INTERN REPORT

ETHICAL HACKING & CYBERSECURITY

ABSTRACT

This documentation is brief report of the Ethical Hacking and Cybersecurity internship held by Supraja Technologies (a unit of CHSMRLSS Technologies Pvt. Ltd.), An ISO 9001:2015 Certified Company, at Vijayawada.

mohanaditya sadhanala

Slot16 | #ST2823 | RGUKT NUZVID

--- INDEX ---

Introduction-

In this total intern period, I was taught with CEH V11 content and WAPT content. Starting from the basics of theory in the cybersecurity like CIA traid, virtualization, installation of OS, sorting out the errors and fixing them while installing softwares and different kind of operating systems, types of hackers, active and passive attacks, phases of hacking, zero-day attacks and many more including the practical sessions like scanning, enumerating, performing NMAP script engines and many more, many topics were covered in this internship.

Performing scanning and attacks on dedicated machines gave me some kind of live experience in the ethical hacking stream. I was happily learned ethical hacking with these supraja technologies mentors, as it was passion learning hacking.

Keywords –

HACK - gain unauthorized access to data in a system or computer.

HACKER – a person who perform/conduct the hack.

VULNERABILITY - exposed to the possibility of being attacked/loophole/weakness.

EXPLOIT - to take advantage of a flaw in a computer system.

PAYLOAD - a piece of code, can be malicious or not, used to exploit the vulnerability.

PENETRATION TESTING - is testing a computer system/network or a website/web application to find security vulnerabilities that an attacker could exploit.

PORT - is the starting/ending point of communication of a service. The end can be one side or the other side.

GITHUB - is an online repository where we can save and share the code as the others can see or work with that.

GIT-CLONE - is the technique of cloning the repository from the source to our system. It is just like downloading.

VIRUS - *computer virus* is a type of *computer* program that, when executed, replicates itself by modifying other *computer* programs and inserting its own code which sometimes can restrict the user to do his works by making files inaccessible.

MALWARE - is generally an application in which contains a number of malicious programs.

TROJAN - is a computer virus hidden inside an application or even in a file.

ROOTKIT - is a malicious software that allows an unauthorized user to have privileged access to a computer.

BACKDOOR - is a type of malware which can give access a higher-level access of the system to the hacker bypassing normal authentication methods.

SERVER - a system which serves the services.

CLIENT - a system/receiver who receives the services of another device.

CONCEPTS I'VE LEARNED…

CIA Triad –

CIA Triad is the very fundamental of the cybersecurity realm. It was like a triangle model which describes the organization security policies to protect the organization's data, reputation and provide promising assurance for their users and to guide the information security within that organization.
CIA is basically the acronym for ***CONFDENTIALITY, INTEGRITY*** and ***AVAILABILITY.***

CIA Triad

Types of Hackers –

There is neither good nor bad in terms of hacking. Every hacker performs the hack with some intention in mind. When we consider the corporate realm or society areas, those hacks may affect them differently. To deal with them, accordingly the hackers were classified into certain types - identified by their actions and knowledge in hacking. They are primarily identified as ***WHITE HAT HACKERS, BLACK HAT HACKERS, GREY HAT HACKERS,*** and secondarily ***SCRIPT KIDDIES, GREEN HAT HACKERS, RED HAT HACKERS, BLUE HAT HACKERS, PURPLE HAT HACKERS, STATE SPONSERED HACKERS, HACKTIVISTS, SUICIDE HACKERS*** and ***INSIDERS.***

WHITE HAT HACKERS –

These hackers were supposed to be professional with expertise in cybersecurity, whom were also called as ETHICAL HACKERS. They usually work for organizations. They work with ethics and policies. They seek permissions from the authorized persons before performing the hack. After performing the hack, they make a report over it and submit it to the supposed persons so that they can take actions accordingly.

BLACK HAT HACKERS –

These hackers were equivalently or more talented hackers than the ethical hackers. They usually work with certain kind of intentions which may cause a lot of reputational damage or wealth damage. They never make a concern of any ethics or policies. They won't seek any permissions from the authorized persons before performing the hack. They just breach into the networks or systems or any kind of personal accounts which can be their juice. After performing the hack, they make their tracks clear and generally make them look like they've never entered. Usually, these hackers perform hacks with personal intentions or they were hired for someone else to make their job done. Or they form as groups and work with a sever intention which can get a major loss for a reputed company, but helpful for other side of corporate.

GREY HAT HACKERS –

Grey hat hackers were certainly identified as a blend of both the white hat and the black hat hackers. But fundamentally, grey hat hackers were those who perform hacks with positive intentions but ended up with negative outcome. They might start the work with considering the companies ethics and policies, but meanwhile they might find something large which may bring them a lot of possession so they can turn up to black hats. They seek permissions from the authorities and use them to perform hacks which they should not.

SCRIPT KIDDIES–

This group is considered as the dumbest but violent group of hackers. They're certainly not hackers. They don't have any kind of much knowledge like as the real hackers do, but they perform hacks using the scripts or tools which were written by someone else since they can't make their own. They might not have the complete knowledge on how a tool functions or how a script run in the backend, but they only work for their job to be done. They won't care any hell that might happen further. Their hacks might lead to massive damages but they wouldn't aware of it. They just perform hack using automated tools.

GREEN HAT HACKERS –

Green hats are usually like script kiddies. But unlike script kiddies, they do with a passion to learn. They're also called as noob hackers or neophytes. They're newbies learning hacking with intentions to excel it. So, they learn by performing hacking.

RED HAT HACKERS –

Red hat hackers were considered as different section of people who perform offensive attacks for an organization, where the organization itself hire them or ask them to do so to check their organization's cybersecurity. These red hat hackers are more skilled hackers as their only intention was to break into the system, so they find their own way to enter or break the system or application.

BLUE HAT HACKERS –

Unlike red hat hackers, blue hat hackers were the same level or more skilled person who perform hacks to defend the organizations integrity in its cyber concerns. They defend the attacks performed by the red team within an organization.

PURPLE HAT HACKERS –

These group of hackers generally handle both the offensive and defending sides of cyber concerns. Usually, the organizations hire them to work as a team in which the red hats and bule hats work together for that organization. They perform hacks with their own practical skills on their own vulnerabilities.

STATE SPONSERED HACKERS –

State/Nation sponsored hackers are those who were appointed or hired by the government itself to gain the confidential information of other countries or nations in the view of saving their own country from supposed upcoming threats. These hackers perform hacks to gain confidential information of other countries and they directly report to their respected governments.

HACKTIVISTS –

Hacktivists are that kind of hackers who hack government assets. Hacktivist can be an individual or a bunch of hackers whose intent is to gain access to government websites and networks. They pose themselves as activists, so known as hacktivists.

SUICIDE HACKERS –

Suicide hackers perform hacks which may result in massive property and wealth loss or that might even take up lives of people. They expose themselves after performing hack and they commit suicide instead of getting caught to the police or government law.

INSIDERS –

Insiders were people who work in a certain company and use their authorization to hack and leak/sell the information to the outside or other companies.

Architecture of virtualization –

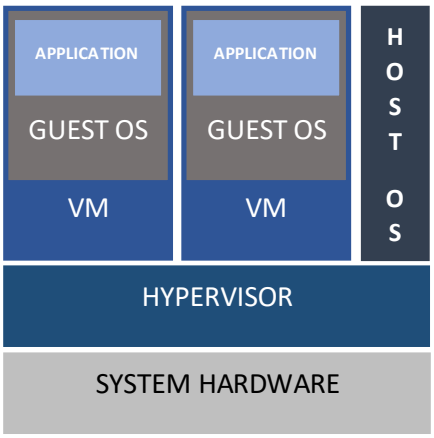
Virtualization architecture model specifies the arrangement of particular components required to deliver a virtual interface rather than a physical interface of physical components like operating systems, storage device, network resources etc.

Hypervisor based virtualization is the most commonly used virtualization method. Hypervisor isolates the operating systems and applications from the underlying computer hardware so the host machine can run multiple virtual machines by sharing the physical hardware resources such as RAM, Storage, Processor cores, Network card.

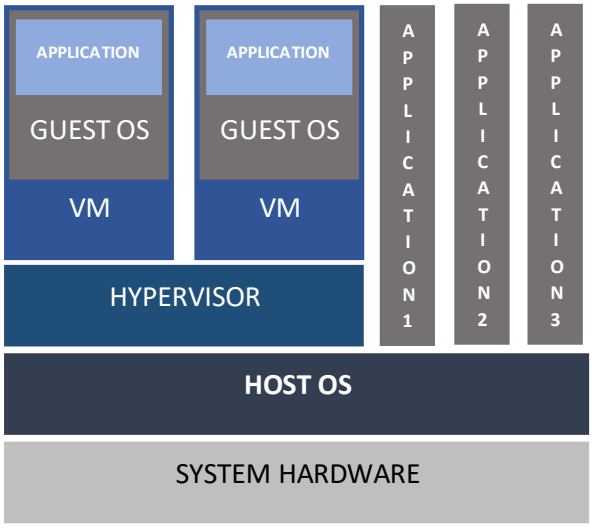
There are two types of hypervisors known as – type1 hypervisor and type2 hypervisor.

type1 Hypervisors runs directly on top of the system hardware. More likely as the host OS, type1 hypervisors offers high availability of hardware resource as their direct access to the hardware provides a better performance and stability. **MICROSOFT HYPER-V** is the most popularly known and used type1 hypervisor.

type2 Hypervisors are the mostly used method of virtualization which is also known as hosted hypervisor. Unlike directly running on the top of the host OS as type1 hypervisor, hosted hypervisor is installed on the top of the host OS. The guest OS or VM runs above the hypervisor. The resources of the hardware can be shared through the hypervisor that is installed on the host OS. Since there is a host OS sitting directly on the system hardware, there will be some limitations to the hardware components in sharing to the VMs/ guest Oss as the host OS consume some of them. **VMWARE WORKSTATION, ORACLE VIRTUALBOX** are the most popularly used type2hypervisor.



type1 Hypervisor



type2 Hypervisor

Active and Passive attacks –

Active attacks are performed with the hacker's active interaction – like intercepting and modifying the data flow which is running lively. In active attacks, the hacker directly participates and gets into the network/the system by making it compromised using his hacking skills. The hacker actively gathers the information and use it to perform the hack on lively running entities. For example, suppose that a hacker intercepts the network and used the intercepted data of the network to gain the credentials of system login/website login which may cause a severe loss to the authorized ones (dependently hacker's intention).

