

# **Experiment Number -4**

## **Aim:**

To study and use the tool Nmap.

## **Introduction:**

Nmap is a tool for network Exploration, host discovery and security auditing. Some of its primary uses are Discovering network component, determining open ports and services running on a host and determine the OS running on the host. These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features. Nmap can adapt to network conditions including latency and congestion during a scan.

## **Lab Scenario:**

A Windows machines with nmap installed in it and with internet access.

## **Download URL:**

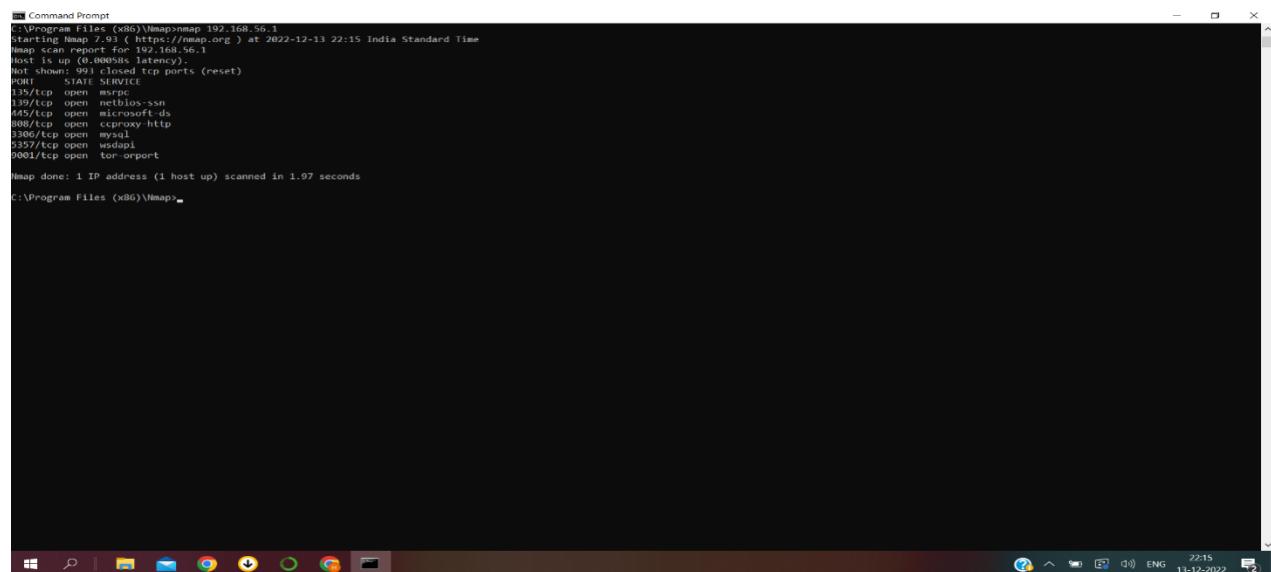
<https://nmap.org/download.html>

## Nmap Commands:

### ● Scan a Range of IP Address

To scan the entire CIDR (classless inter-domain routing) range of IP addresses, you can use the command.

**>> nmap <IP range>**



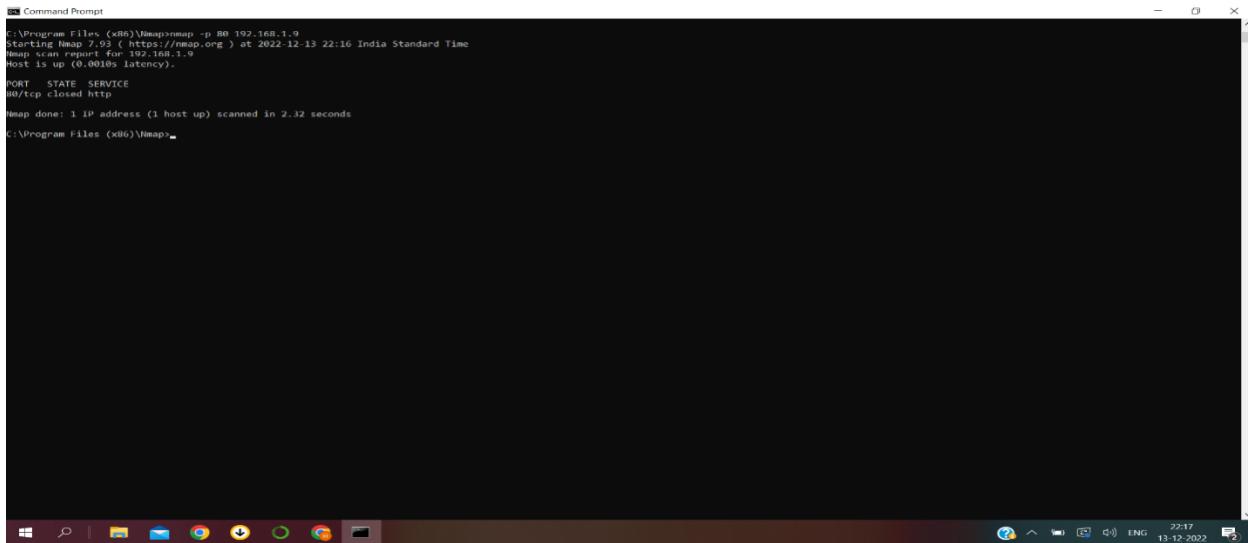
```
Windows Command Prompt
C:\Program Files (x86)\Nmap>nmap 192.168.56.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 22:15 India Standard Time
Nmap scan report for 192.168.56.1
Host is up (0.000000 latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
139/tcp    open  msrpc
139/udp   open  msrpc
445/tcp    open  microsoft-ds
8080/tcp   open  cproxy http
3306/tcp   open  mysql
3357/tcp   open  esql
9001/tcp   open  tor-orport

Nmap done: 1 IP address (1 host up) scanned in 1.07 seconds
C:\Program Files (x86)\Nmap>
```

### ● Port Scanning

Performing port scans will provide details about port services and states and not just that Nmap also provides options to scan popular ports and discover open ports. We will see that in the latter section of the article.

**>> nmap -p <numeric value> <IP>**



```
C:\> Command Prompt
C:\Program Files (x86)\Nmap>nmap -p 80 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 22:16 India Standard Time
Nmap scan report for 192.168.1.9
Host is up (0.0010s latency).

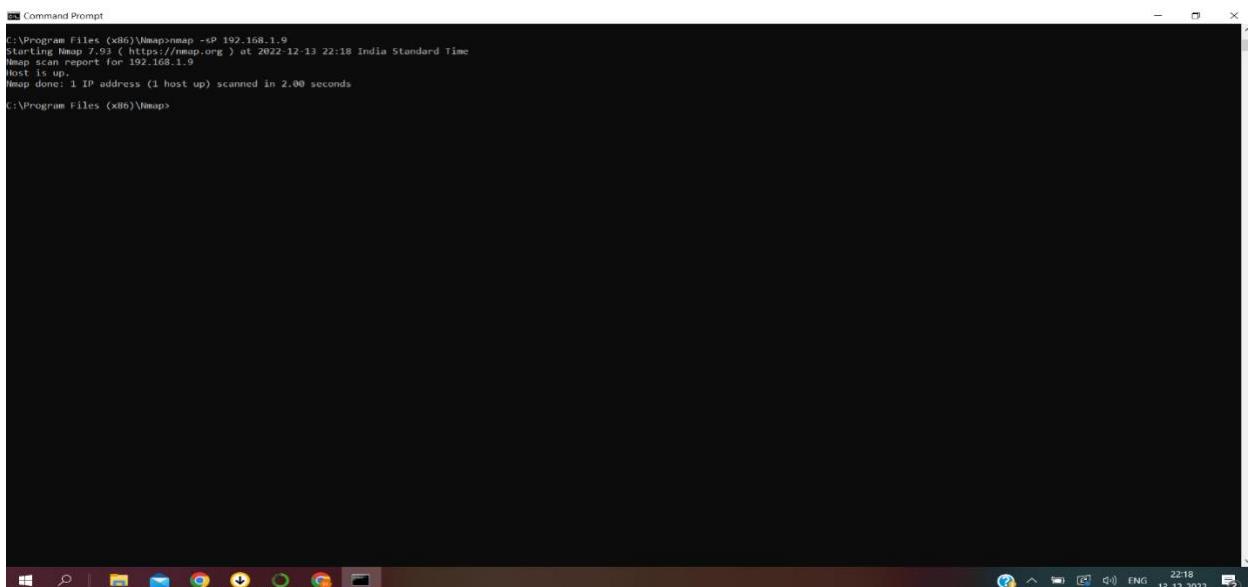
PORT      STATE    SERVICE
80/tcp    closed   http

Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
C:\Program Files (x86)\Nmap>
```

## ● Ping Scan Using Nmap

It also provides the option to find out multiple hosts or any specific host. This command returns the IP address and MAC (Media Access Control) address of available hosts but provides no information about ports. In simple words, it finds all devices in the defined range and then we can check if there are any IP addresses that we are not familiar with or we cannot account for. This command sends an ICMP (Internet Control Message Protocol) echo request to all IP addresses of the network.

**>> nmap -sP <target>**



```
C:\> Command Prompt
C:\Program Files (x86)\Nmap>nmap -sP 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 22:18 India Standard Time
Nmap scan report for 192.168.1.9
Host is up.

Nmap done: 1 IP address (1 host up) scanned in 2.00 seconds
C:\Program Files (x86)\Nmap>
```

## ● Most Popular Ports Scanning

To apply this command, we must use the “–top-ports” option with a specific numeric value. This option gives you the ability to scan top ports. However, in Nmap, you also have the option to select the number of top ports to scan. This command allows users to get better and faster results.

**>> nmap –top-ports <numeric value> <IP address/Domain>**

```
C:\Program Files (x86)\Nmap>nmap -top-ports 15 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 22:19 India Standard Time
Nmap scan report for 192.168.1.9
Host is up (0.00072s latency).

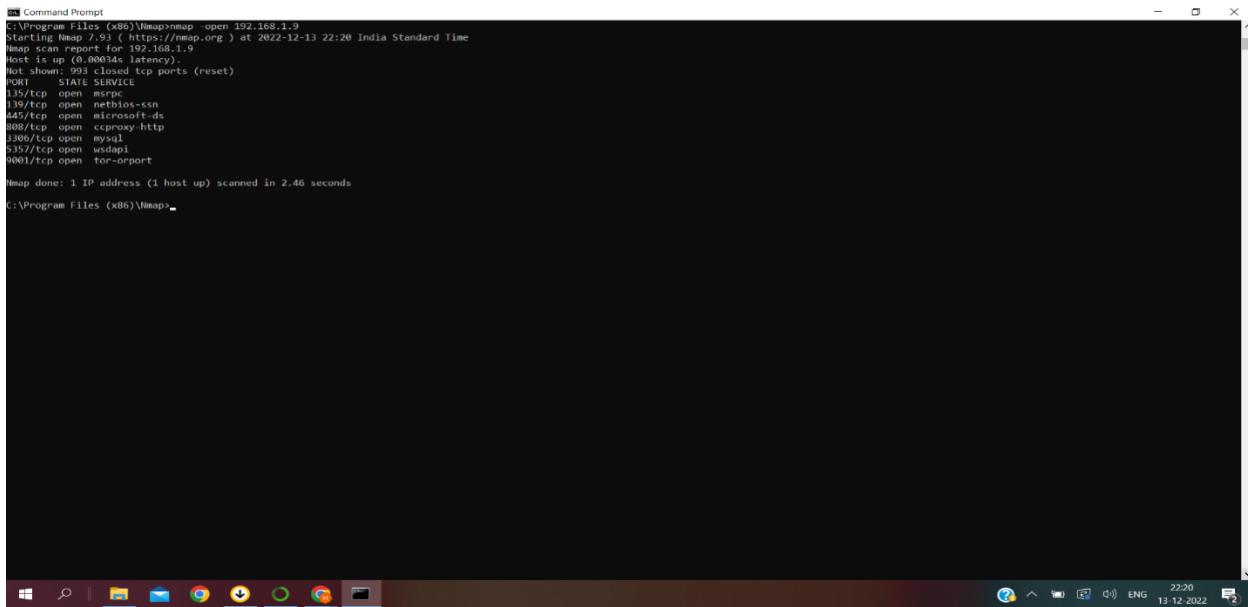
PORT      STATE SERVICE
21/tcp    closed  ftp
22/tcp    closed  ssh
23/tcp    closed  telnet
25/tcp    closed  smtp
53/tcp    closed  domain
80/tcp    open   http
110/tcp   closed pop3
135/tcp   open   msrpc
139/tcp   closed netbios-ssn
143/tcp   closed imap
443/tcp   closed https
8000/tcp  open   microsoft-ds
3389/tcp  closed ms-wbt-server
8080/tcp  closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds
C:\Program Files (x86)\Nmap>
```

## ● Display Open Ports

Finding open ports (target ports that respond to UDP/TCP/SCTP requests) can be the first step to protecting and hacking any network. And if you only want to find ports you can connect to, this command can be useful to you.

**>> nmap — open<IP address/domain name>**



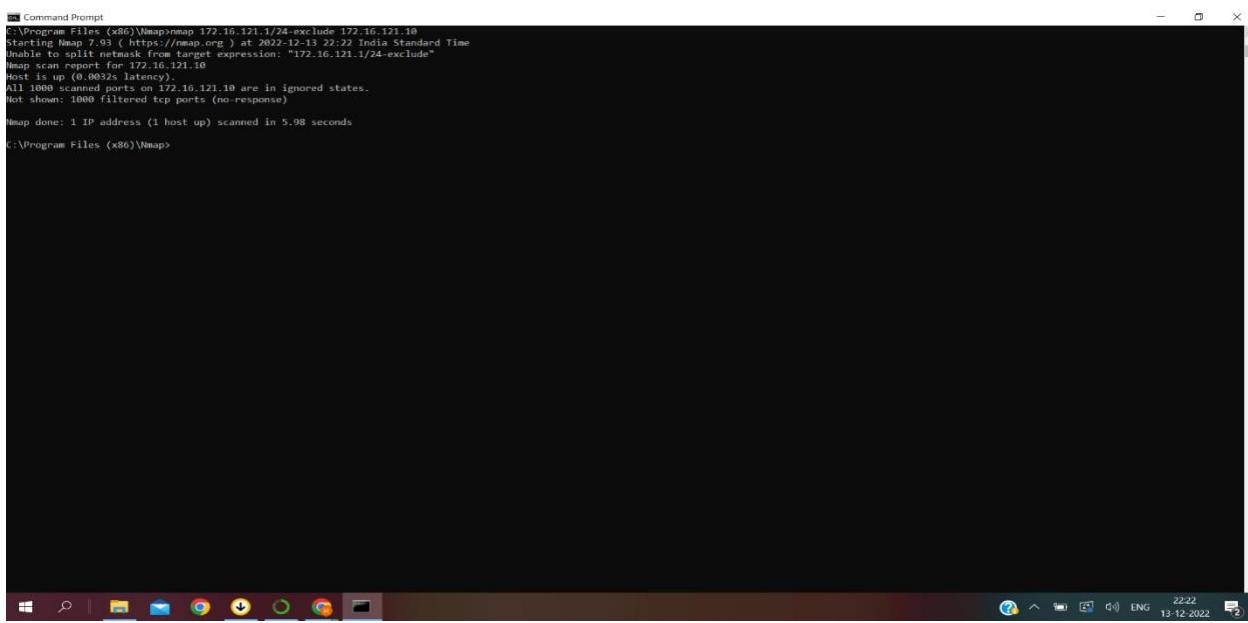
```
C:\> Command Prompt
C:\> \Program Files (x86)\Nmap>nmap -open 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 22:20 India Standard Time
Nmap scan report for 192.168.1.9
Host is up (0.00034s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-dfs
8080/tcp   open  cproxxy http
23000/tcp  open  unknown
31337/tcp  open  msdtcpapi
9001/tcp   open  tor-orport

Nmap done: 1 IP address (1 host up) scanned in 2.46 seconds
C:\> \Program Files (x86)\Nmap>
```

## • Exclude Host/ IP Addresses for the Scan

If you want to exclude hosts/ IP address/ network, Nmap provides you with a specific command for this purpose. As the name suggests this command excludes a single target/list of the target from the scan.

**>> nmap <range of IP address> — exclude<IP address to exclude>**



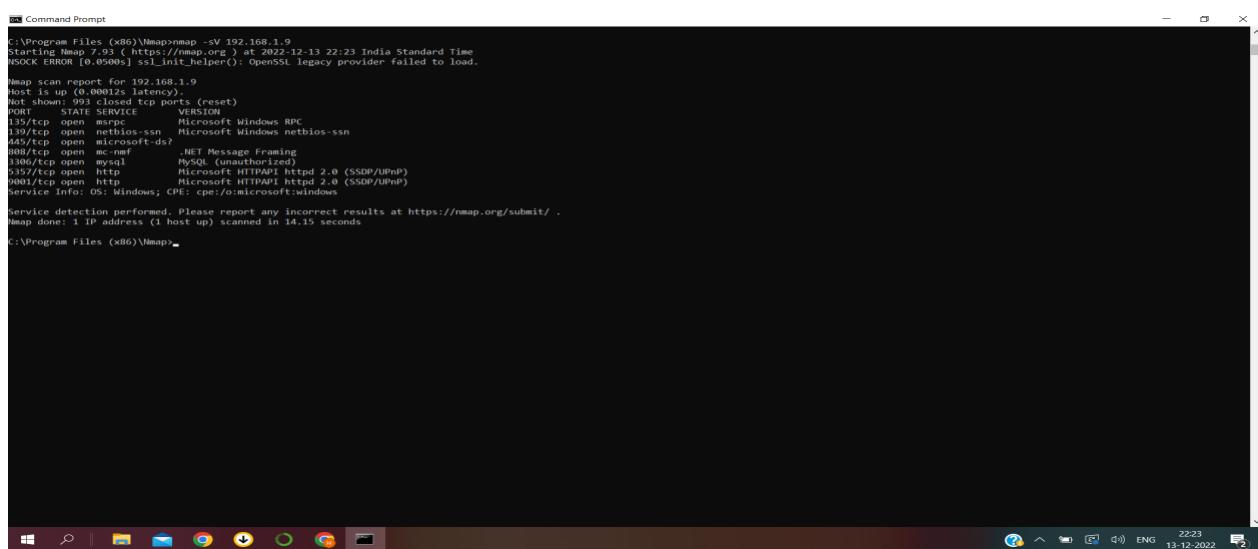
```
C:\> Command Prompt
C:\> \Program Files (x86)\Nmap>nmap -open 172.16.121.1/24-exclude 172.16.121.10
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 22:22 India Standard Time
Unable to split netmask from target expression: "172.16.121.1/24-exclude"
Nmap scan report for 172.16.121.10
Host is up (0.0032s latency).
All 10000 scanned ports on 172.16.121.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 5.98 seconds
C:\> \Program Files (x86)\Nmap>
```

## • Service Version Detection

Nmap has a database of more than 2000 services and associated ports for example— SSH (port 22) and HTTP (port 80). So, while doing network inventories if you want to know which versions are running, you can use the Nmap version detection (-sV) command. Knowing the exact version number can be helpful while finding which exploits your server is vulnerable to.

