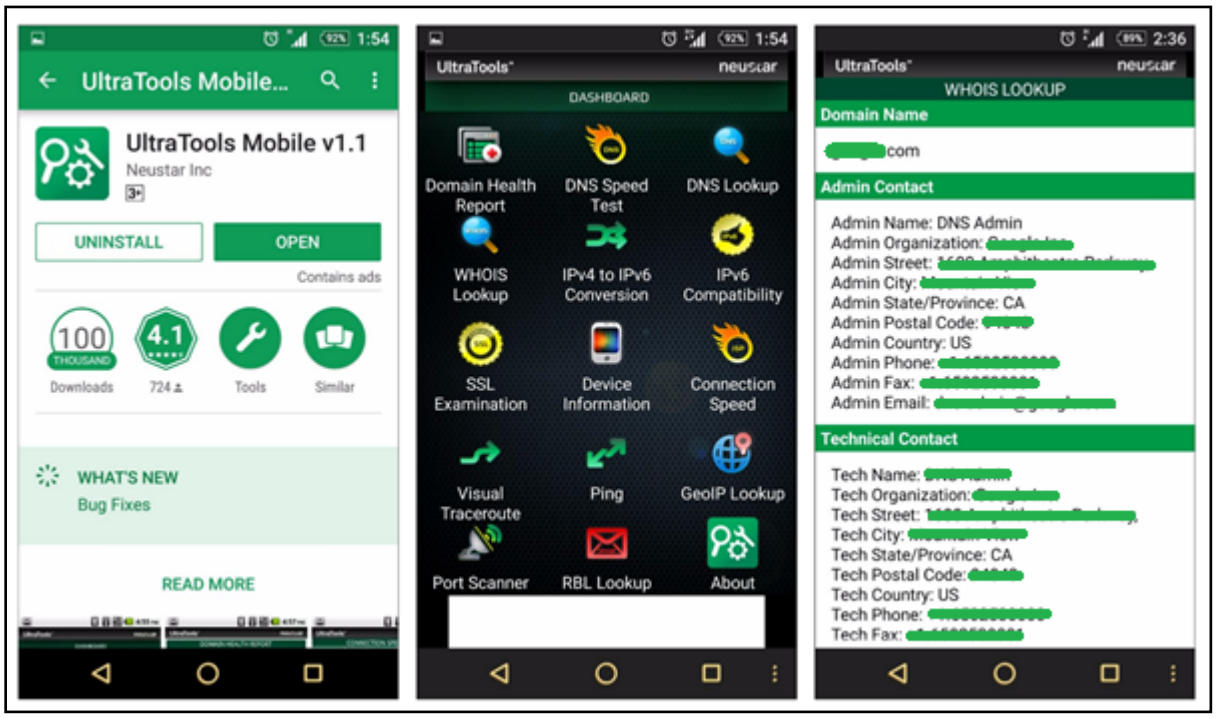


Figure 2-34 Ultra Tool Mobile Application

DNS Footprinting

DNS lookup information is helpful to identify a host within a targeted network. There are several tools available on internet which perform DNS lookup. Before proceeding to the DNS lookup tools and the result overview of these DNS tools, you must know DNS record type symbols and there mean: -

Record Type	Description
A	The host's IP address
MX	Domain's Mail Server
NS	Host Name Server
CNAME	Canonical naming allows aliases to a host
SDA	Indicate authority for the domain
SRV	Service records
PTR	IP-Host Mapping
RP	Responsible Person
HINFO	Host Information
TXT	Unstructured Records

Table 2-09 DNS Record Type

Extracting DNS Information using DNSStuff

Go to the URL: **https://www.dnsstuff.com**

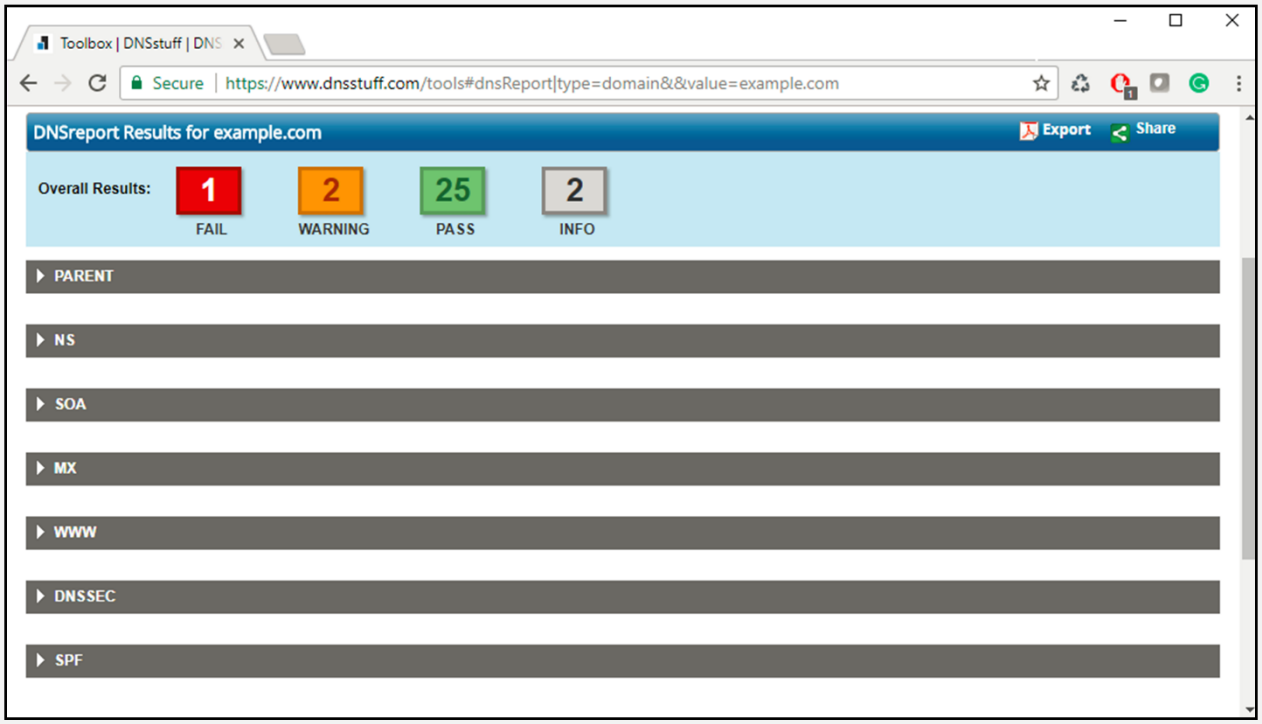


Figure 2-35 DNSStuff.com

Above figure is the output For example**.com.** You can expand fields to extract information.

As shown in the following output, you can expand the desired fields to gain detailed information as shown below:

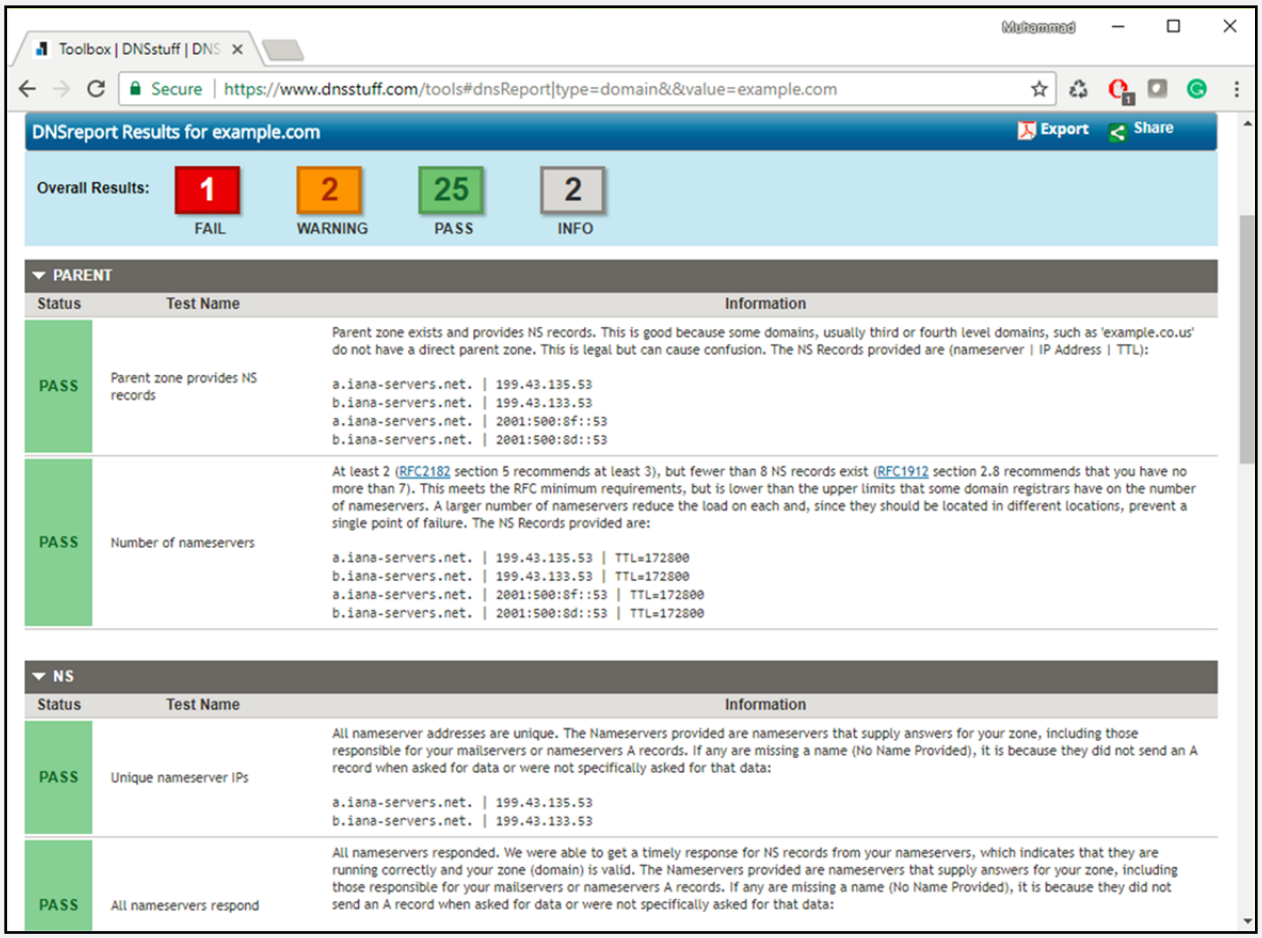


Figure 2-36 DNS Footprinting

Extracting DNS Information using Domain Dossier

Go to website https://centralops.net/co/ and enter the IP address of Domain you like to search.

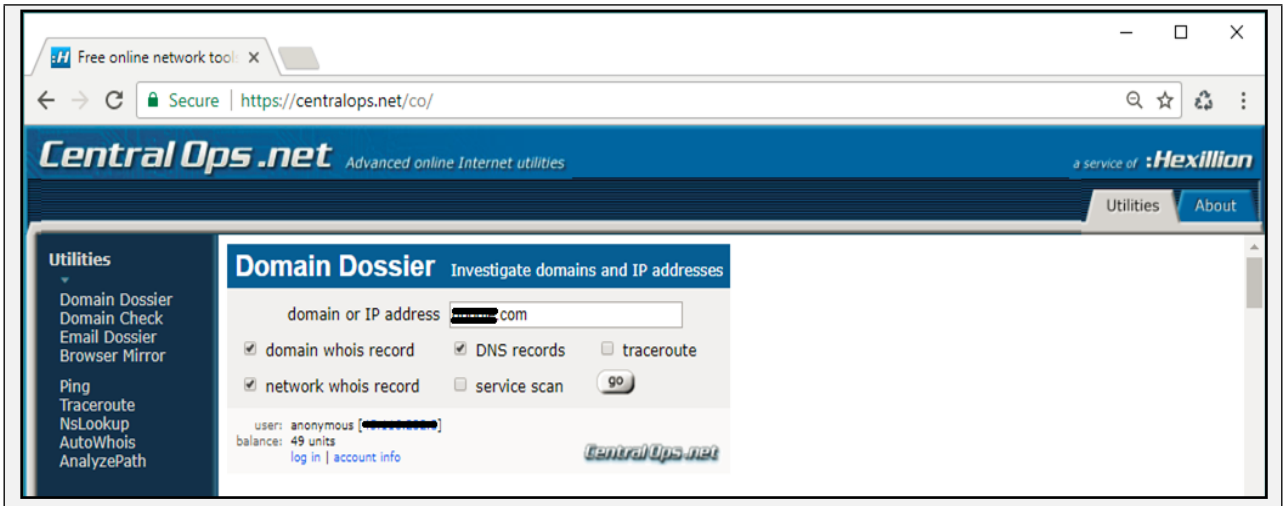


Figure 2-37 Domain Dossier tool

The result brings the canonical name, aliases, IP address, Domain whois records, Network whois records and DNS Records. Consider the figure below.

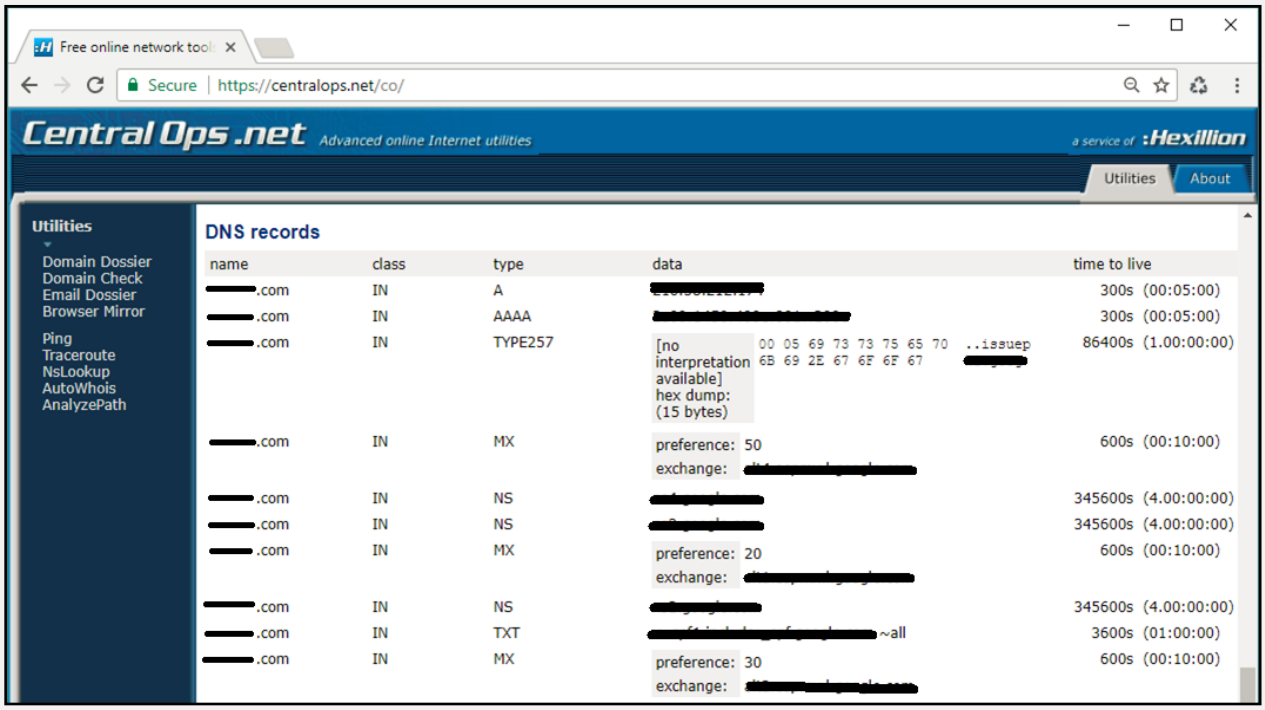


Figure 2-38 Domain Dossier Search Results

DNS Interrogation Tools

There are a lot of online tools available for DNS lookup information, some of them are listed below: -

- http://www.dnsstuff.com
- http://network-tools.com
- http://www.kloth.net
- http://www.mydnstools.info

- http://www.nirsoft.net
- http://www.dnswatch.info
- http://www.domaintools.com
- http://www.dnsqueries.com
- http://www.ultratools.com
- http://www.webmaster-toolkit.com

Network Footprinting

One of the important types of footprinting is network footprinting. Fortunately, there are several tools available which can be used for network footprinting to gain information about the target network. Using these tools, an information seeker can create a map of the targeted network. Using these tools, you can extract information such as: -

- Network address ranges
- Hostnames
- Exposed hosts
- OS and application version information
- Patch state of the host and the applications
- Structure of the applications and back-end servers

Tools for this purpose are listed below: -

- Whois
- Ping
- Nslookup
- Tracert

Traceroute

Tracert options are available in all operating system as a command line feature. Visual traceroute, graphical and other GUI based traceroute applications are also available. Traceroute or Tracert command results in the path information from source to destination in the hop by hop manner. The result includes all hops in between source to destination. The result also includes latency between these hops.

Traceroute Analysis

Consider an example, in which an attacker is trying to get network information by using tracert. After observing the following result, you can identify the network map.

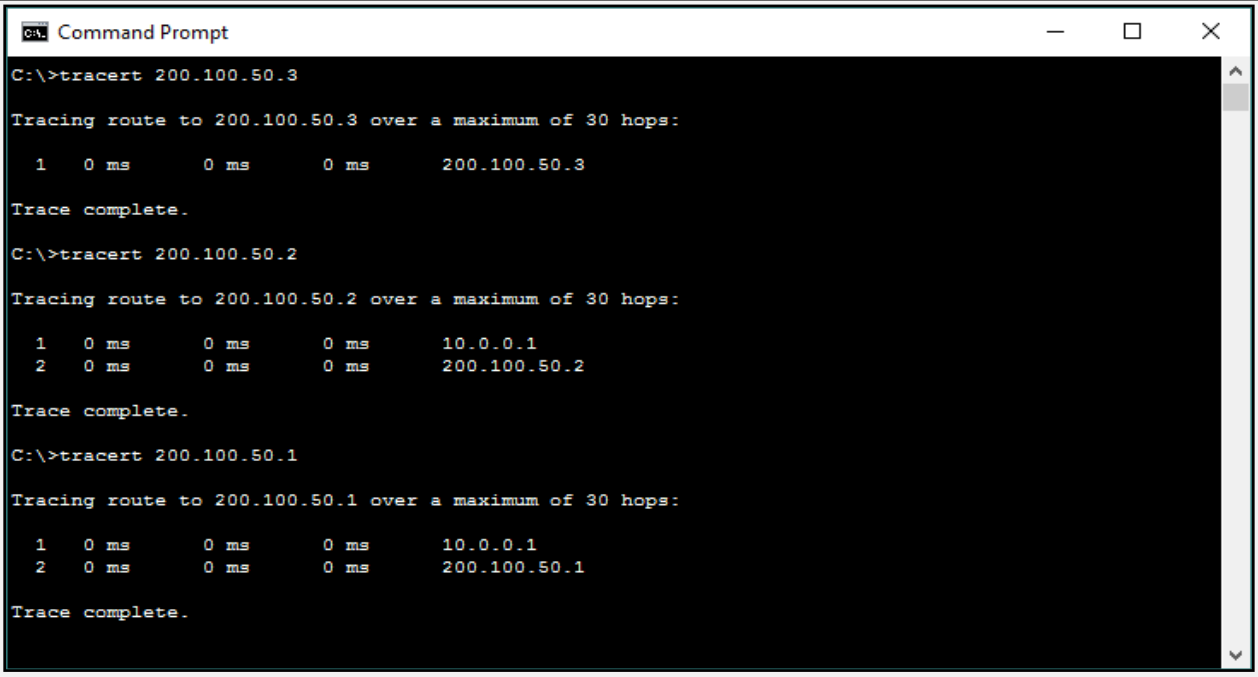


Figure 2-39 Tracert

10.0.0.1 is the first hop, which means it is the gateway. Tracert result of 200.100.50.3 shows, 200.100.50.3 is another interface of first hop device whereas connected IP includes 200.100.50.2 & 200.100.50.1.

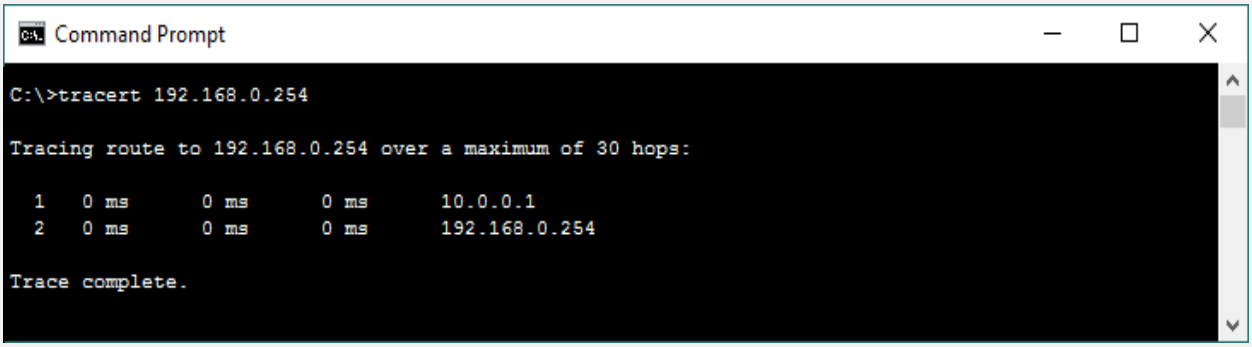


Figure 2-40 Tracert

192.168.0.254 is next to last hop 10.0.0.1. It can either connected to 200.100.50.1 or 200.100.50.2. To verify, trace next route.