Passive attacks are performed with the hacker's passive/physical engagement. The hacker might keep himself into the scenario to gather the information and even perform the attack directly on the hardware at the same time. For example, suppose a hacker intentionally entered an office that which was his target and he found a system there without any person nearby, he then bypassed the credentials and entered the system directly and he uses a *BAD-USB* or a *MALICIOUS FLASHDRIVE/PENDRIVE or a SPECIALLY DESIGNED DRIVE WHICH CAN AUTOMATICALLY UPLOAD THE PAYLOADS AND INSTALL TROJANS/ROOTKITS/BACKDOORS (IN FAVOUR TO THE HACKER)* to upload a backdoor to create a persistent connection for further actions.

Phases of hacking –

A hack is performed in a particular way according to the expected result. To make sure the outcome in an expected manner, the hack should be performed using a proper technique and follow the proper methodology. To describe this methodology, we derive it into certain phases. There are 5 main phases of hacking (any kind). The hacker performs the hack according to these phases to achieve the supposed result. The five phases are ***RECONNAISSANCE, SCANNING, GAINING ACCESS, MAINTAING ACCESS*** and ***CLEARING TRACKS.***

RECONNAISSANCE –

Reconnaissance is the first step of the hacking. Usually, it is also called as **INFORMATION GATHERING** or **FOOTPRINTING**. This is the phase where any kind of hacker uses his utmost techniques to collect required/ all the possible information available about his target. The information gathering can be done actively or passively according to the hacker's feasibility.

SCANNING –

Scanning is the further step for a hacker after performing information gathering. In this phase, the hacker scans the network/system to find the vulnerabilities by using which he can enter into the network/system. Generally, the hacker scans for the ports and vulnerabilities which can be exploited. After performing the scanning, the hacker usually enumerates the things he noticed while scanning so that they can help him in further phases.

GAINING ACCESS –

Gaining access is the profound and actual phase of the hacking. The hacker exploits the vulnerabilities that he found by performing scanning. He might various techniques to get into the network/system the he trying to hack. Many hackers mostly use the tools to create the payloads and get a session with the targeted device. Some hackers write the payload on their own and send them directly or indirectly to the victim and waits until the victim to fall in the trap. Even though there are several tools which can help hackers to get their job done, but ***METASPLOIT*** is the ultimate tool for many hackers which fulfil their requirement in this phase. Many noobs might directly get into this step without completely performing the previous phases, which results them to fail in the process.

MAINTAINING ACCESS –

After gaining the access of the system/network of the victim, the hacker needs to have a persistent back connection with him to continue the communication with that device if he needed to. Usually, the hacker might

create a backdoor payload and upload it to the victim's system and the backdoors do their job afterward. They create a persistent connection between the hacker's machine and the victim's machine so that even the victim turns off/ shut the system down, the hacker has a way back connection quite after the victim turn his system on again. Generally, the backdoors can be in the form of rootkits, trojans or other malicious files. This is the optional phase for many hackers as not all wants to have a back connection with the victim according to the hack they perform.

CLEARING TRACKS –

This is the final phase of the hacking methodology. In this phase the hacker ensures to destroy all the evidence about his entry to exits observation. The systems/devices record logs of the actions happening within their network or within their connections. Almost any kind of action would be recorder in the logs. Since the hackers doesn't want themselves get caught, they try to clear all those logs which have been recorded after their arrival. They can modify the logs, alter them, or corrupt them so that they can't be readable (by the machine or by the human), or delete them so they can't be accessible further.

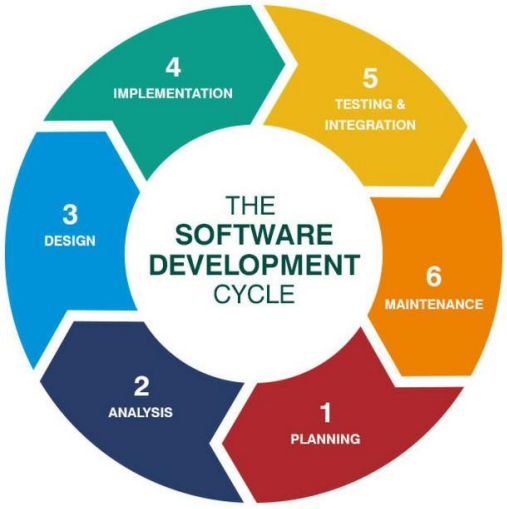
Clearing tracks is the final steps for the hackers, but most of the ethical hackers have nothing to do with this phase since they have the permissions and authority to enter. And for ethical hackers, they have to make a report mentioning all actions throughout the process, vulnerabilities found and other things and submit to the authorized persons.

Zero-day attacks –

A vulnerability which was not patched from the day the code was developed is a zero-day vulnerability. Exploiting such kind of vulnerabilities is known as zero-day attacks. These vulnerabilities are commonly created by the code developer and wasn't noticed by any one until exploited by some hacker.

Software Development Lifecycle (SDLC) –

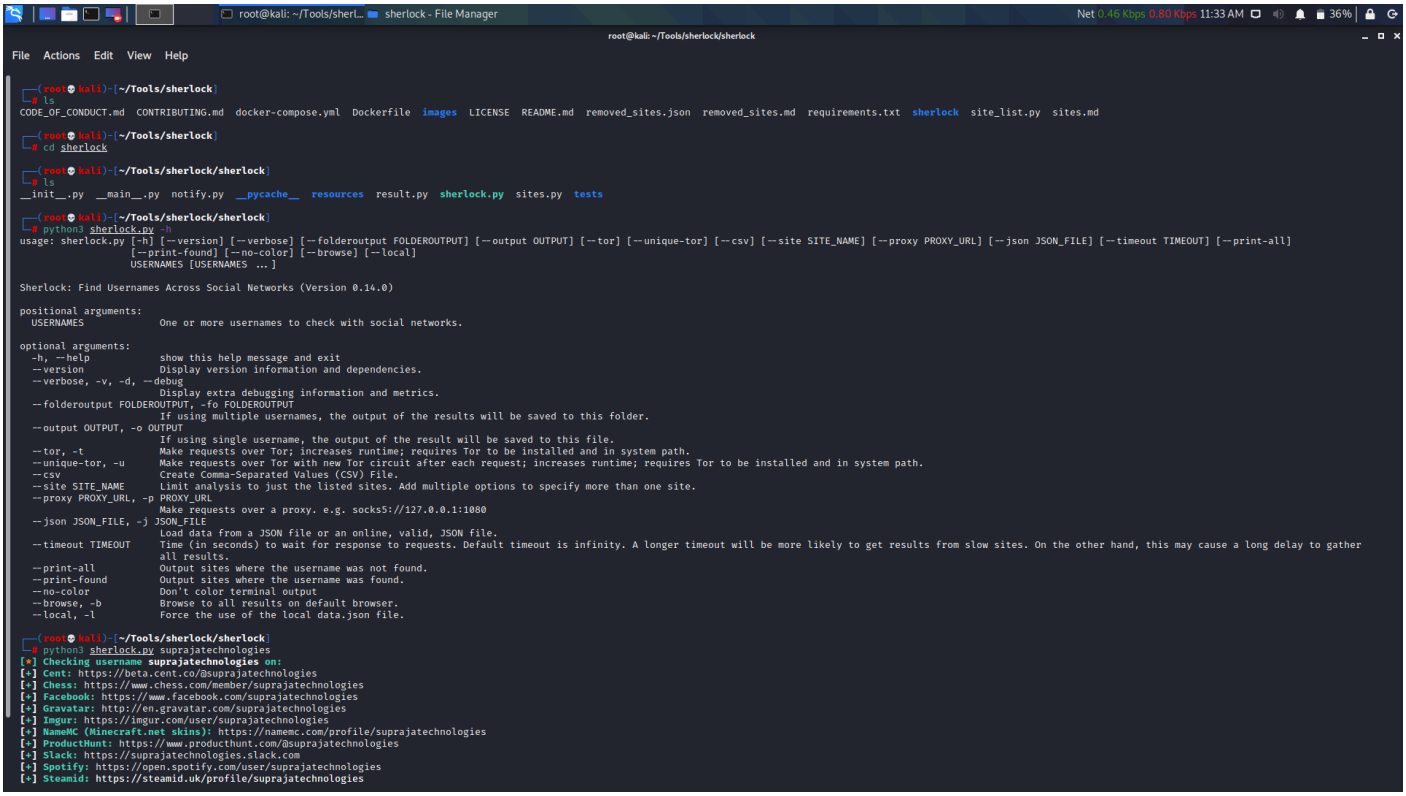
Software development life cycle is a process used by the software industries to develop good quality softwares. The process includes planning, analysis, design, implementation, testing & debugging, and maintenance.



Software Development Lifecycle

Sherlock –

Sherlock is a reconnaissance tool to hunt the social media accounts by usernames across social networks. The tool is directly available on the github (github.com/sherlock-project/sherlock) or the webpage (sherlock-project.github.io). Since this is a github project, we have to clone the git repository to download the tool. After installing the requirements with pip, we can run the tool using python3 since the tool was developed in python3.



Sherlock-POC-1

Sherlock-POC-2

Types of networks –

When a computer or a group of computers connected to the server/datacentre/network device/ISP, a network is formed between them. Interconnection of two or more computers forms a computer network. When a computer is connected to network/computer network, data transmission will happen between them. These computers or servers or other devices which were connected to a network will follow some set of protocols to transmit the data or to share the resources. According the network formed in between the devices, they are classified into different types networks. There are several classifications of networks, including mainly ***PAN, LAN, WLAN, MAN, WAN, VLAN.***

PERSONAL AREA NETWORK (PAN) –

Personal Area Network is the most basic type of network in which hardly only two or three devices connected together. **BLUETOOTH** is the best example for personal area network.