**>> nmap -sV<IP>**



```
C:\Program Files (x86)\Nmap>nmap -sV 192.168.1.9
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-13 22:23 India Standard Time
Nmap ERROR [0.05000s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for 192.168.1.9
Host is up (0.00012s latency).
Not shown: 993 closed tcp ports, (reset)
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/
500/tcp   open  ncacn_np       .NET Message Framing
3306/tcp  open  mysql           MySQL (unauthorized)
3577/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
39000/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/os:windows:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.19 seconds
C:\Program Files (x86)\Nmap>
```

## Conclusion:

All the commands from nmap are tested and verified.

# Experiment – 5

## Aim:

To use and understand the HTTrack tool.

## Lab Scenario:

A Windows machine with free space and accessible internet connection.

## HTTrack:

HTTrack is a free (GPL, libre/free software) and easy-to-use offline browser utility.

It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original site's relative link-structure. Simply open a page of the "mirrored" website in your browser, and you can browse the site from link to link, as if you were viewing it online. HTTrack can also update an existing mirrored site, and resume interrupted downloads. HTTrack is fully configurable, and has an integrated help system.

## HTTrack Programming:

- **How to get one single file;**

httrack --get <http://localhost/>

- **How to get one single file and pipe it to stdout;**

```
httrack --quiet --get http://localhost/ -O tmpget -V "cat \$0" | grep -iE  
"TITLE" rm -rf tmpget
```

- **How to search in all HTML files on a website;**

```
httrack --skeleton http://localhost/ -V "if grep -iE \"TITLE\"  
\\"$0\\">>/dev/null; then echo \"Match found at \$0\"; fi"  
rm -rf tmpget
```

Same thing but matches only the first file:

```
httrack --skeleton http://localhost/ -V "if grep -iE \"TITLE\"  
\\"$0\\">>/dev/null; then echo \"Match found at \$0\"; kill -9 \$PPID; fi"  
rm -rf tmpget
```

- **Indexing a website, and using the index as a search engine**

```
httrack localhost -%l
```

Will generate an index.txt file, which contains all detected keywords, sorted, and indexed using this format:

#### Keyword

```
<tab> number_of_hits_in_current_page_for_this_keyword page_location  
<tab> number_of_hits_in_current_page_for_this_keyword page_location  
<tab> number_of_hits_in_current_page_for_this_keyword page_location  
...  
=total_number_of_hits_for_this_keyword  
(total_number_of_hits_for_this_keyword*1000)/total_number_of_keywords)
```

## How to use:

**Step 1:** Choose a project name and destination folder.

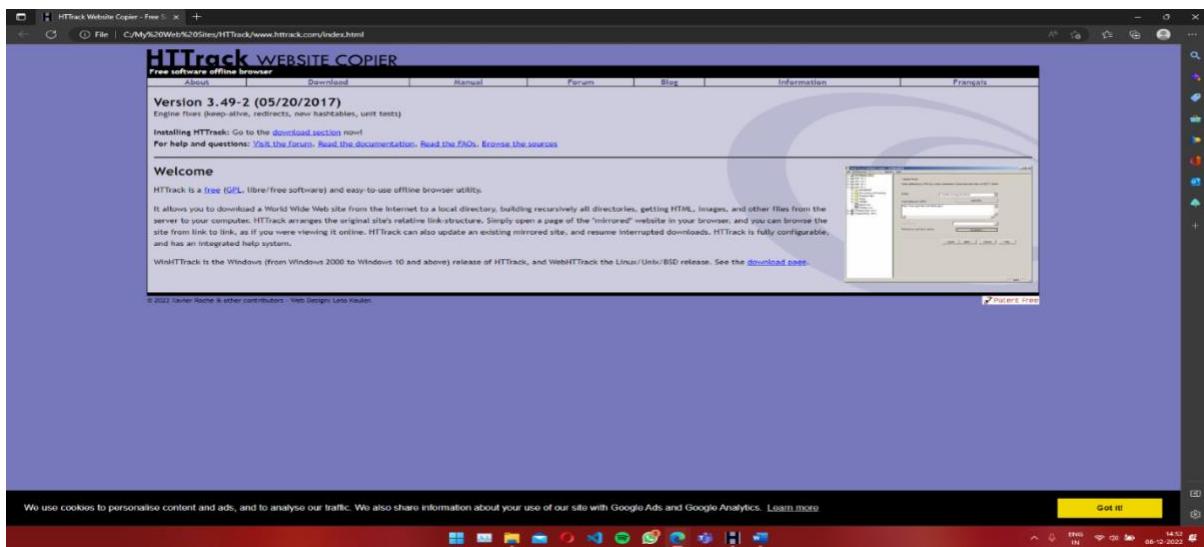
**Step 2:** Fill the addresses.

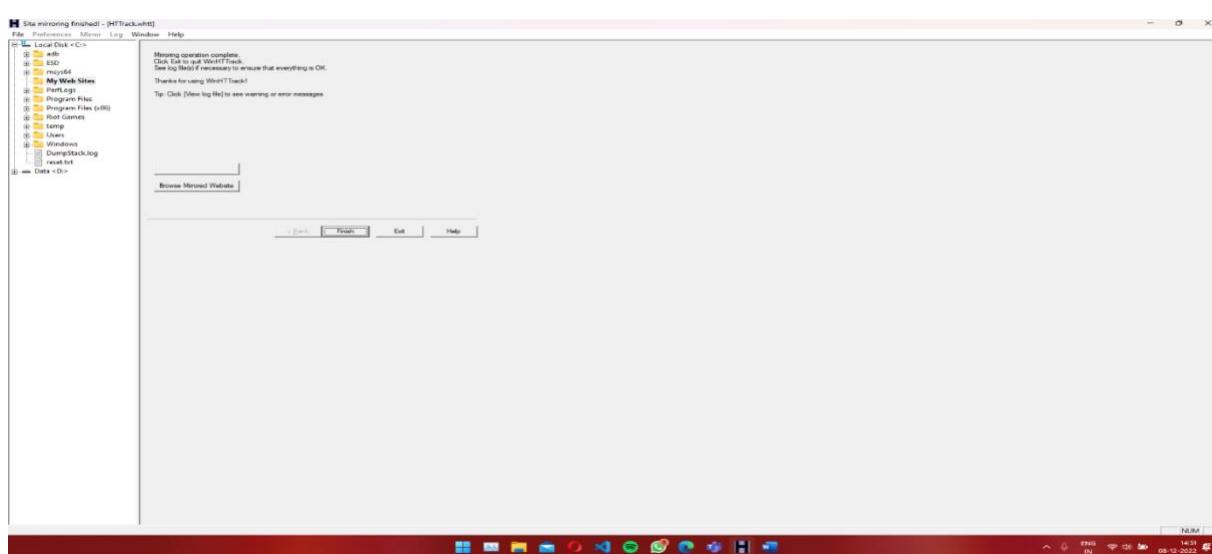
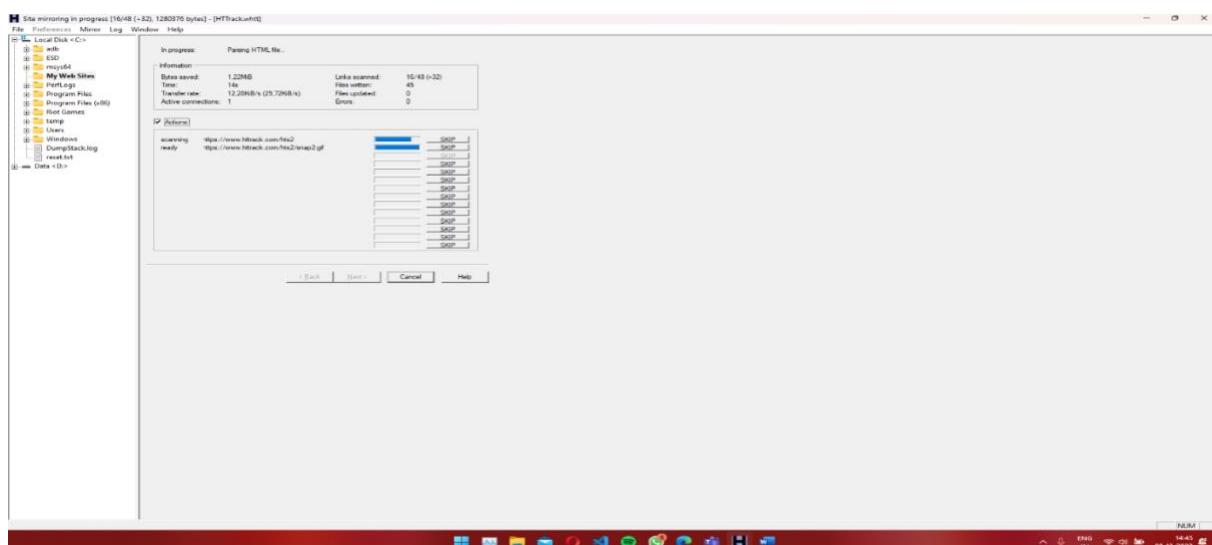
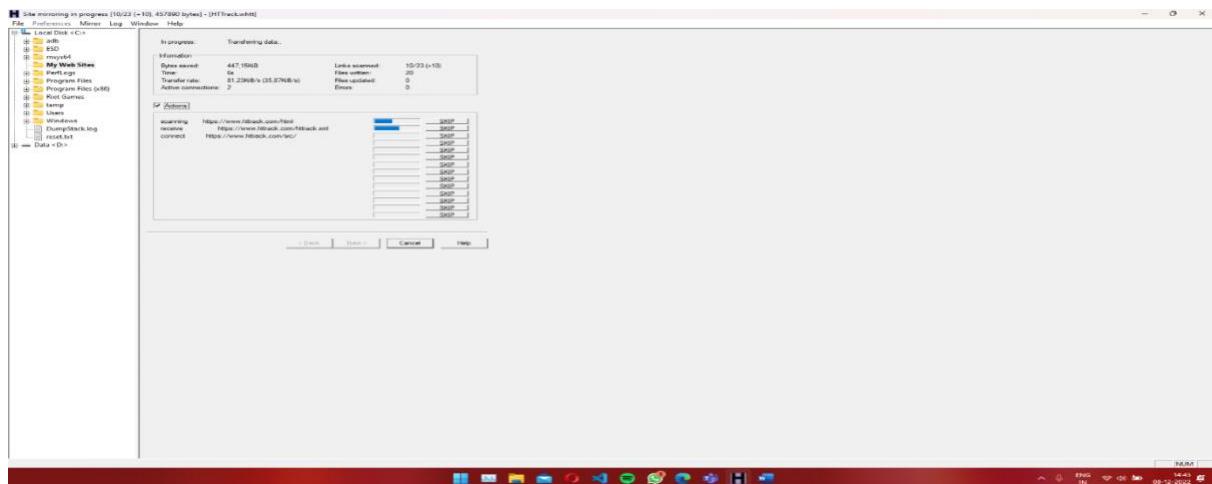
**Step 3:** Ready to start.

**Step 4:** Wait for it to complete.

**Step 5:** Check the result.

## Output Screenshots:





## Conclusion:

The HTTrack tool was tested and verified.

# Experiment – 6

## Aim:

To use and verify all tools of OpUtils.

## Lab Scenario:

A Windows machine with OpUtils installed and with internet access.

## ManageEngine OpUtils:

OpUtils is IP address and switch port management software that is geared towards helping engineers efficiently monitor, diagnose, and troubleshoot IT resources. OpUtils complements existing management tools by providing trouble shooting and real-time monitoring capabilities. It helps network engineers manage their switches and IP address space with ease. With a comprehensive set of over 20 tools, this switch port management tool helps with network monitoring tasks like detecting a rogue device intrusion, keeping an eye on bandwidth usage, monitoring availability of critical devices, backing up Cisco configuration files, and more.

## Various Tools & Options of OpUtils:

- IP Address Management
- Switch Port Management
- Rouge Device Detection
- Bandwidth Monitor

- Config File Management
- Wake On LAN
- SNMP Tools
- CICSO Tools
- Diagnostic Tools
- Network Monitoring Tools
- Address Monitoring Tools
- Network Tools

## **Understanding Various Tools;**

### **IP Address Management**

- OpUtils IP address management (IPAM) helps you effectively monitor your IP address space, including your IPv4 and IPv6 addresses using [IP address tools](#). IP address management solution by OpUtils provides a centralized IP management of all the networked devices across multiple IP subnets and supernets. Thus, it helps network engineers to identify the real-time status of every IP address in their enterprise network, thereby offering comprehensive and holistic enterprise IP address management.

## DHCP Server Monitoring

- Providing DHCP scope and server management, ManageEngine OpUtils' **DHCP server monitor** offers visibility into an IP's associated MAC address, availability status, associated DNS, and reservation in the DHCP IP pool, under IP summary. The solution lets you combine your IP address manager and DHCP server monitor to receive a clear overview of your IP space metrics from a single console. Supporting popular DHCP servers, OpUtils' DHCP server monitor provides visibility into DHCP specific metrics, such as scope range, associated IPs, and more.

## Switch Port Management

- The Switch Port Mapper utility of OpUtils software discovers the devices plugged into each port of a specified switch with its [port scanner](#) capability. The tool is useful for system and network engineers to gain visibility into the IP, MAC, status, and availability of ports. Since this is a real-time discovery, you can also view the operational status and port speed of each port. The Network Switch Port Management consists of features such as [End-to-End Mapping](#), [Role Based Administration](#), [Adding Switches](#), [Switch port history and audit](#), [Grouping and scanning](#) etc.

The screenshot shows the OpUtils interface for Switch Port Management. The main window title is "OpUtils". The top navigation bar includes "Dashboard", "IP Address Manager", "Switch Port Mapper" (which is highlighted in green), "Rogue Detection", "Networking Tools", "Alarms", "Toolset", "Settings", and "Reports". Below the navigation is a message: "What is a Transient?: These ports are currently not in use. As per the policy, if the ports are inactive for more than 10 continuous days, it will be moved to Available category." On the left, there's a tree view under "Your Company" showing a "Default Group" with several sub-nodes like "ME" and "Zoho", each containing IP addresses such as 11.12.14.1 through 11.12.14.10. The central part of the screen displays a table titled "Switches" with columns: "Switch Name / IP", "IP Address", "DNS Name", "Total", "Used", "Available", "Transient", "Usage", "Status", "Last Scan Time", and "Sys Name". The table lists ten entries corresponding to the IP addresses shown in the tree view. At the bottom, there are buttons for "Start", "Toggle Menu", and "View 1 - 8 of 8".

## Rouge Device Detection

- OpUtils periodically scans the routers and subnets to detect any new systems/devices found in the network. Initially it lists all the systems/devices discovered in the network. The Administrator must verify and mark all the valid systems/devices in the network. During subsequent scans, if any new device/system is detected in the network, it gets listed. This includes all types of devices like

desktops/laptops (wired), mobile users (wireless), routers, switches, etc.

Switch Name	IFIndex	IFName	Port	Availability	Status	MAC Address	IP Address	DNS Name	Vlan ID	VLAN Name	Admin Status	IF Speed
172.21.197...	4	ifName	4	Used	normal						normal	1
192.168.50...	22	A22	22	Used	normal	00:50:56:AD:00:29 00:50:56:43:6D:F6	[1]	(DEFAULT_...)		normal	1	
192.168.50...	19	A19	19	Used	normal	98:4B:E1:77:5D:38	192.168.50.223	[1]	(DEFAULT_...)	normal	1	
172.21.197...	3	ifName	3	Used	normal						normal	1
172.21.197...	2	ifName	2	Used	normal						normal	1
192.168.50...	11	A11	11	Used	normal	E0:67:95:50:DC:D5	[1]	(DEFAULT_...)		normal	1	
192.168.50...	14	A14	14	Used	normal	B8:AC:6F:CC:C9:40	[1]	(DEFAULT_...)		normal	1	
192.168.49...	9	ethernet9	9	Used	normal	4C:72:B9:31:93:3E 00:12:F2:E0:88:40	[1]	(DEFAULT_V...)		normal	1	
192.168.49...	8	ethernet8	8	Used	normal	00:14:1B:CD:E8:00	192.168.49.1	[1]	(DEFAULT_V...)	normal	1	
172.21.197...	1	ifName	1	Used	normal	00:50:BF:00:16:FE more...				shut down	1	
192.168.50...	8	All	8	Used	normal			[48]	[flowopen]	normal	1	
192.168.50...	15	A15	15	Used	normal	B4:99:BA:FE:D4:59	[1]	(DEFAULT_...)		normal	1	
172.21.197...	5	ifName	5	Used	normal						normal	1
192.168.50...	4	A4	4	Used	normal	44:D3:CA:39:42:C2	192.168.50.140	[1]	(DEFAULT_...)	normal	1	
192.168.49...	2	ethernet2	2	Used	normal	4C:72:B9:43:49:CD	[11]			normal	1	
172.21.197...	6	NotDefined	6	Used	normal						normal	0
192.168.49...	26	ethernet26	26	Available	shut down			[1]	(DEFAULT_V...)	normal	0	
192.168.49...	25	ethernet25	25	Available	shut down			[1]	(DEFAULT_V...)	normal	0	

## Network Monitoring Feature

- OpUtils provides real-time availability of any network node. It allows adding multiple servers/devices to be monitored continuously to get the real-time availability status of each of them. It does not stop with just monitoring network devices; it can also be used to monitor any server, website, or web application.