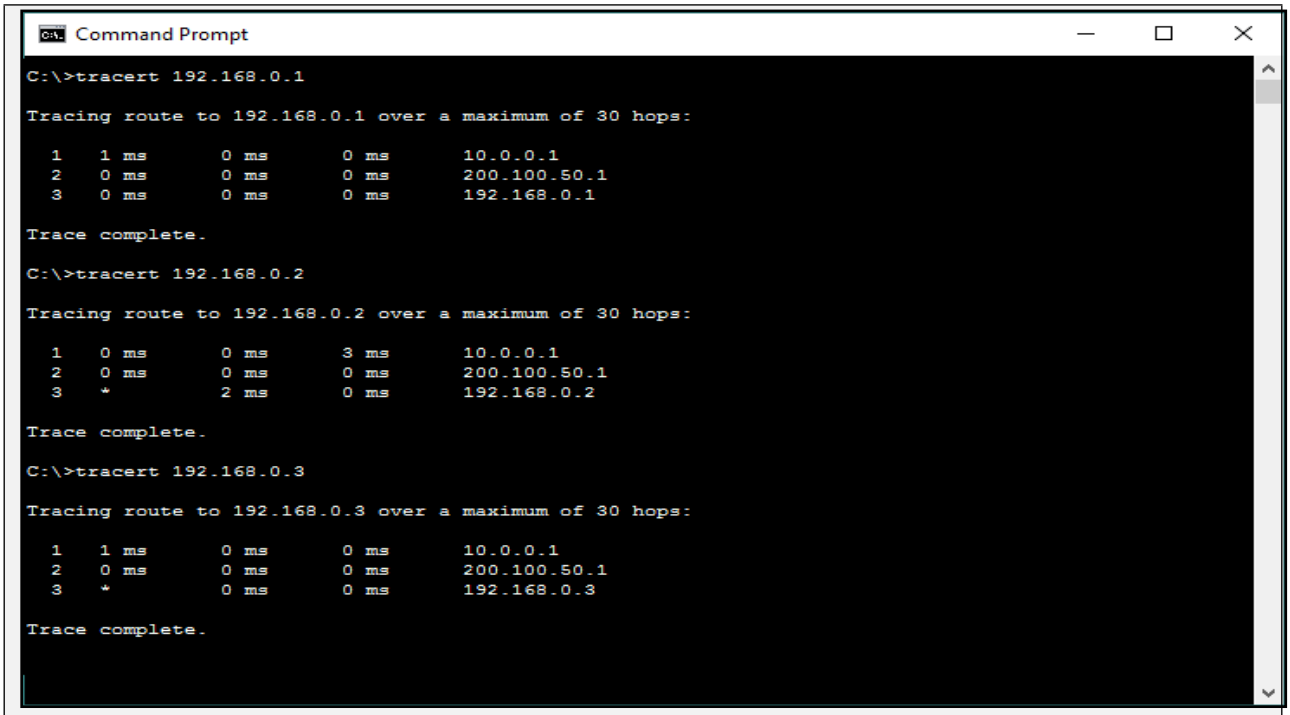


Figure 2-41 Tracert

192.168.0.254 is another interface of the network device, i.e. 200.100.50.1 connected next to 10.0.0.1. 192.168.0.1, 192.168.0.2 & 192.168.0.3 are connected directly to 192.168.0.254.

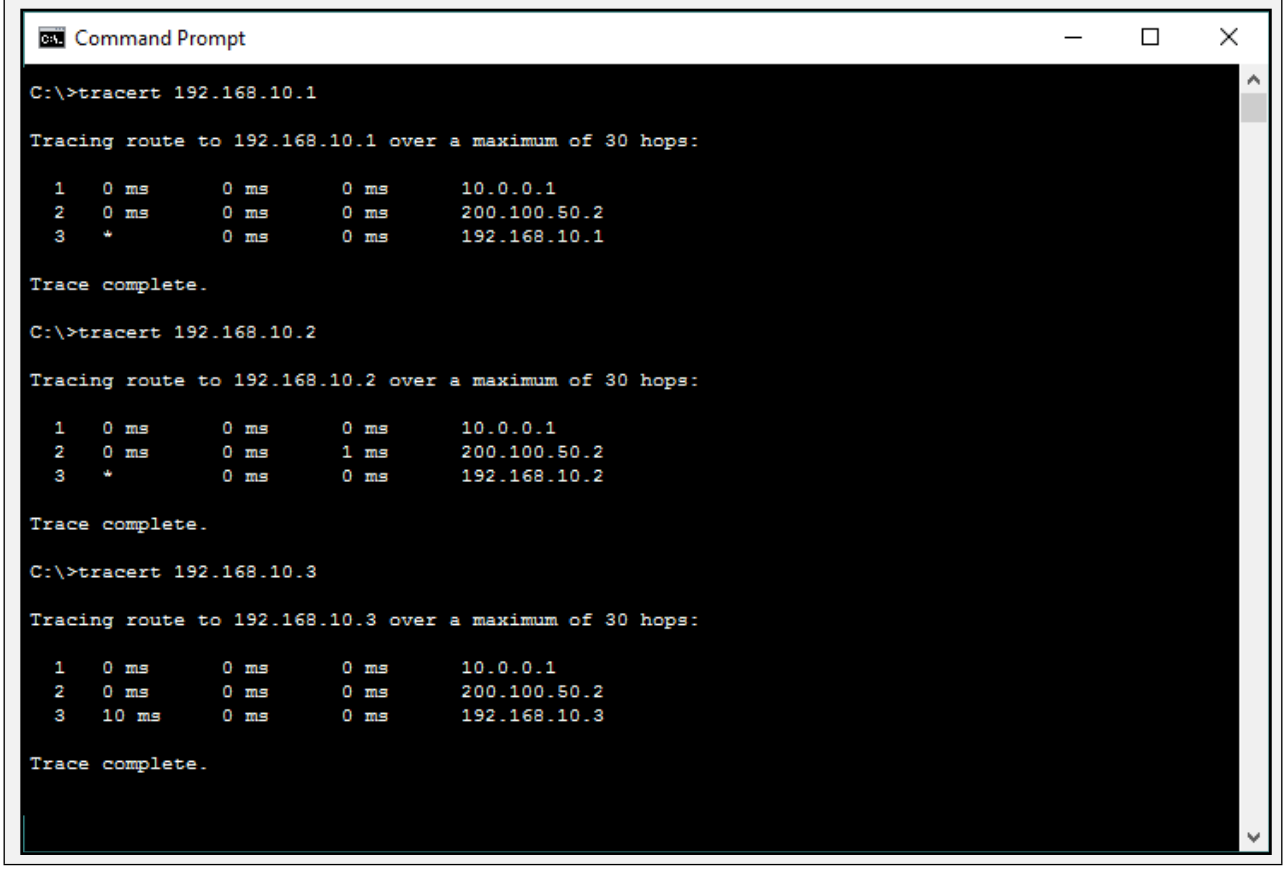


Figure 2-42 Tracert

192.168.10.254 is another interface of the network device i.e. 200.100.50.2 connected next to 10.0.0.1. 192.168.10.1, 192.168.10.2 & 192.168.10.3 are connected directly to 192.168.10.254.

Traceroute Tools

Traceroute tools are listed below: -

Traceroute Tools	Website
Path Analyzer Pro	www.pathanalyzer.com
Visual Route	www.visualroute.com
Troute	www.mcafee.com
3D Traceroute	www.d3tr.de

Table 2-10 Traceroute tools

The following figure shows graphical view and other trace information using Visual Route tool.

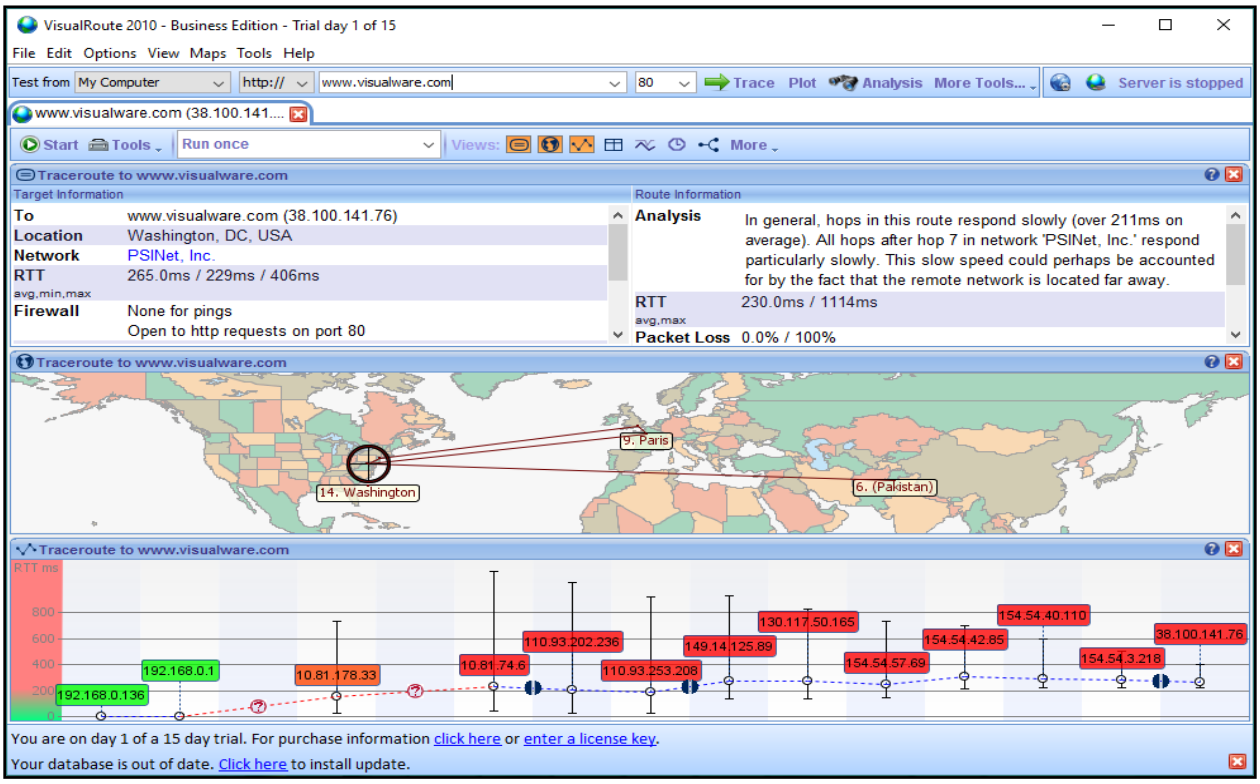


Figure 2-43 Visual Route Application

Footprinting through Social Engineering

In footprinting, the one of the easiest component to hack is human being itself. We can collect information from a human quite easily than fetching information from systems. Using Social Engineering, some basic social engineering techniques are: -

- Eavesdropping
- Shoulder Surfing
- Dumpster Diving
- Impersonation

Social Engineering

You can understand the social engineering as an art of extracting sensitive information from peoples. Social Engineers keep themselves undetected, people are unaware and careless and share their valuable information. This information is related to the type of social engineering. In Information Security aspects, Footprinting through Social engineering gathers information such as: -

- Credit card information.
- Username & Passwords.
- Security devices & Technology information.
- Operating System information.
- Software information.
- Network information.
- IP address & name server's information.

Eavesdropping

Eavesdropping is a type of Social Engineering footprinting in which the Social Engineer is gathers information by listening to the conversation covertly. Listening conversations includes listening, reading or accessing any source of information without being notified.

Phishing

In the Phishing process, Emails sent to a targeted group contains email message body which looks legitimate. The recipient clicks the link mentioned in the email assuming it as a legitimate link. Once the reader clicks the link, enticed for providing information. It redirects users to the fake webpage that looks like an official website. For example, Recipient is redirected to a fake bank webpage, asking for sensitive information. Similarly, the redirected link may download any malicious script onto the recipient's system to fetch information.

Shoulder Surfing

Shoulder Surfing is another method of gathering information by standing behind a target when he is interacting with sensitive information. By Shoulder surfing, passwords, account numbers, or other secret information can be gathered depending upon the carelessness of the target.

Dumpster Diving

Dumpster Diving is the process of looking for treasure in trash. This technique is older but still effective. It includes accessing the target's trash such as printer trash, user desk, company's trash for finding phone bills, contact information's, financial information, source codes, and other helpful material.

Footprinting Tool

Maltego

Maltego is a data mining tools that are powered by Paterva. This interactive tool gathers data and represents graphs for analysis. The measure purpose of this Data mining tools is an online investigation of relationships among different pieces of information obtained from various sources lies over the internet. Using Transform, Maltego automate the process of gathering information from different data sources. Nodes based graph represents this information. There is 3 version of Maltego Client software: -

- Maltego CE
- Maltego Classic
- Maltego XL

Lab 02-1: Maltego Tool Overview

Procedure:
You can download Maltego from Paterva website (i.e., https://www.paterva.com). Registration is required to download the software. After Download, Installation needs a license key to run the application with full features.

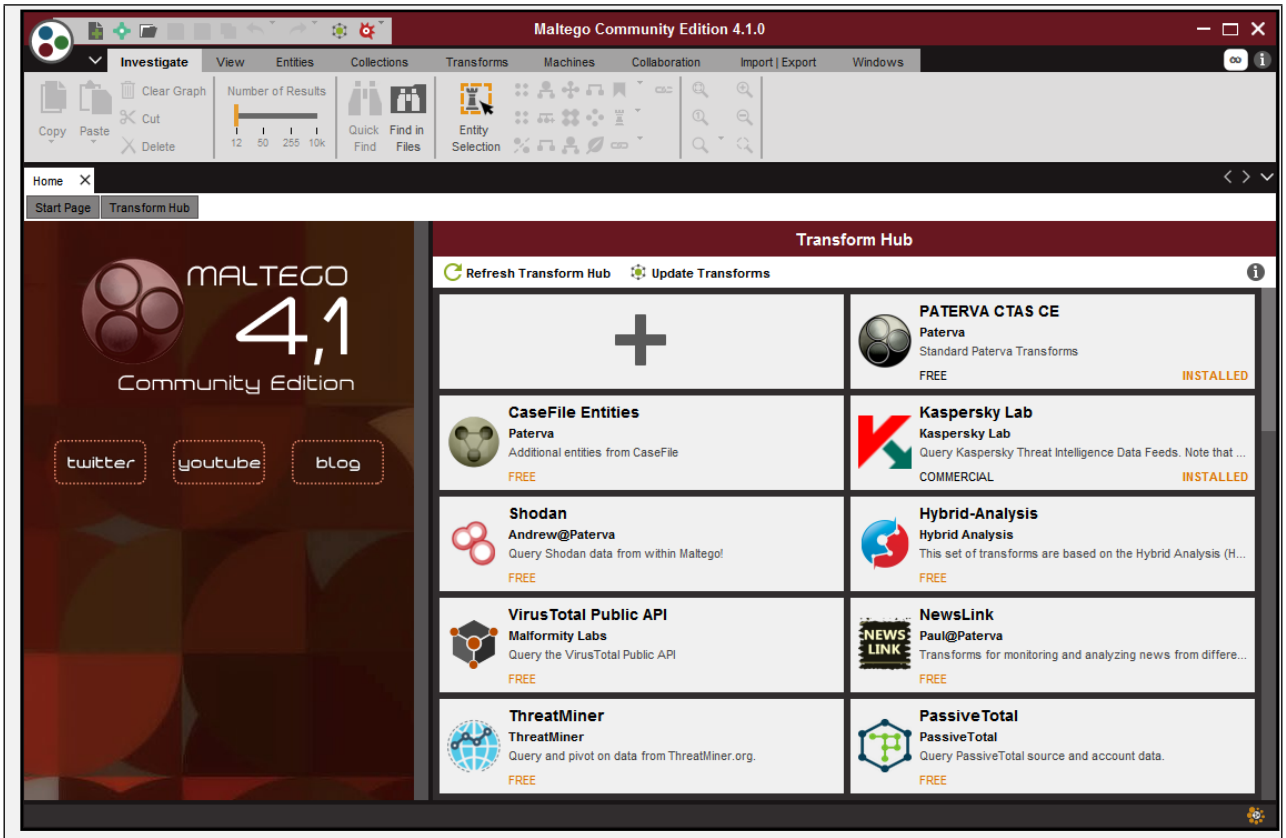


Figure 2-44 Maltego Home Page

Above is the Home page of Maltego Community Edition (CE). On the topmost, Click create new graph Icon  .

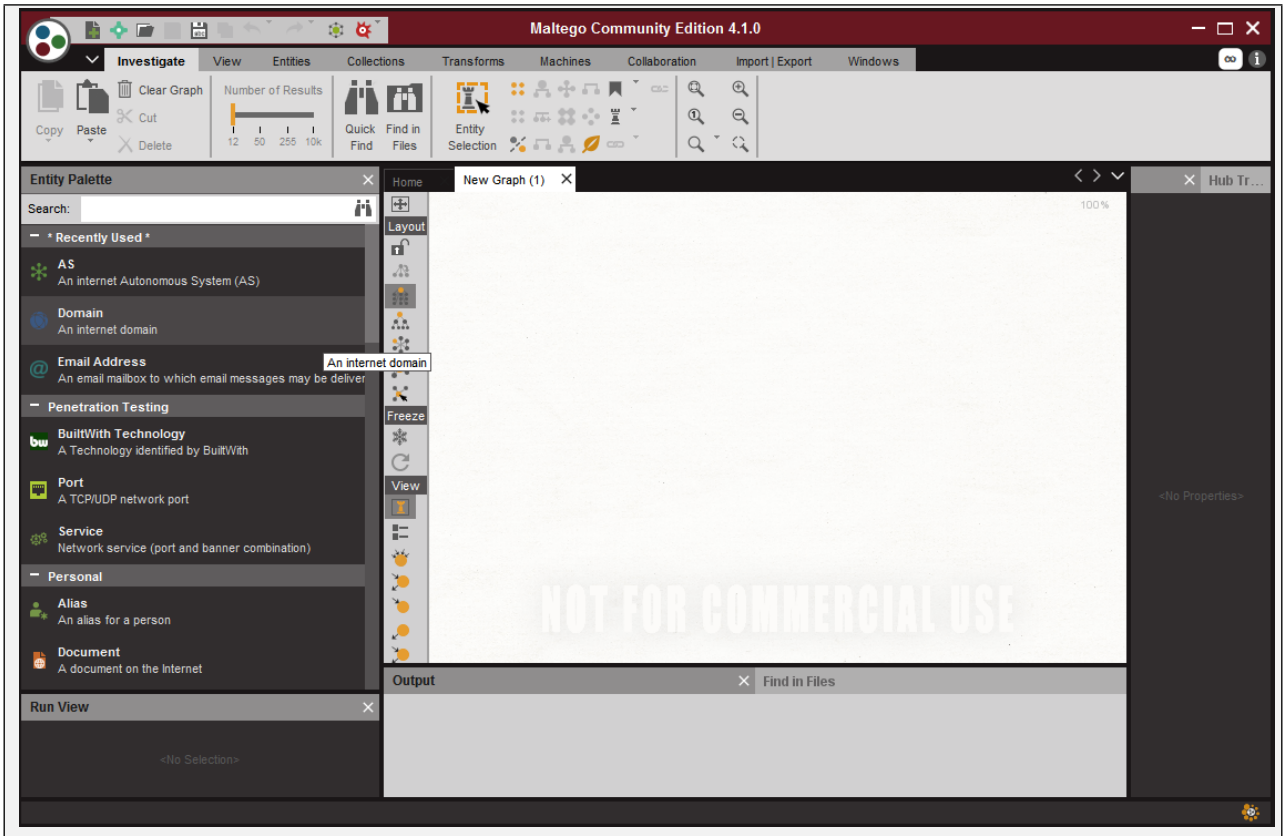


Figure 2-45 Maltego

You can select the ***Entity Palette*** according to your type of query. In our case, For example, ***Domain*** is Selected.