LOCAL AREA NETWORK (LAN) –

Local Area Network is the simplest and most original and common type of network. In LAN type of network certain number of computers or devices were connected together which were in shorter distances like offices, colleges, or larger building etc. The connections in this type of network were made using ethernet cables.

WIRELESS LOCAL AREA NETWORK (WLAN) –

Wireless Local Area Network is the same kind as LAN but with Wireless Tech. In WLAN, Wi-Fi and Access points were used.

METROPOLITAN AREA NETWORK (MAN) –

Metropolitan Area Network is the just like the LAN, but for larger areas like cities and towns.

WIDE AREA NETWORK (WAN) –

Wide Area Network is the largest network where a larger number of devices get connected together. **INTERNET/WORLD WIDE WEB** is the best example for WAN type.

VIRTUAL LOCAL AREA NETWORK (VLAN) –

Virtual Local Area Network is the customized network – created from one or more local area networks.

Types of network devices –

There are certain devices which are specially designed and dedicated to the manage the data sharing by forming network. Such devices are called as network devices. ***HUB, SWITCH, ROUTER*** are the three types of network devices.

HUB –

Hub – which is also called known as repeater and sometimes called as dumb – is the most basic and simplest network device. Hub helps two or more computers to connect together by using ethernet cables and share the data among them. Hub can not identify and share the data to a particular device/computer that is connected in the network. Hub just shares/repeats the data among the network of computers which can be accessed by any computer on that network which is connected to that hub. Hubs are less used these days.

SWITCH –

Switch is multiport network device which functions more a way intelligent than the hub. Switch shares the data among the network according the computers connected among the network. Switch uses MAC addresses of the systems that are connected to it and share the data by reading the data packets and then to the computers which were authorized to access the data. Switches are more secure than hubs.

ROUTER –

Router is a general-purpose networking device that interconnects two or more different networks and is considered as more intelligent networking device since it transmits the data to the devices that are in the network by using more specified routing/data-sharing methods. Routers establishes the communication by maintaining tables about destinations and local connections. A router contains the information about the systems connected to it. Routers are also used to divide internal networks into two or more subnetworks. Router is so important when you want to get access to the internet as you have to get the connection from ISP. Routers are most secure networking devices as they can provide firewalls for the network.

Intranet, Extranet, Internet –

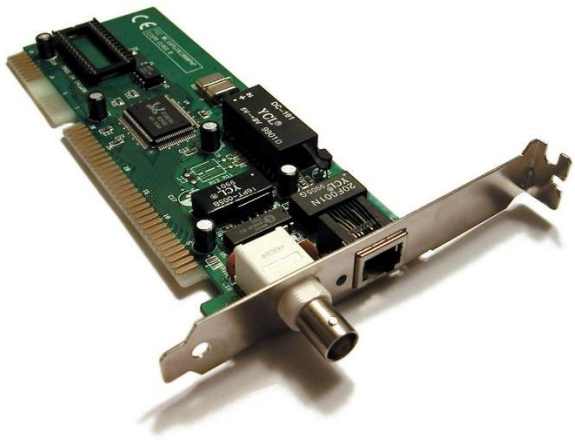
Intranet is a local network. Intranet is only available to those who were inside the local network. The devices which were connected to the local network can only access the data inside the intranet. No other device which is an outer for this local network couldn't make a connection with the devices inside the intranet or access the data which is shared in the intranet. Certainly, Organizations, Colleges, Universities, Research centres, Companies with sensitive data, larger libraries, commercial buildings use intranet to share the data within their entities.

Extranet is also the local network where a certain amount of authorization or permission is allowed to the other users which are outside from the local network. Some files are shared to the certain people/devices using extranet.

Internet is the larger network where anyone can access anything within this network if they have an access/permission to that data which is being accessed. **WORLD WIDE WEB (WWW)** is the best example for internet.

Network Interface Controller card (NIC card) –

Network Interface Controller card is a hardware – which is quietly required to provide the system a network interface by using which the system can further connect to different networks. NIC card is mostly available on any device that can be connected to a network. A special address called **HARDWARE ADDRESS** which is recognised as **MAC ADDRESS** is provided and explicitly printed on the NIC card. Every NIC card has its own and unique MAC address, which is used to identify the system particular when connected to some network.



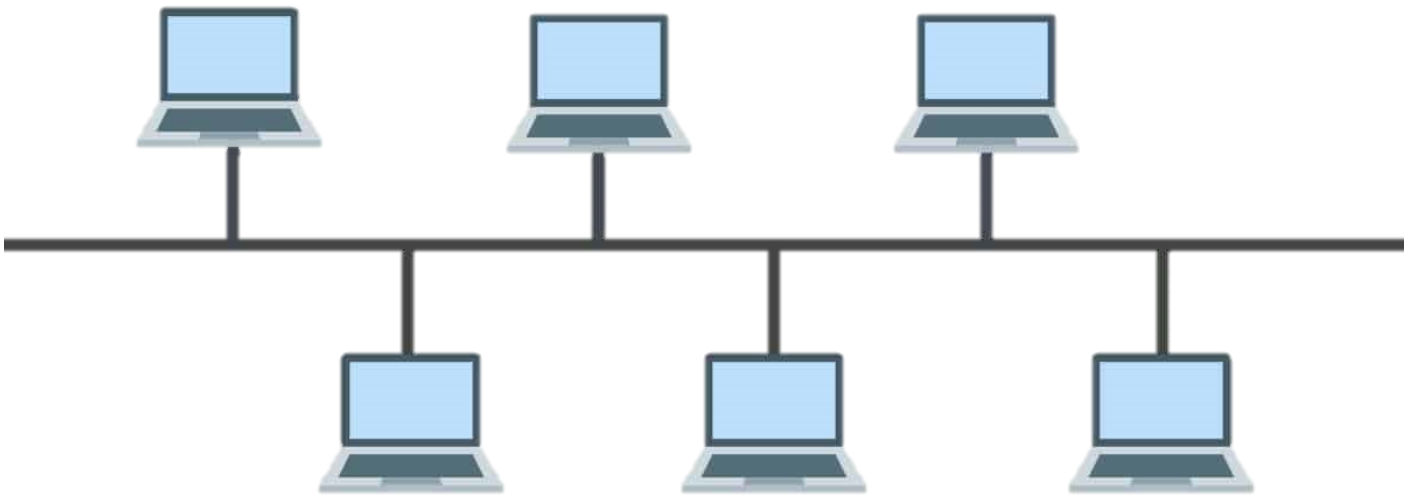
Network Interface Controller card

Network Topologies –

It would be a lot messier when groups of computers connected to the network. To avoid that mess, computers and other network devices were connected in a certain manner which we call them as different topologies of networks. There are various types of network topologies primarily including ***BUS TOPOLOGY, RING TOPOLOGY, STAR TOPOLOGY, MESH TOPOLOGY, TREE TOPOLOGY,*** and ***HYBRID TOPOLOGY,*** and WIRELESS NETWORK TOPOLOGIES including ***AD HOC*** and ***WIRELESS MESH.***

BUS TOPOLOGY –

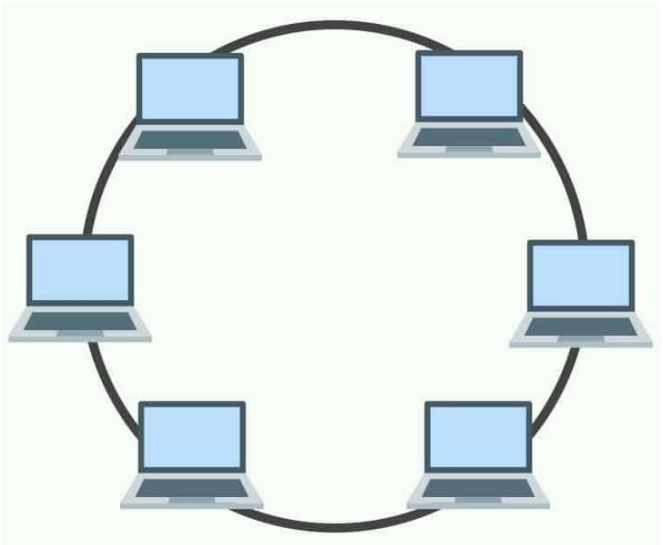
A bus network is network topology which is mostly used in LANs where all the systems/devices connected together using a single coaxial cable (called as backbone). This network topology is simplest and is better choice when there are only limited number of computers. But if the backbone gets damaged/ brake, then there will be no communication happens between the devices connected. And this is less secure form of network communication as the first system sends a message to the last system, it has to pass through all the system in-between. So, there might be a chance to the data getting intercepted. Bus topology is a less suggested topology until it better fits the scenario.



BUS TOPOLOGY

RING TOPOLOGY –

Ring topology is most similar to the bus topology and the only difference is it is in the form of a ring/circle. The data transfer happens the same way as bus topology but the major difference is ring topology provides only a one-way data transfer – either clockwise or anti clockwise.