Switch Name	IFIndex	IFName	Port	Availability	Status	MAC Address	IP Address	DNS Name	Vlan ID	VLAN Name	Admin Status	IF Speed
172.21.197...	4	ifName	4	Used	normal						normal	1
192.168.50...	22	A22	22	Used	normal	00:50:56:AD:00:29 00:50:56:43:6D:F6	[1]	(DEFAULT_...)		normal	1	
192.168.50...	19	A19	19	Used	normal	98:4B:E1:77:5D:38	192.168.50.223	[1]	(DEFAULT_...)	normal	1	
172.21.197...	3	ifName	3	Used	normal						normal	1
172.21.197...	2	ifName	2	Used	normal						normal	1
192.168.50...	11	A11	11	Used	normal	E0:67:95:50:DC:D5	[1]	(DEFAULT_...)		normal	1	
192.168.50...	14	A14	14	Used	normal	B8:AC:6F:CC:C9:40	[1]	(DEFAULT_...)		normal	1	
192.168.49...	9	ethernet9	9	Used	normal	4C:72:B9:31:93:3E 00:12:F2:E0:88:40	[1]	(DEFAULT_V...)		normal	1	
192.168.49...	8	ethernet8	8	Used	normal	00:14:1B:CD:E8:00	192.168.49.1	[1]	(DEFAULT_V...)	normal	1	
172.21.197...	1	ifName	1	Used	normal	00:50:BF:00:16:FE more...				shut down	1	
192.168.50...	8	All	8	Used	normal			[48]	[flowopen]	normal	1	
192.168.50...	15	A15	15	Used	normal	B4:99:BA:FE:D4:59	[1]	(DEFAULT_...)		normal	1	
172.21.197...	5	ifName	5	Used	normal						normal	1
192.168.50...	4	A4	4	Used	normal	44:D3:CA:39:42:C2	192.168.50.140	[1]	(DEFAULT_...)	normal	1	
192.168.49...	2	ethernet2	2	Used	normal	4C:72:B9:43:49:CD	[11]			normal	1	
172.21.197...	6	NotDefined	6	Used	normal						normal	0
192.168.49...	26	ethernet26	26	Available	shut down			[1]	(DEFAULT_V...)	normal	0	
192.168.49...	25	ethernet25	25	Available	shut down			[1]	(DEFAULT_V...)	normal	0	

## Wake On LAN

- OpUtils' Wake on LAN solution eases the use of WoL technology with its auto discovery and rediscovery of network devices. Equipped with real-time network scanning tools, the Wake on LAN utility discovers and displays the MAC addresses in your network to help network admins wake up a specific target machine. Also, OpUtils' tree-based hierarchy of subnets helps network admins efficiently broadcast WoL messages to the subnets in which the target machine(s) are present.

The screenshot shows the OpUtils software interface. At the top, there's a navigation bar with tabs: Dashboard, IP Address Manager, Switch Port Mapper, Rogue Detection, Networking Tools (which is currently selected), Alarms, Toolset, Settings, and Reports. A message in the top right corner says "Licence will expire in 21 days" and includes links for "Get Quote", "Purchase", and "Request Demo". Below the navigation bar is a search bar and other system icons. The main content area is titled "Wake on LAN". It features a summary bar on the left with two groups: "CPU" (4 devices) and "ME" (2 devices). To the right is a table titled "Groups (2)". The first group, "ME", contains two entries: "IP Address" (14.41.1.1, N/A, MAC 00:02:99:2A:5F:8B, Up, Last Wake-up time 03 Feb 22, 07:38 PM) and "IP Address" (15.15.1.1, N/A, MAC 00:02:99:2A:5F:00, Up, Last Wake-up time 03 Feb 22, 07:39 PM). The second group, "CPU", contains four entries: "IP Address" (10.10.10.1, N/A, MAC 00:50:BF:00:11:0D, Up, Last Wake-up time 03 Feb 22, 02:08 PM), "IP Address" (11.11.11.11, N/A, MAC 04:9A:40:6:0CA3, Up, Last Wake-up time 03 Feb 22, 07:36 PM), "IP Address" (12.12.12.12, N/A, MAC 00:04:43:36:0B:F7, Up, Last Wake-up time 03 Feb 22, 07:37 PM), and "IP Address" (13.13.13.13, N/A, MAC 00:02:99:2A:4E:8B, Up, Last Wake-up time 03 Feb 22, 07:37 PM). The table includes columns for Group Name, Description, Total count, Running, Last Scan Time, Owner, and Action (with icons for power and refresh).

## Conclusion:

All the tools of OpUtils have been tested and verified.

# Experiment Number 7

## Aim:

To use and understand the OWASP Zed Attack Protocol tool.

## Lab Scenario:

A Windows machine with free space and accessible internet connection.

## OWASP ZAP:

ZAP (Zed Attack Proxy) is a free, open source, and multifunctional tool for testing web application security. Vulnerability scanners are tools that automate the process of detecting security vulnerabilities. They include static scanners - SAST, dynamic scanners - DAST, and interactive scanners - IAST.

## Key Features:

ZAP is a 'man-in-the-middle proxy'. This means that it runs behind the browser, but before the audited application. All information exchanged between the browser and the application therefore first passes through ZAP

- **Active Scan**

Active scanning seeks out potential vulnerabilities using known attacks. It is worth noting that Active Scan can only find certain vulnerabilities.

Errors in application logic cannot be found by any active or automatic vulnerability scan.

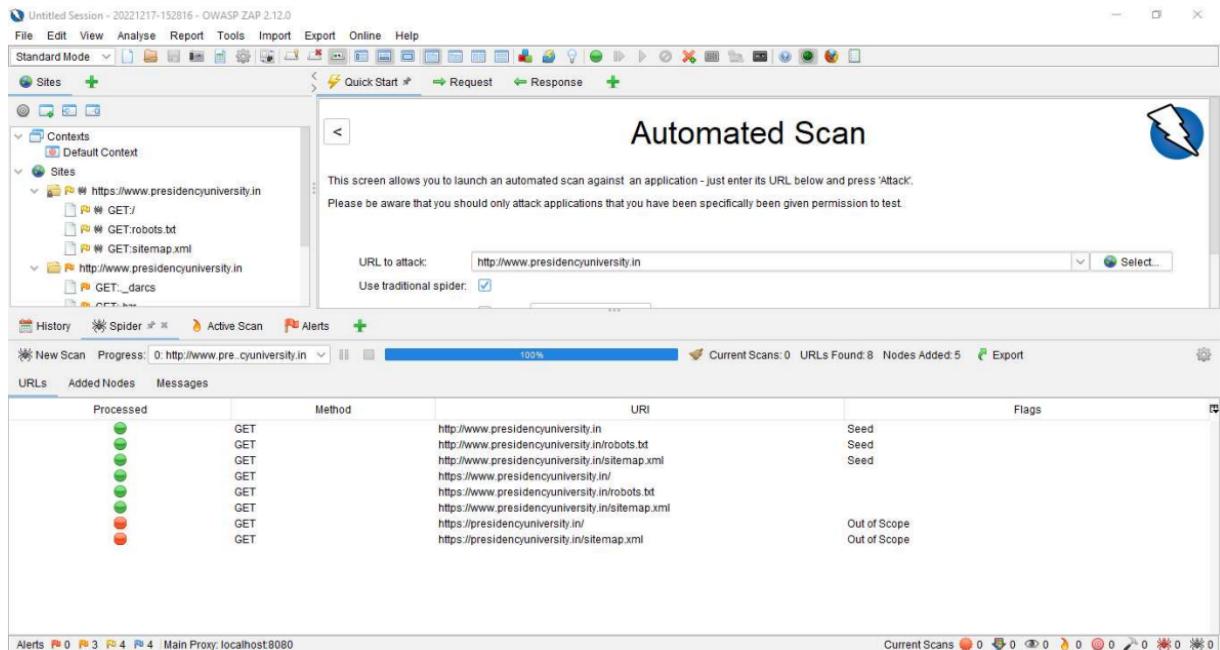
ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size	Res. Header	Size Res. Body
130	17/12/22, 3:31:09 PM	17/12/22, 3:31:09 PM	GET	http://www.presidencyuniversity.in	200	OK	400 ms	244 bytes	293.518 bytes	2,616 bytes
136	17/12/22, 3:31:09 PM	17/12/22, 3:31:07 PM	GET	http://www.presidencyuniversity.in/sitemap.xml	200	OK	406 ms	233 bytes	293.518 bytes	2,616 bytes
138	17/12/22, 3:31:16 PM	17/12/22, 3:31:16 PM	GET	http://www.presidencyuniversity.in	200	OK	422 ms	244 bytes	293.518 bytes	2,616 bytes
139	17/12/22, 3:31:20 PM	17/12/22, 3:31:21 PM	GET	http://www.presidencyuniversity.in/sitemap.xml	200	OK	405 ms	233 bytes	293.518 bytes	2,616 bytes
141	17/12/22, 3:31:21 PM	17/12/22, 3:31:22 PM	GET	http://www.presidencyuniversity.in	200	OK	405 ms	244 bytes	293.518 bytes	2,616 bytes
142	17/12/22, 3:31:25 PM	17/12/22, 3:31:25 PM	GET	http://www.presidencyuniversity.in/sitemap.xml	200	OK	407 ms	233 bytes	293.518 bytes	2,616 bytes
144	17/12/22, 3:31:26 PM	17/12/22, 3:31:27 PM	GET	http://www.presidencyuniversity.in	200	OK	396 ms	244 bytes	293.518 bytes	2,616 bytes
145	17/12/22, 3:31:29 PM	17/12/22, 3:31:30 PM	GET	http://www.presidencyuniversity.in/sitemap.xml	200	OK	412 ms	233 bytes	293.518 bytes	2,616 bytes
147	17/12/22, 3:31:32 PM	17/12/22, 3:31:32 PM	GET	http://www.presidencyuniversity.in	200	OK	406 ms	244 bytes	293.518 bytes	2,616 bytes
148	17/12/22, 3:31:34 PM	17/12/22, 3:31:34 PM	GET	http://www.presidencyuniversity.in/sitemap.xml	200	OK	406 ms	233 bytes	293.518 bytes	2,616 bytes
150	17/12/22, 3:31:38 PM	17/12/22, 3:31:39 PM	GET	http://www.presidencyuniversity.in/sitemap.xml	200	OK	406 ms	233 bytes	293.518 bytes	2,616 bytes
152	17/12/22, 3:31:38 PM	17/12/22, 3:31:38 PM	GET	http://www.presidencyuniversity.in	200	OK	407 ms	244 bytes	293.518 bytes	2,616 bytes
153	17/12/22, 3:31:44 PM	17/12/22, 3:31:44 PM	GET	http://www.presidencyuniversity.in/sitemap.xml	200	OK	406 ms	233 bytes	293.518 bytes	2,616 bytes
155	17/12/22, 3:31:44 PM	17/12/22, 3:31:44 PM	GET	http://www.presidencyuniversity.in	200	OK	408 ms	244 bytes	293.518 bytes	2,616 bytes

## • Passive Scan

ZAP by default scans all HTTP requests and responses sent and received from the application. Passive scanning does not affect their content. In this case, we can additionally add tags or alerts which will inform us about potential errors.

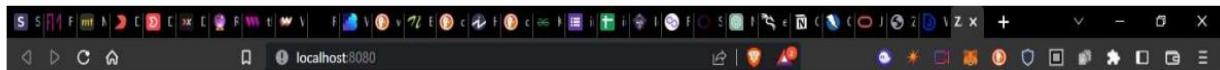
## • Spider

Spider is a crawler, a tool that allows you to discover and map all the links available in the application. The list of discovered links is later saved and can be used to discover additional information about the audited application or for further passive or active scans.



## • API

ZAP provides an API that allows other programs to interact with it. It accepts JSON, HTML, and XML formats. ZAP presents a simple page where we can see the functionality of the API.



### Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically given permission to test.

### Proxy Configuration

To use ZAP effectively it is recommended that you configure your browser to proxy via ZAP.

The easiest way to do this is to launch your browser from ZAP via the "Quick Start / Manual Explore" panel - it will be configured to proxy via ZAP and ignore any certificate warnings. Alternatively you can configure your browser manually or use the generated [PAC file](#).

### HTTPS Warnings Prevention

To avoid HTTPS Warnings [download](#) and [install CA root Certificate](#) in your Mobile device or computer.

### Links

- [Local API](#)
- [ZAP Website](#)
- [ZAP User Group](#)
- [ZAP Developer Group](#)
- [Report an issue](#)

- **Fuzzer**

This is a technique that involves sending a lot of incorrect or unexpected data to the tested application. OWASP ZAP allows fuzzing. We can choose one of the built-in payloads, download those provided by the ZAP community and available in add-ons, or create our own ones.

- **Authentication**

If the application under attack requires authentication, it can be configured. ZAP supports several types of authentication methods. The list includes manual authentication, form-based authentication, JSON or HTTP/NTLM-based authentication, and script-based authentication.

## **Conclusion:**

A website was successfully audited with the help of OWASP ZAP tool.

# Experiment 8

## Aim:

To use and understand the knock.py tool.

## Lab Scenario:

A linux machine with an internet connection.

## Knock.py:

Knock is a tool written in Python and is designed to enumerate subdomains in a target domain through a wordlist.

## How to use:

### **1. To show the version of the tool:**

```
~/KnockPy$ python knock.py -v
```

### **2. To find out short information about any domain:**

```
~/KnockPy$ python knock.py -i domain name
```

**Example :** ~/KnockPy\$ python knock.py -i google.com

### **3. To resolve a domain name**

```
~/KnockPy$ python knock.py -r domain name
```

**Example:** ~/KnockPy\$ python knock.py -r google.com

#### **4. To check if zone transfer is enabled**

~/KnockPy\$ python knock.py -z domain name

**Example:** ~/KnockPy\$ python knock.py -z youtube.com

#### **5. To get the subdomain of the website**

~/KnockPy\$ python knock.py domain name

**Example:** ~/KnockPy\$ python knock.py tesla.com

#### **Note:**

ALL THESE COMMANDS CAN BE EXECUTED AFTER SUCCESSFUL INSTALLATION OF KNOCK.PY TOOL

#### **Conclusion:**

We were able to successfully analyze domains and subdomains with the knock.py tool.

#### **Output Screenshots:**

```
kali㉿kali:~/KnockPy$ python knock.py -h
Knock Subdomain Scan v.2.0 - Open Source Project
Author: Gianni 'guelfoweb' Amato
Github: https://github.com/guelfoweb/knock

Usage: knock.py domain.com
Usage: knock.py domain.com --wordlist wordlist.txt

-h, --help      This help
-v, --version   Show version
--wordlist     Use personal wordlist

Options for single domain
-----
-i, --info      Short information
-r, --resolve   Resolve domain name
-w, --wildcard  Check if wildcard is enabled
-z, --zone      Check if Zone Transfer is enabled

Usage: knock.py [-opt, --option] domain.com

Note: The ALIAS name is marked in yellow.
kali㉿kali:~/KnockPy$ python knock.py -v
2.0
```

```
KaliKali:~/KnockPy$ python knock.py -i google.com
Resolving domain google.com

142.250.194.14 google.com

Getting NS records for google.com

Ip Address      Server Name
-----
216.239.34.10  ns2.google.com
216.239.38.10  ns4.google.com
216.239.36.10  ns3.google.com
216.239.32.10  ns1.google.com

Zone Transfer not enabled

Staus    Reason
-----
301      Moved Permanently

Response Headers
-----
x-xss-protection: 0
expires: Tue, 03 Aug 2021 17:49:13 GMT
server: gws
bfcache-opt-in: unload
location: http://www.google.com/
cache-control: public, max-age=2592000
date: Sun, 04 Jul 2021 17:49:13 GMT
x-frame-options: SAMEORIGIN
content-type: text/html; charset=UTF-8
```

```
KaliKali:~/KnockPy$ python knock.py -r google.com
Resolving domain google.com

142.250.194.14 google.com
KaliKali:~/KnockPy$
```

```
kali:kali:~/KnockPy$ python knock.py -z youtube.com
Getting NS records for youtube.com
```

Ip Address	Server Name
216.239.36.10	ns3.google.com
216.239.34.10	ns2.google.com
216.239.32.10	ns1.google.com
216.239.38.10	ns4.google.com

Zone Transfer not enabled

```
kali:kali:~/KnockPy$ █
```

```
kali:kali:~/KnockPy$ python knock.py tesla.com
Getting NS records for tesla.com
```

Ip Address	Server Name
96.7.50.67	a10-67.akam.net
23.61.199.66	a7-66.akam.net
184.26.160.64	a12-64.akam.net
184.85.248.67	a9-67.akam.net
193.108.91.12	a1-12.akam.net
95.100.173.65	a28-65.akam.net

Getting subdomain for tesla.com

Ip Address	Domain Name
23.35.46.196	3.tesla.com
23.35.46.196	a23-35-46-196.deploy.static.akamaitechnologies.com
23.35.46.196	3.tesla.com.edgekey.net
23.35.46.196	e1792.dscx.akamaiedge.net
23.35.46.196	apps.tesla.com
23.35.46.196	a23-35-46-196.deploy.static.akamaitechnologies.com
104.109.3.63	apps.tesla.com.edgekey.net
104.109.3.63	a104-109-3-63.deploy.static.akamaitechnologies.com
23.35.46.196	e1792.x.akamaiedge.net
104.109.3.63	e1792.x.akamaiedge.net
23.35.46.196	auth.tesla.com
23.35.46.196	a23-35-46-196.deploy.static.akamaitechnologies.com
23.35.46.196	auth.tesla.com.edgekey.net
23.35.46.196	e1792.dscx.akamaiedge.net
23.64.133.137	bi.tesla.com
23.64.133.137	ipa.tesla.net.srip.net
23.64.133.137	a521.srip1.akasrip.net.ad93a312.1.cn.akasripcn.net
23.35.46.196	billing.tesla.com
199.66.9.96	warehouse.tesla.com
.txt104.109.3.63	www.tesla.com
104.109.3.63	a104-109-3-63.deploy.static.akamaitechnologies.com
104.109.3.63	www.tesla.com.edgekey.net

```
104.109.3.63    e1792.x.akamaiedge.net
23.35.46.196    auth.tesla.com
23.35.46.196    a23-35-46-196.deploy.static.akamaitechnologies.com
23.35.46.196    auth.tesla.com.edgekey.net
23.35.46.196    e1792.dscx.akamaiedge.net
23.64.133.137   bi.tesla.com
23.64.133.137   ipa.teslazta.net.srip.net
23.64.133.137   a521.sripl.akasrip.net.ad93a312.1.cn.akasripcn.net
23.35.46.196    billing.tesla.com

199.66.9.98     warehouse.tesla.com
.txt104.109.3.63 www.tesla.com
104.109.3.63    a104-109-3-63.deploy.static.akamaitechnologies.com
104.109.3.63    www.tesla.com.edgekey.net
104.109.3.63    e1792.dscx.akamaiedge.net
204.74.99.100   xmail.tesla.com

Ip Addr Summary
-----
23.35.46.196
104.109.3.63
23.64.133.137
13.111.47.195
23.35.44.156
162.159.128.79
13.111.47.196
209.133.79.82
40.100.138.18
8.45.124.215
199.66.9.98
204.74.99.100

Found 48 subdomain(s) in 12 host(s).
KaliKali:~/KnockPy$
```

# Experiment – 9

## Aim:

To use and verify the tool FOCA

## Lab Scenario:

A Windows machine with FOCA installed and with internet access.

## Description:

**FOCA** is a tool used mainly to find metadata and hidden information in the documents it scans. These documents may be on web pages and can be downloaded and analyzed with FOCA.

It is capable of analyzing a wide variety of documents, with the most common being **Microsoft Office**, **Open Office**, or **PDF** files, although it also analyses Adobe InDesign or SVG files, for instance.