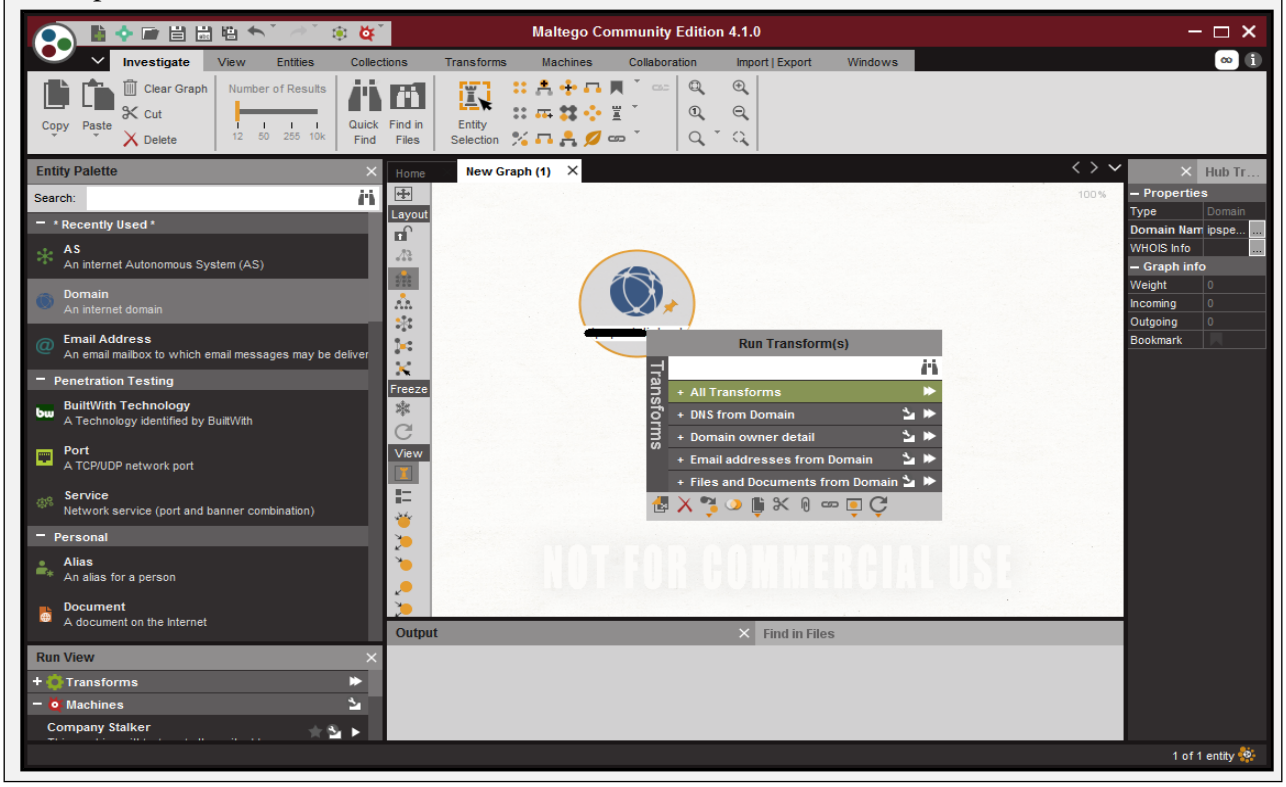


Figure 2-46 Maltego

Edit the Domain and Right Click on the Domain Icon to Select ***Run Transform*** Option. Select the option and observed the results shown. Available options are: -

- All Transform
- DNS from Domain
- Domain Owner details
- Email Addresses from Domain
- Files and Documents from Domain

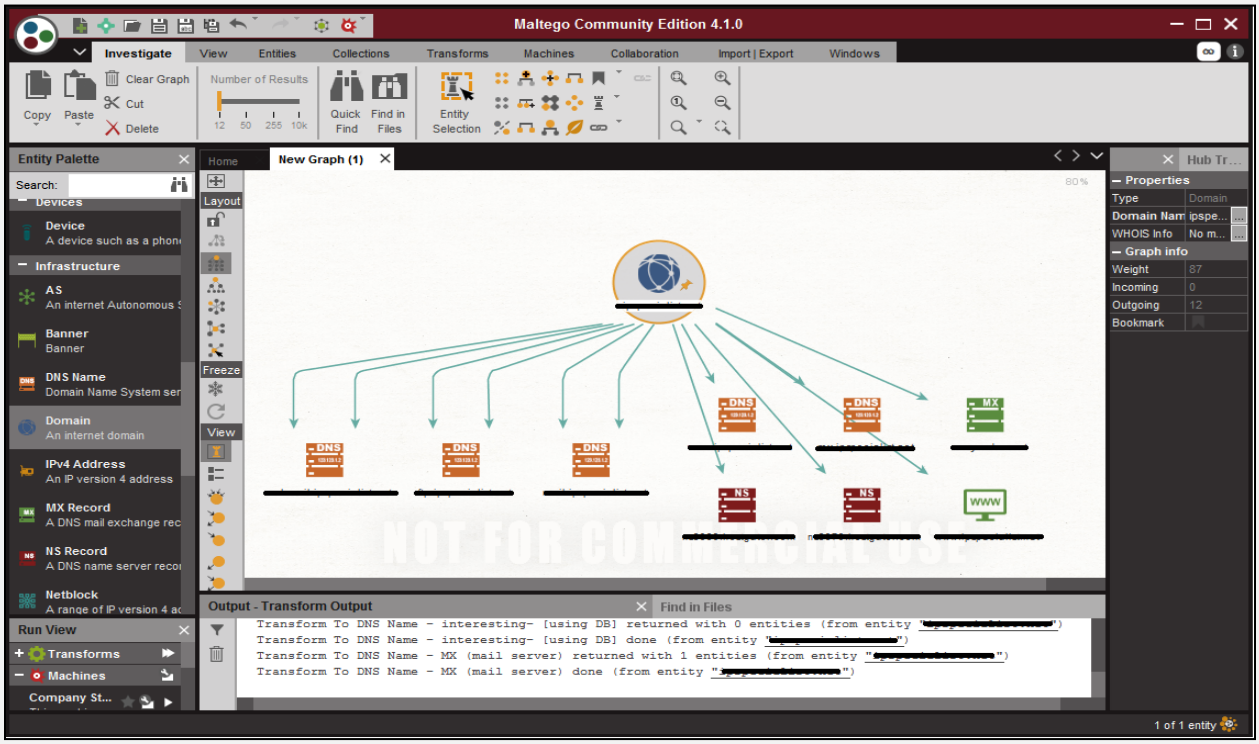


Figure 2-47 Maltego

Recon-ng

Recongo-ng is a full feature Web Reconnaissance framework used for information gathering purpose as well as network detection. This tool is written in python, having independent modules, database interaction and other features. You can download the software from www.bitbucket.org. This Open Source Web Reconnaissance tool requires kali Linux Operating system.

Lab 02-2: Recon-ng Overview

Procedure:
Open Kali Linux and run Recong-ng

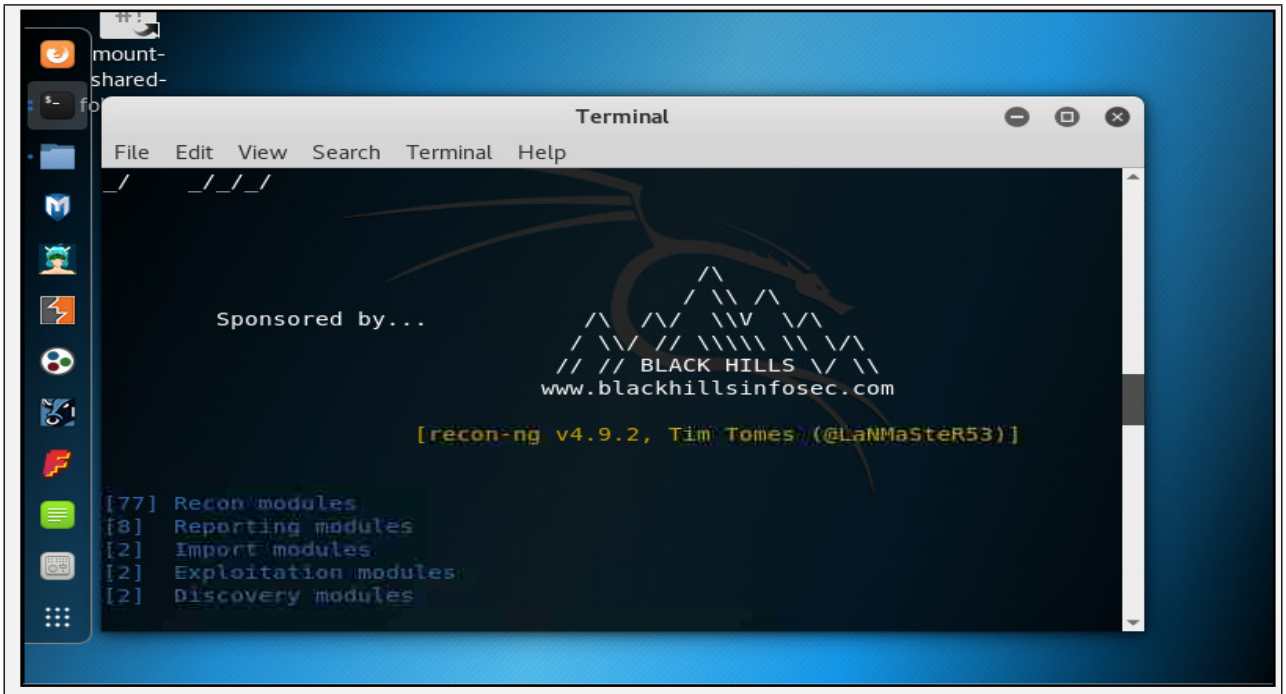


Figure 2-48 Recon-ng

Run the Application Recon-ng or open the terminal of Kali-Linux and type recon-ng and hit enter.

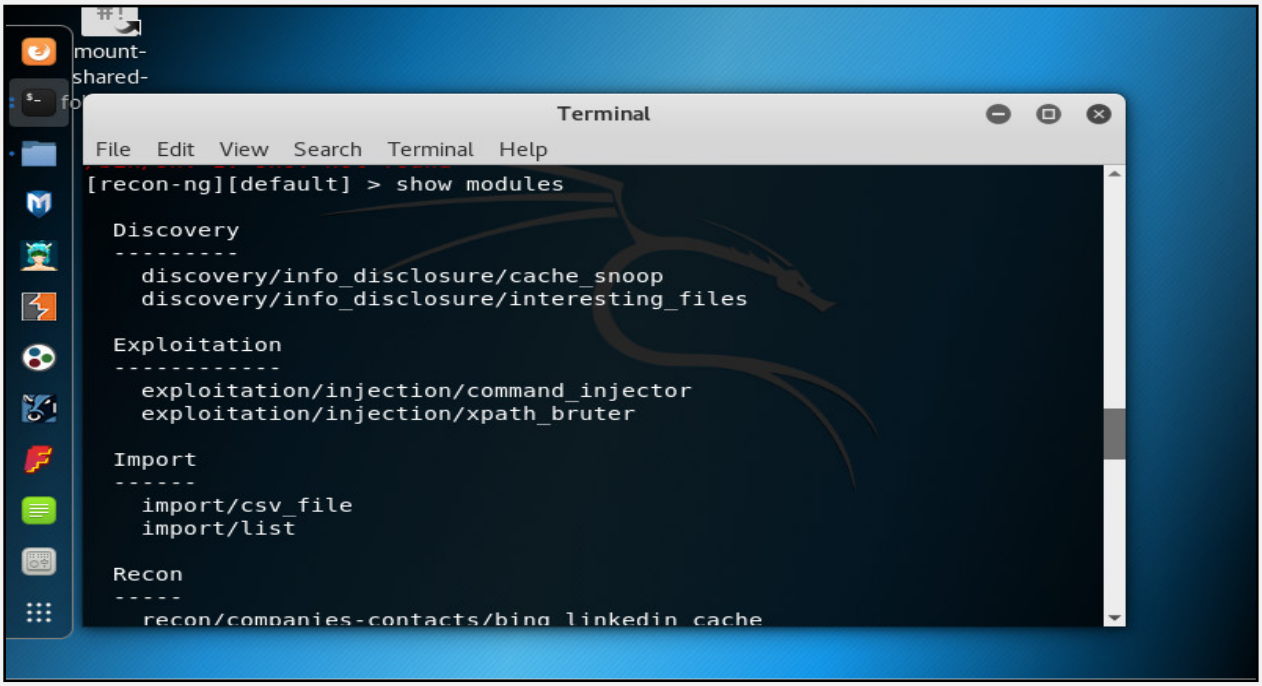


Figure 2-49 Recon-ng (Show module command)

Enter the command "***show modules***" to show all independent modules available.

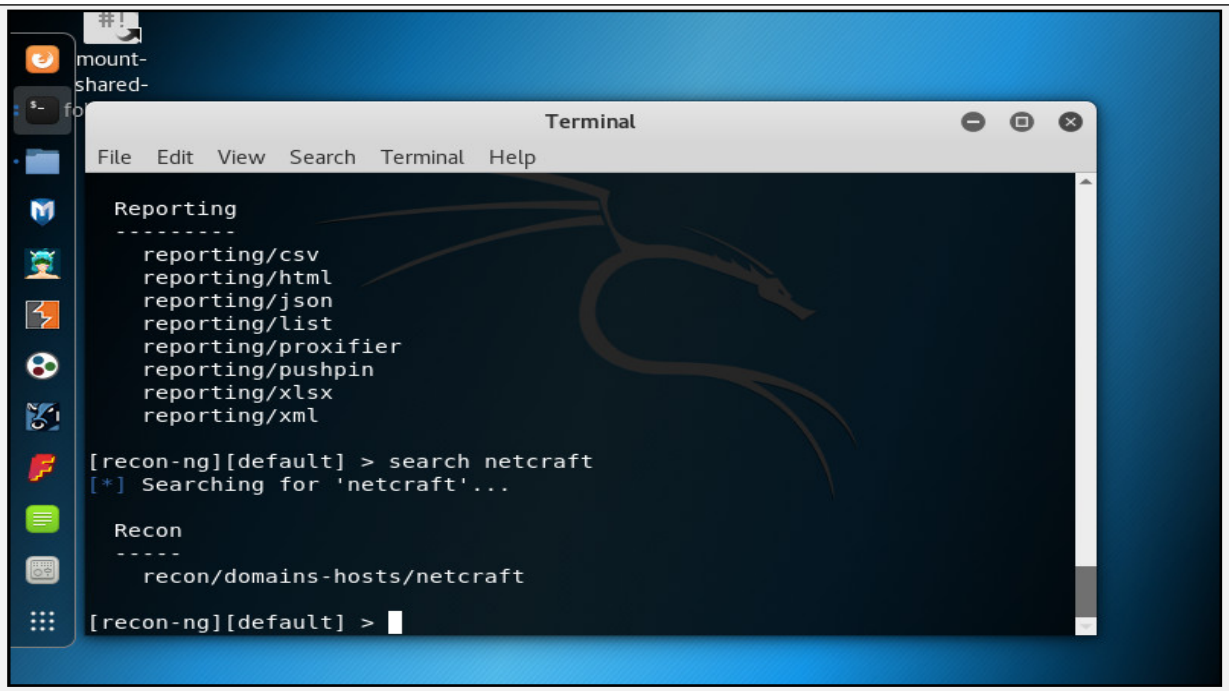


Figure 2-50 Recon-ng (Search command)

You can search for any entity within a module. For example, in above figure, the command "***Search Netcraft***" is used.

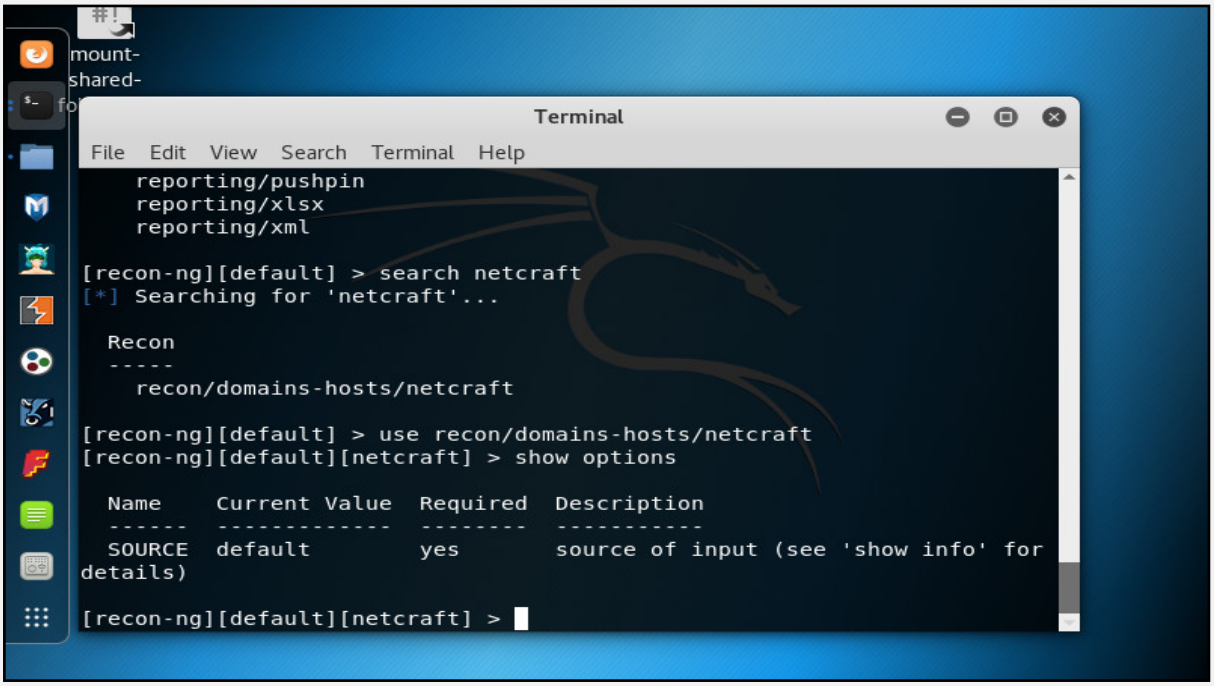


Figure 2-51 Using Netcraft through Recon-ng

To use the Netcraft module, use the command syntax "***use recon/domain-hosts/Netcraft***" and hit enter.

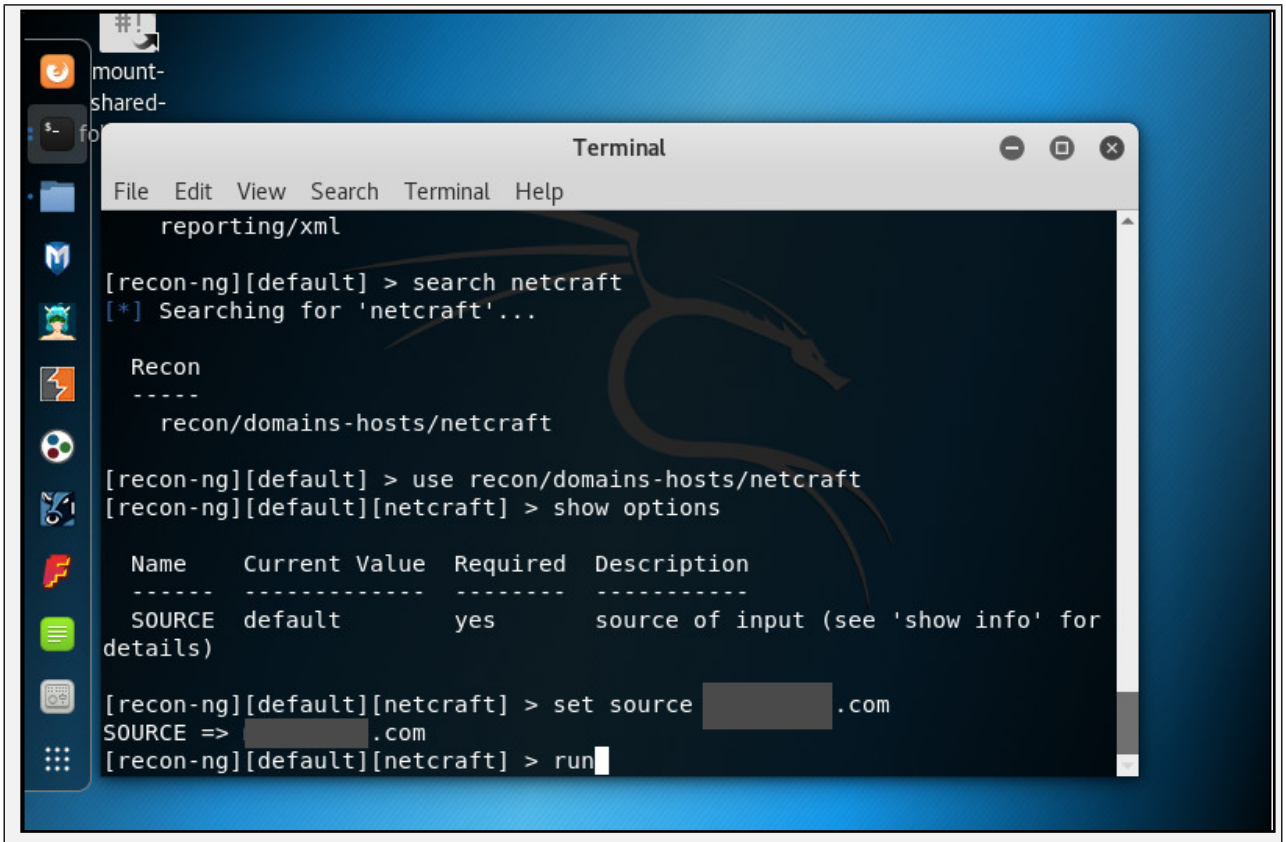


Figure 2-52 Searching for Target Domain

Set the source by the command "***set source*** *[domain].*" Press enter to continue. Type ***Run*** to execute and press enter.

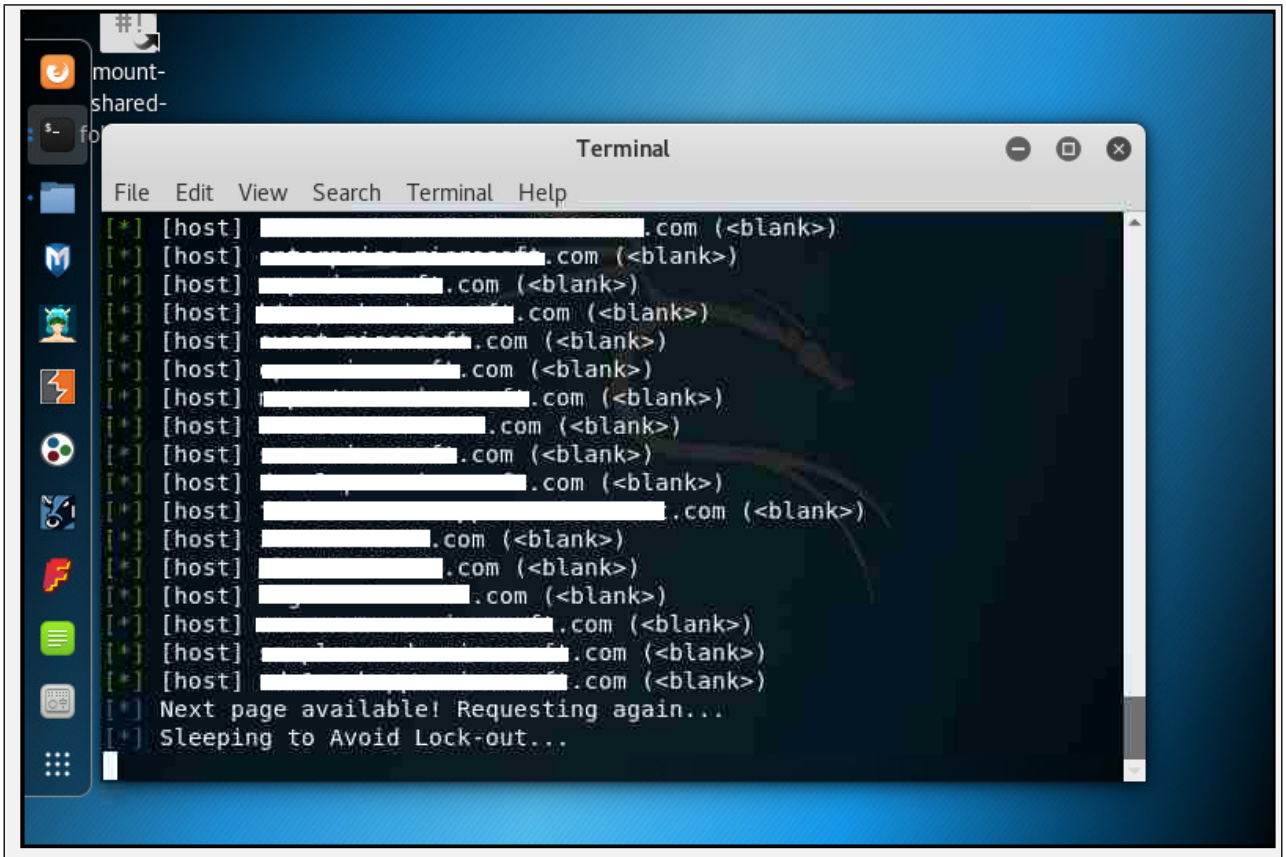


Figure 2-53 Search Result of Target Domain

Recon-ng is gathering the information of target domain.