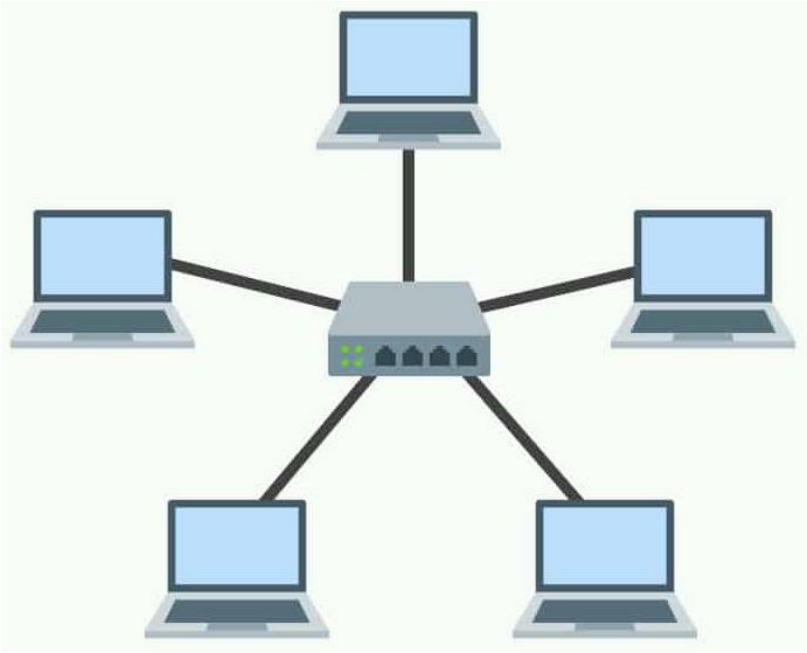


RING TOPOLOGY

STAR TOPOLOGY –

A switch/hub is placed as central device and all the other device/computers (generally referred here as nodes) were connected to that central device. Every device in the network is directly connected to the central device

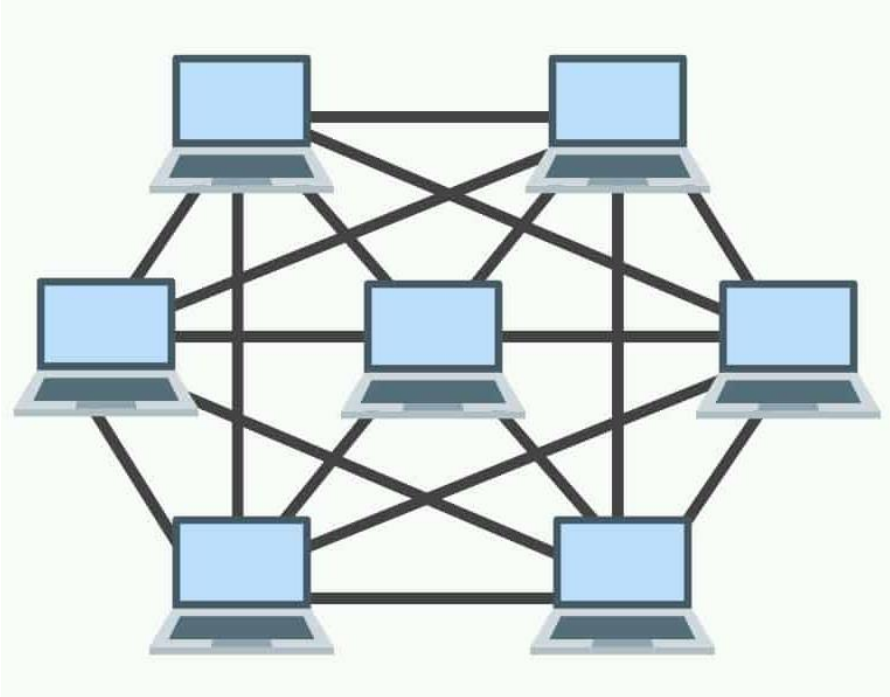
and was indirectly connected with the other via the central device. When a system sends the data to another system, the data first received by the central device and then shared to the destination by central device. This adds a security layer in sharing the data rather than sharing the data all the system in some cases as discussed above. But the major disadvantage is if the central device gets damaged or get down, the entire communication in that network fails.



STAR TOPOLOGY

MESH TOPOLOGY –

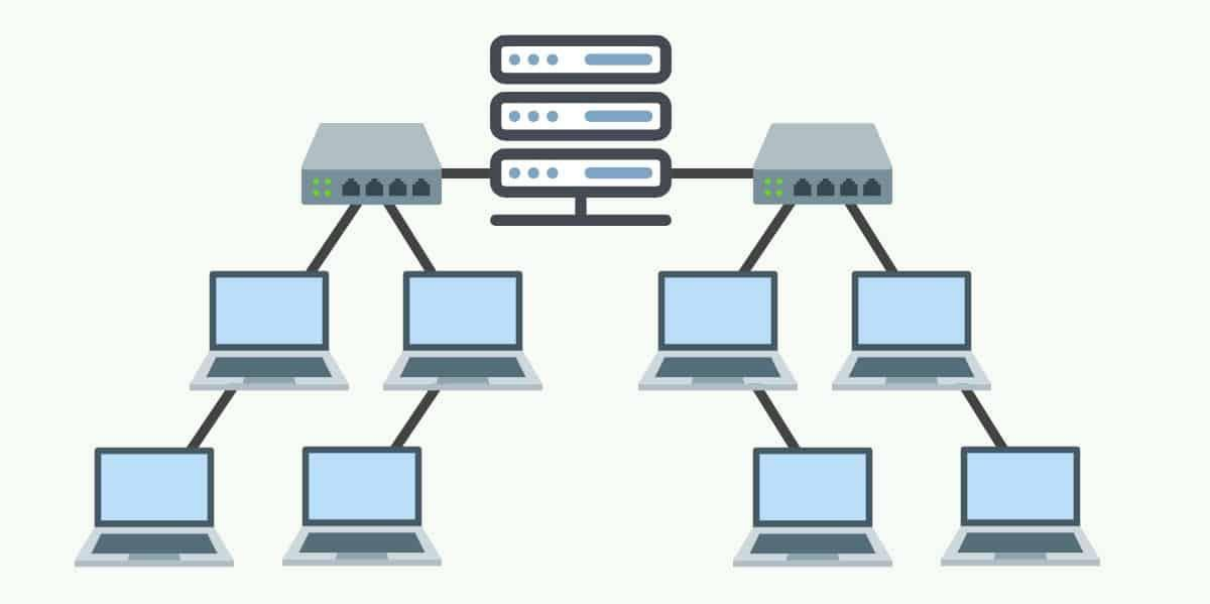
In mesh topology, each and every node is connected with each other node in the network. Every system is connected directly to the other network. Data transmission happens faster in this network topology since there is no much data traffic as the systems connected together directly. But the cost factor to implement this is high and maintenance of this type of network would be difficult than others.



MESH TOPOLOGY

TREE TOPOLOGY –

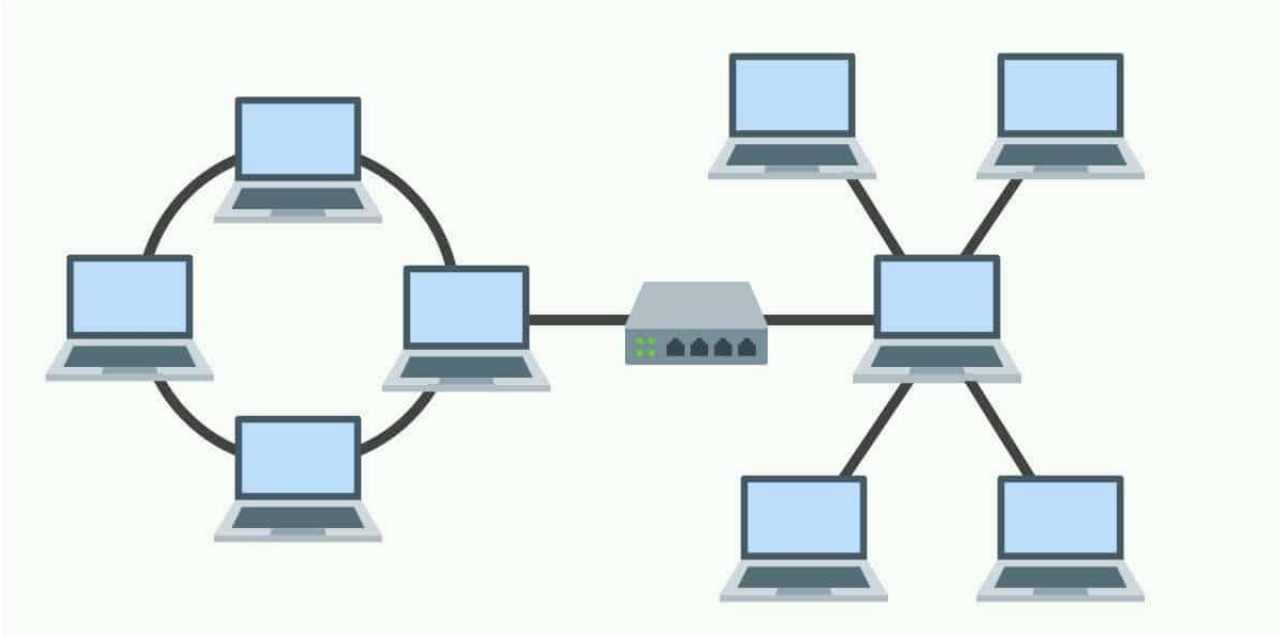
Tree topology network is structured as just like the tree with its branches. There is a root node which is connected to other nodes by forming hierarchy as parent-child, where there is only one individual connection with parent to every child. Tree topology is the best practice for implementation in larger commercial areas and organizations.