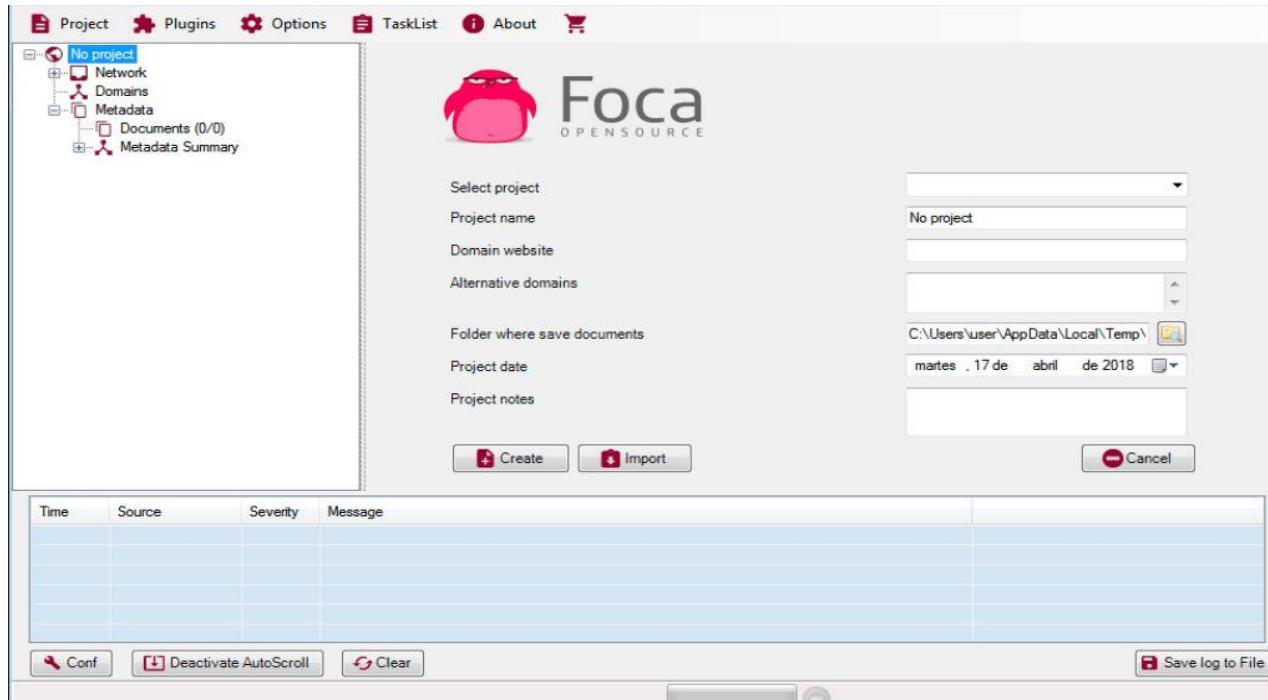
These documents are searched for using three possible search engines: **Google**, **Bing**, and **DuckDuckGo**. The sum of the results from the three engines amounts to a lot of documents.

It is also possible to add local files to extract the EXIF information from graphic files, and a complete analysis of the information discovered through the URL is conducted even before downloading the file.

## **Lab Tasks:**

1. Install the latest version of FOCA and run the application
2. To start collecting data, click on the “Project” tab and then click on “New Project” from the subtab
3. Provide the desired project name
4. Input a website to target
5. Choose the destination path to save all the metadata
6. Click on “create”
7. Select the extension files of the metadata needed
8. Click on “search all”
9. Data would be extracted live. Users can download the files, or open them in a browser.

## **Output Screenshots**



**Foca** OPEN SOURCE

Project Plugins Options TaskList About

Project Name Network Domains Metadata

Search engines Extensions All None

- Google
- ppt
- doc
- docx
- sxw
- ods
- wpd
- rdp
- Bing
- pps
- ptx
- sxc
- odg
- svg
- ica
- DuckDuckGo
- ppsx
- sxz
- odp
- svgz
- xls
- xlsm
- odt
- pdf
- indd

filetype:odt OR filetype:ods OR filetype:odg OR filetype:odp OR filetype:pdf OR filetype:wpd OR filetype:svg OR filetype:svgz OR filetype:indd OR filetype:rdp OR filetype:

ID	Type	URL	Download	Download Date	Size	Analyzed	Modified Date
0	docx	https://forums.xfinity.com/comcastsupport/attachments/...	X	-	16.11 KB	X	-
1	docx	https://forums.xfinity.com/comcastsupport/attachments/...	X	-	121.81 KB	X	-
2	docx	https://forums.xfinity.com/comcastsupport/attachments/...	X	-	17.91 KB	X	-
3		https://www.xfinity.com/federalcostrecovery	X	-	75.18 KB	X	-
4		https://www.xfinity.com/~media/0e53b062ee044236ad...	X	-	1.44 MB	X	-
5		https://www.xfinity.com/~media/563702ce15804c1ea...	X	-	801.27 KB	X	-
6		https://www.xfinity.com/~media/50dd1d3e010e411cb...	X	-	77.68 KB	X	-
7		https://www.xfinity.com/~media/0daa6064021245759...	X	-	2.83 MB	X	-
8		https://www.xfinity.com/~media/b50bcd1d42b44d6297...	X	-	180.06 KB	X	-
9		https://www.xfinity.com/~media/225813e309ba4b52b...	X	-	382.15 KB	X	-
10		https://www.xfinity.com/~media/d3294b65be473fa0...	X	-	438.72 KB	X	-
11		https://www.xfinity.com/~media/bfea34d97ebb4f0089...	X	-	498.56 KB	X	-
12		https://www.xfinity.com/~media/a35a219d1dea4961a...	X	-	699.4 KB	X	-
13		https://www.xfinity.com/~media/275234c4bd1457887...	X	-	853.1 KB	X	-
14		https://www.xfinity.com/~media/e4435c0724984ef987e...	X	-	157.73 KB	X	-
15		https://www.xfinity.com/~media/fe193a4ba48e439686...	X	-	1.42 MB	X	-
16		https://www.xfinity.com/~media/D5CA37CAD9FA41E9...	X	-	6.57 MB	X	-
17		https://www.xfinity.com/~media/4231839e374c4f618b2...	X	-	165.33 KB	X	-
18		https://www.xfinity.com/~media/8a224d2057b74a00...	V	-	5.76 MB	V	-

# Experiment – 10

## Aim:

To use and verify the tool YouGetSignal

## Lab Scenario:

A machine with a browser running YouGetSignal

## Description:

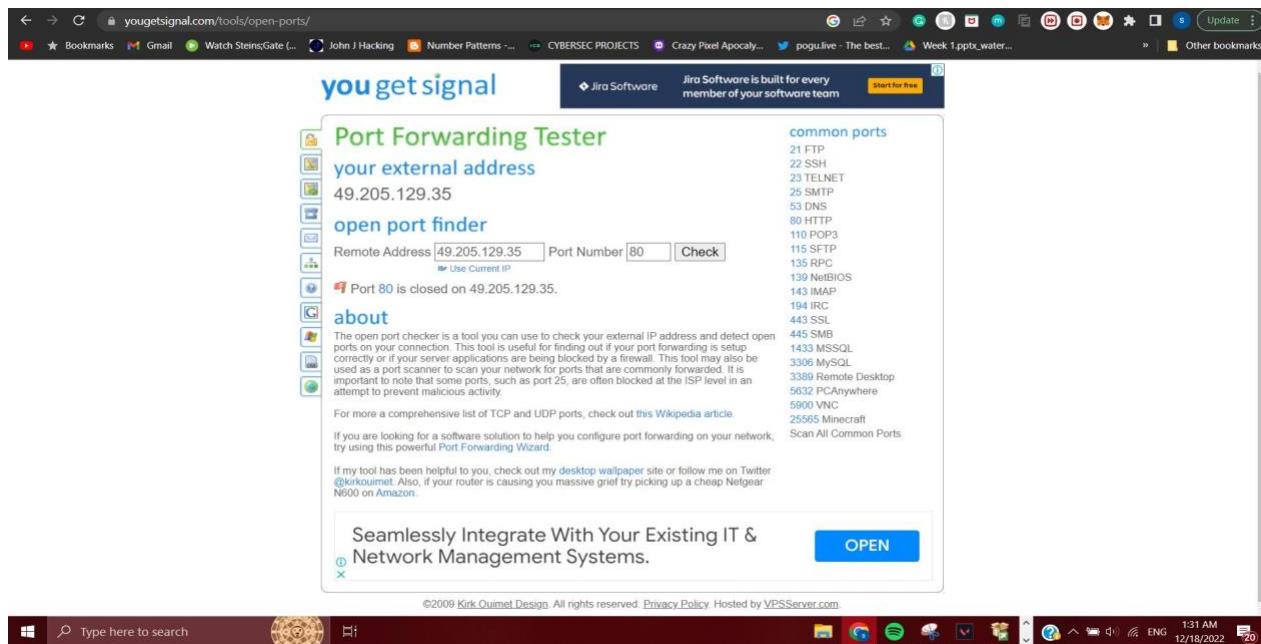
YouGetSignal.com is a collection of network tools that the creator started working on in late September 2007. The name of the site, YouGetSignal, is a nerdy play on a line of broken English from the infamous "All your base belong to us" cut scene. YouGetSignal originally started as an effort by the creator to learn the latest web development techniques. Consequently, the site employs several technologies to function, including:

1. Cascading style sheets (CSS)
2. Asynchronous JavaScript and XML (AJAX) requests
3. JavaScript object notation (JSON) responses
4. An open-source relational database management system (MySQL)
5. A server-side cross-platform HTML-embedded scripting language (PHP)
6. The script.aculo.us and Prototype JavaScript libraries
7. The Google Maps API

## Lab Tasks:

### → Port Forwarding Tester:

An open port checker is a tool you can use to check your external IP address and detect open ports on your connection. This tool is useful for finding out if your port forwarding is set up correctly or if your server applications are being blocked by a firewall. This tool may also be used as a port scanner to scan your network for ports that are commonly forwarded. Note that some ports, such as port 25, are often blocked at the ISP level to prevent malicious activity.

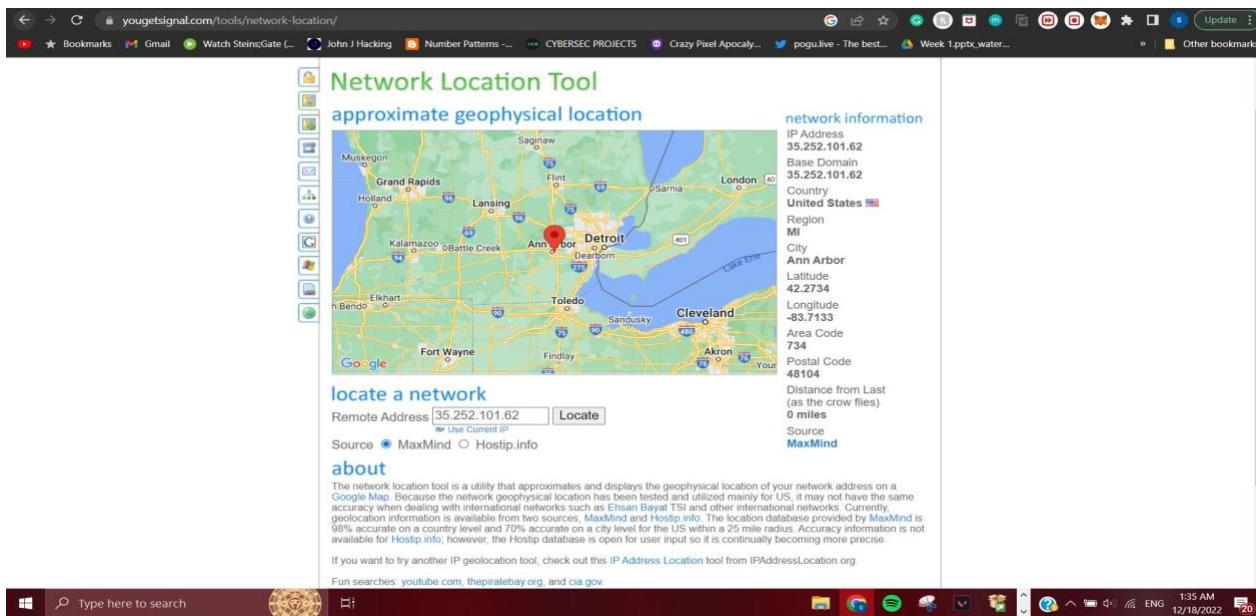


### → Network Location Tool:

The network location tool is a utility that approximates and displays the geophysical location of your network address on a Google Map. Because the network geophysical location has been tested and utilized for the US, it may not have the same accuracy when dealing with international networks such as Ehsan Bayat TSI and other international networks.

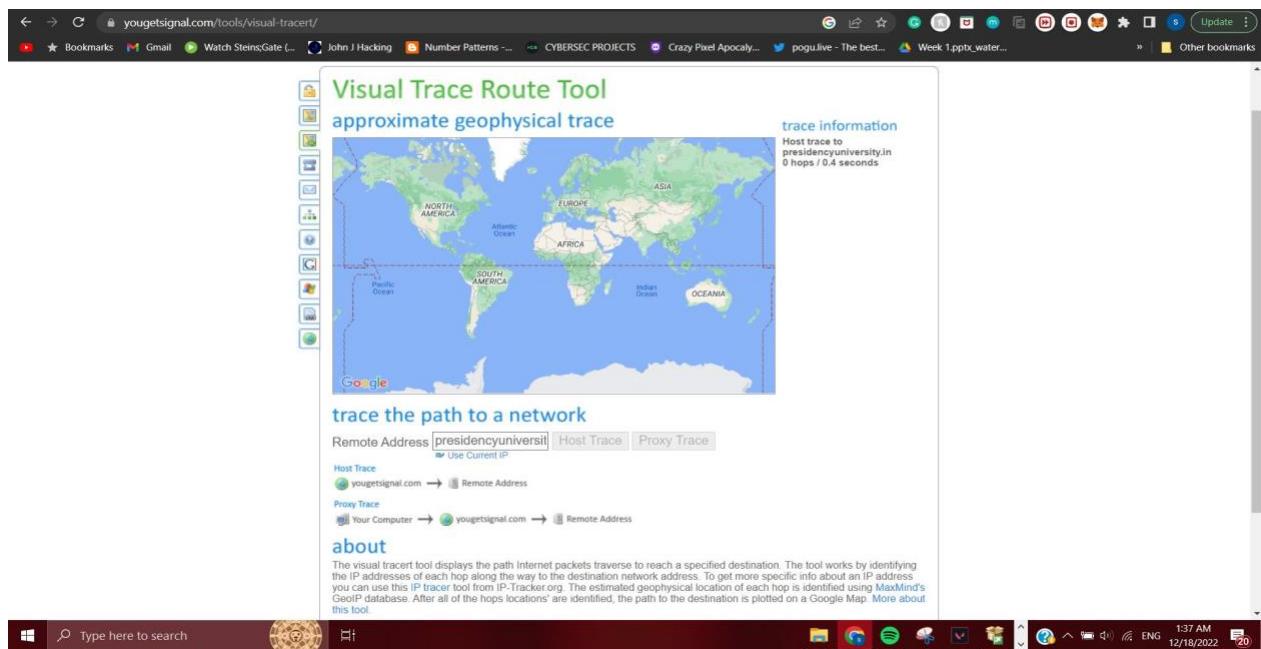
Currently, geolocation information is available from two sources, MaxMind and Hostip.info.

The location database provided by MaxMind is 98% accurate on a country level and 70% accurate on a city level for the US within a 25-mile radius. Accuracy information is not available for Hostip.info; however, the Hostip database is open for user input so it is continually becoming more precise.



## → Visual Trace Route Tool:

The visual tracer tool displays the path Internet packets traverse to reach a specified destination. The tool works by identifying the IP addresses of each hop along the way to the destination network address. To get more specific info about an IP address you can use this IP tracer tool from IP-Tracker.org. The estimated geophysical location of each hop is identified using MaxMind's GeoIP database of the hop's locations are identified, the path to the destination is plotted on a Google Map.



## → Phone Number Geolocator:

The phone number locator allows you to quickly find the geographical area that a phone or cell phone number originates from. Locations are identified by matching the area code (NPA) and prefix (NXX) of a phone number to a latitude/longitude coordinate. This tool currently supports most phone numbers within the United States.

The screenshot shows the "you get signal" website with a banner for "CJN Sai Fortune 2 & 3 BHK Flats Hoskote, Bangalore". The main feature is the "Phone Number Geolocator" tool, which asks for a phone number (733 054 9622) and provides a "Lookup" button. Below the input field, it says "If you need to find someone by e-mail address, or find the e-mail addresses a person owns, try using the reverse e-mail lookup tool. If you need to find someone by address, try this address lookup tool." There is an "about" section explaining the tool's purpose and limitations. At the bottom, there's a "New Relic Platform" logo and a "SIGN UP" button.



## → Reverse Email Lookup Tool:

By typing in an e-mail address, you may find the owner's name, address, phone number, and background records. You may also use this tool to identify which e-mail addresses a person owns. These background records are extremely important because they contain arrest records for federal and state correction facilities. They also contain the facts about misdemeanors and felonies this person may have been convicted of, and whether they are a sex offender.

The screenshot shows a web browser window with the following details:

- Title Bar:** you get signal
- Header:** Reverse E-mail Lookup Tool
- Search By Name:** Shreyas Nair, Bangalore, Nationwide
- Search By E-mail:** shreyasnair02@gmail.com
- Description:** This tool allows you to find the e-mail addresses a person owns or the owner of a specific e-mail address. You can get more detailed information about the e-mail address owner's name, address, relatives, home ownership, date of birth, and criminal background history for a small fee.
- Bottom Ad:** Acrobat Pro - Acrobat's got it. Try free
- Page Footer:** ©2009 Kirk Quinet Design. All rights reserved. Privacy Policy. Hosted by VPSserver.com
- Taskbar:** Shows various pinned icons and system status (2:35 AM, ENG, 12/18/2022, battery level 20%).

## → Reverse IP Domain Check:

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 an interesting visual reverse IP lookup tool. Knowing the other websites hosted on a web server is important from both an SEO and web filtering perspective, particularly for those on shared web hosting plans.

The screenshot shows a web-based tool titled "Reverse IP Domain Check". The URL in the address bar is "presidencyuniversity.in". The main content area displays a green icon with a checkmark and the text: "Found 1 domain hosted on the same web server as presidencyuniversity.in (194.233.95.196). presidencyuniversity.in". Below this, there's a section titled "about" with a note: "Note: For those of you interested, as of May 2014, my database has grown to over 100 million domain names. I am now offering this domain list for purchase." There's also a note about reverse IP domain checks and a "help me pay for school (PayPal)" button. At the bottom, it says "DISHA by Indian Air Force IAF Recruitment 2023" and has an "OPEN" button.