Additional Footprinting Tools

FOCA stands for Fingerprinting Organizations with Collected Archives. FOCA tool finds Metadata, and other hidden information within a document may locate on web pages. Scanned searches can be downloaded and Analyzed. FOCA is a powerful tool which can support various types of documents including Open Office, Microsoft Office, Adobe InDesign, PDF, SVG, and others. Search uses three search engines, Google, Bing, and DuckDuckGo.

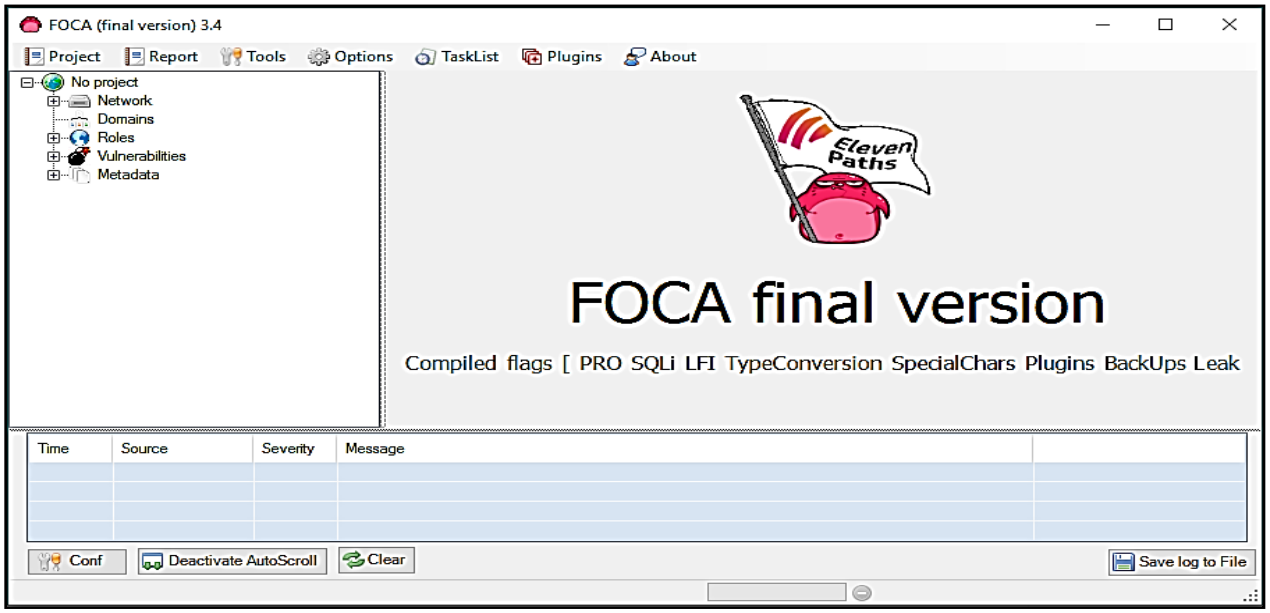


Figure 2-54 FOCA Dashboard

Lab 02-3: FOCA Tool Overview

Procedure:

Download the software ***FOCA*** from https://www.elevenpaths.com. Now, Go to ***Project*** > ***New Project.***

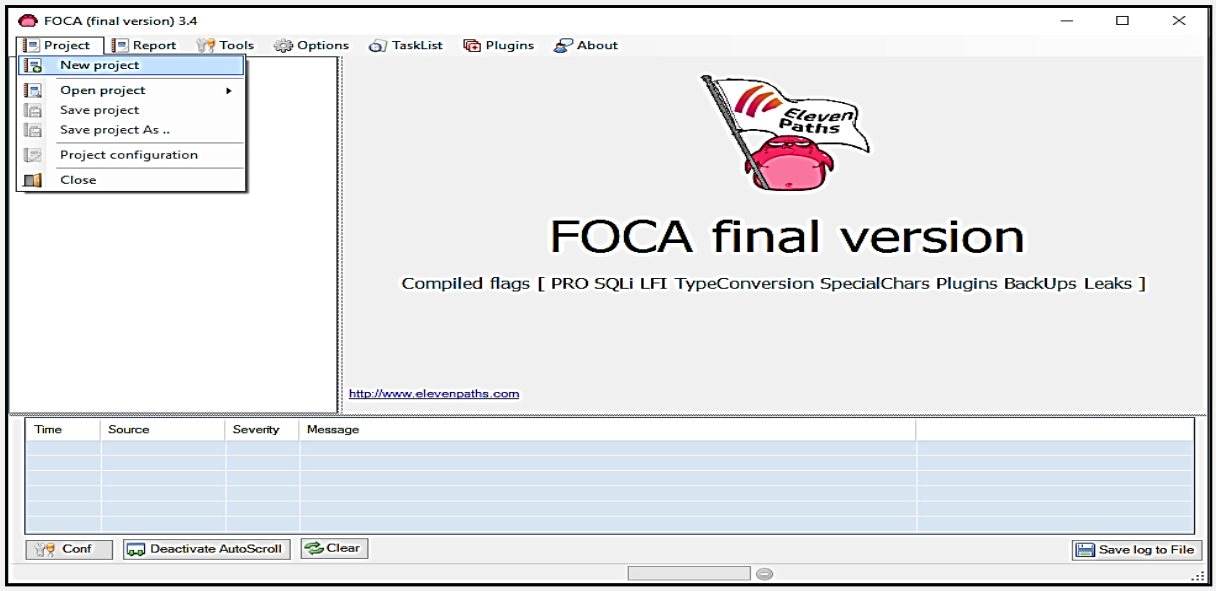
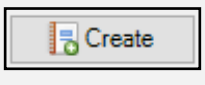


Figure 2-55 Creating New Project using FOCA

Now, Enter the Project Name, Domain Website, Alternate Website (if required), Directory to save the results, Project Date. Click Create  to proceed.

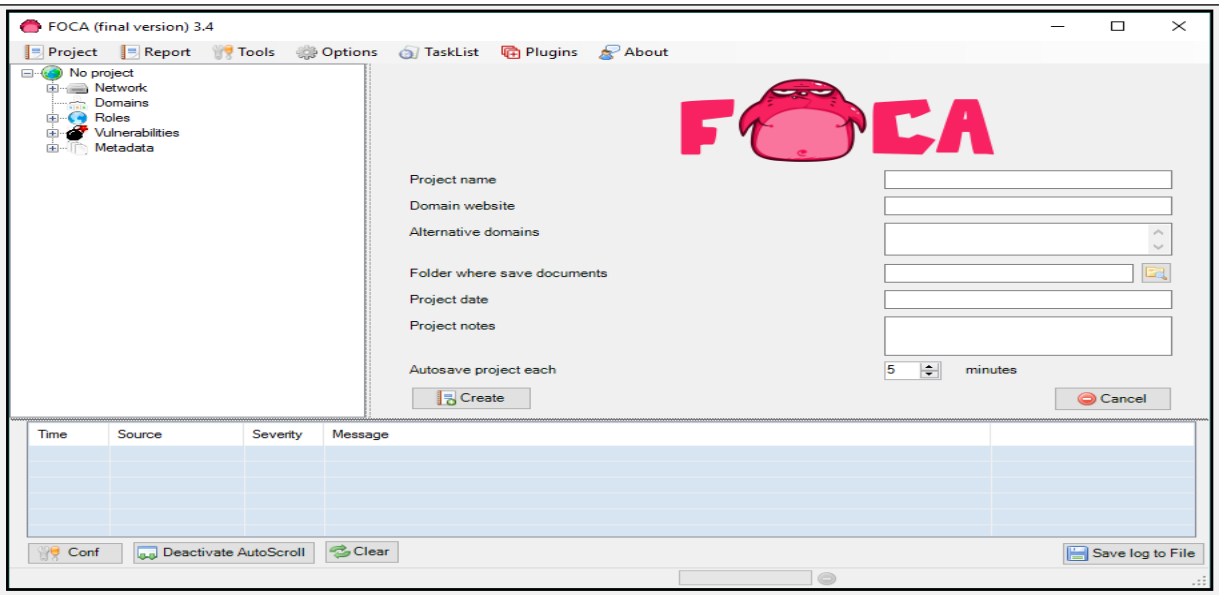
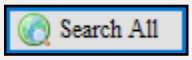


Figure 2-56 Creating New Project using FOCA

Select the Search Engines, Extensions, and other parameters as required. Click on Search All Button. 

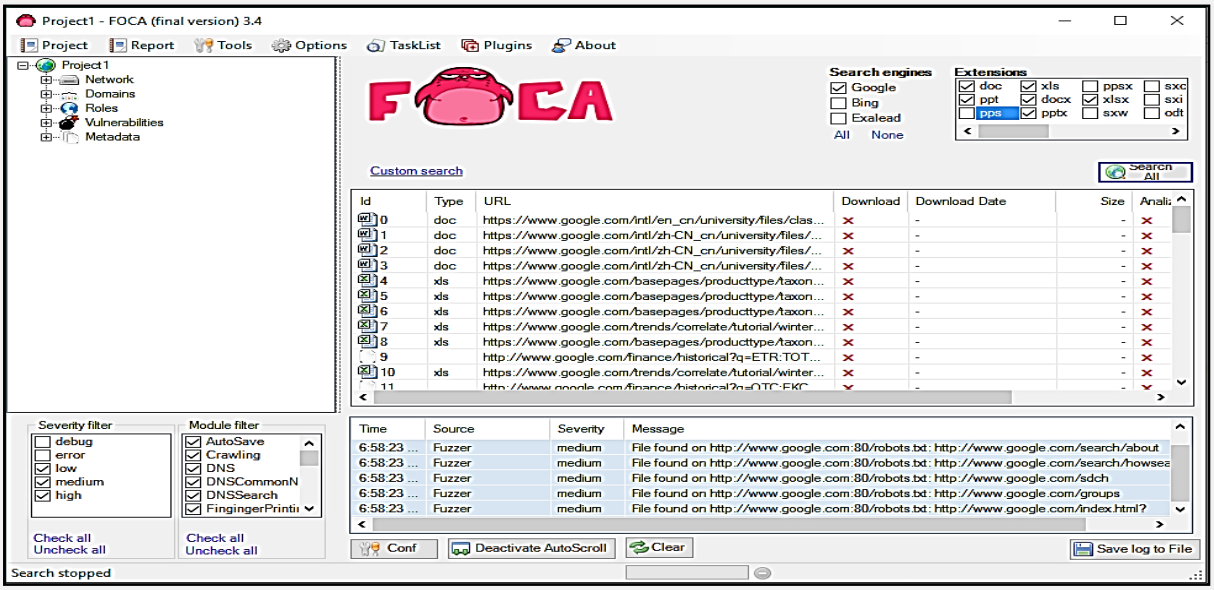


Figure 2-57 Search using FOCA

Once Search completes, the search box shows multiple files. You can select the file, download it, Extract Metadata, and gather other information like username, File creation date, and Modification.

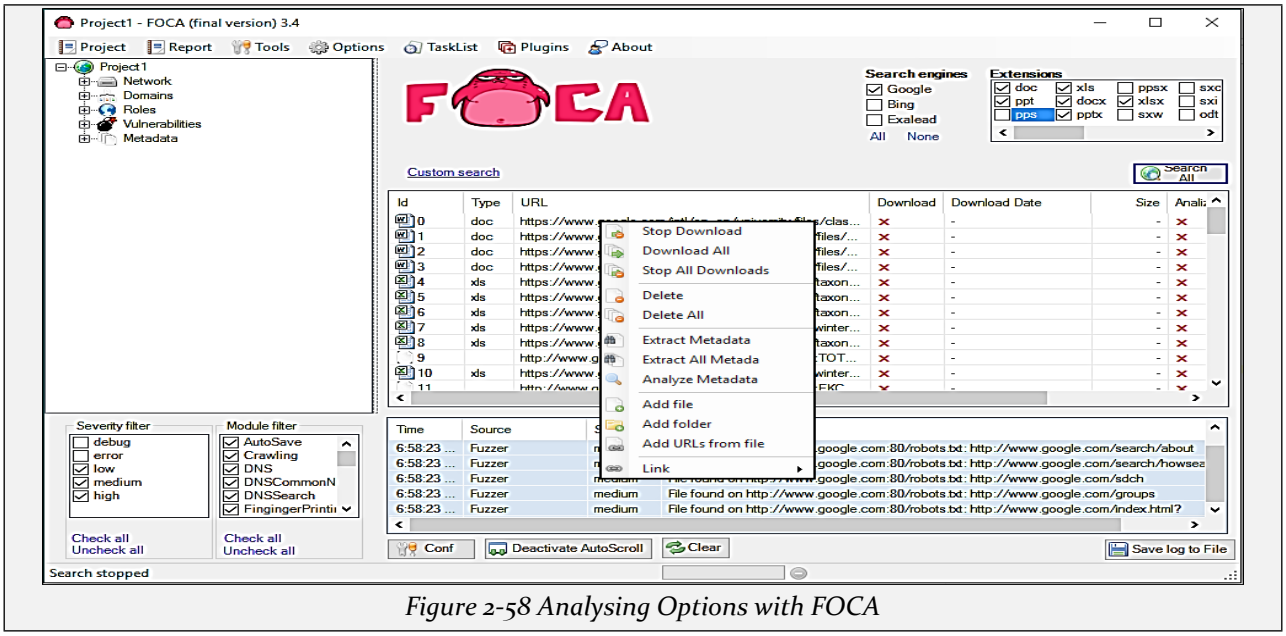


Figure 2-58 Analysing Options with FOCA

Additional Footprinting Tools

Some other footprinting tools are: -

Tools	Websites
Prefix WhoIs	http://pwhois.org
Netmask	http://www.phenoelit.org
DNS-Digger	http://www.dnsdigger.com
Email Tracking Tool	http://www.filley.com
Ping-Probe	http://www.ping-probe.com
Google Hacks	http://code.google.com

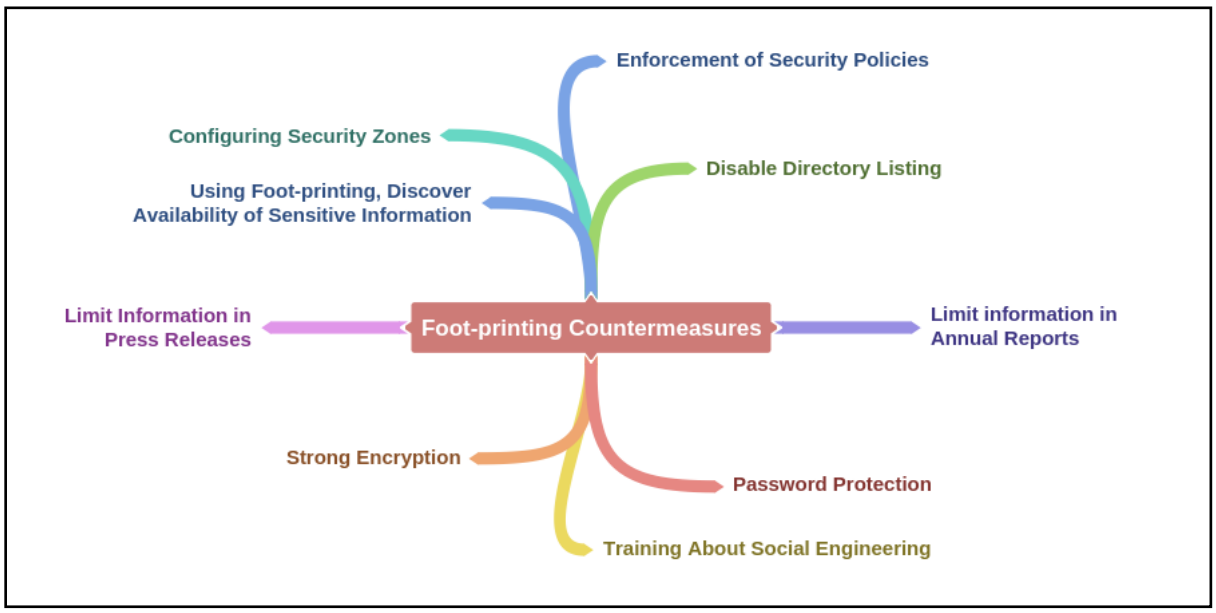
Table 2-11 Additional Footprinting tools

Countermeasures of Footprinting

Footprinting countermeasure includes the following measures to mitigate footprinting:

- Employees on an organization must be restricted to access social networking sites from the corporate network.
- Devices and Servers are configured to avoid data leakage.
- Provide education, training, and awareness of footprinting, impact, methodologies, and countermeasures to the employees of an organization.
- Avoid revealing sensitive information in Annual reports, Press releases, etc.
- Prevent search engines to cache web pages.

Mind Map



Lab 2-4: Gathering information using Windows Command Line Utilities

Case Study: Consider a network where you have access to a Windows PC connected to the Internet. Using Windows-based tools, let's gather some information about the target. You can assume any target domain or IP address, in our case, we are using **example.com** as a target.

Topology Diagram:

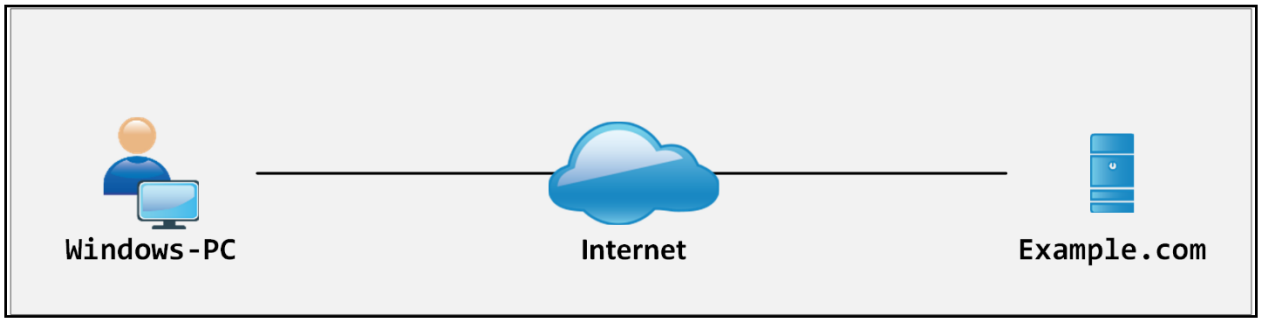


Figure 2-59: Topology Diagram

Procedure:
Open Windows Command Line (cmd) from Windows PC.

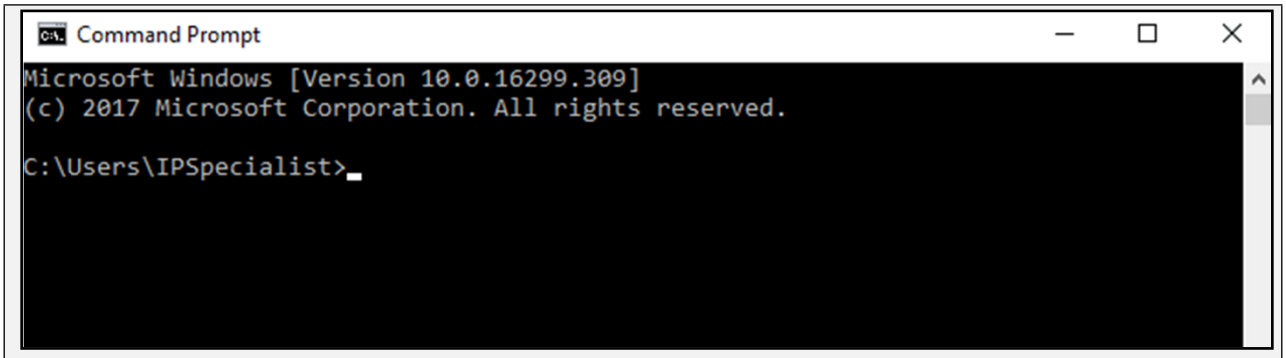


Figure 2-60: Windows Command Prompt

Enter the command "**`Ping example.com`**" to ping.

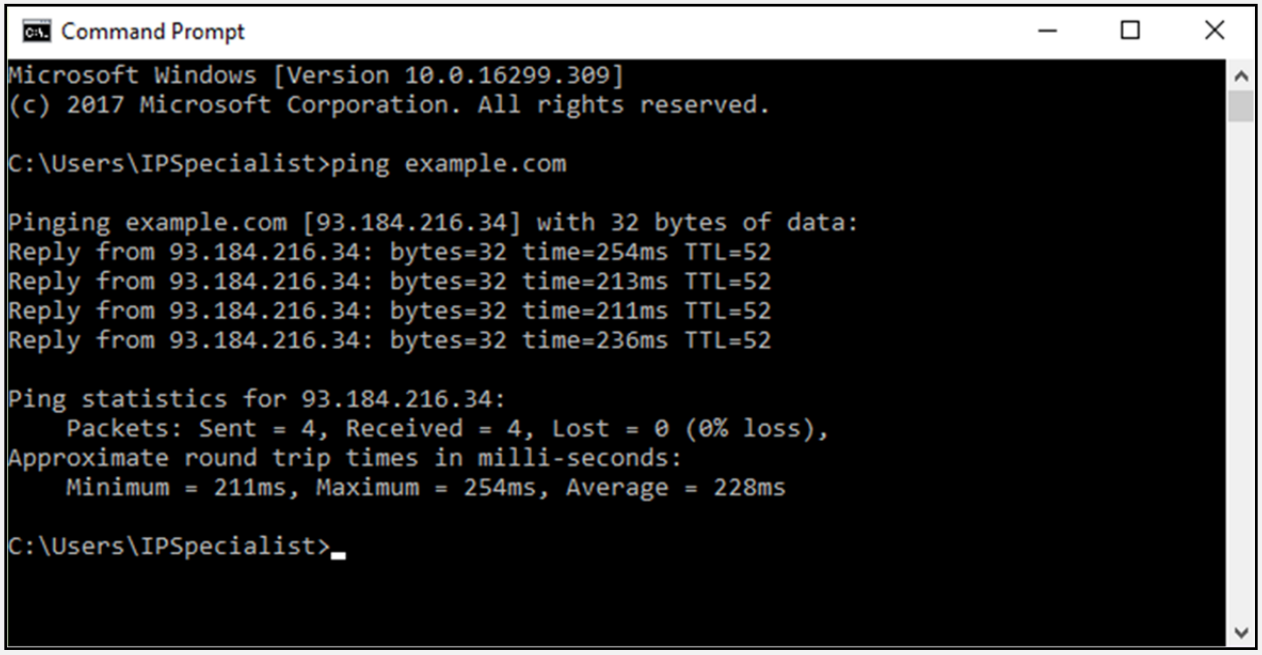


Figure 2-61: Ping example.com

From the output, you can observe and extract the following information:

1. Example.com is live
2. IP address of example.com.
3. Round Trip Time
4. TTL value
5. Packet loss statistics

Now, Enter the command "**`Ping example.com -f -l 1500`**" to check the value of fragmentation.