TREE TOPOLOGY

HYBRID TOPOLOGY –

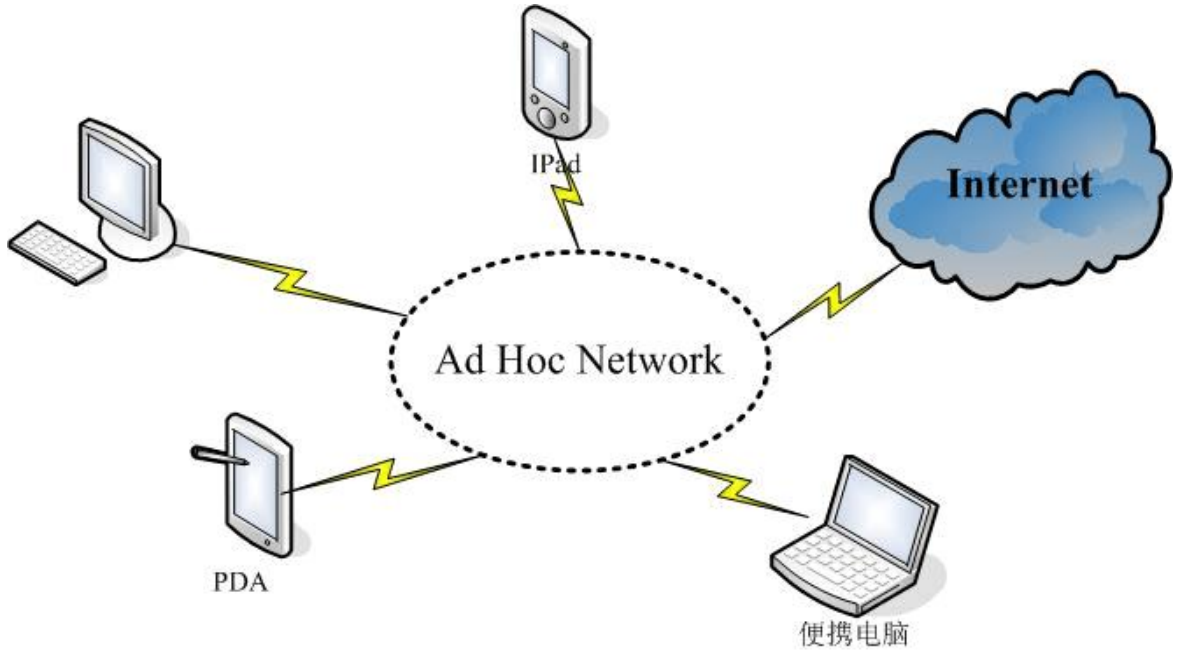
Hybrid topology is composed of two or more different topologies. Hybrid topologies are most suitable for larger companies. The handling and maintaining the hybrid topology is a way more flexible than other topologies even the security concerns included. It might be difficult to implement this might costs a way more than any other topology. The main factor in this hybrid topology is it is scalable, thus it more suitable for larger networks in complex buildings.



HYBRID TOPOLOGY

ADHOC NETWORK –

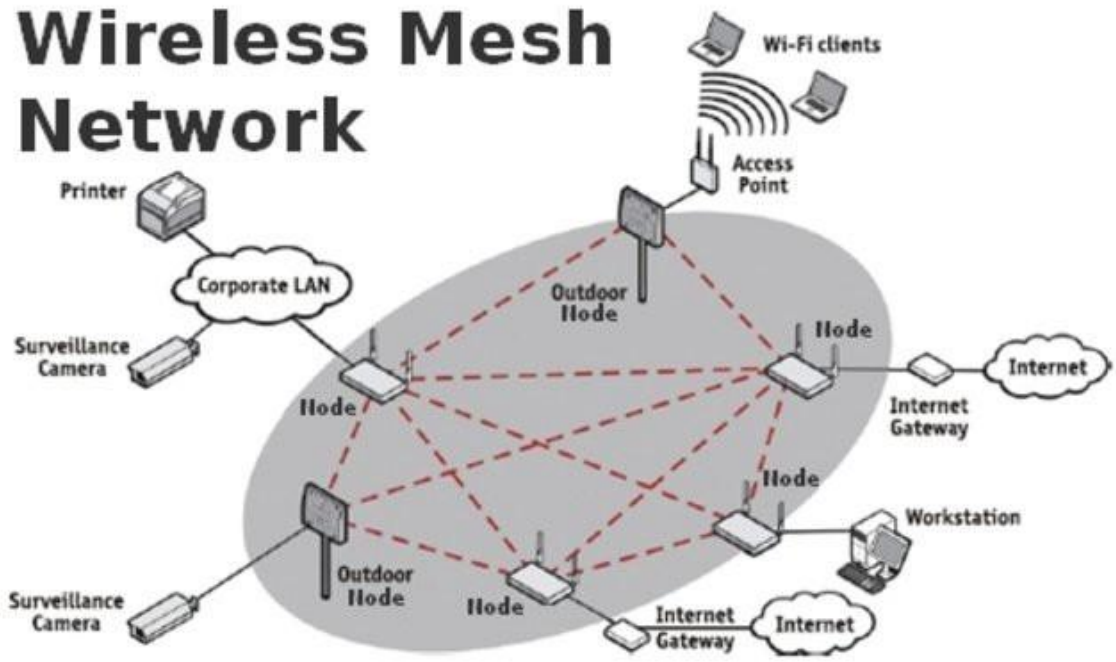
AD HOC networks are mostly considered as wireless local area networks. In this type of networks one particular device serves as host and the devices connect to the host to establish communication in that network. MOBILE HOTSPOTS are the best examples for AD HOC network.



AD HOC NETWORK

WIRELESS MESH NETWORK –

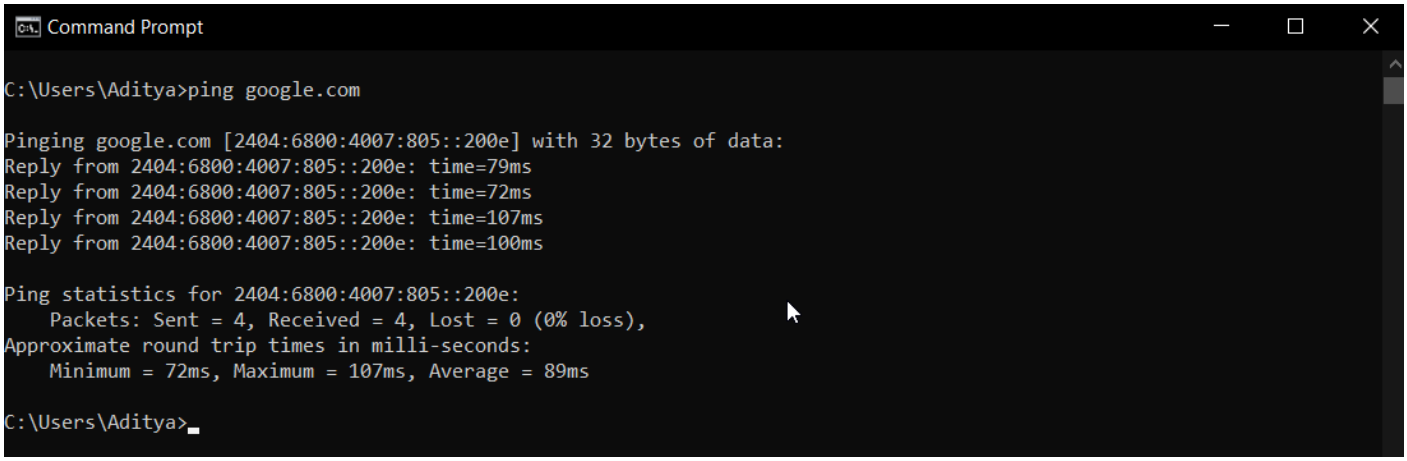
Wireless mesh network is more likely to a mesh network topology but here the data is transmitted wirelessly. Here the nodes are connected and is accessed wirelessly with other nodes as shown in the below figure.



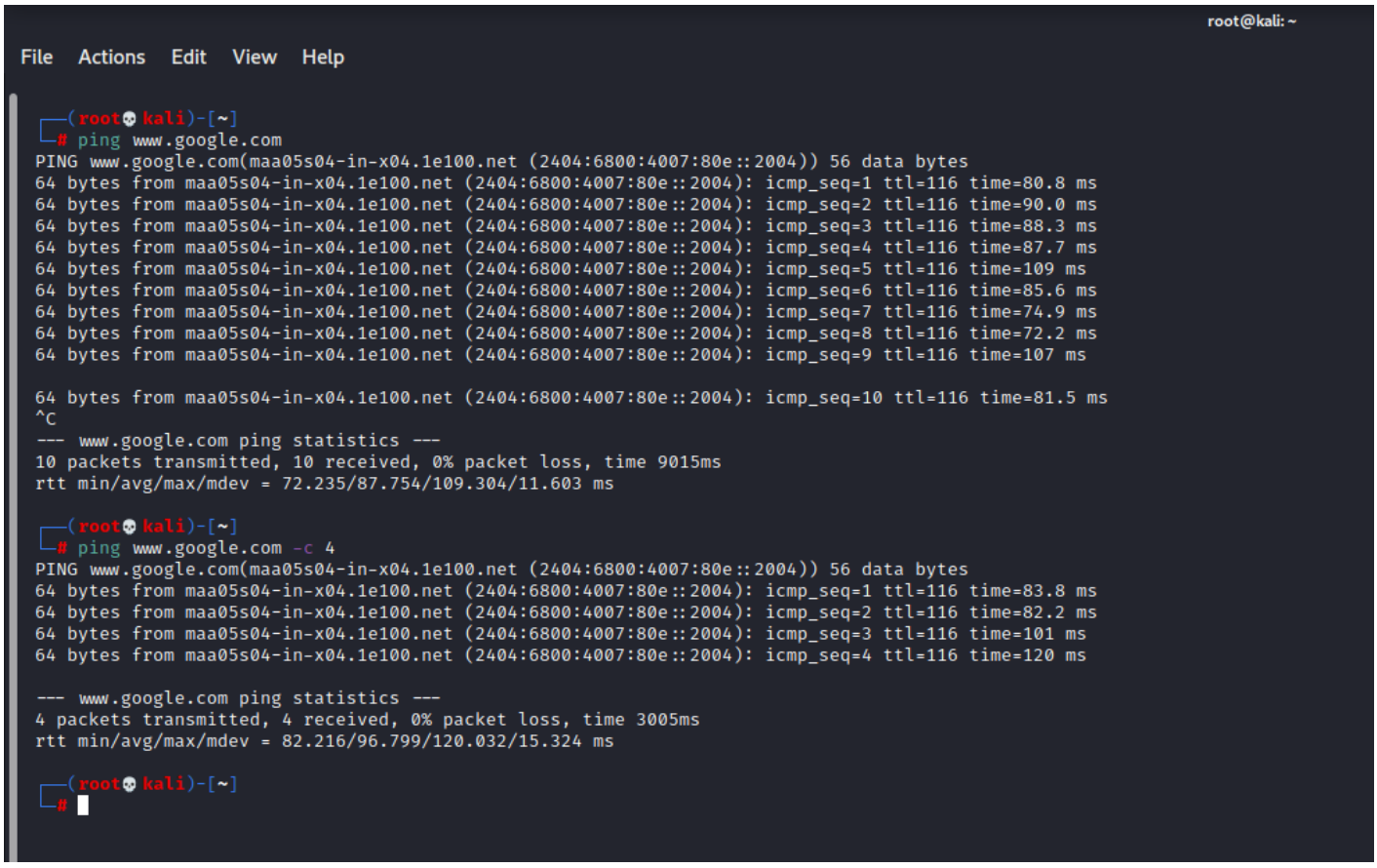
WIRELESS MESH NETWORK

Ping & Tracert/Traceroute commands –

PING is the basic command used to ping an IP or a host address. Ping command is mostly used to find whether the host is dead or alive, or to find the latency between the host and our machine. Ping command first converts the host address to IP address and the sends the data packets to the IP. If the host address is alive, the packets sent were sent to back to our system and it calculates the time between this process which is also called as latency.