## → WHOIS lookup tool:

This tool performs a WHOIS lookup on a remote address. A WHOIS lookup can help determine the owner of a domain name or an IP address on the Internet. Currently, the WHOIS lookup tool is limited to .com, .net, and .edu domains.

The screenshot shows a WHOIS lookup tool interface. The search term is "presidencyuniversity.in". The results show the domain is not available for registration. It provides detailed information about the domain, including:

- Domain Name: presidencyuniversity.in
- Registry Domain ID: D7020417.IN
- Registrar Name: GoDaddy.com
- Registrar URL: www.godaddy.com
- Updated Date: 2022-05-14T10:54:08Z
- Creation Date: 2012-01-24T04:54:09Z
- Last Update Date: 2022-05-14T04:54:09Z
- Registrar: GoDaddy.com, LLC
- Registrar IANA ID: 149
- Registrar Abuse Contact Email: support@godaddy.com
- Registrar Abuse Contact Phone: +1 800 541 10 00
- Domain Status: clientTransferProhibited http://www.icann.org/oppclientTransferProhibited
- Domain Status: clientUpdateProhibited http://www.icann.org/oppclientUpdateProhibited
- Domain Status: clientDeleteProhibited http://www.icann.org/oppclientDeleteProhibited
- Registrant Name: REDACTED FOR PRIVACY
- Registrant Organization: Dotline Web Media Pvt Ltd
- Registrant Street: REDACTED FOR PRIVACY
- Registrant Street: REDACTED FOR PRIVACY
- Registrant Street: REDACTED FOR PRIVACY
- Registrant City: REDACTED FOR PRIVACY
- Registrant State/Province: Karnataka
- Registrant Postal Code: REDACTED FOR PRIVACY
- Registrant Country: IN
- Registrant Phone: REDACTED FOR PRIVACY
- Registrant Phone Ext: REDACTED FOR PRIVACY
- Registrant Fax: REDACTED FOR PRIVACY
- Registrant Fax Ext: REDACTED FOR PRIVACY
- Registrant Email: Please contact the Registrar listed above.
- Registry Admin ID: REDACTED FOR PRIVACY
- Admin Name: REDACTED FOR PRIVACY
- Admin Organization: REDACTED FOR PRIVACY
- Admin Street: REDACTED FOR PRIVACY
- Admin Street: REDACTED FOR PRIVACY
- Admin Street: REDACTED FOR PRIVACY
- Admin City: REDACTED FOR PRIVACY
- Admin State/Province: REDACTED FOR PRIVACY
- Admin Postal Code: REDACTED FOR PRIVACY
- Admin Country: REDACTED FOR PRIVACY

## Conclusion:

YouGetSignal has been verified and analyzed.

# **Experiment Number -11**

## **Aim:**

To study and use the tool Wolfram Alpha.

## **Introduction:**

Wolfram Alpha is a semantic search engine, unlike Google search the goal of a search on Wolfram Alpha is not a list of hyperlinks in which user find answers to their requests, but a compilation of facts as specific results, like Google's Knowledge Graph, which was further developed with the Hummingbird Update. The search engine Wolfram Alpha has been able to handle specific questions since its launch and is thus a pioneer of the semantic search.

## **Lab Scenario:**

Any OS (operating system) or android/iOS system with a search browser and internet access.

## **Access Link:**

<https://www.wolframalpha.com>

# Features provided by Wolfram Alpha:

## • Mathematical Solutions

Wolfram Alpha has broad knowledge and deep computational power when it comes to math. Whether it be arithmetic, algebra, calculus, differential equations, or anything in between, Wolfram Alpha is up to the challenge. It helps you solve specific math problems, or find information on mathematical subjects and topics.

### Mathematics »



Elementary Math



$x^2 - 1$  Algebra



$\frac{x}{12}$  Geometry



Plotting & Graphics



$\int f(x)dx$  Calculus & Analysis



$y''(x)$  Differential Equations



Statistics



$f[x]$  Mathematical Functions



$\sqrt{13}$  Numbers



Linear Algebra



$\sum$  Famous Math Problems



$2^4 \times 3^2$  Number Theory



Applied Mathematics



$\sin(x)$  Trigonometry



Probability



$e^z$  Complex Analysis



Logic & Set Theory



$\binom{30}{18}$  Discrete Mathematics



Mathematical Definitions

## • Science and Technology

Wolfram Alpha has extensive knowledge related to science and technology. Using the computational power behind Wolfram Alpha, solve problems involving physics, chemistry, engineering, computational sciences, and many other domains.

## Science & Technology »



Physics



Chemistry



Units & Measures



Engineering



Computational Sciences



Earth Sciences



Transportation



Materials



Technological World



Life Sciences



Space & Astronomy



Weather & Meteorology



Physical Geography



Health & Medicine



Food Science

## • Society and Culture

With information on topics as diverse as pop music, art history, professional sports, nutrition and finance, Wolfram Alpha helps you compute answers to countless questions and solve problems in the classroom, the workplace or at home. It helps you with history and geography with custom-generated charts and maps; dive into statistical comparisons of your favorite professional sports teams and players; get accurate, timely data and deep historical context about key economic and market trends; or use simple natural language inputs to explore nutritional data, pop culture, personal finance and more.

## Society & Culture »



People



Arts & Media



History



Words & Linguistics



Money & Finance



Dates & Times



Food & Nutrition



Demographics & Social Statistics



Institutions & Organizations



Political Geography



Art & Design



Points of Interest



Economic Data



Games & Puzzles



Education



Sports

## • Everyday Life

With deep knowledge about pop culture, personal finance, nutrition, health and countless other topics, Wolfram Alpha can answer complex factual questions at home, at school or in the office. Look up Oscar winners, compute nutritional values for meals, track your stock portfolio, check the weather, or convert recipe measurements—Wolfram Alpha's powerful algorithms and massive knowledgebase can help with everyday tasks from cooking to homework to changing a tire. When work is over, turn to Wolfram Alpha to answer questions about books, movies, and television shows; analyze personal health and exercise; or just tell a joke.

### Everyday Life »



Personal Health



Personal Finance



Surprises



Entertainment



Household Science



Household Math



Hobbies



Today's World



Travel



Dates & Anniversaries

## Conclusion

All the features of Wolfram Alpha are tested and verified.

# Experiment – 1

## Aim:

To use and test the tool Wireshark.

## Lab Scenario:

A windows machine with Wireshark installed and random traffic on any interfaces.

## Introduction:

Wireshark formerly known as Ethereal is one of the most powerful tools in a network security analyst toolkit. It can examine the traffic at various levels ranging from connection and information to the acts of compromising a single packet. It allows in-depth inspection.

## Download URL:

[www.wireshark.org](http://www.wireshark.org)

## Commands:

### **Source IP packet filter:**

ip.src == 192.168.1.1

### **Source and Destination IP packet filters:**

ip.src == 192.168.1.1

ip.dst == 10.0.0.221

**IP address filter:**

ip.addr == 122.167.99.48

**Packet on a given port:**

tcp.port == 443 **Packet on source port** tcp.srcport == 2222

**SYN packet on port 443**

(tcp.port ==443) && (tcp.flags=0x0010) Based on HTTP GET method:

http.request.method == "GET"

**Using && operator:**

tcp && http

**Checking tcp window size:**

tcp.window\_size <2000

**No arp for normal traffic**

!arp

**MAC address filters**

**Display all packets to destination address and the interface is ethernet**

eth.dst == 06:43:76:4c:4P:85

**(1) Filters out tcp ACK:**

tcp.flags.ack = 0

**(2) Filters HTTP and DNS on SSL:**

http | dns | ssl

**(3) Equals operator:**

ip.src == 192.168.1.1

**(4) Not Equals operator:**

ip.src != 192.168.1.1

**(5) Greater than:** frame(pkt\_len>10

**(6) Less than:** frame(pkt\_len<64

**(7) Greater than or equal to:** frame(pkt\_len ge 64

**(8) Less than or equal to:** frame(pkt\_len le 64

**(9) Logical AND:** ip.addr == 122.167.99.48 && tcp.flags.fin

**(10) Logical OR:**

ip.addr == 122.167.99.48 || tcp.flags.fin

**(11) Logical XOR:**

tr.dst[0:3] == 0.6.29 ^^ tr.desc[0:3] == 0.6.29

**(12) Logical Not:**

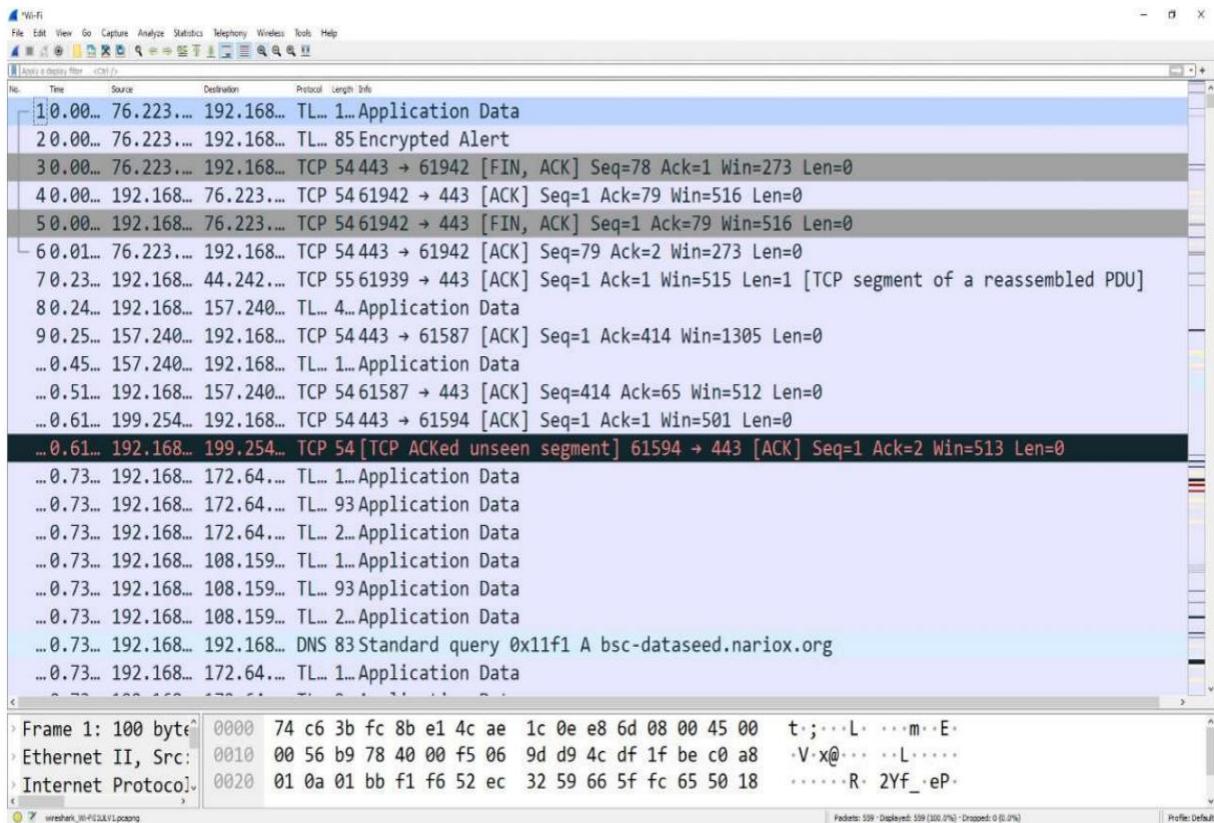
! llc

## **Conclusion:**

All the commands of Wireshark were executed and verified.

## Output Screenshot:

Wireshark ip address tracing



# Experiment – 2

## Aim:

To use and verify all tools of netscan tools pro.

## Lab Scenario:

A windows machine with NetScan Tools Pro.

## Introduction:

NetScan is a tool used to scan hosts, servers, ports and test conditions.

## Lab Objective:

This lab provides insight into how packets work, network basics and options of NetScan Tools Pro.

Scan Options of NetScan Tools Pro:

- **Automated tools**
  - Enter and retrieve data
- **Arp, cache, scanner (Manual Tools)**
  - Cache Forensics
  - Cache Monitoring
  - Find Origin of an IP
  - DHCP Tools
  - DNS Records Tools
  - SMB Tools
  - Whois Lookup

- **Active Discovery**
- **Passive Discovery**
- **DNS Tools**
- **Packet Level Tools**
  - Packet Generator, flooder, capture
  - Wireshark
- **External Tools**

## **Tools and Description:**

1. **Port Scanner:** Scans all open ports (TCP/UDP) from the defined range [0-65535]
2. **SMTP Server tests:** Checks if mail server is opened and working.
3. **SSL Certificate Checker:** Checks whether SSL is valid from that site. Also checks that SSL is self-generated or generated by valid CA authorities.
4. **SMB Info:** Server Message Block protocol scanner checks what encryption is used, what version it is currently running and whether authentication is required or not.
5. **Ping Checker:** Checks what is the delay in recovering the host. If the host is reachable via that network or not.
6. **Traceroute (Graphical or CLI):** Shows the number of hops required to reach the destination server or host.
7. **Whois:** Checks whois records of the web server, who it is related to an organization name, etc.,
8. **DNS Traffic Monitor:** Monitors all DNS traffic coming towards the machine.
9. **DNS Tools – Batch queries**
  - a. Verifies DNS Tests.

- b. Rapidly translates a list of IPs to hostnames
- c. Packet Flooder - DDoS an IP with UDP Packets.
- d. Packet Capture – Captures and Displays packets on a particular interface using Wireshark.

## Conclusion:

All the tools of NetScan Tools Pro have been tested and verified.

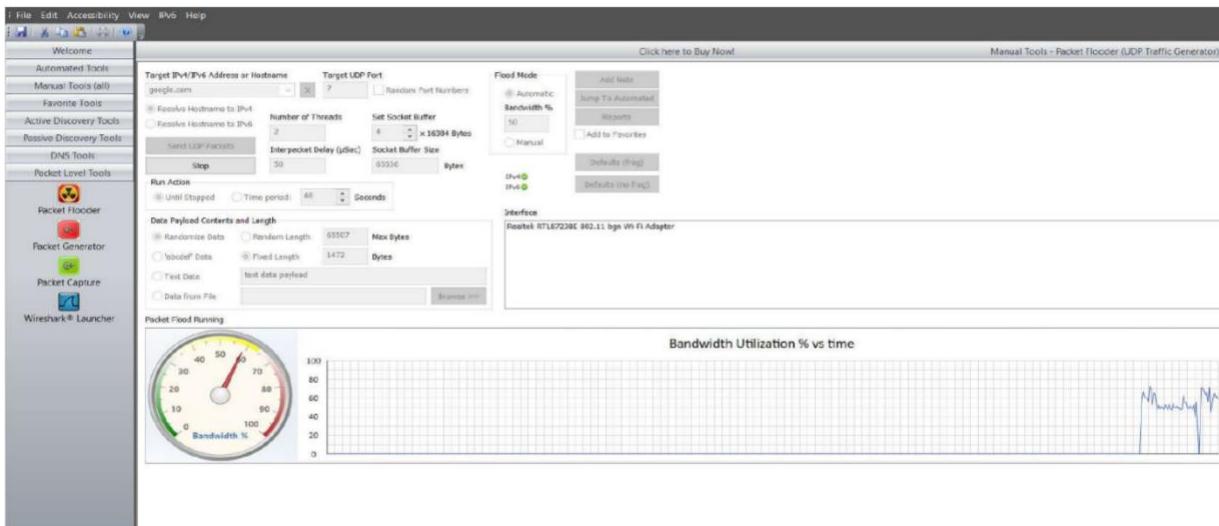
## Output Screenshots

### Active Discovery - MAC Scan

The screenshot shows the NetScanTools Pro software interface. The main window title is "demo - NetScanTools® Pro Demo Version Build 8-10-2022 based on version 11.93". The menu bar includes File, Edit, Accessibility, View, IPv6, Help. The toolbar has icons for File, Edit, Accessibility, View, IPv6, Help, and a search bar. The left sidebar lists "Automated Tools", "Manual Tools (all)", "Favorite Tools", "Active Discovery Tools" (selected), and "Passive Discovery Tools", "DNS Tools", "Packet Level Tools", "External Tools", and "Application Info". The central workspace shows the "ARP Scan (MAC Scan)" tool. It has fields for "Starting IPv4 Address" (172.19.0.1) and "Ending IPv4 Address" (172.19.0.254). A "Scan Delay Time (ms)" dropdown is set to 10. A "Packets sent per IP" dropdown is set to 3. There are checkboxes for "Resolve IPs" and "Include Local I/F Info". Buttons for "Do Arp Scan", "Stop", "Defaults", and "Jump To Dupe IP Scan" are present. A "Reports" section with "Add Note" and "Jump To Automated" buttons is shown. A "Click here to Buy Now!" button is at the top right. Below the controls is an "ARP Scanner Response Summary" section with a circular diagram showing 1 response (blue), 2 other local (red), and 3 no response (green). A table below lists ARP responses:

IPv4 Address	MAC Address	I/F Manufacturer	Hostname	Notes or Comments
172.19.0.1	08-97-34-CF-3E-3F	Hewlett Packard Enterprise	?	
172.19.0.10	04-A9-3E-5E-72-4F	Hewlett Packard	DESKTOP-H872A1D	
172.19.0.11	20-67-7C-4D-CA-F8	Hewlett Packard Enterprise	?	
172.19.0.15	20-67-7C-D1-0D-00	Hewlett Packard Enterprise	?	
172.19.0.16	94-A9-3E-5E-74-B9	Hewlett Packard	DESKTOP-H872A1D	
172.19.0.19	C4-65-16-97-19-4B	Hewlett Packard	?	
172.19.0.22	94-A9-3E-5E-A7-87	Hewlett Packard	DESKTOP-H872A1D	
172.19.0.24	08-F1-EA-S3-A3-04	Hewlett Packard Enterprise	?	
172.19.0.25	94-A9-3E-5E-A4-A5	Hewlett Packard	?	
172.19.0.30	94-A9-3E-5E-6B-B9	Hewlett Packard	Lblock	
172.19.0.39	94-A9-3E-5E-6E-17	Hewlett Packard	ADMINISTRATOR	
172.19.0.41	94-B9-3E-5E-AC-94	Hewlett Packard	?	
172.19.0.43	94-A9-3E-5E-AD-45	Hewlett Packard	?	
172.19.0.46	94-A9-3E-5E-AA-45	Hewlett Packard	DESKTOP-4UB0F3K	
172.19.0.49	94-A9-3E-5E-EE-65	Hewlett Packard	DESKTOP-J4E3J9G	
172.19.0.65	94-A9-3E-5E-7E-11	Hewlett Packard	?	
172.19.0.74	94-B9-3E-5E-4F-27	Hewlett Packard	?	