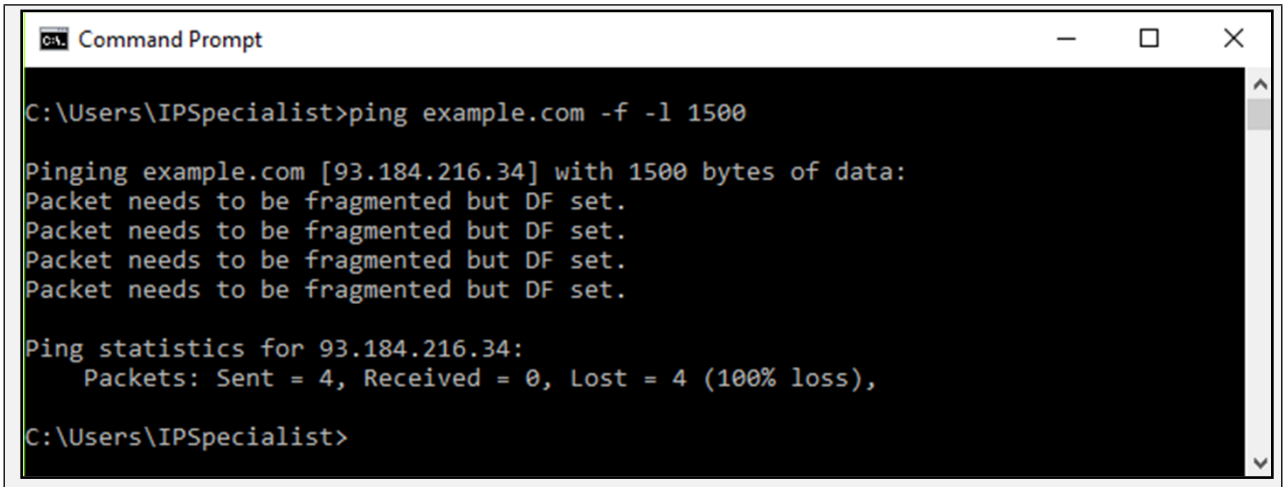


Figure 2-62: Ping example.com with DF bit set

The output shows "**`Packet needs to be fragmented but DF set`**" which means 1500 bits will require being fragmented. Let's try again with smaller value:

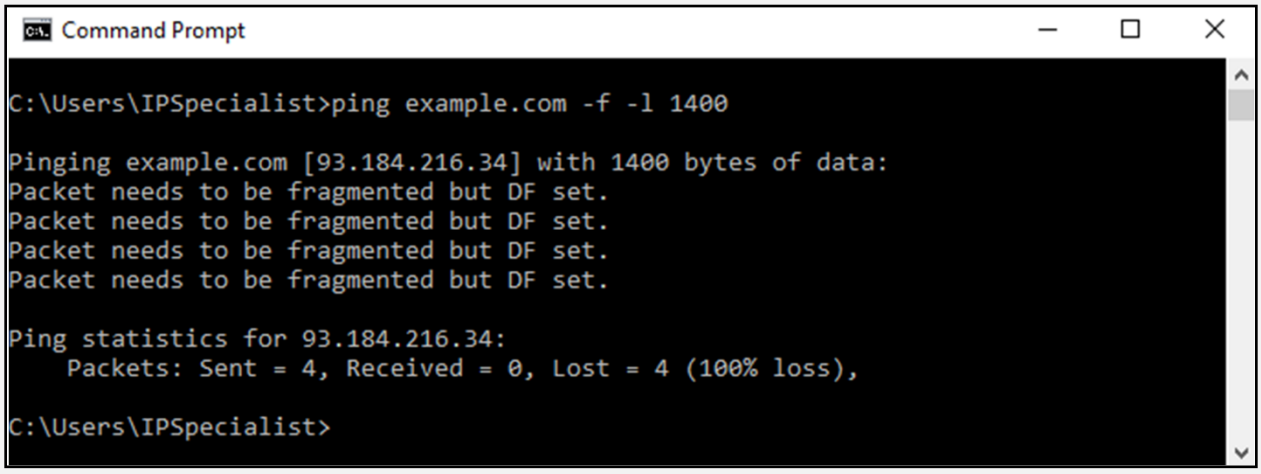


Figure 2-63: Ping example.com with DF bit set

Output again shows "**`Packet needs to be fragmented but DF set`**" which means 1400 bits will require being fragmented. Let's try again with smaller value:

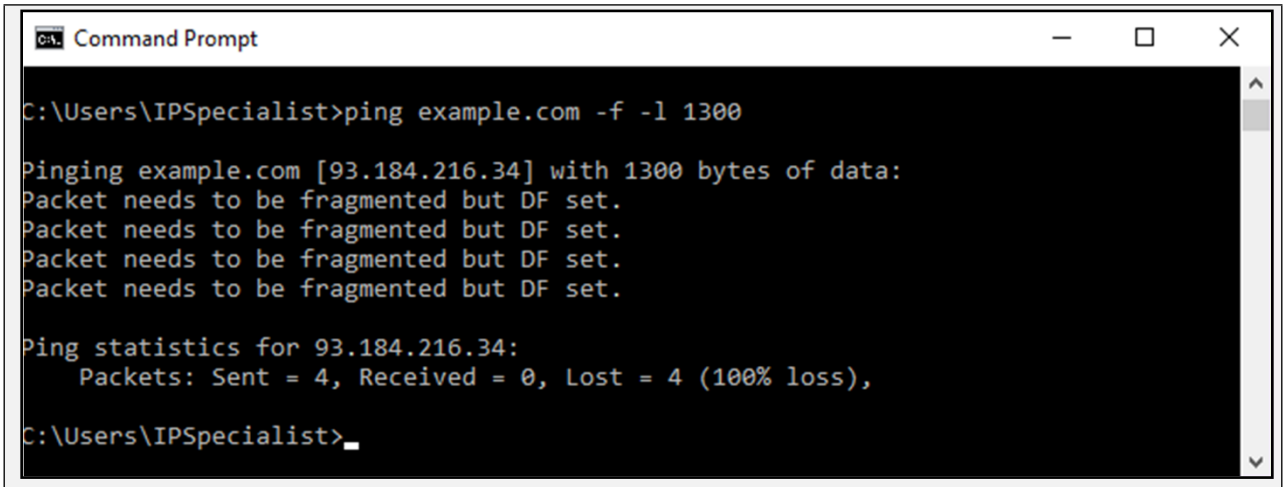


Figure 2-64: Ping example.com with DF bit set

Output again shows "**`Packet needs to be fragmented but DF set`**" which means 1300 bits will require being fragmented. Let's try again with smaller value:

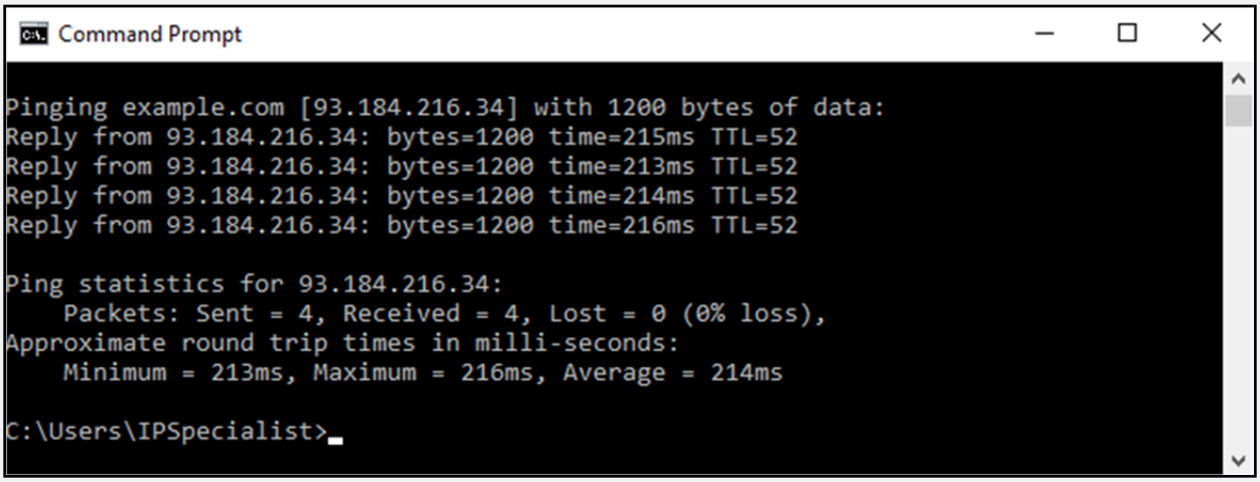


Figure 2-65: Ping example.com with DF bit set

The output shows the reply now, which means 1200 bits will not require being fragmented. You can try again to get the more appropriate fragment value.

Now, Enter the command "**`Tracert example.com`**" to trace the target.

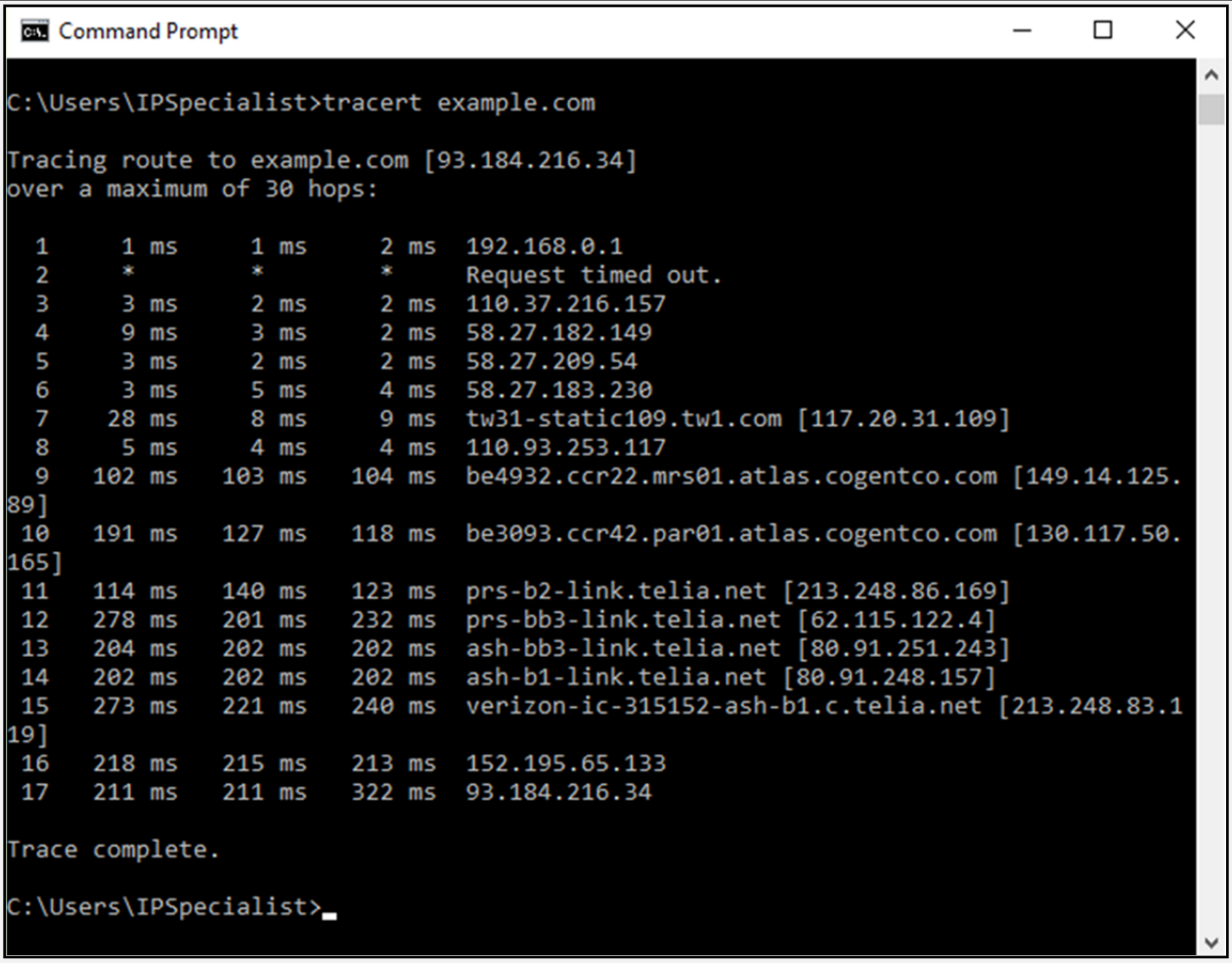


Figure 2-66: Ping example.com with DF bit set

From the output, you can get the information about hops between the source (your PC) and the destination (example.com), response times and other information.

Lab 2-5: Downloading a Website using Website Copier tool (HTTrack)

Case Study: We are using Windows Server 2016 for this lab. You can check the compatibility of HTTrack Website copier tool on different platforms such as Windows, Linux, and Android from the website **http://www.httrack.com**. Download and install HTTrack tool. In this lab, we are going to copy a website into our local directory and browse it from there in an offline environment.

Procedure:
Download and Install the WinHTTrack Website Copier Tool.

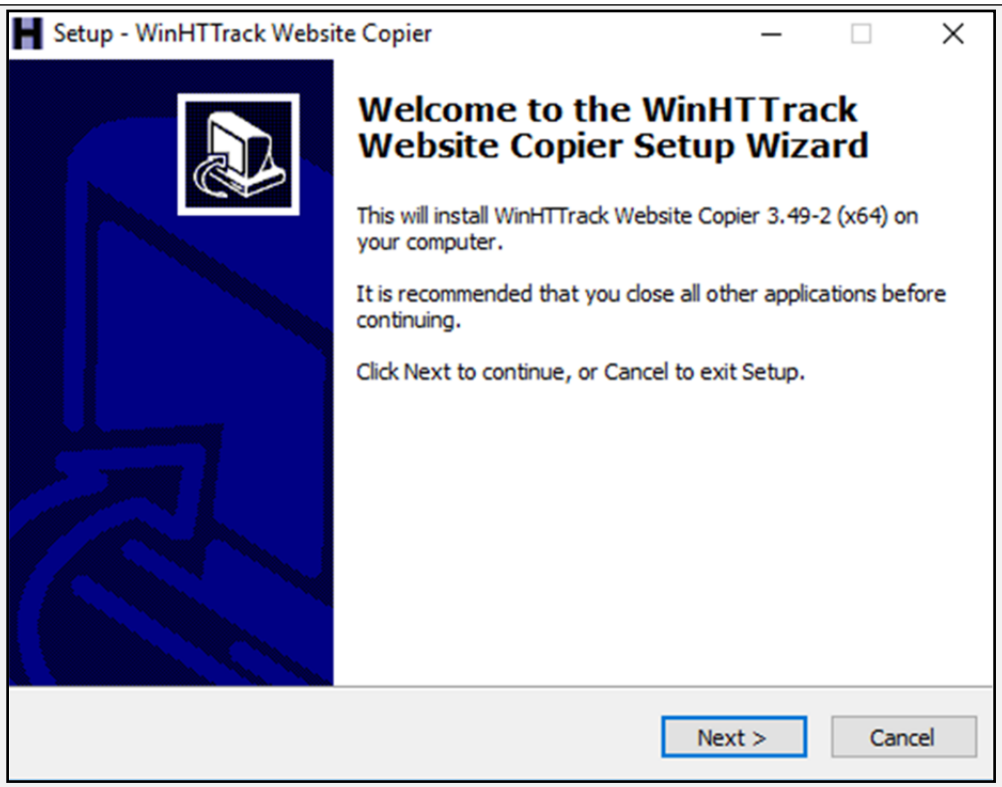


Figure 2-67: WinHTTrack Website Copier

HTTrack Website Copier tool installation.