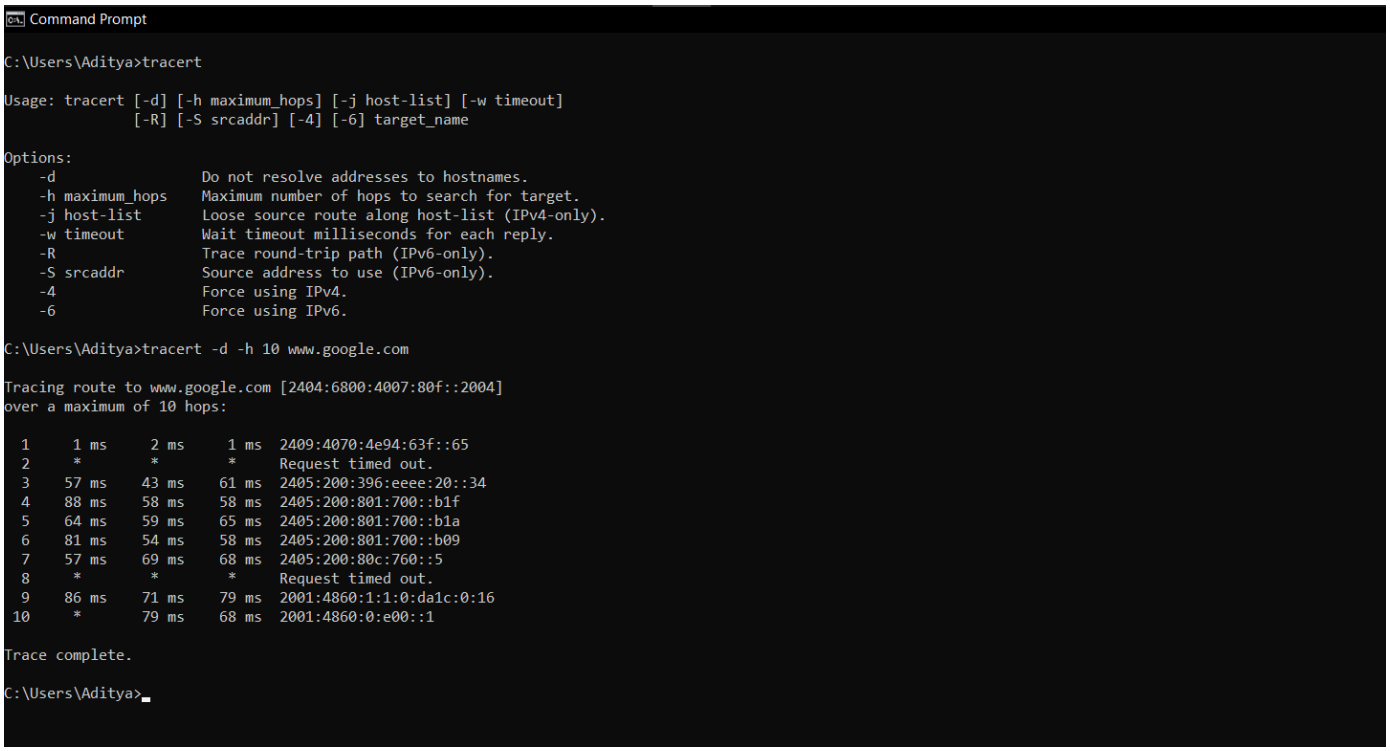


PING-POC-WINDOWS

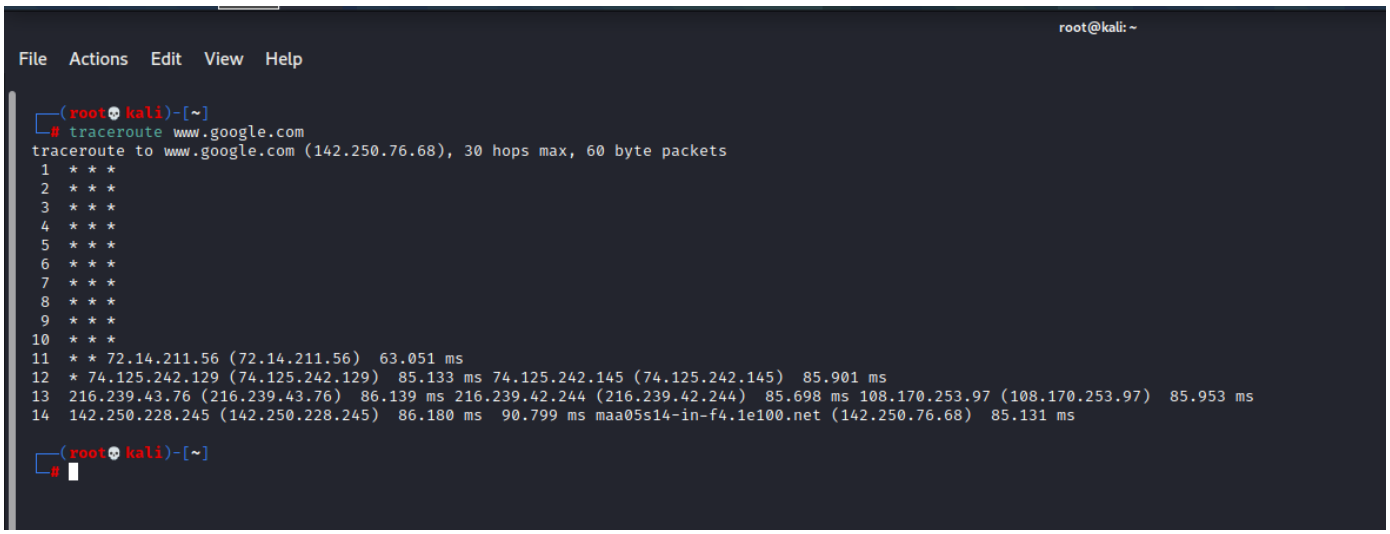


PING-POC-KALI LINUX

TRACEROUTE (in Linux) and **tracert** (in Windows) is the command used to find the route that the data transfer from our machine to the destination address. We can find the number of hops, latency, and route/path that the data is being transferred to reach destination by running this command. Tracert command also works just like the ping, but it sends the data packets to the hops first and then follows the path to destination/host address. For every hop, it sends three different kinds of data packets which resembles for different identifications and calculate the latency for that hop.



TRACERT-WINDOWS

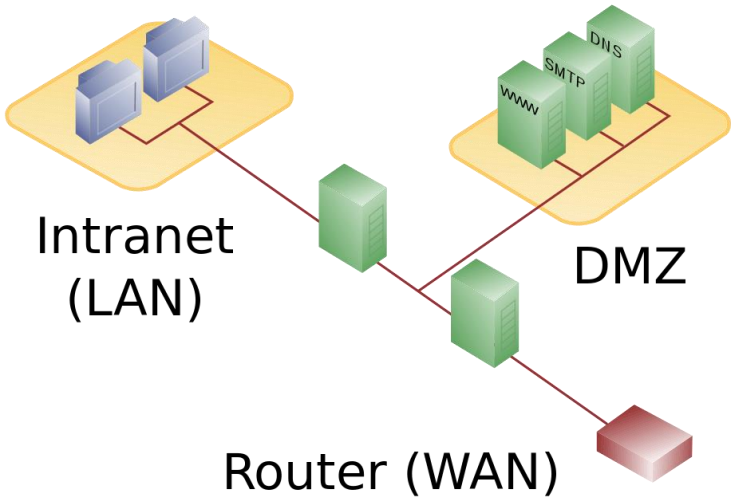


TRACEROUTE-POC-KALI LINUX

(The stars symbols represent to the request timeout)