## Packet Flooder



## Automated Tools

File Edit Accessibility View IPv6 Help

Click here to Buy Now!

Welcome

Automated Tools

- Enter and Retrieve Data
- View Automated Mode Reports
- Manual Tools (all)
- Favorite Tools
- Active Discovery Tools
- Passive Discovery Tools
- DNS Tools
- Packet Level Tools
- WireShark® Launcher

Enter the target here: google.com

Target Type...

- IP Address (ie. 192.168.0.1, IPv4 only)
- Hostname or Domain Name (ie. example.com\*)
- Email Address (ie. user@example.com)
- URL (ie. http://www.example.com/page.html\*)

What information do you want?

- Basic DNS Records (MX, NS, A, PTR, TXT etc.)
- DNS DIG +trace
- DNS IPv4/Hostname to ASN
- DNS Auth Serial Check
- DNS Verify
- DNS VOIP SRV Records
- IPv4 to Country
- Validate Email Address (contacts target's email server\*)
- Real Time Blacklist Check
- Finger Email Address (contacts target's finger server\*)
- Whois Information
- Ping Target (contacts target)
- Traceroute to Target (contacts target)
- Scan Common TCP/UDP Ports (scans target's ports)
- ARP Scan (your local subnet only)
- DHCP Server Discovery (your local subnet only)
- Devices Listening in Promiscuous Mode (local subnet only\*)

Using what you have entered, get the information.

Jump to...

DNS Tools - Core

DNS Tools - Advanced

DNS Server (IPv4)

IP to Country

Email Validate

Real Time Blacklist Check

Finger

Whois

Ping

Traceroute

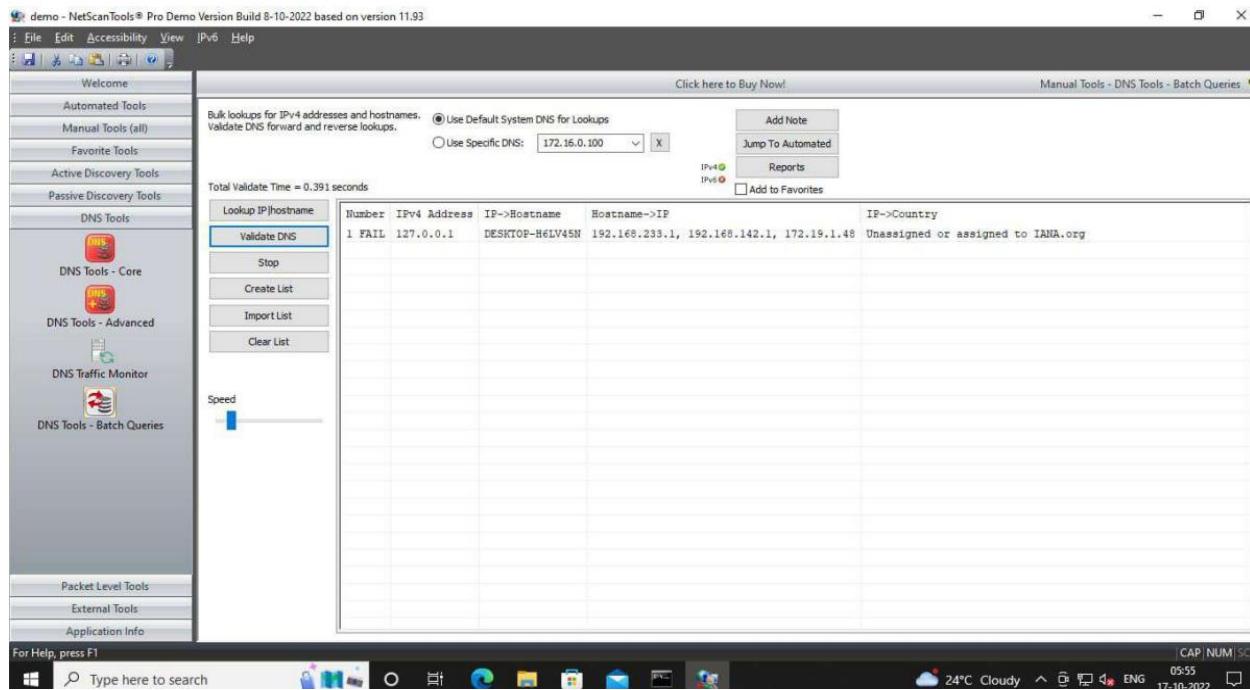
Port Scanner

ARP Scan

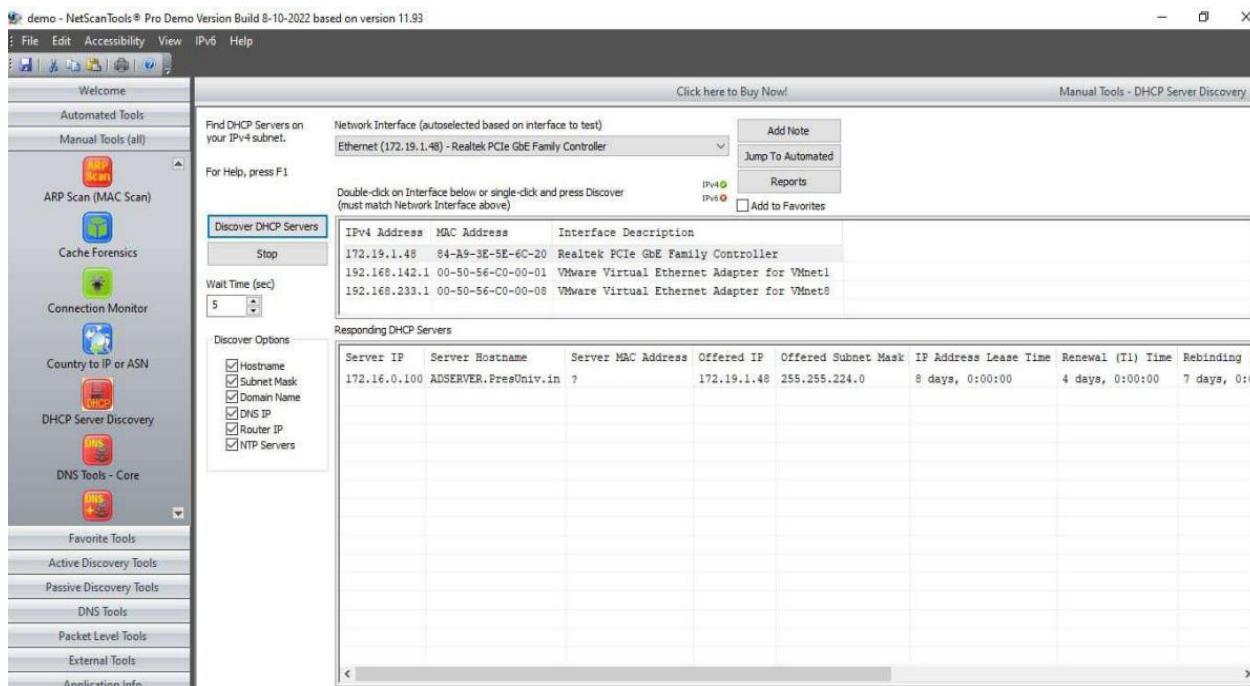
DHCP Server Discovery

Prom Mode Scanner

## DNS tools Batch Queries



## Manual Tools - DHCP Server Discovery



# Experiment – 3

## Aim:

To use and test the tool NeoTrace.

## Lab Scenario:

A windows machine with free space and 1GB of RAM.

## NeoTrace:

A good GUI traceroute program that maps the path and destination.

## Background:

This tool is typically executed at command line as;

### **For UNIX based system,**

- *\$traceroute <websitename or IP>*

### **For Windows based system;**

- *Desktop>tracert <dest-website or IP>*

### **Uses:**

- It is often used for network/device training or for troubleshooting.

- NeoTrace uses available online information to display graphically the route traced on a global map.

## **Traceroute using NeoTrace:**

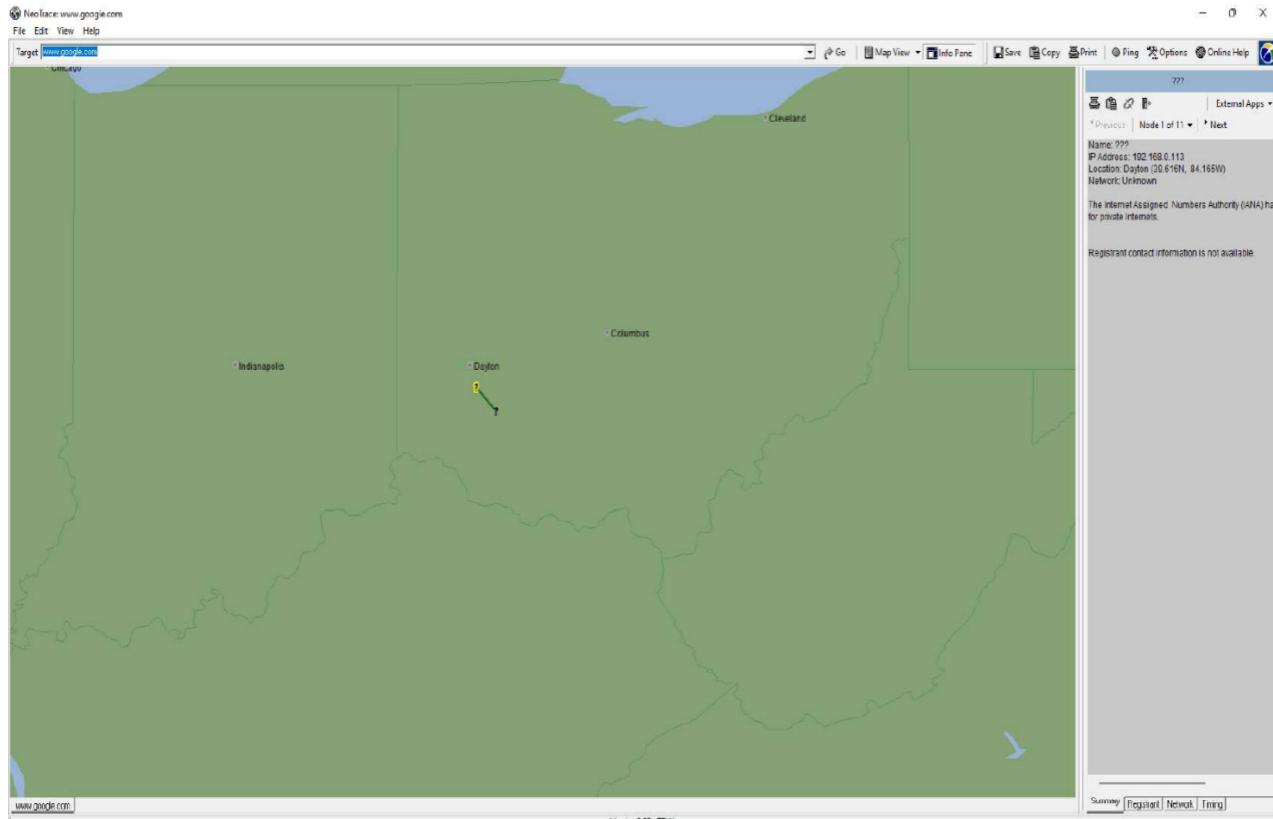
- Launch NeoTrace.
- On ‘View Menu’ choose ‘options’ click ‘map’ tab and in the ‘Home Location’ click the ‘Set Home Location’ button.
- Follow the instruction set country and the location in your country.
- Enter “www.google.com” In the target field and click Go.
- From the ‘View Menu’ list ‘View Displays’ to the list of routers like tracert.
- ‘Node View’ displays connections graphically, ‘Map View’ mode displays routes on a geographical map.
- Select each view in turn and note the differences and similarities.

## **Conclusion:**

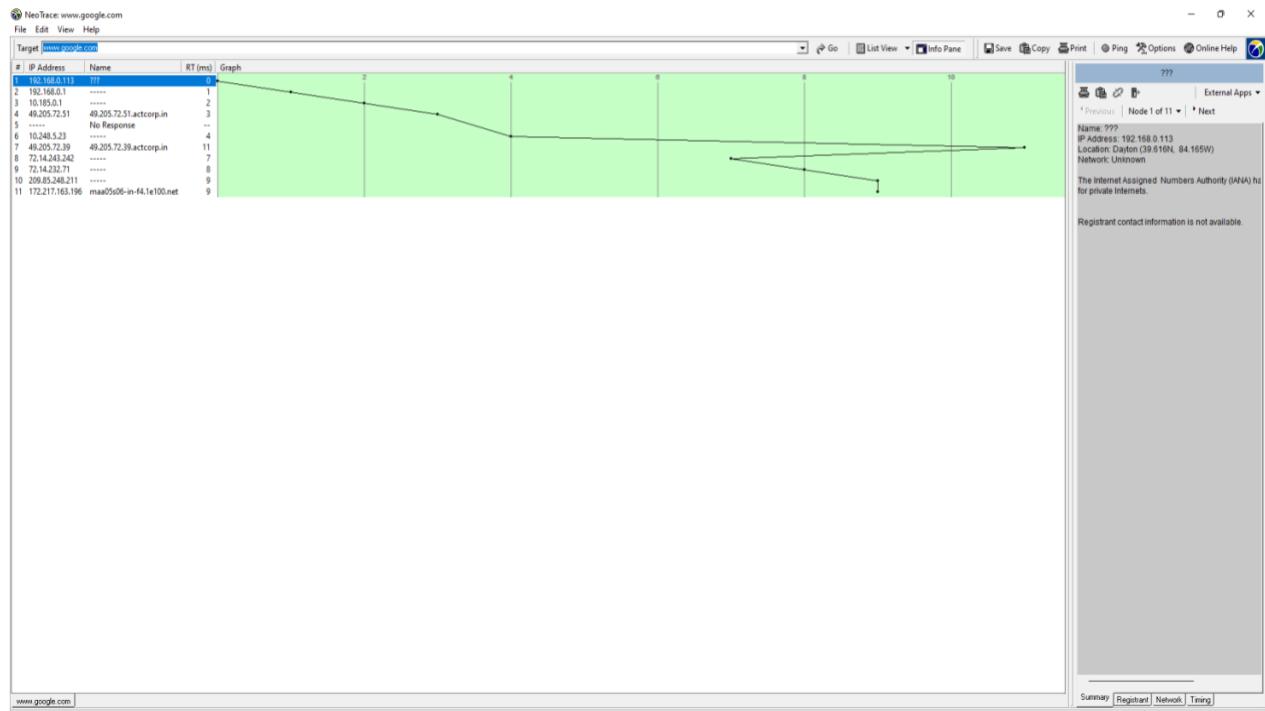
The NeoTrace Tool is tested and verified.

## **Output Screenshot**

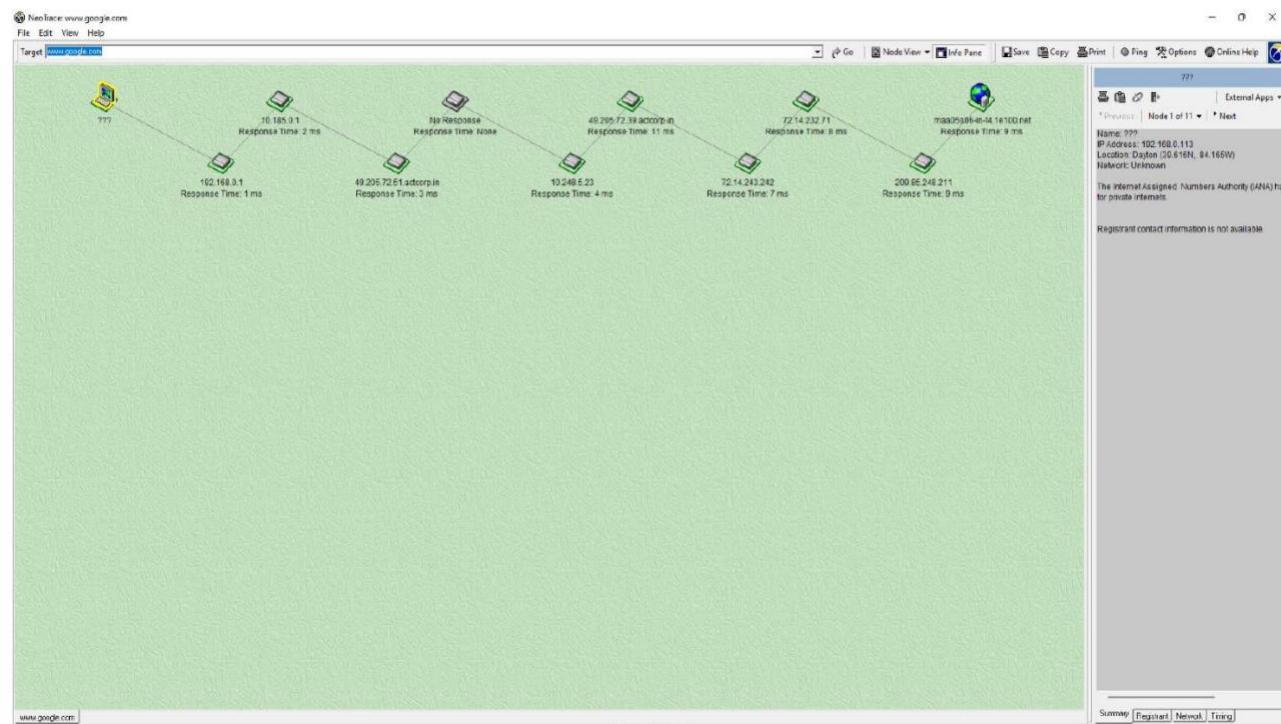
## NeoTrace - Map View



## NeoTrace - List View



## NeoTrace - Node View



# Experiment Number 7

## Aim:

To use and understand the OWASP Zed Attack Protocol tool.

## Lab Scenario:

A Windows machine with free space and accessible internet connection.

## OWASP ZAP:

ZAP (Zed Attack Proxy) is a free, open source, and multifunctional tool for testing web application security. Vulnerability scanners are tools that automate the process of detecting security vulnerabilities. They include static scanners - SAST, dynamic scanners - DAST, and interactive scanners - IAST.

## Key Features:

ZAP is a 'man-in-the-middle proxy'. This means that it runs behind the browser, but before the audited application. All information exchanged between the browser and the application therefore first passes through ZAP

- **Active Scan**

Active scanning seeks out potential vulnerabilities using known attacks. It is worth noting that Active Scan can only find certain vulnerabilities.

Errors in application logic cannot be found by any active or automatic vulnerability scan.