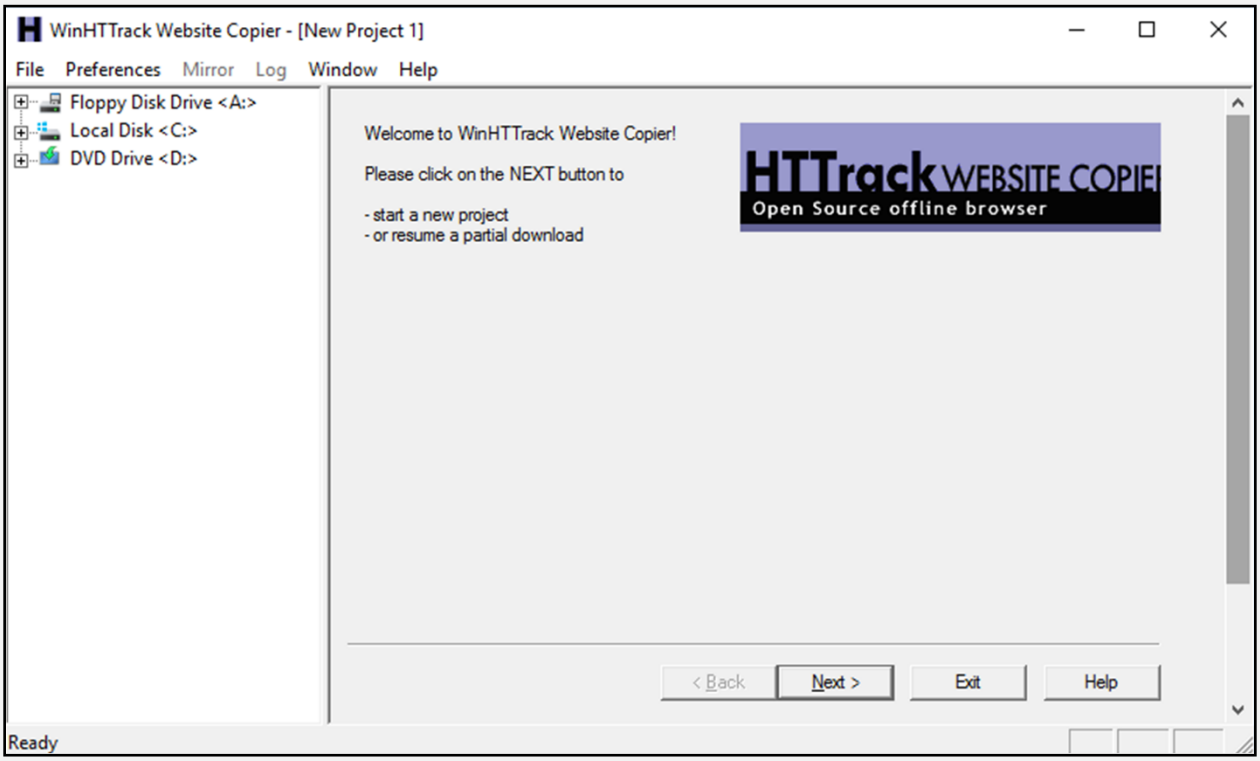


Figure 2-68: WinHTTrack Website Copier

Click Next

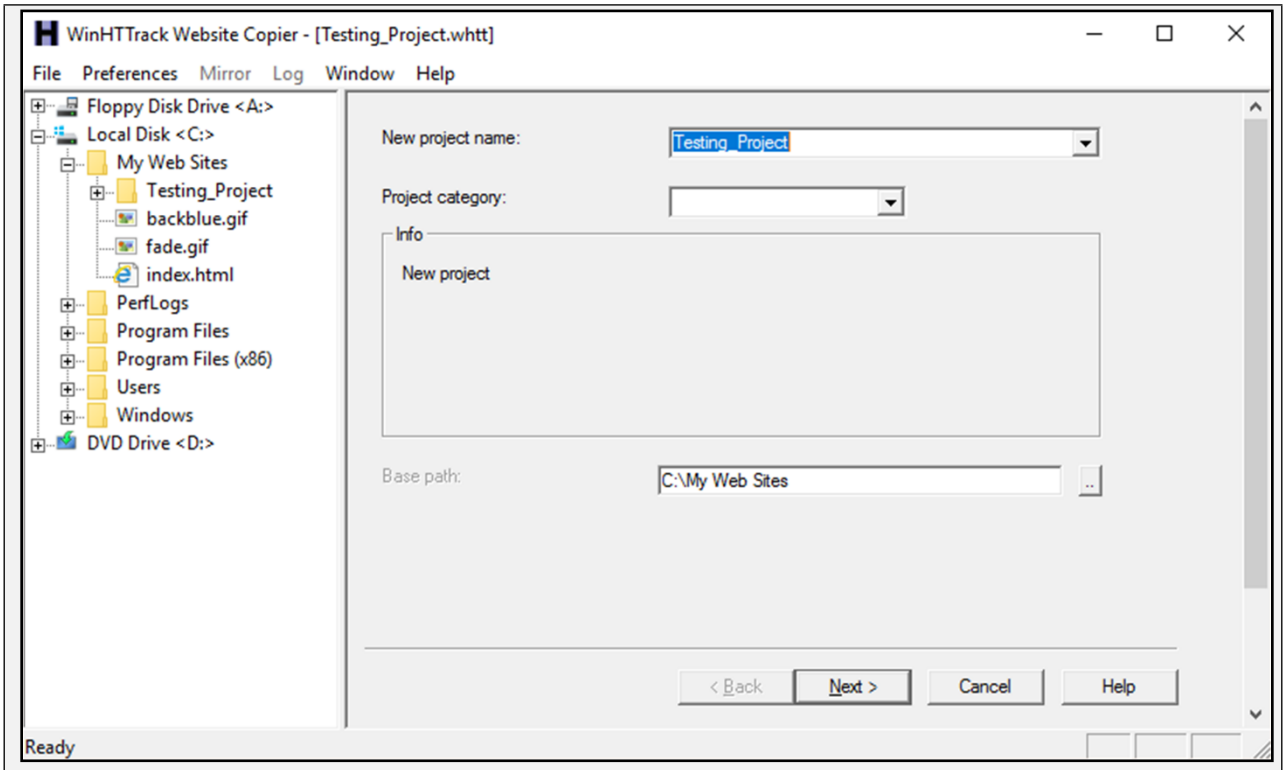


Figure 2-69: Creating a new project

Enter a Project name, as in our case, **Testing_Project.**

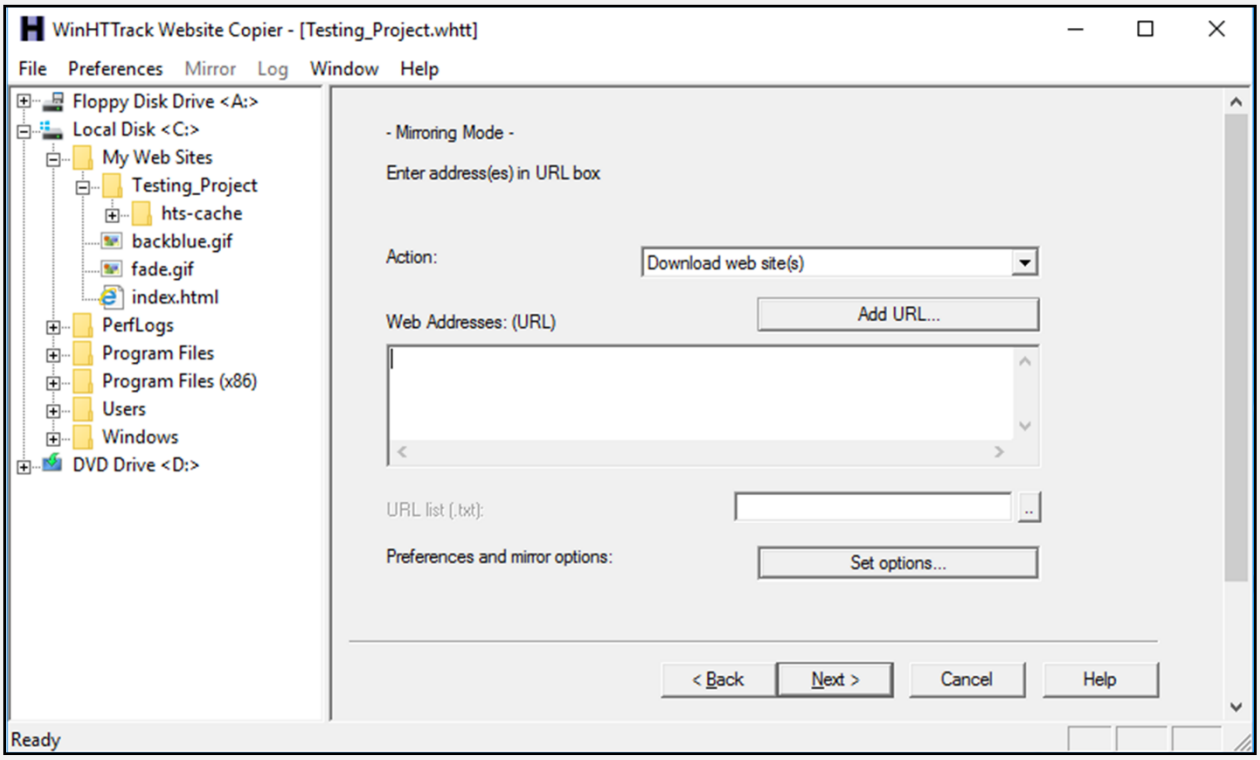


Figure 2-70: Setting Target

Click on **Set Options** button.

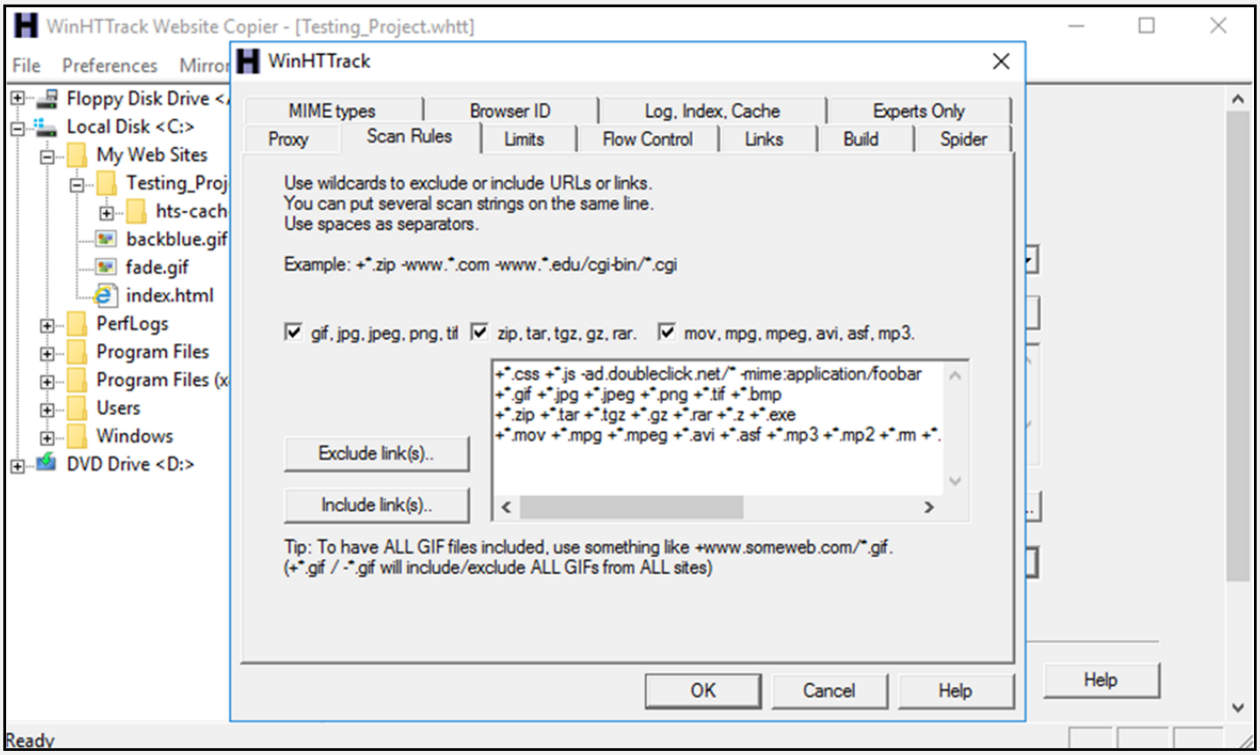


Figure 2-71: Configuring Options

Go to **Scan Rules** Tab and Select options as required.

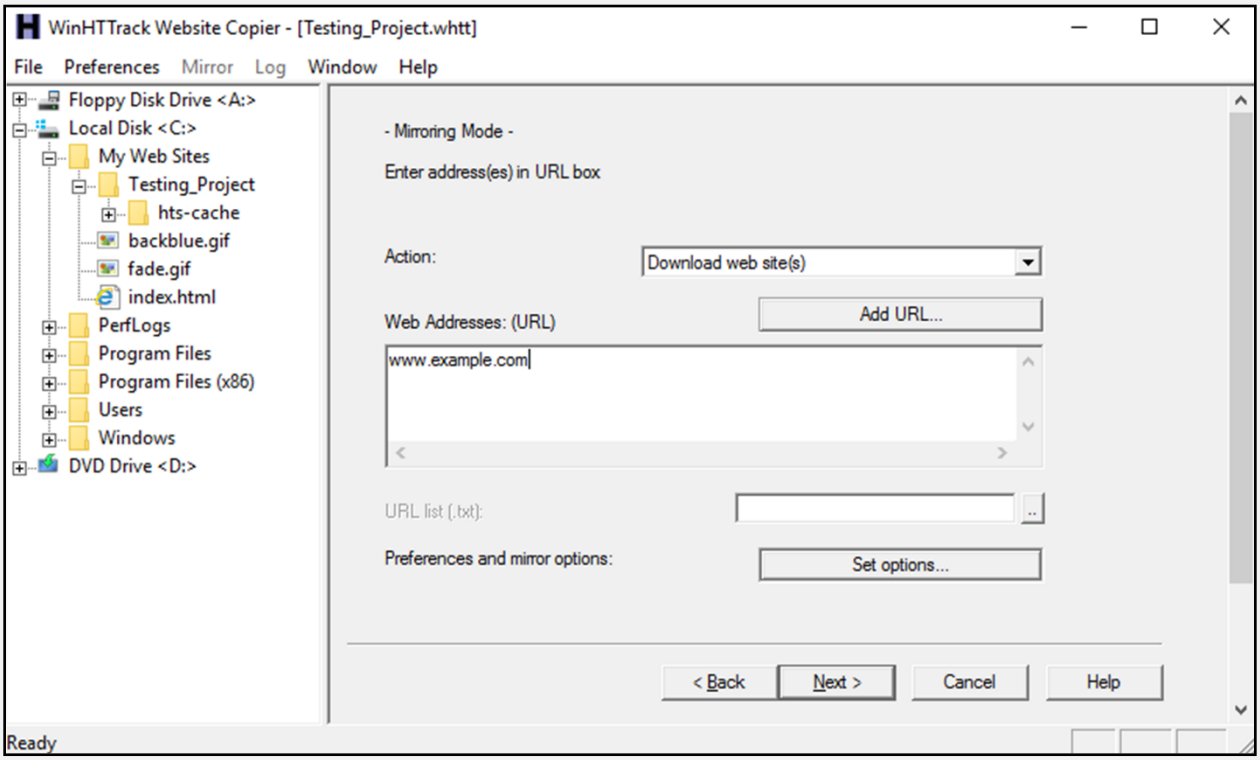


Figure 2-72: Configuring Options

Enter the Web Address in the field and Click Next.

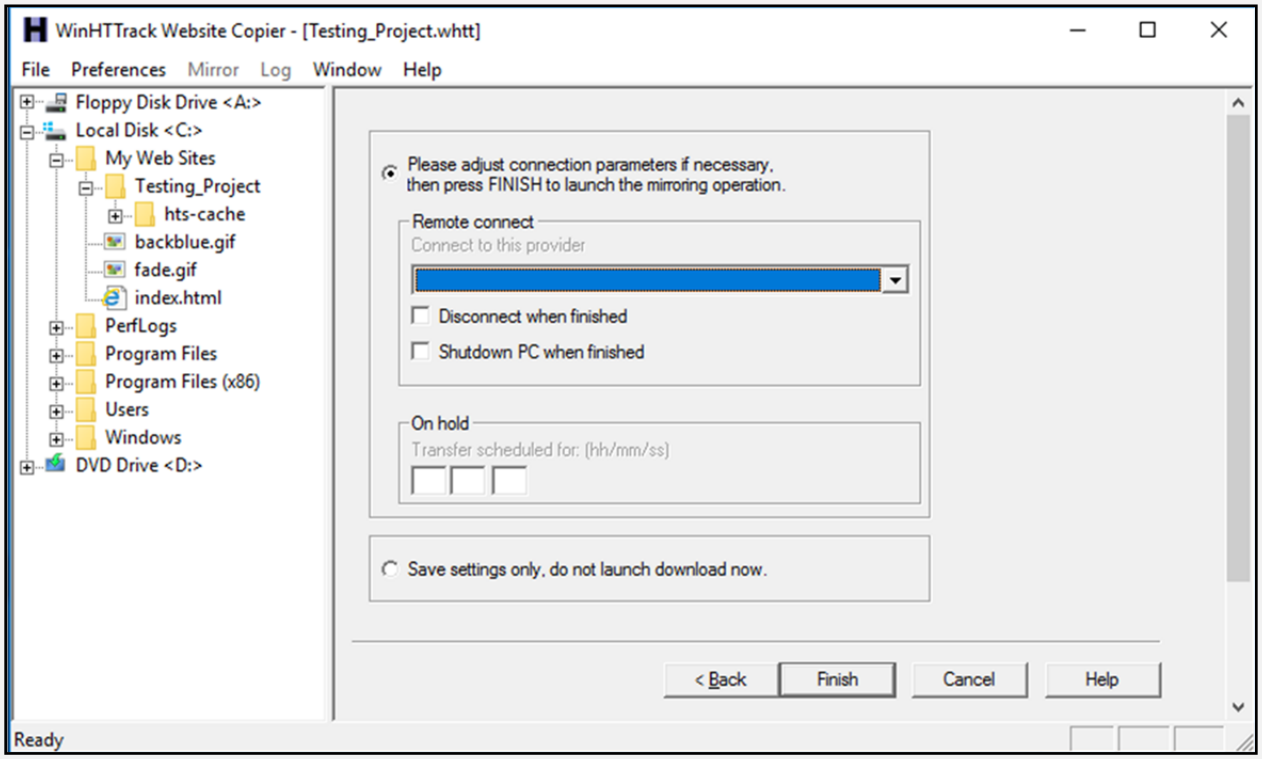


Figure 2-73: Configuring Options

Click Next.

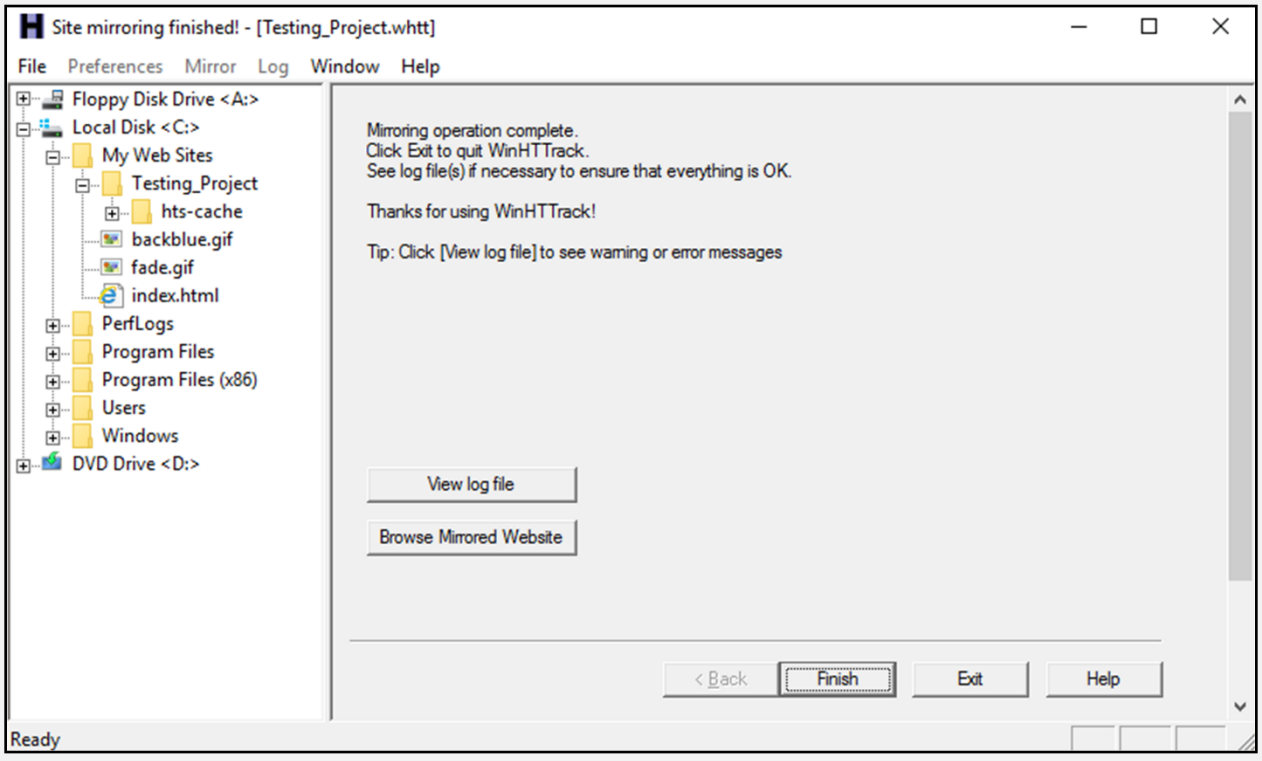


Figure 2-74: Copying complete

Click **Browse Mirrored Website**.

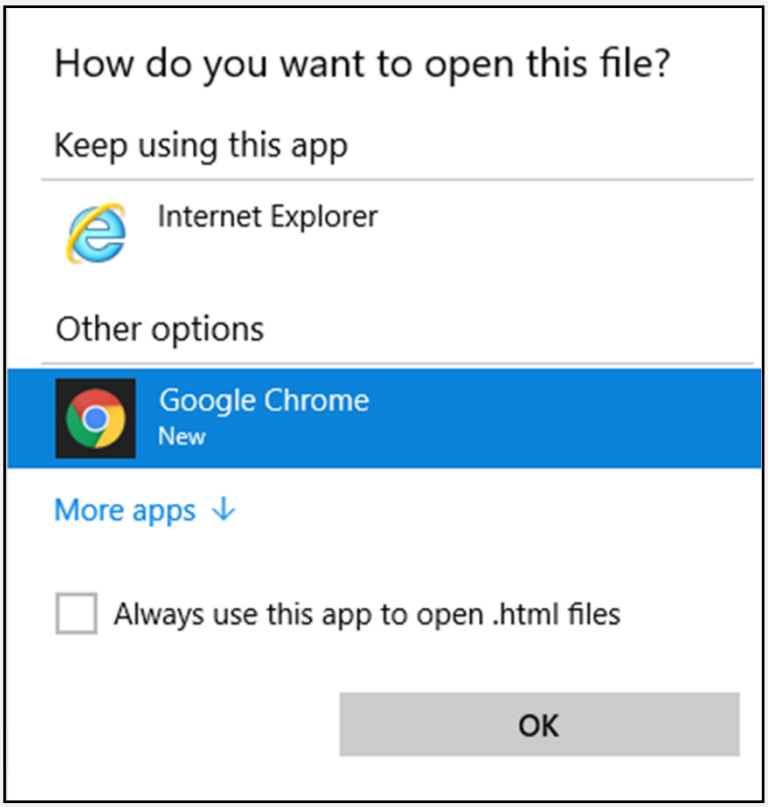


Figure 2-75: Browsing Copied Website

Select your favorite web browser.

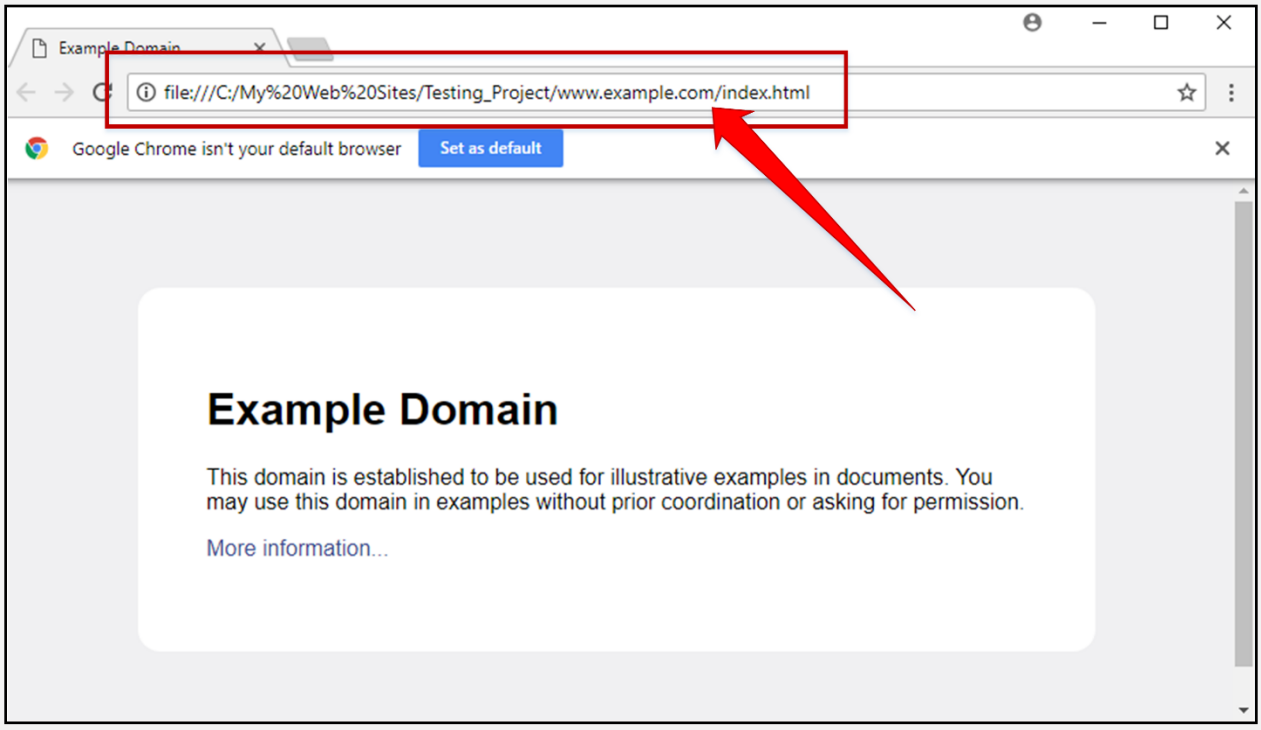


Figure 2-76: Website browse from a local directory

Observed the above output. Example.com website is copied into a local directory and browsed from there. Now you can explore the website in an offline environment for the structure of the website and other parameters.