Demilitarized zone (DMZ) –

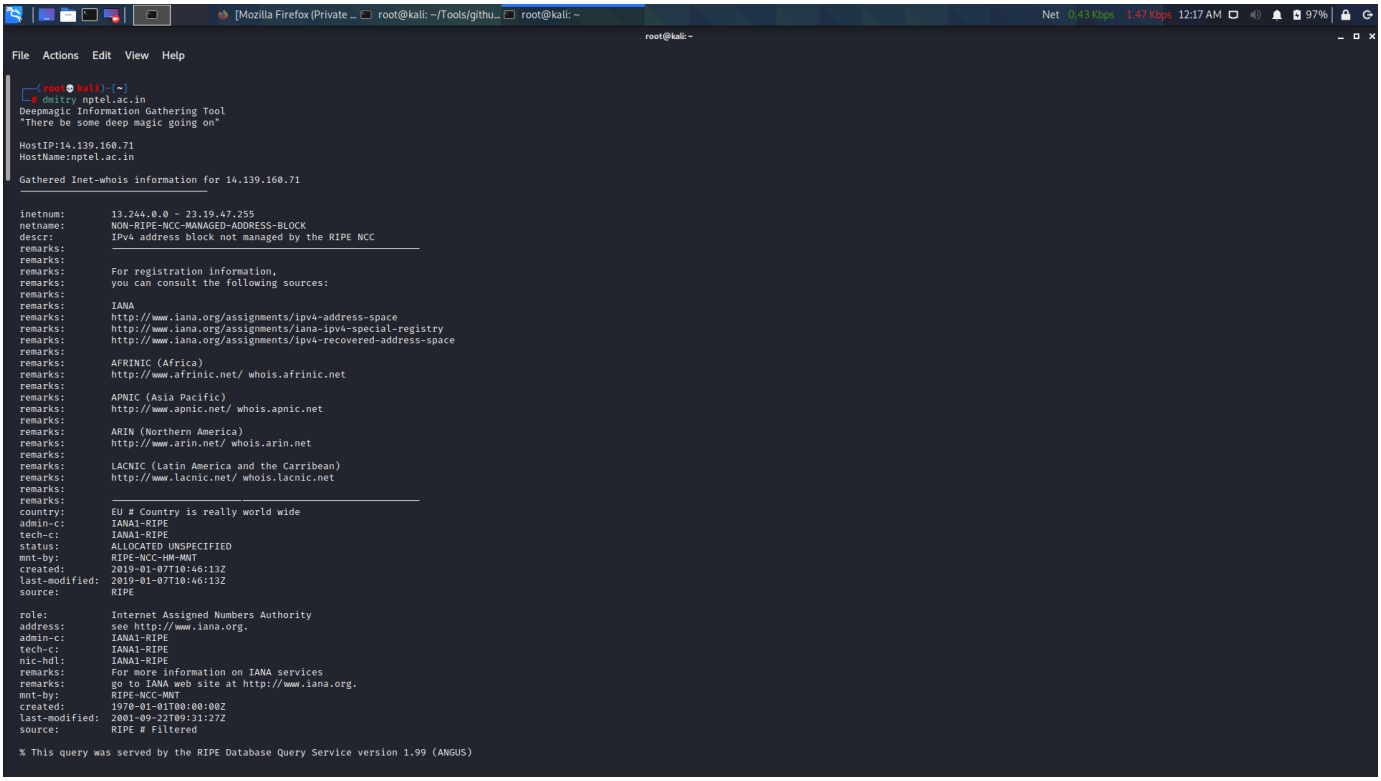
Demilitarized zone is referred to the servers of an organization which are outside the militarized zone (which is protected by the dedicated firewalls). In the network architecture, certain types of servers were supposed to be accessed by users and other servers which were not supposed to accessed by the users or any others expect the authorities were protected with dedicated external firewalls. The servers which are outside to the firewall protection and can be accessed by the users was called as DEMILITARIZED ZONE (DMZ).



DEMILITARIZED ZONE

Dmitry tool –

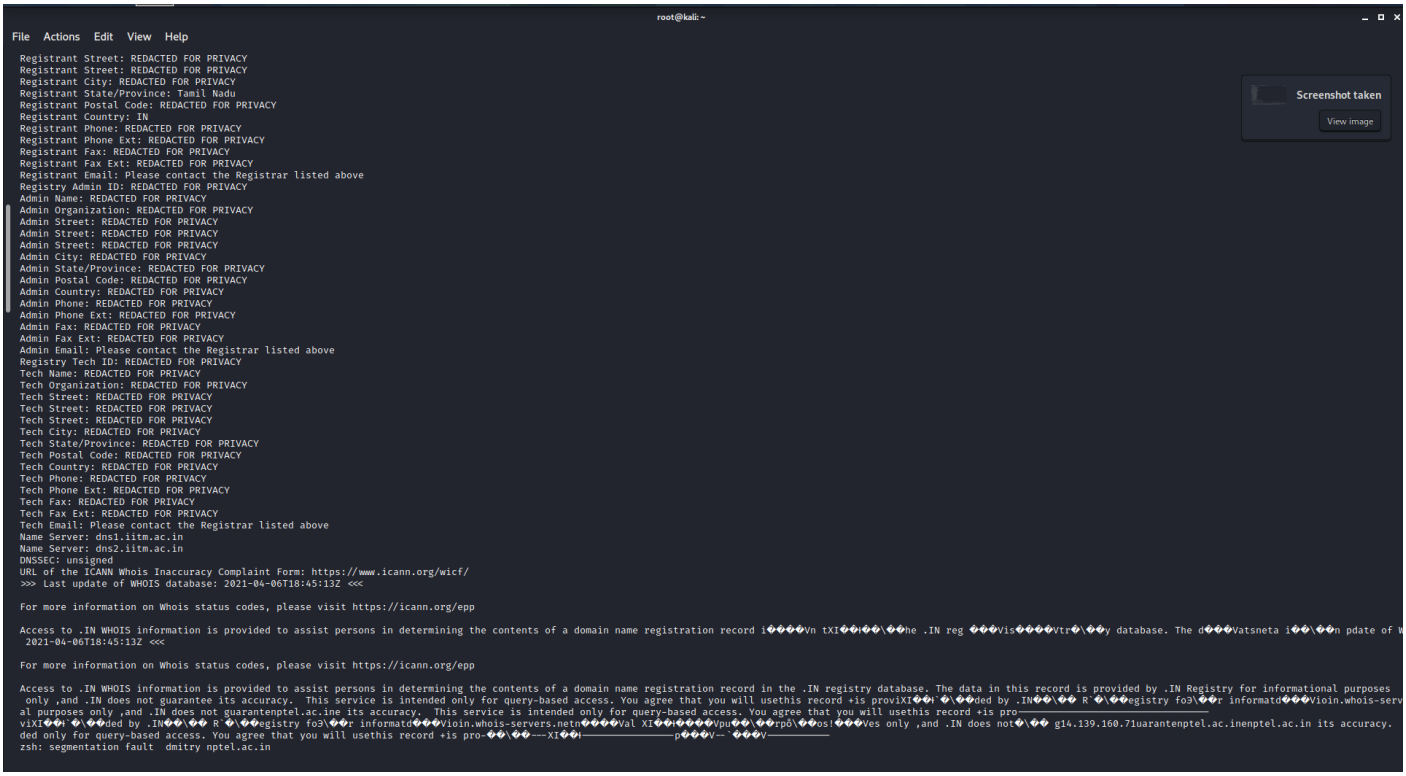
Deep magic information gathering (DMITRY) tool is a command line utility in Kali Linux which comes inbuilt. Dmitry is developed to get the public information about any target host. It collects the Who Is lookup information, DNS information, email addresses, subdomains, TCP port scans.



```
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~]
└─# dmitry nptel.ac.in
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:14.139.160.71
HostName:nptel.ac.in

Gathered Inet-whois information for 14.139.160.71
---------------------------------

inetnum:        13.244.0.0 - 23.19.47.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        -----------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        -----------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2019-01-07T10:46:13Z
last-modified:  2019-01-07T10:46:13Z
source:         RIPE

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.99 (ANGUS)
```

DMITRY-POC-1

DMITRY-POC-2



DMITRY-POC-3

Open-Source Intelligence (OSINT) –

Open-Source Intelligence – simply referred as OSINT is a methodology that is used to collect and analyse the data of any target that is publicly available on the internet. OSINT involves many methods, techniques and also tools to get the job done more accurately.
OSINT Framework is a framework developed to provide the more accurate information about the target using free resources and free tools.

There are many tools to collect/gather the information of any target. But certain targets were focussed to certain industries. So, to gather more accurate information about such kind of targets we have to use the supposed tools for that operation.
MALTEGO, RECON-NG, THEHARVESTER, SHODAN, SEARCHCODE are the mostly used tools for OSINT.

Banner grabbing –

Banner grabbing is technique used to find the information about a computer or a device that is connected to network and the information open about the ports and services running on those ports. ***NCAT, NETCAT, TELNET*** are some tools used to gain such information.

HTTP & HTTPS & SSL & TLS –

Hyper Text Transfer Protocol (HTTP) is a protocol which is used to send the web pages through the internet. This protocol is developed to form communication between the browsers and servers. HTTP runs on port number 80 which is specially dedicated for that service.

Hyper Text Transfer Protocol Secured (HTTPS) is developed as an extension to the HTTP to make the communications between browsers and servers in a secure way, so that the data can not be intercepted in between. The secured authorization for websites is given by a digital certificate which is also known as SSL certificate.

Secure Socket Layer (SSL) is a protocol which establishes a trust factor by implements authorization and providing encryption to the data/data-packets, making them more secure and trustable to send through the website. SSL also have version in it by increasing security factors. SSL 1.0, SSL 2.0, SSL 3.0 are the versions till now.

Transport Layer Security (TLS) is brought up like an extension to the SSL by including cryptographic techniques which provide more security and authenticity. TLS also have versions in it just like SSL. TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 are the version till now.

Subdomain hunting –

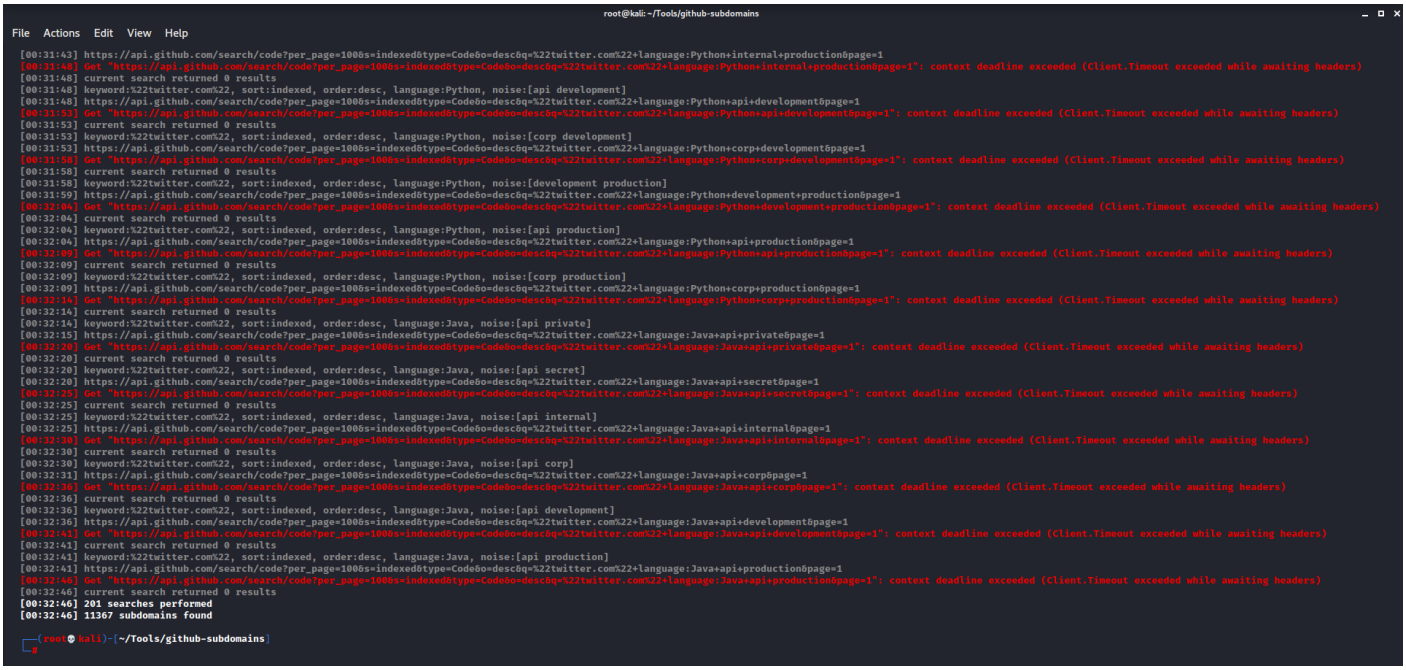
Subdomain hunting is an important part of website penetration testing or web hacking. We can't find bugs always on the main pages only. Sometimes the bugs were left unchecked in some subdomains of the website which is juice for hacker as he can use the bug in them and exploit the website further. There are several tools to hunt/find the subdomains but ***SUBLIST3R, GITHUB-SUBDOMAINS, THEHARVESTER*** are popularly used.