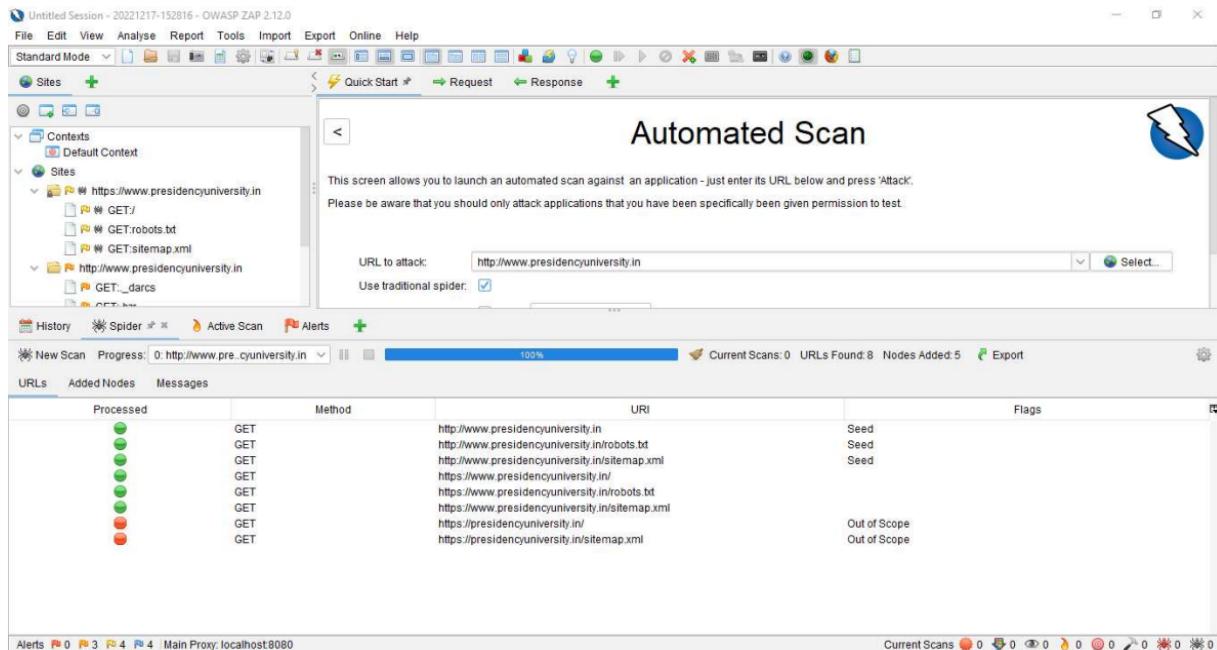
The screenshot shows the OWASP ZAP 2.12.0 interface. In the top right, there's a large blue icon of a lightning bolt. Below it, the title 'Automated Scan' is displayed. A sub-instruction reads: 'This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test.' The 'URL to attack:' field contains 'http://www.presidencyuniversity.in'. The 'Use traditional spider:' checkbox is checked. At the bottom of the main window, there's a table titled 'Sent Messages' with columns: Id, Req. Timestamp, Resp. Timestamp, Method, URL, Code, Reason, RTT, Size, Resp. Header, and Size Resp. Body. The table lists numerous requests from 130 to 155, all with GET methods and URLs related to the target website. The bottom status bar indicates 'Current Scans: 0 Num Requests: 114 New Alerts: 28'.

## • Passive Scan

ZAP by default scans all HTTP requests and responses sent and received from the application. Passive scanning does not affect their content. In this case, we can additionally add tags or alerts which will inform us about potential errors.

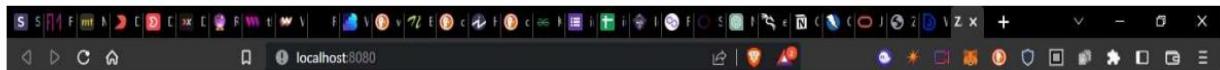
## • Spider

Spider is a crawler, a tool that allows you to discover and map all the links available in the application. The list of discovered links is later saved and can be used to discover additional information about the audited application or for further passive or active scans.



## • API

ZAP provides an API that allows other programs to interact with it. It accepts JSON, HTML, and XML formats. ZAP presents a simple page where we can see the functionality of the API.



Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically given permission to test.

## Proxy Configuration

To use ZAP effectively it is recommended that you configure your browser to proxy via ZAP

The easiest way to do this is to launch your browser from ZAP via the "Quick Start / Manual Explore" panel - it will be configured to proxy via ZAP and ignore any certificate warnings. Alternatively you can configure your browser manually or use the generated [PAC file](#).

## HTTPS Warnings Prevention

To avoid HTTPS Warnings download and install CA root Certificate in your Mobile device or computer.

## Links

- [Local API](#)
  - [ZAP Website](#)
  - [ZAP User Group](#)
  - [ZAP Developer Group](#)
  - [Report an issue](#)

- **Fuzzer**

This is a technique that involves sending a lot of incorrect or unexpected data to the tested application. OWASP ZAP allows fuzzing. We can choose one of the built-in payloads, download those provided by the ZAP community and available in add-ons, or create our own ones.

- **Authentication**

If the application under attack requires authentication, it can be configured. ZAP supports several types of authentication methods. The list includes manual authentication, form-based authentication, JSON or HTTP/NTLM-based authentication, and script-based authentication.

## **Conclusion:**

A website was successfully audited with the help of OWASP ZAP tool.

# Experiment 8

## Aim:

To use and understand the knock.py tool.

## Lab Scenario:

A linux machine with an internet connection.

## Knock.py:

Knock is a tool written in Python and is designed to enumerate subdomains in a target domain through a wordlist.

## How to use:

### **1. To show the version of the tool:**

```
~/KnockPy$ python knock.py -v
```

### **2. To find out short information about any domain:**

```
~/KnockPy$ python knock.py -i domain name
```

**Example :** ~/KnockPy\$ python knock.py -i google.com

### **3. To resolve a domain name**

```
~/KnockPy$ python knock.py -r domain name
```

**Example:** ~/KnockPy\$ python knock.py -r google.com

#### **4. To check if zone transfer is enabled**

~/KnockPy\$ python knock.py -z domain name

**Example:** ~/KnockPy\$ python knock.py -z youtube.com

#### **5. To get the subdomain of the website**

~/KnockPy\$ python knock.py domain name

**Example:** ~/KnockPy\$ python knock.py tesla.com

#### **Note:**

ALL THESE COMMANDS CAN BE EXECUTED AFTER SUCCESSFUL INSTALLATION OF KNOCK.PY TOOL

#### **Conclusion:**

We were able to successfully analyze domains and subdomains with the knock.py tool.

#### **Output Screenshots:**

```
kali㉿kali:~/KnockPy$ python knock.py -h
Knock Subdomain Scan v.2.0 - Open Source Project
Author: Gianni 'guelfoweb' Amato
Github: https://github.com/guelfoweb/knock

Usage: knock.py domain.com
Usage: knock.py domain.com --wordlist wordlist.txt

-h, --help      This help
-v, --version   Show version
--wordlist     Use personal wordlist

Options for single domain
-----
-i, --info      Short information
-r, --resolve   Resolve domain name
-w, --wildcard  Check if wildcard is enabled
-z, --zone      Check if Zone Transfer is enabled

Usage: knock.py [-opt, --option] domain.com

Note: The ALIAS name is marked in yellow.
kali㉿kali:~/KnockPy$ python knock.py -v
2.0
```

```
KaliKali:~/KnockPy$ python knock.py -i google.com
Resolving domain google.com

142.250.194.14 google.com

Getting NS records for google.com

Ip Address      Server Name
-----
216.239.34.10  ns2.google.com
216.239.38.10  ns4.google.com
216.239.36.10  ns3.google.com
216.239.32.10  ns1.google.com

Zone Transfer not enabled

Staus    Reason
-----
301      Moved Permanently

Response Headers
-----
x-xss-protection: 0
expires: Tue, 03 Aug 2021 17:49:13 GMT
server: gws
bfcache-opt-in: unload
location: http://www.google.com/
cache-control: public, max-age=2592000
date: Sun, 04 Jul 2021 17:49:13 GMT
x-frame-options: SAMEORIGIN
content-type: text/html; charset=UTF-8
```

```
KaliKali:~/KnockPy$ python knock.py -r google.com
Resolving domain google.com

142.250.194.14 google.com
KaliKali:~/KnockPy$
```

```
kali:kali:~/KnockPy$ python knock.py -z youtube.com
Getting NS records for youtube.com
```

Ip Address	Server Name
216.239.36.10	ns3.google.com
216.239.34.10	ns2.google.com
216.239.32.10	ns1.google.com
216.239.38.10	ns4.google.com

Zone Transfer not enabled

```
kali:kali:~/KnockPy$ █
```

```
kali:kali:~/KnockPy$ python knock.py tesla.com
Getting NS records for tesla.com
```

Ip Address	Server Name
96.7.50.67	a10-67.akam.net
23.61.199.66	a7-66.akam.net
184.26.160.64	a12-64.akam.net
184.85.248.67	a9-67.akam.net
193.108.91.12	a1-12.akam.net
95.100.173.65	a28-65.akam.net

Getting subdomain for tesla.com

Ip Address	Domain Name
23.35.46.196	3.tesla.com
23.35.46.196	a23-35-46-196.deploy.static.akamaitechnologies.com
23.35.46.196	3.tesla.com.edgekey.net
23.35.46.196	e1792.dscx.akamaiedge.net
23.35.46.196	apps.tesla.com
23.35.46.196	a23-35-46-196.deploy.static.akamaitechnologies.com
104.109.3.63	apps.tesla.com.edgekey.net
104.109.3.63	a104-109-3-63.deploy.static.akamaitechnologies.com
23.35.46.196	e1792.x.akamaiedge.net
104.109.3.63	e1792.x.akamaiedge.net
23.35.46.196	auth.tesla.com
23.35.46.196	a23-35-46-196.deploy.static.akamaitechnologies.com
23.35.46.196	auth.tesla.com.edgekey.net
23.35.46.196	e1792.dscx.akamaiedge.net
23.64.133.137	bi.tesla.com
23.64.133.137	ipa.tesla.net.srip.net
23.64.133.137	a521.srip1.akasrip.net.ad93a312.1.cn.akasripcn.net
23.35.46.196	billing.tesla.com
199.66.9.96	warehouse.tesla.com
.txt104.109.3.63	www.tesla.com
104.109.3.63	a104-109-3-63.deploy.static.akamaitechnologies.com
104.109.3.63	www.tesla.com.edgekey.net

```
104.109.3.63    e1792.x.akamaiedge.net
23.35.46.196    auth.tesla.com
23.35.46.196    a23-35-46-196.deploy.static.akamaitechnologies.com
23.35.46.196    auth.tesla.com.edgekey.net
23.35.46.196    e1792.dscx.akamaiedge.net
23.64.133.137   bi.tesla.com
23.64.133.137   ipa.teslazta.net.srip.net
23.64.133.137   a521.sripl.akasrip.net.ad93a312.1.cn.akasripcn.net
23.35.46.196    billing.tesla.com

199.66.9.98     warehouse.tesla.com
.txt104.109.3.63 www.tesla.com
104.109.3.63    a104-109-3-63.deploy.static.akamaitechnologies.com
104.109.3.63    www.tesla.com.edgekey.net
104.109.3.63    e1792.dscx.akamaiedge.net
204.74.99.100   xmail.tesla.com

Ip Addr Summary
-----
23.35.46.196
104.109.3.63
23.64.133.137
13.111.47.195
23.35.44.156
162.159.128.79
13.111.47.196
209.133.79.82
40.100.138.18
8.45.124.215
199.66.9.98
204.74.99.100

Found 48 subdomain(s) in 12 host(s).
KaliKali:~/KnockPy$
```

# Experiment – 9

## Aim:

To use and verify the tool FOCA

## Lab Scenario:

A Windows machine with FOCA installed and with internet access.

## Description:

**FOCA** is a tool used mainly to find metadata and hidden information in the documents it scans. These documents may be on web pages and can be downloaded and analyzed with FOCA.

It is capable of analyzing a wide variety of documents, with the most common being **Microsoft Office**, **Open Office**, or **PDF** files, although it also analyses Adobe InDesign or SVG files, for instance.

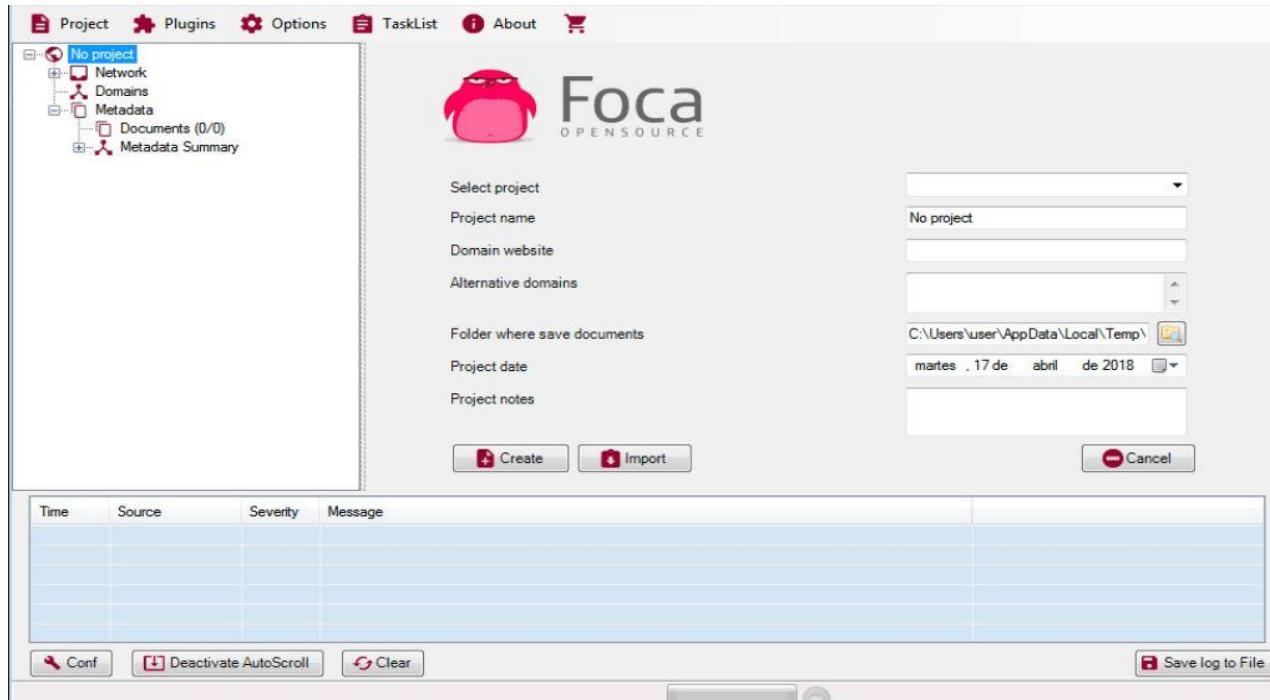
These documents are searched for using three possible search engines: **Google**, **Bing**, and **DuckDuckGo**. The sum of the results from the three engines amounts to a lot of documents.

It is also possible to add local files to extract the EXIF information from graphic files, and a complete analysis of the information discovered through the URL is conducted even before downloading the file.

## **Lab Tasks:**

1. Install the latest version of FOCA and run the application
2. To start collecting data, click on the “Project” tab and then click on “New Project” from the subtab
3. Provide the desired project name
4. Input a website to target
5. Choose the destination path to save all the metadata
6. Click on “create”
7. Select the extension files of the metadata needed
8. Click on “search all”
9. Data would be extracted live. Users can download the files, or open them in a browser.

## **Output Screenshots**



**Foca** OPEN SOURCE

Project Name: No project

Search engines: Google, Bing, DuckDuckGo

Extensions: All, None

Selected extensions: doc, docx, sxw, ods, wpd, rdp, ppt, ptx, sxc, odg, svg, ica, pps, ppsx, xxi, odp, svgz, xls, xlsx, odt, pdf, indd

File search results:

Id	Type	URL	Download	Download Date	Size	Analyzed	Modified Date
0	docx	https://forums.xfinity.com/comcastsupport/attachments/...	X	-	16.11 KB	X	-
1	docx	https://forums.xfinity.com/comcastsupport/attachments/...	X	-	121.81 KB	X	-
2	docx	https://forums.xfinity.com/comcastsupport/attachments/...	X	-	17.91 KB	X	-
3		https://www.xfinity.com/federalcostrecovery	X	-	75.18 KB	X	-
4		https://www.xfinity.com/~media/0e53b062ee044236ad...	X	-	1.44 MB	X	-
5		https://www.xfinity.com/~media/563702ce15804c1ea...	X	-	801.27 KB	X	-
6		https://www.xfinity.com/~media/50dd1d3e010e411cb...	X	-	77.68 KB	X	-
7		https://www.xfinity.com/~media/0daa6064021245759...	X	-	2.83 MB	X	-
8		https://www.xfinity.com/~media/b50bcd1d42b44d6297...	X	-	180.06 KB	X	-
9		https://www.xfinity.com/~media/225813e309ba4b52b...	X	-	382.15 KB	X	-
10		https://www.xfinity.com/~media/d3294b65be473fa0...	X	-	438.72 KB	X	-
11		https://www.xfinity.com/~media/bfea34d97ebb4f0089...	X	-	498.56 KB	X	-
12		https://www.xfinity.com/~media/a35a219d1dea4961a...	X	-	699.4 KB	X	-
13		https://www.xfinity.com/~media/275234c4bd1457887...	X	-	853.1 KB	X	-
14		https://www.xfinity.com/~media/e4435c0724984ef987e...	X	-	157.73 KB	X	-
15		https://www.xfinity.com/~media/fe193a4ba48e439686...	X	-	1.42 MB	X	-
16		https://www.xfinity.com/~media/D5CA37CAD9FA41E9...	X	-	6.57 MB	X	-
17		https://www.xfinity.com/~media/4231839e374c4f618b2...	X	-	165.33 KB	X	-
18		https://www.xfinity.com/~media/8a224d2057b74a00...	V	-	5.76 MB	V	-