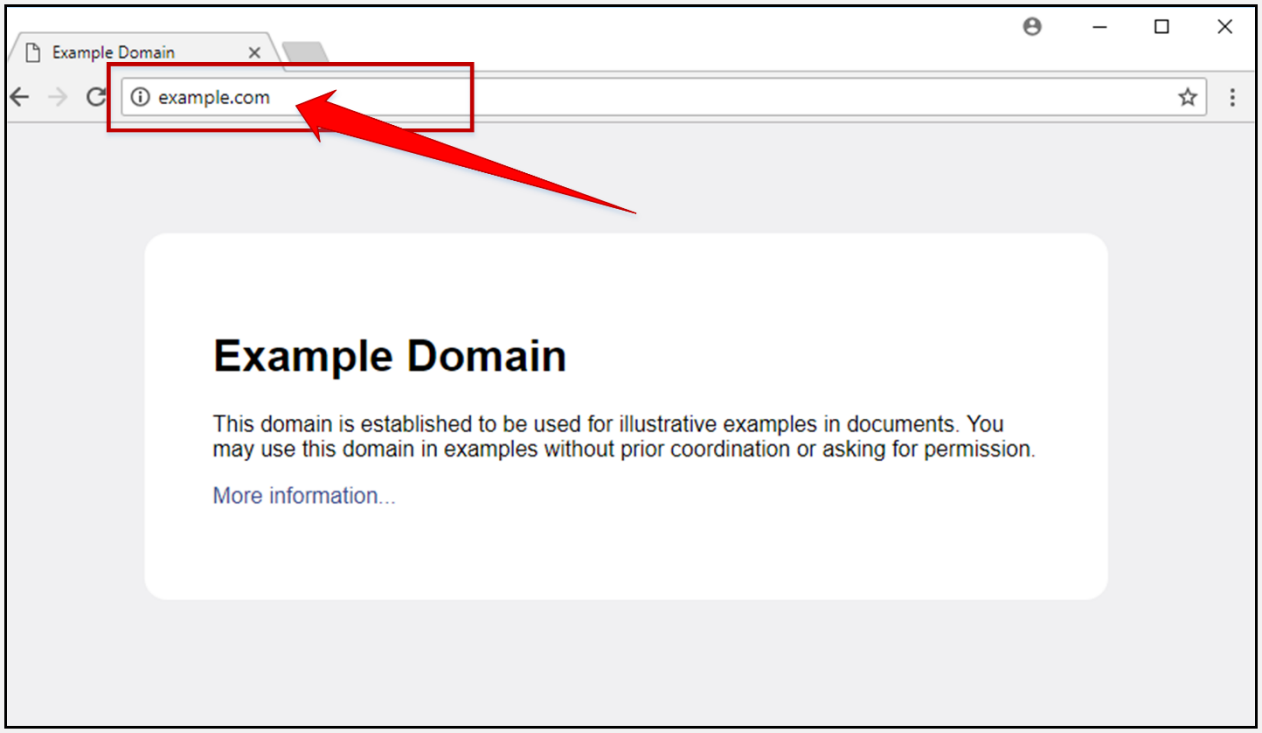


Figure 2-77: Original Website

To make sure, compare the website to the original example.com website. Open a new tab and go to URL example.com.

Lab 2-6: Gathering information using Metasploit

Case Study: In this lab, we are using Metasploit Framework, default application in Kali Linux for gathering more information about the host in a network. A Metasploit Framework is a powerful tool, popularly used for scanning & gathering information in the hacking environment. Metasploit Pro enables you to automate the process of discovery and exploitation and provides you with the necessary tools to perform the manual testing phase of a penetration test. You can use Metasploit Pro to scan for open ports and services, exploit vulnerabilities, pivot further into a network, collect evidence, and create a report of the test results.

Topology Information: In this lab, we are running Metasploit Framework on a private network 10.10.50.0/24 where different hosts are live including Windows 7, Kali Linux, Windows Server 2016 and others.

Procedure:

Open Kali Linux and Run Metasploit Framework.

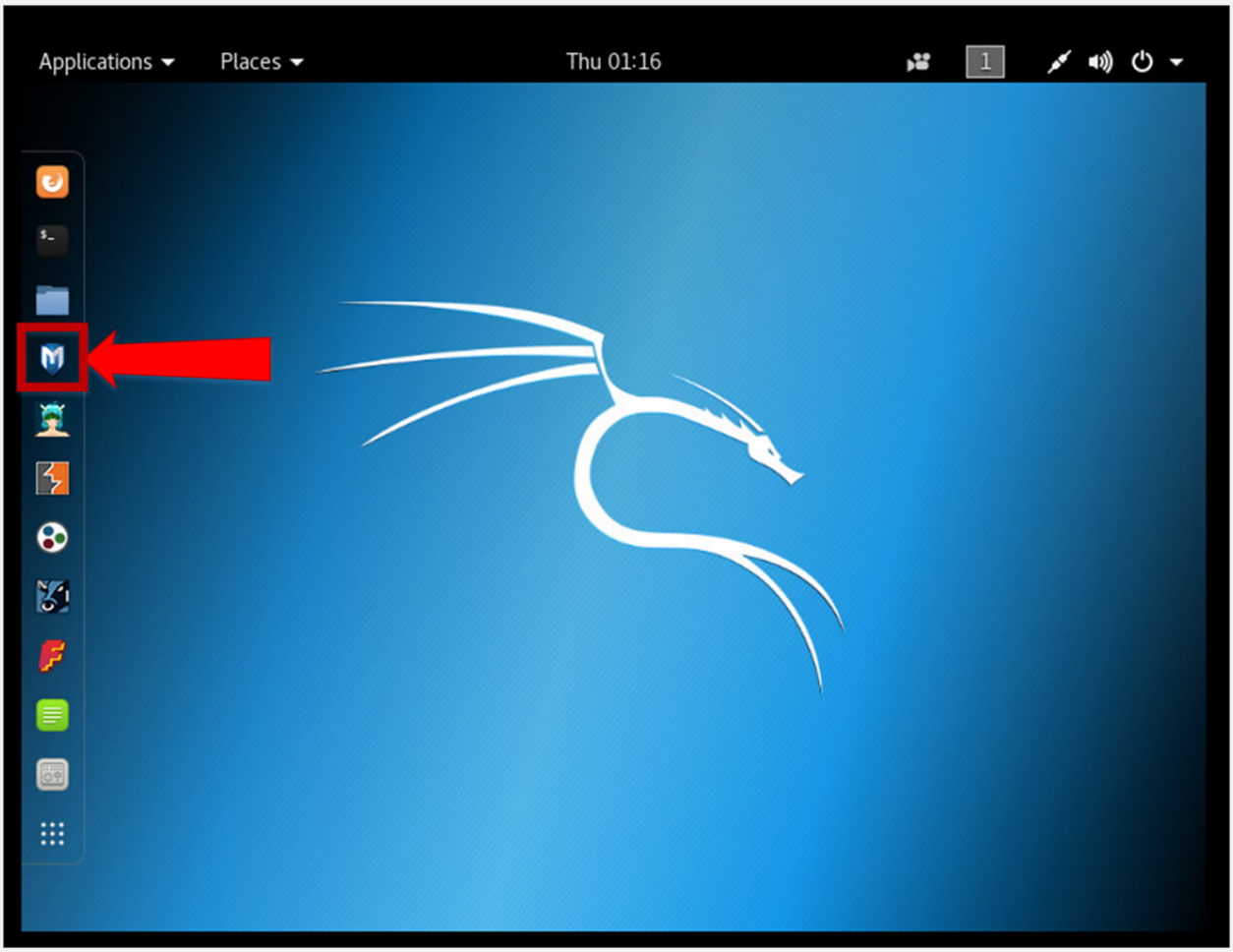


Figure 2-78: Kali Linux Desktop

Metasploit Framework initialization as shown below in the figure.

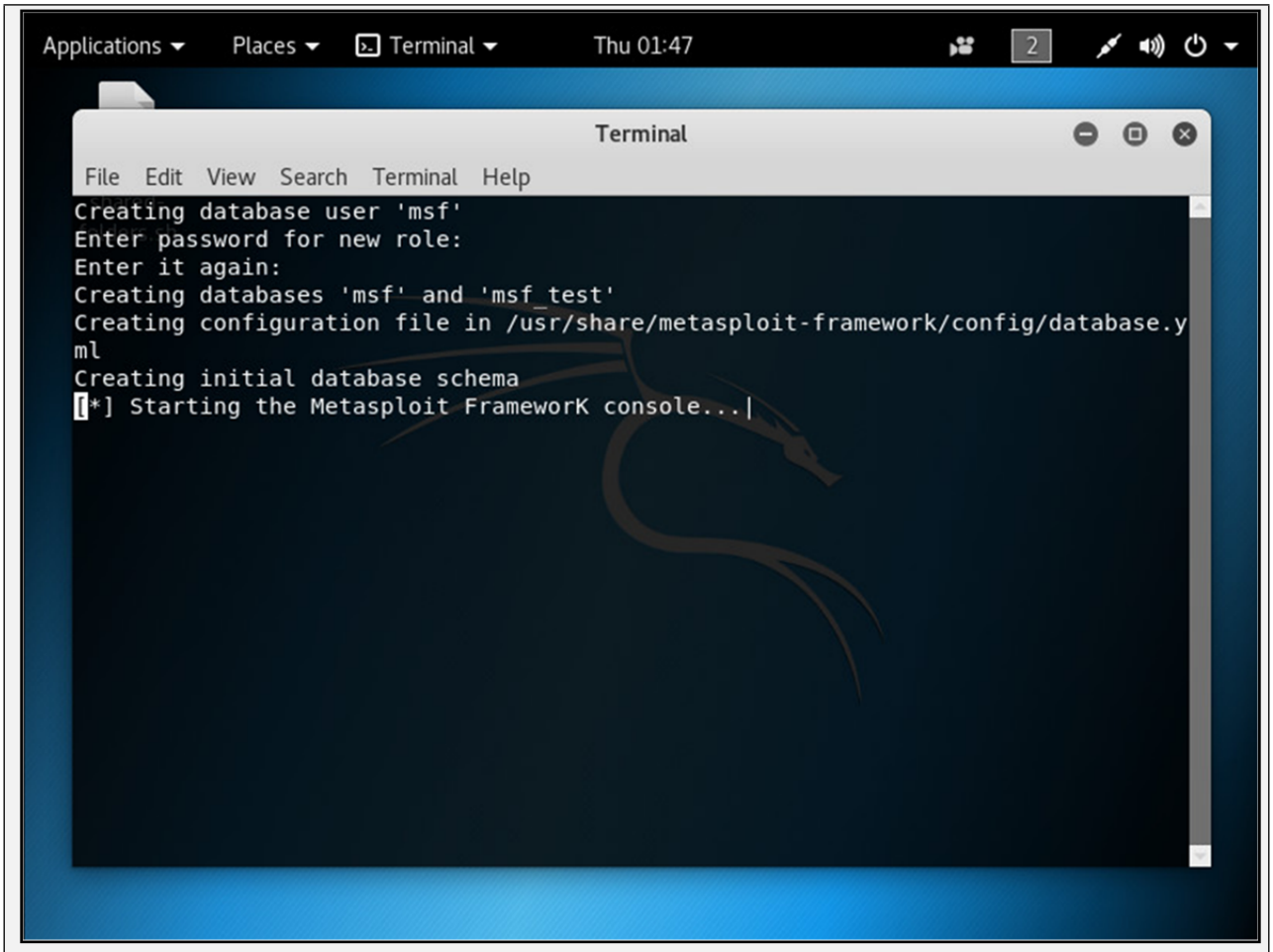


Figure 2-79: Metasploit Framework

msf > **db_status**

```
[*] postgresql connected to msf

// If your database is not connected, it means your database is not initiated. You will need to exit msfconsole & restart the postgresql service.

// Performing nmap Scan for ping sweep on the subnet 10.10.50.0/24
```

msf > **nmap -Pn -sS -A -oX Test 10.10.50.0/24**

```
[*] exec: nmap -Pn -sS -A -oX Test 10.10.50.0/24
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-26 01:49 EDT
Stats: 0:04:31 elapsed; 247 hosts completed (8 up), 8 undergoing Script Scan
NSE Timing: About 99.77% done; ETC: 01:53 (0:00:00 remaining)
Stats: 0:05:04 elapsed; 247 hosts completed (8 up), 8 undergoing Script Scan
NSE Timing: About 99.79% done; ETC: 01:54 (0:00:00 remaining)
Stats: 0:06:21 elapsed; 247 hosts completed (8 up), 8 undergoing Script Scan
NSE Timing: About 99.93% done; ETC: 01:55 (0:00:00 remaining)
Nmap scan report for 10.10.50.1
Host is up (0.0012s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE    VERSION
```

```
22/tcp   open  ssh        Cisco SSH 1.25 (protocol 1.5)
| ssh-hostkey:
|_  512 ca:9c:c7:d2:d4:b0:78:82:3e:34:8f:cf:00:9d:75:db (RSA1)
|_sshv1: Server supports SSHv1
23/tcp   open  telnet     Cisco router telnetd
5060/tcp open  sip-proxy  Cisco SIP Gateway (IOS 15.2.4.M4)
|_sip-methods: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE,
NOTIFY, INFO, REGISTER
5061/tcp open  tcpwrapped
MAC Address: C0:67:AF:C7:D9:80 (Cisco Systems)
OS details: Cisco 836, 890, 1751, 1841, 2800, or 2900 router (IOS 12.4 - 15.1), Cisco
Aironet 1141N (IOS 12.4) or 3602I (IOS 15.3) WAP, Cisco Aironet 2600-series WAP (IOS
15.2(2))
Network Distance: 1 hop
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

TRACEROUTE
HOP RTT     ADDRESS
1   1.15 ms 10.10.50.1

Nmap scan report for 10.10.50.10
Host is up (0.00030s latency).
Not shown: 990 filtered ports
PORT     STATE  SERVICE         VERSION
22/tcp   open   ssh             OpenSSH 5.6 (protocol 2.0)
| ssh-hostkey:
|   1024 e3:93:64:12:9c:c0:70:72:35:e1:ac:61:af:cc:49:ec (DSA)
|_  2048 2a:0b:42:38:f4:ca:d6:07:95:aa:87:ed:52:de:d1:14 (RSA)
80/tcp   open   http            VMware ESXi Server httpd
|_http-title: Did not follow redirect to https://10.10.50.10/
427/tcp  open   svrloc?
443/tcp  open   ssl/http        VMware ESXi Server httpd
|_http-title: " + ID_EESX_Welcome + "
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2014-01-15T03:42:31
|_Not valid after:  2025-07-16T03:42:31
|_ssl-date: 2018-04-25T19:58:24+00:00; -9h53m36s from scanner time.
| vmware-version:
|   Server version: VMware ESXi 5.1.0
|   Build: 1065491
|   Locale version: INTL 000
|   OS type: vmnix-x86
|_  Product Line ID: embeddedEsx
902/tcp  open   ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
5988/tcp closed wbem-http
5989/tcp open   ssl/wbem        SBLIM Small Footprint CIM Broker
```

```
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2014-01-15T03:42:31
|_Not valid after:  2025-07-16T03:42:31
|_ssl-date: 2018-04-25T19:58:23+00:00; -9h53m36s from scanner time.
8000/tcp open   http-alt?
8100/tcp open   tcpwrapped
8300/tcp closed tmi
MAC Address: F8:72:EA:A4:A1:CC (Cisco Systems)
Aggressive OS guesses: VMware ESXi 5.0 - 5.5 (96%), VMware ESXi 5.5 (96%), VMware
ESXi 4.1 (95%), VMware ESXi 6.0.0 (93%), FreeBSD 7.0-RELEASE-p1 - 10.0-CURRENT (93%),
VMware ESXi 4.1.0 (93%), VMware ESX Server 4.0.1 (91%), FreeBSD 5.2.1-RELEASE (91%),
FreeBSD 8.0-BETA2 - 10.1-RELEASE (90%), FreeBSD 5.3 - 5.5 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: localhost.localdomain; CPE: cpe:/o:vmware:esxi,
cpe:/o:vmware:ESXi:5.1.0

Host script results:
|_clock-skew: mean: -9h53m36s, deviation: 0s, median: -9h53m36s

TRACEROUTE
HOP RTT     ADDRESS
1   0.30 ms 10.10.50.10

Nmap scan report for 10.10.50.11
Host is up (0.00058s latency).
Not shown: 990 filtered ports
PORT     STATE  SERVICE         VERSION
22/tcp   open   ssh             OpenSSH 5.6 (protocol 2.0)
| ssh-hostkey:
|   1024 6f:d3:3d:cb:54:0b:83:3e:bd:25:1c:da:67:b6:92:fb (DSA)
|_  2048 f9:bc:20:c5:6e:db:6a:86:ea:f5:24:06:57:c6:d9:6f (RSA)
80/tcp   open   http            VMware ESXi Server httpd
|_http-title: Did not follow redirect to https://10.10.50.11/
427/tcp  open   svrloc?
443/tcp  open   ssl/http        VMware ESXi Server httpd
|_http-title: " + ID_EESX_Welcome + "
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2014-01-18T05:33:03
|_Not valid after:  2025-07-19T05:33:03
|_ssl-date: 2018-04-25T19:50:12+00:00; -10h01m33s from scanner time.
| vmware-version:
|   Server version: VMware ESXi 5.1.0
|   Build: 1065491
|   Locale version: INTL 000
```

```
|   OS type: vmnix-x86
|_  Product Line ID: embeddedEsx
902/tcp  open   ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
5988/tcp closed wbem-http
5989/tcp open   ssl/wbem        SBLIM Small Footprint CIM Broker
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=VMware,
Inc/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2014-01-18T05:33:03
|_Not valid after:  2025-07-19T05:33:03
|_ssl-date: 2018-04-25T19:50:25+00:00; -10h01m35s from scanner time.
8000/tcp open   http-alt?
8100/tcp open   tcpwrapped
8300/tcp closed tmi
MAC Address: F8:72:EA:A4:A1:2C (Cisco Systems)
Device type: specialized
Running: VMware ESXi 5.X
OS CPE: cpe:/o:vmware:esxi:5
OS details: VMware ESXi 5.0 - 5.5
Network Distance: 1 hop
Service Info: Host: localhost.localdomain; CPE: cpe:/o:vmware:esxi,
cpe:/o:vmware:ESXi:5.1.0

Host script results:
|_clock-skew: mean: -10h01m34s, deviation: 1s, median: -10h01m35s

TRACEROUTE
HOP RTT     ADDRESS
1   0.58 ms 10.10.50.11

Nmap scan report for vc.ooredoocloud.qa (10.10.50.20)
Host is up (0.00065s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8d:b4:b0:01:63:84:eb:c7:bf:cf:f7:b0:c3:12:0e:13 (RSA)
|   256 02:31:3e:d3:75:97:f2:10:88:30:6a:c1:ca:a4:82:bf (ECDSA)
|_  256 c5:21:3a:a7:81:f5:a6:00:ee:5e:76:94:88:68:03:1d (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:72:4A:C1 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.65 ms 10.10.50.20

Nmap scan report for 10.10.50.100
Host is up (0.00078s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE         VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp   open  ssl/http        VMware VirtualCenter Web service
|_http-title: Site doesn't have a title (text; charset=plain).
| ssl-cert: Subject: commonName=VMware/countryName=US
| Not valid before: 2017-12-19T17:36:01
|_Not valid after:  2018-12-19T17:36:01
|_ssl-date: TLS randomness does not represent time
| vmware-version:
|   Server version: VMware Workstation 12.5.6
|   Build: 5528349
|   Locale version: INTL
|   OS type: win32-x86
|_  Product Line ID: ws
445/tcp   open  microsoft-ds    Windows 7 Professional 7601 Service Pack 1 microsoft-
ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1025/tcp  open  msrpc           Microsoft Windows RPC
1026/tcp  open  msrpc           Microsoft Windows RPC
1027/tcp  open  msrpc           Microsoft Windows RPC
1028/tcp  open  msrpc           Microsoft Windows RPC
1030/tcp  open  msrpc           Microsoft Windows RPC
1031/tcp  open  msrpc           Microsoft Windows RPC
2869/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server   Microsoft Terminal Service
| ssl-cert: Subject: commonName=Win7-PC
| Not valid before: 2017-12-12T19:55:25
|_Not valid after:  2018-06-13T19:55:25
|_ssl-date: 2018-04-26T05:47:49+00:00; -3m54s from scanner time.
5357/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
MAC Address: 00:0C:29:95:04:33 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
```

```
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server
2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN7-PC; OS: Windows; CPE: cpe:/o:microsoft:windows,
cpe:/o:vmware:Workstation:12.5.6

Host script results:
|_clock-skew: mean: -3m54s, deviation: 0s, median: -3m54s
|_nbstat: NetBIOS name: WIN7-PC, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:95:04:33 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Win7-PC
|   NetBIOS computer name: WIN7-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2018-04-26T10:47:56+05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2018-04-26 01:48:04
|_  start_date: 2018-03-27 07:26:43

TRACEROUTE
HOP RTT     ADDRESS
1   0.78 ms 10.10.50.100

Nmap scan report for 10.10.50.202
Host is up (0.00096s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Windows 7 Professional 7601 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=Win7-1-PC
| Not valid before: 2018-03-05T06:10:47
```

```
|_Not valid after:  2018-09-04T06:10:47
|_ssl-date: 2018-04-26T05:51:38+00:00; -28s from scanner time.
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49156/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  msrpc         Microsoft Windows RPC
49160/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 00:0C:29:20:C4:A9 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server
2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN7-1-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -28s, deviation: 0s, median: -28s
|_nbstat: NetBIOS name: WIN7-1-PC, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:20:c4:a9 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: Win7-1-PC
|   NetBIOS computer name: WIN7-1-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2018-04-25T22:51:33-07:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2018-04-26 01:51:33
|_  start_date: 2018-03-29 05:57:42

TRACEROUTE
```

```
HOP RTT     ADDRESS
1   0.96 ms 10.10.50.202

Nmap scan report for 10.10.50.210
Host is up (0.00065s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3c:9c:fb:cb:58:35:f9:d7:d7:32:6f:ad:6a:f8:c7:9b (RSA)
|   256 70:e7:d9:a2:6a:54:92:e6:07:c9:89:58:b5:99:7d:0d (ECDSA)
|_  256 b1:be:a6:62:96:69:76:64:aa:23:bb:ad:54:cc:c0:db (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:EA:BD:DF (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.65 ms 10.10.50.210

Nmap scan report for 10.10.50.211
Host is up (0.00037s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-2HMGPM3UAD7
| Not valid before: 2018-03-28T12:23:16
|_Not valid after:  2018-09-27T12:23:16
|_ssl-date: 2018-04-26T05:51:41+00:00; -5s from scanner time.
MAC Address: 00:0C:29:BA:AC:AA (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 6.X (85%)
OS CPE: cpe:/o:FreeBSD:FreeBSD:6.2
Aggressive OS guesses: FreeBSD 6.2-RELEASE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:Microsoft:windows

Host script results:
|_clock-skew: mean: -5s, deviation: 0s, median: -5s
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.37 ms 10.10.50.211

Nmap scan report for 10.10.50.200
Host is up (0.000042s latency).
All 1000 scanned ports on 10.10.50.200 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 256 IP addresses (9 hosts up) scanned in 384.48 seconds


//Importing Nmap XML file
msf > db_import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.8.1'
[*] Importing host 10.10.50.1
[*] Importing host 10.10.50.10
[*] Importing host 10.10.50.11
[*] Importing host 10.10.50.20
[*] Importing host 10.10.50.100
[*] Importing host 10.10.50.202
[*] Importing host 10.10.50.210
[*] Importing host 10.10.50.211
[*] Importing host 10.10.50.200
[*] Successfully imported /root/Test
```