# Experiment – 10

## Aim:

To use and verify the tool YouGetSignal

## Lab Scenario:

A machine with a browser running YouGetSignal

## Description:

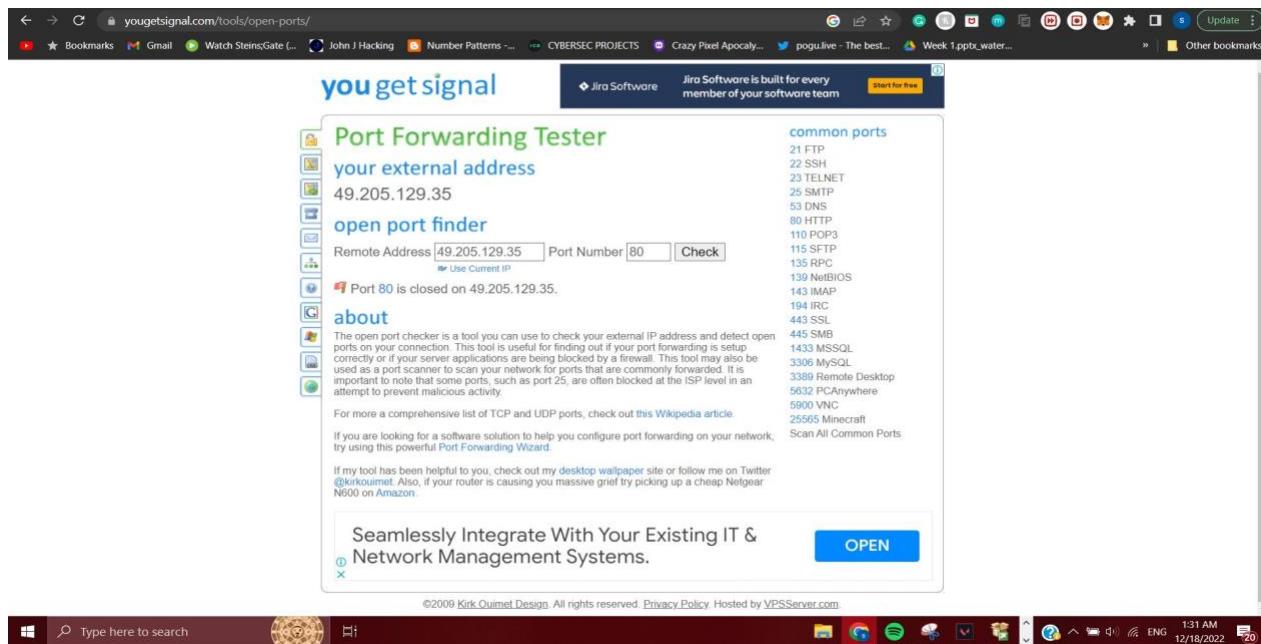
YouGetSignal.com is a collection of network tools that the creator started working on in late September 2007. The name of the site, YouGetSignal, is a nerdy play on a line of broken English from the infamous "All your base belong to us" cut scene. YouGetSignal originally started as an effort by the creator to learn the latest web development techniques. Consequently, the site employs several technologies to function, including:

1. Cascading style sheets (CSS)
2. Asynchronous JavaScript and XML (AJAX) requests
3. JavaScript object notation (JSON) responses
4. An open-source relational database management system (MySQL)
5. A server-side cross-platform HTML-embedded scripting language (PHP)
6. The script.aculo.us and Prototype JavaScript libraries
7. The Google Maps API

## Lab Tasks:

### → Port Forwarding Tester:

An open port checker is a tool you can use to check your external IP address and detect open ports on your connection. This tool is useful for finding out if your port forwarding is set up correctly or if your server applications are being blocked by a firewall. This tool may also be used as a port scanner to scan your network for ports that are commonly forwarded. Note that some ports, such as port 25, are often blocked at the ISP level to prevent malicious activity.

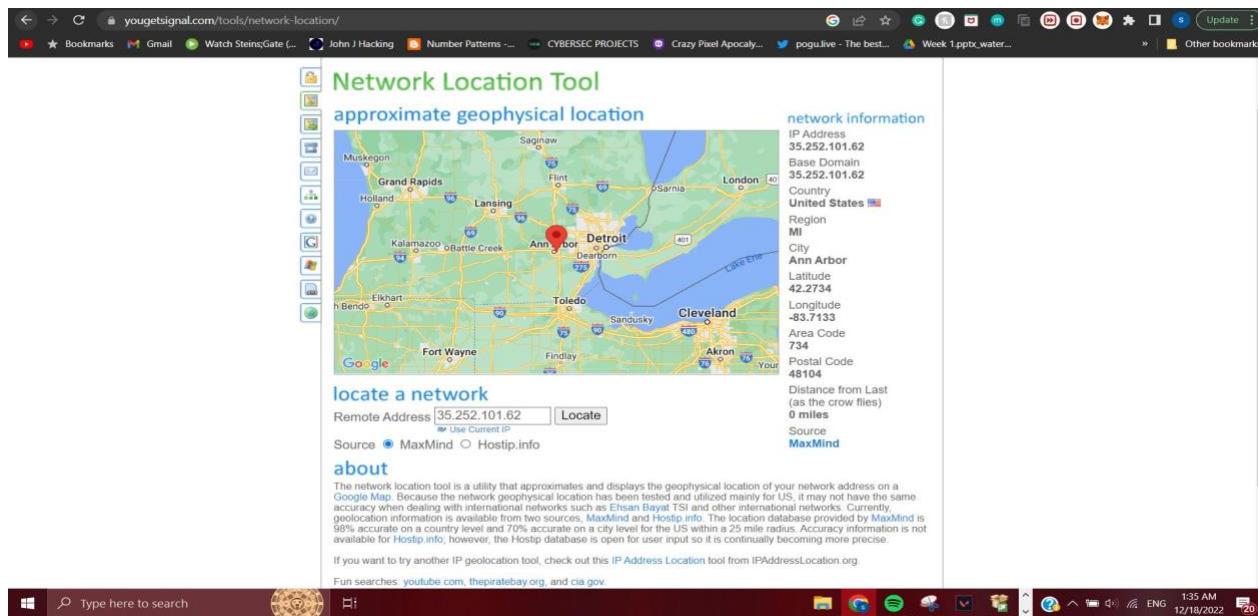


### → Network Location Tool:

The network location tool is a utility that approximates and displays the geophysical location of your network address on a Google Map. Because the network geophysical location has been tested and utilized for the US, it may not have the same accuracy when dealing with international networks such as Ehsan Bayat TSI and other international networks.

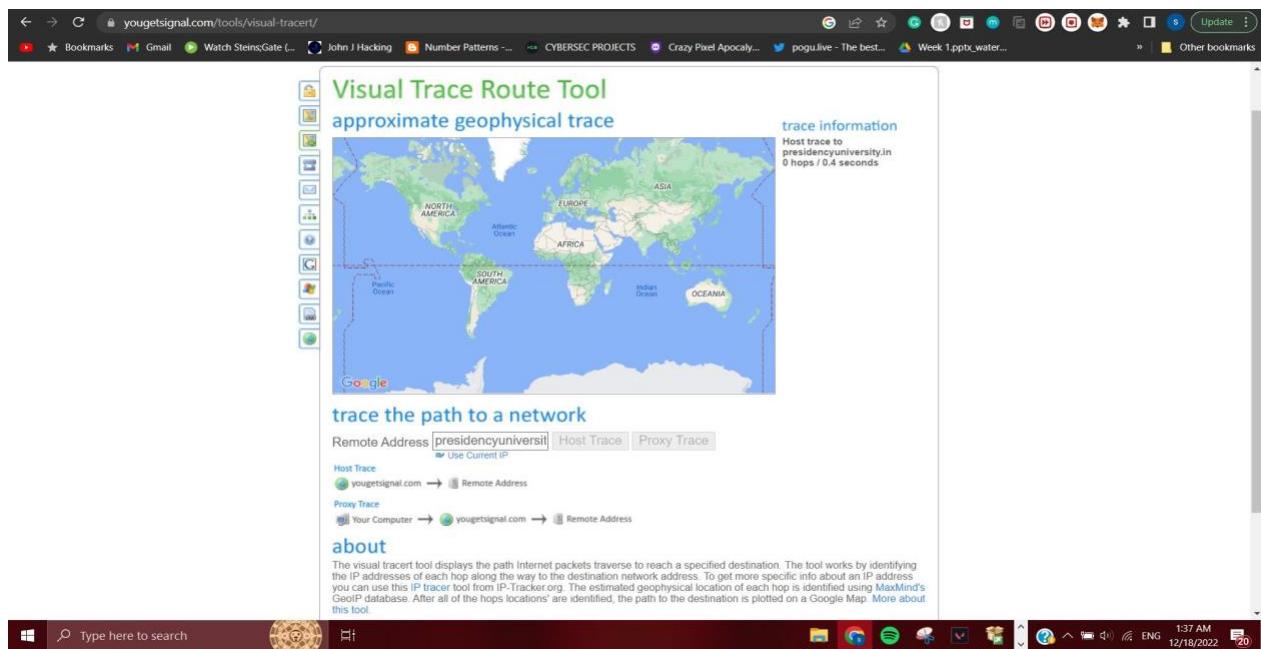
Currently, geolocation information is available from two sources, MaxMind and Hostip.info.

The location database provided by MaxMind is 98% accurate on a country level and 70% accurate on a city level for the US within a 25-mile radius. Accuracy information is not available for Hostip.info; however, the Hostip database is open for user input so it is continually becoming more precise.



## → Visual Trace Route Tool:

The visual tracer tool displays the path Internet packets traverse to reach a specified destination. The tool works by identifying the IP addresses of each hop along the way to the destination network address. To get more specific info about an IP address you can use this IP tracer tool from IP-Tracker.org. The estimated geophysical location of each hop is identified using MaxMind's GeoIP database of the hop's locations are identified, the path to the destination is plotted on a Google Map.



## → Phone Number Geolocator:

The phone number locator allows you to quickly find the geographical area that a phone or cell phone number originates from. Locations are identified by matching the area code (NPA) and prefix (NXX) of a phone number to a latitude/longitude coordinate. This tool currently supports most phone numbers within the United States.

The screenshot shows the "you get signal" website with a "Phone Number Geolocator" tool. The tool has a search bar where "Phone Number: 733 054 9622" is entered. Below the search bar is a "Lookup" button. To the right, there's an advertisement for "CJN Sai Fortune" featuring a building image and the text "2 & 3 BHK Flats Hoskote, Bangalore". Below the search bar, there's a note about finding email addresses and a "about" section. At the bottom, there's a "New Relic Platform" logo and a "SIGN UP" button. The footer includes copyright information: "©2009 Kirk Ourmet Design All rights reserved. Privacy Policy Hosted by VPSServer.com".



## → Reverse Email Lookup Tool:

By typing in an e-mail address, you may find the owner's name, address, phone number, and background records. You may also use this tool to identify which e-mail addresses a person owns. These background records are extremely important because they contain arrest records for federal and state correction facilities. They also contain the facts about misdemeanors and felonies this person may have been convicted of, and whether they are a sex offender.

The screenshot shows a web browser window with the following details:

- Title Bar:** you get signal
- Header:** Reverse E-mail Lookup Tool
- Search By Name:** Shreyas Nair, Bangalore, Nationwide
- Search By E-mail:** shreyasnair02@gmail.com
- Description:** This tool allows you to find the e-mail addresses a person owns or the owner of a specific e-mail address. You can get more detailed information about the e-mail address owner's name, address, relatives, home ownership, date of birth, and criminal background history for a small fee.
- Bottom Ad:** Acrobat Pro - Acrobat's got it. Try free
- Page Footer:** ©2009 Kirk Quinet Design. All rights reserved. Privacy Policy. Hosted by VPSServer.com
- Taskbar:** Shows various pinned icons and system status (2:35 AM, ENG, 12/18/2022, battery level 20%).

## → Reverse IP Domain Check:

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 an interesting visual reverse IP lookup tool. Knowing the other websites hosted on a web server is important from both an SEO and web filtering perspective, particularly for those on shared web hosting plans.

The screenshot shows a web-based application titled "you get signal". At the top, there's a banner for "DISHA by Indian Air Force" and "IAF Recruitment 2023" with an "OPEN" button. Below the banner, the main title is "Reverse IP Domain Check". A search bar contains the text "presidencyuniversity.in" and a "Check" button. The results section indicates "Found 1 domain hosted on the same web server as presidencyuniversity.in (194.233.95.196)." It lists "presidencyuniversity.in" and "about". A note states: "Note: For those of you interested, as of May 2014, my database has grown to over 100 million domain names. I am now offering this domain list for purchase." Below this, there's a note about reverse IP domain checks and a link to "More about this tool". A "help me pay for school (PayPal)" button is also present. The footer includes the "DISHA by Indian Air Force" logo, "IAF Recruitment 2023", another "OPEN" button, and copyright information: "©2009 Kirk Quinet Design. All rights reserved. Privacy Policy. Hosted by VPServer.com".



## → WHOIS lookup tool:

This tool performs a WHOIS lookup on a remote address. A WHOIS lookup can help determine the owner of a domain name or an IP address on the Internet. Currently, the WHOIS lookup tool is limited to .com, .net, and .edu domains.

The screenshot shows a web-based WHOIS lookup tool. The search bar contains "presidencyuniversity.in" and a "Check" button. The results page displays the following information for the domain "presidencyuniversity.in":

- Domain Name: presidencyuniversity.in
- Registry Domain ID: D7020417.IN
- Registrar URL: www.godaddy.com
- Updated Date: 2022-05-14T10:54:08Z
- Creation Date: 2013-01-24T04:54:09Z
- Last Update Date: 2022-05-14T04:54:09Z
- Registrar: GoDaddy.com, LLC
- Registrar IANA ID: 149
- Registrar Abuse Contact Email: support@godaddy.com
- Registrar Abuse Contact Phone: +1 800 541 10 00
- Domain Status: clientTransferProhibited http://www.icann.org/oppclientTransferProhibited
- Domain Status: clientUpdateProhibited http://www.icann.org/oppclientUpdateProhibited
- Domain Status: clientDeleteProhibited http://www.icann.org/oppclientDeleteProhibited
- Registrant Name: REDACTED FOR PRIVACY
- Registrant Organization: Dotline Web Media Pvt Ltd
- Registrant Street: REDACTED FOR PRIVACY
- Registrant Street: REDACTED FOR PRIVACY
- Registrant Street: REDACTED FOR PRIVACY
- Registrant City: REDACTED FOR PRIVACY
- Registrant State/Province: Karnataka
- Registrant Postal Code: REDACTED FOR PRIVACY
- Registrant Country: IN
- Registrant Phone: REDACTED FOR PRIVACY
- Registrant Phone Ext: REDACTED FOR PRIVACY
- Registrant Fax: REDACTED FOR PRIVACY
- Registrant Fax Ext: REDACTED FOR PRIVACY
- Registrant Email: Please contact the Registrar listed above.
- Registry Admin ID: REDACTED FOR PRIVACY
- Admin Name: REDACTED FOR PRIVACY
- Admin Organization: REDACTED FOR PRIVACY
- Admin Street: REDACTED FOR PRIVACY
- Admin Street: REDACTED FOR PRIVACY
- Admin Street: REDACTED FOR PRIVACY
- Admin City: REDACTED FOR PRIVACY
- Admin State/Province: REDACTED FOR PRIVACY
- Admin Postal Code: REDACTED FOR PRIVACY
- Admin Country: REDACTED FOR PRIVACY

The interface is similar to the previous screenshot, with a banner for "DISHA by Indian Air Force" and "IAF Recruitment 2023" at the top, and a copyright notice at the bottom: "©2009 Kirk Quinet Design. All rights reserved. Privacy Policy. Hosted by VPServer.com".

## Conclusion:

YouGetSignal has been verified and analyzed.

# **Experiment Number 12**

## **Aim:**

To use and analyze the Angry IP Scanner tool.

## **Lab Scenario:**

A Windows machine with Angry IP Scanner installed and with internet access.

## **Angry IP Scanner:**

Angry IP Scanner is a free, lightweight, cross-platform, and open-source tool to scan networks. It helps you to scan a range of IP addresses to find live hosts, open ports, and other relevant information of each and every IP address.

## **Lab Tasks:**

1. Install and launch Angry IP Scanner.
2. Enter the start and endpoint in IP Range.
3. Enter the Hostname. i.e., Name of the device.
4. Optimize the fetchers and preferences settings from Tools section.

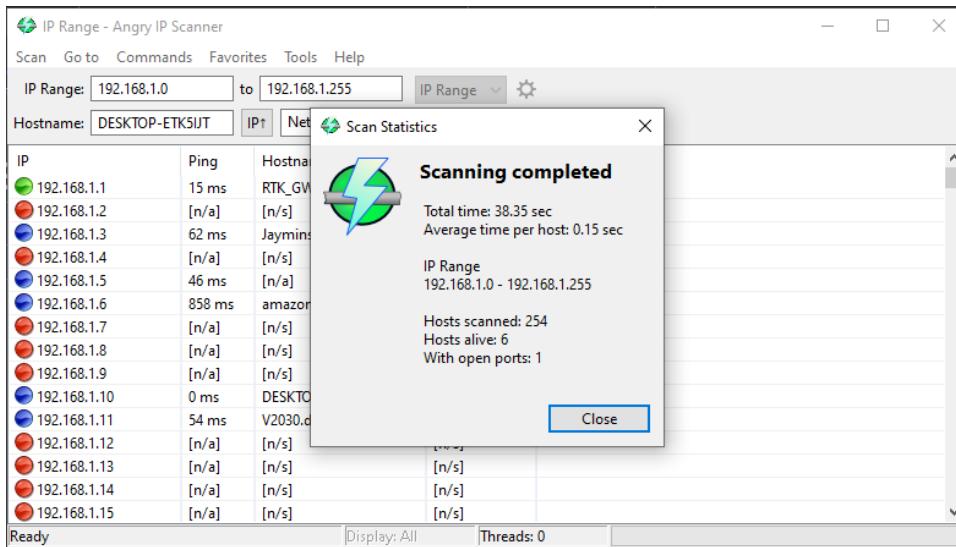
5. Click on "Start".

6. A new window with Scan Statistics appears after scanning.

## **Conclusion:**

We were able to successfully analyze the Angry IP Scanner tool.

## **Output Screenshot**



# **Experiment Number 13**

## **Aim:**

To use and analyze the tool Maltego.

## **Lab Scenario:**

A Windows machine with Maltego installed and with internet access.

## **Maltego:**

Maltego is a comprehensive tool for graphical link analyses that offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable.

With Maltego, you can easily mine data from dispersed sources, automatically merge matching information in one graph, and visually map it to explore your data landscape. Maltego offers the ability to easily connect data and functionalities from diverse sources using Transforms. Via the Transform Hub, you can connect data from over 80 data partners, a variety of public sources (OSINT) as well as your own data.

## **Lab Task:**

1. Open Maltego software after installation.
2. Click "New" from the top left corner to open a new graph.
3. Drag and drop an entity of your choice from the "Entity Pallet" from the left side. (Here we have selected the "Domain" entity.)
4. Now click and right click on the entity in your graph to see various "transforms" that can be applied on the entity to gather the necessary information.
5. Select "All Transforms".
6. Choose any required transforms from the dropdown list to create the remaining data gathering graph.
7. You can change the layout of the graph by selecting from different layout buttons from those available on the left side of the graph.

They are:

- Block Layout
- Hierarchical Layout
- Circular Layout
- Organic Layout

There are 2 types of views for the obtained Maltego graph.

They are:

- Graph View
- List View

8. We have obtained a maltego graph by gathering information for the required entity (here, domain).

## Conclusion:

We have successfully analyzed the tool Maltego

# Output Screenshot