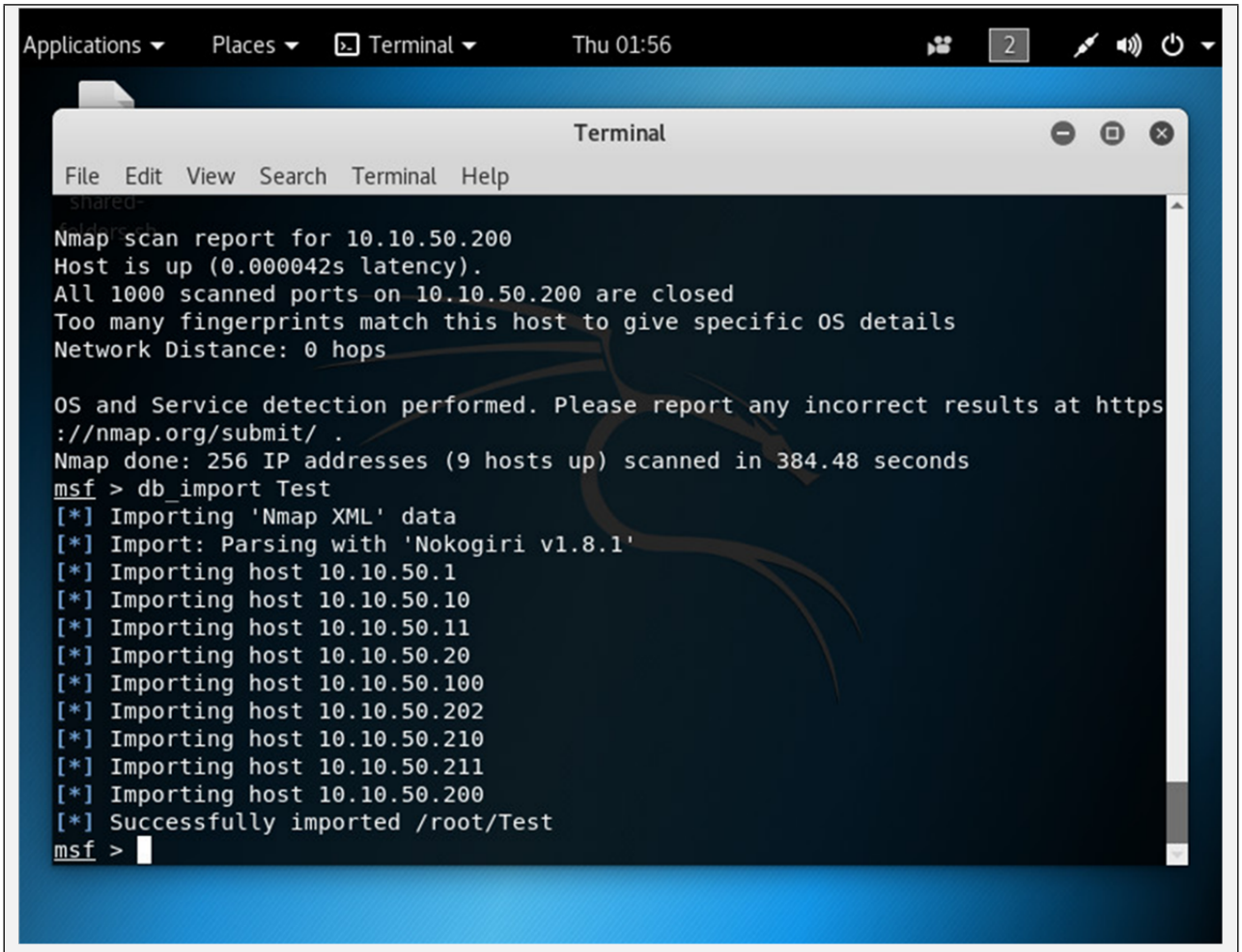


Figure 2-80: Importing Results

msf > hosts

```
Hosts
=====

Address            mac                name    os_name    os_flavor  os_sp  purpose
info  comments
-------            ---                ----    -------    ---------  -----  -------  -
---
10.10.50.1         c0:67:af:c7:d9:80          IOS                   12.X   device
10.10.50.10        f8:72:ea:a4:a1:cc          ESXi                  5.X    device
10.10.50.11        f8:72:ea:a4:a1:2c          ESXi                  5.X    device
10.10.50.20        00:0c:29:72:4a:c1          Linux                 3.X    server
10.10.50.100       00:0c:29:95:04:33          Windows 7                    client
10.10.50.200                                  Unknown                      device
10.10.50.202       00:0c:29:20:c4:a9          Windows 7                    client
10.10.50.210       00:0c:29:ea:bd:df          Linux                 3.X    server
10.10.50.211       00:0c:29:ba:ac:aa          FreeBSD               6.X    device
```

```
//Performing Services scan
```

msf > **db_nmap -sS -A 10.10.50.211**

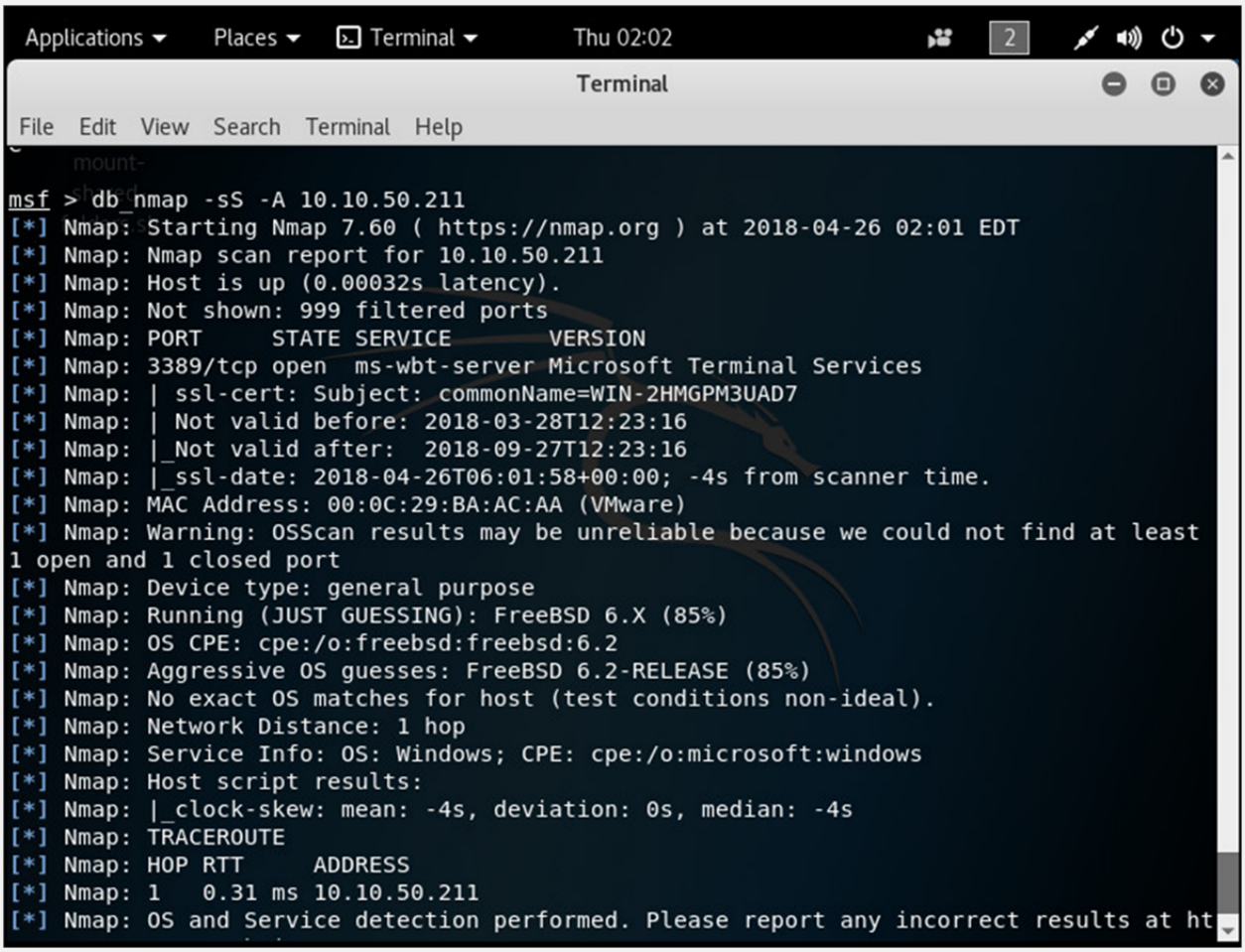


Figure 2-81: Service Scan

Observe the scan result showing different services, open and closed port information of live hosts.

msf > **services**

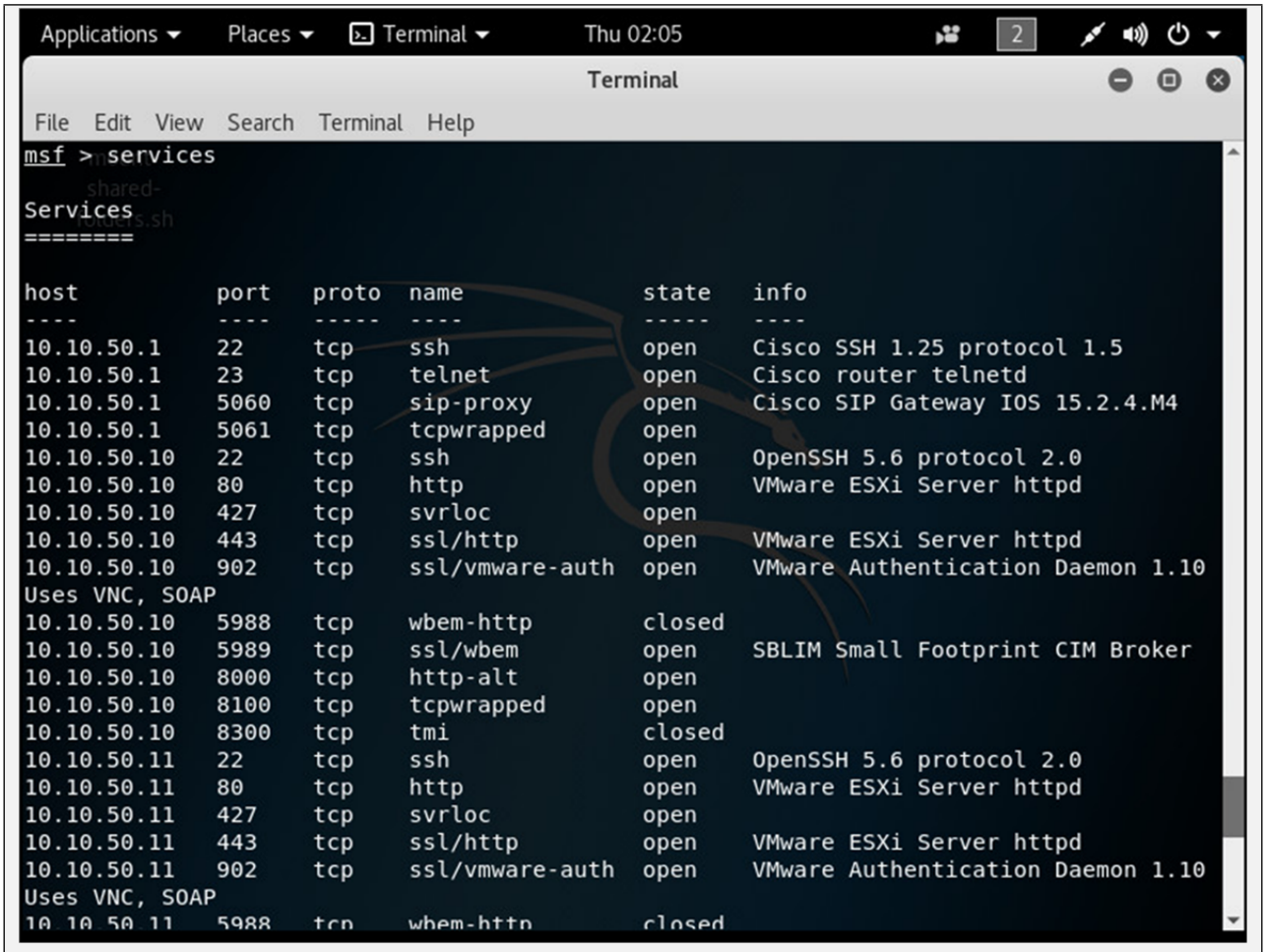


Figure 2-82: Service Scan results

msf > **use scanner/smb/smb_version**

msf auxiliary(scanner/smb/smb_version) > **show options**

```
Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   SMBDomain.                  no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads
```

msf auxiliary(scanner/smb/smb_version) > **set RHOSTS 10.10.50.100-211**

```
RHOSTS => 10.10.50.100-211
```

msf auxiliary(scanner/smb/smb_version) > **set THREADS 100**

```
THREADS => 100
```

msf auxiliary(scanner/smb/smb_version) > **show options**

```
Module options (auxiliary/scanner/smb/smb_version):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS     10.10.50.100-211 yes       The target address range or CIDR identifier
   SMBDomain.                  no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    100              yes       The number of concurrent threads
```

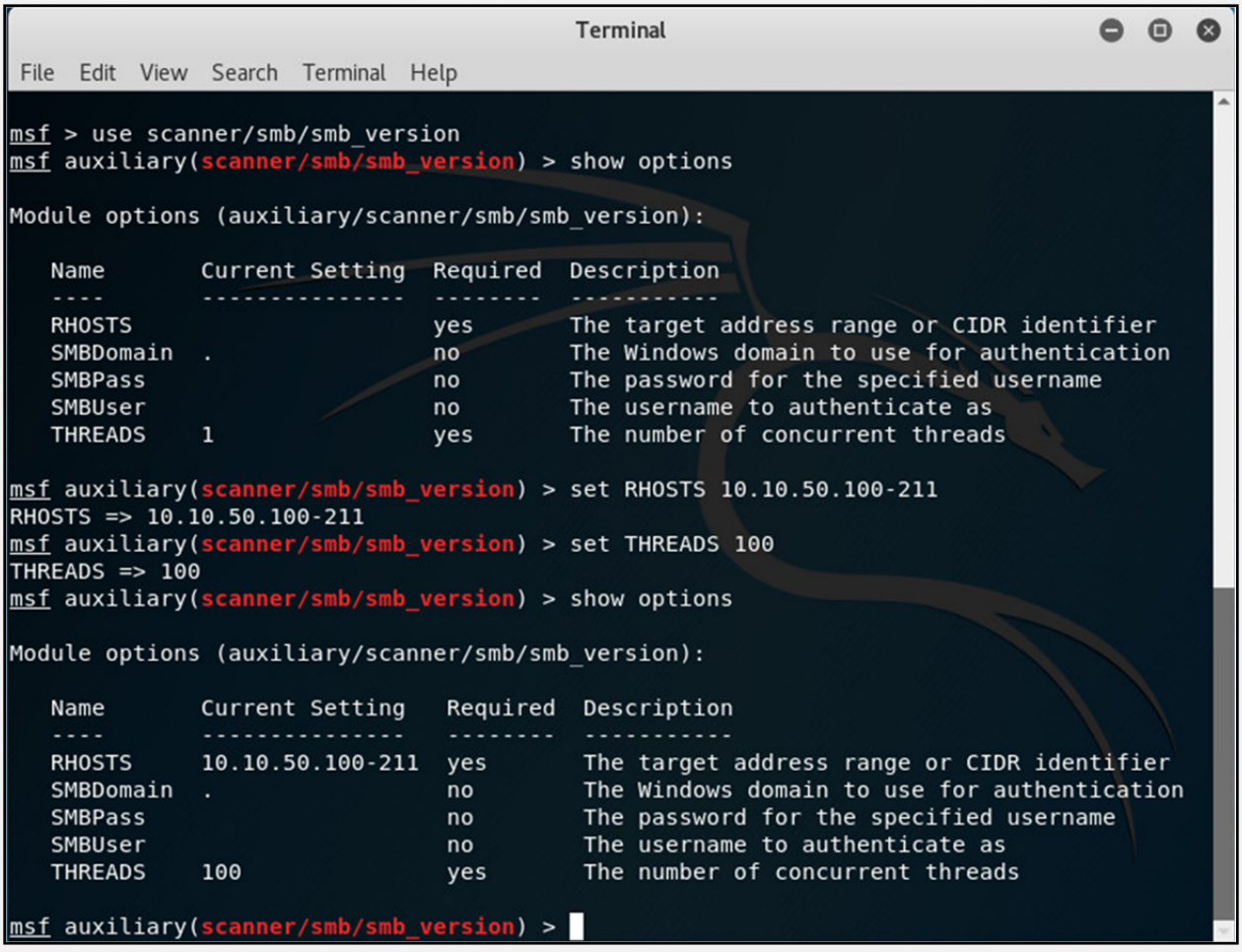


Figure 2-83: SMB Scan results

msf auxiliary(scanner/smb/smb_version) > **run**

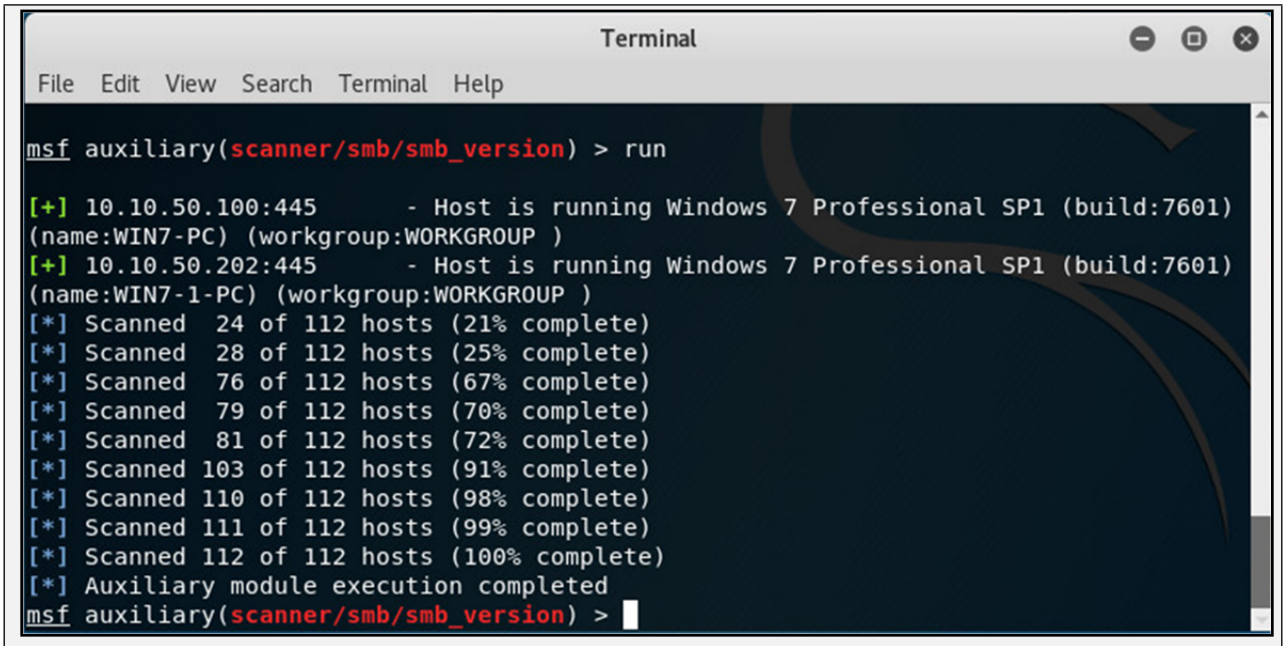


Figure 2-84: Running SMB Scan

msf auxiliary(scanner/smb/smb_version) > **hosts**

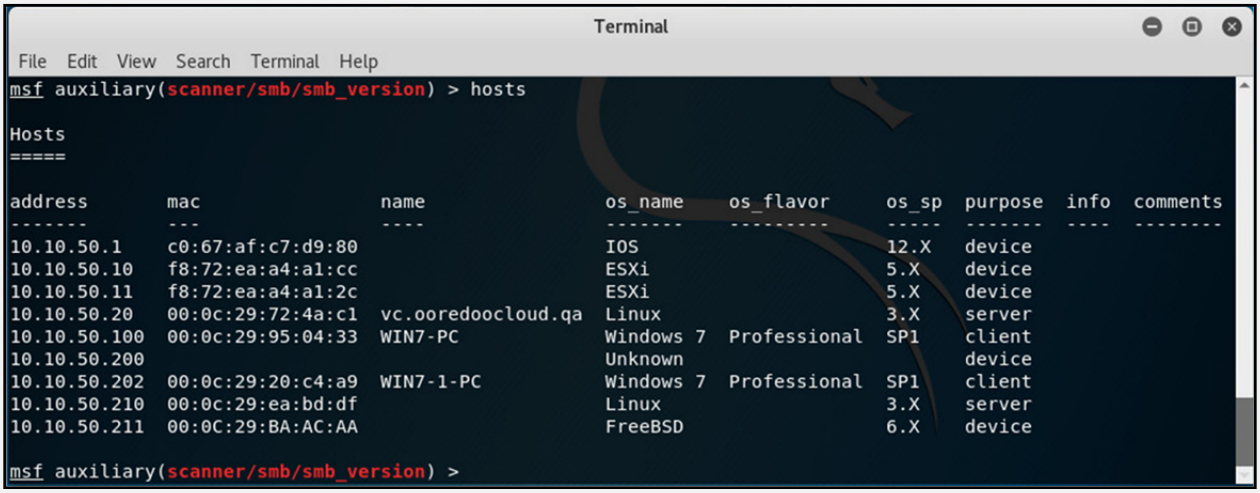


Figure 2-85: SMB Scan results

Observe the OS_Flavor field. SMB scanning scans for Operating System Flavor for the RHOST range configured.