GitHub-subdomains –

GitHub-subdomains is subdomain hunter tool which is very much powerful as it seeks all the pages that are available entirely on the GitHub by fetching them and finds the subdomains for a given target host. To access the github pages, it needs github tokens. We can generate them in GitHub for free. It is possible to fetch more subdomains if we have more tokens as it will fetch all the pages on github. The tokens can't be used immediately after we use them once before. The tool is directly available on GitHub as github.com/gwen001/github-subdomains. After cloning the repository install it using go or manually. Generally, this task takes some more time than usual tools but provides the best results than other.

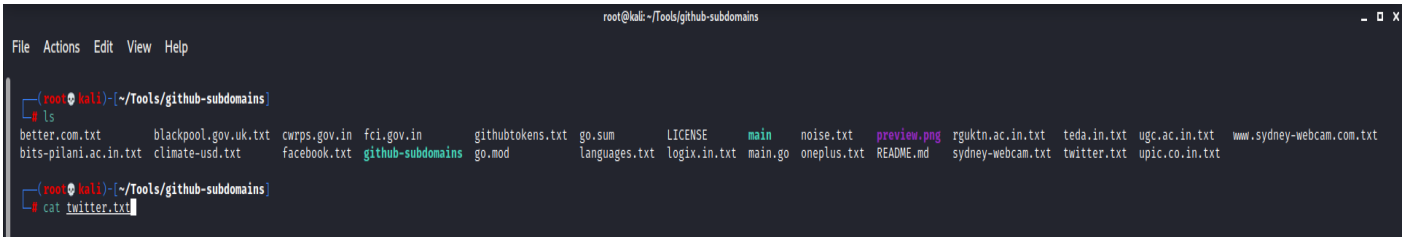
github-subdomains-POC-1

(the syntax and the tokens were just used to produce the result shown below)



github-sudomains-POC-2

(POC showing that the large number of subdomains were found)



github-sudomains-POC-3

(Reading the fetched subdomains which are saved in the output file given in the syntax command)

github-sudomains-POC-4

(Sample of subdomains found after performing the command in github-subdomains tool)

Internet Protocol (IP) –

Generally, IP is referred as an address which is mostly a set of numbers in the format XXX.XXX.XXX.XXX or XXXX.XXXX.XXXX.XXXX.XXXX.XXXX.XXXX.XXXX where each X represents a number or hexadecimal character. But fundamentally Internet protocol is the principle of communicating protocols which governs the data that is sent through the internet or any local network. Those IP addresses are used to identify the systems which are connected to the network.

Every device which is connected to the internet will contain its own IP address which is assigned by the router. They were assigned similarly when the systems get connected to the same network and they might assign differently when connected to different networks. Every system gets two kinds of IP addresses knowns PUBLIC IP ADDRESS – where it is used to make communication with outer network devices than within the network, and PRIVATE IP ADDRESS – which is used to make communication between other devices within the network.

There are 2 versions of IP address. They are **IPV4** (IP version 4), and **IPV6** (IP version 6). IPV4 address are of 32bits long and IPV6 addresses are of 128bits long. By assigning unique IP address for every system on the internet using IP version 4 can be satisfied up to 4,294,967,296 devices (approximately 4 billion). But as the internet usage get increased these days, there are a greater number of devices online more than 4billion. The version 4 IP address assigning method can't fulfil the entire devices that are on the internet. To overcome this, IETF has developed and introduced the version 6 IP addresses (2^128) method which cannot be exhausted or ran out of IP addresses as version 4.

These IP addresses are user friendly and readable for humans but not for computers as they only understand binary. So these IP addresses gets converted from numbers and hexes to binary using certain method of conversions. IPV4 uses 8-bit Octet Chart to convert the decimal to binary, and IPV6 uses the 4-bit Hexadecimal Chart to convert the hexadecimals to binary.

When dealing/studying more IP address it would be a lot more difficult to sort. To make it simple and understandable, all the IPV4 addresses are classified into different classes as shown below.

Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental
Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback testing.		

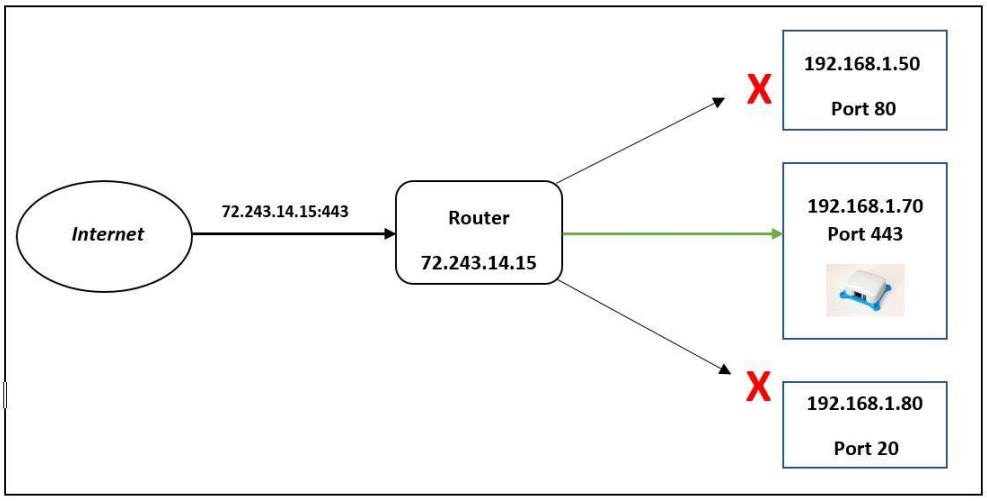
IP CLASSES

IP sharing –

IP sharing is the method in which the same public IP was provided to all the devices that are connected to the network. Single public IP is assigned to every system in the network. Even though the private IPs were different for every system, the data sharing must be done using port forwarding methods.

Port forwarding –

Port forwarding is a method in networking that allows users to use services/computers that are in private networks to connect over the internet with other private or public computers. The IPs are assigned with certain port numbers to open/run the service on that port which can now be accessed from any device on the internet.



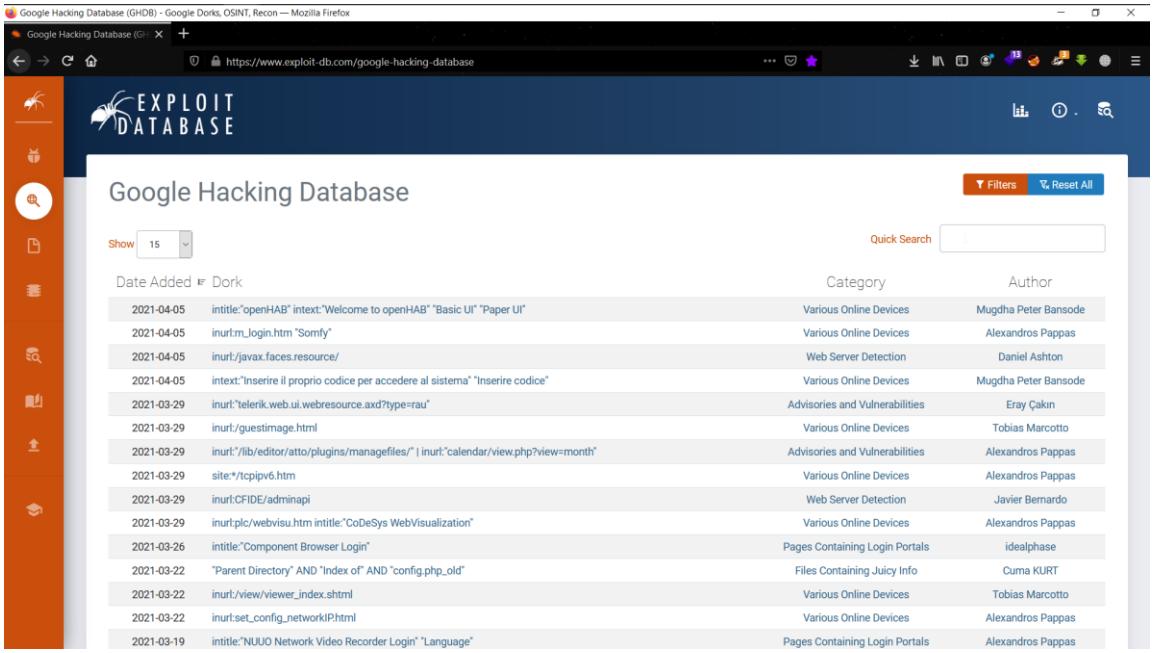
PORT FORWARDING

Information Gathering using tools –

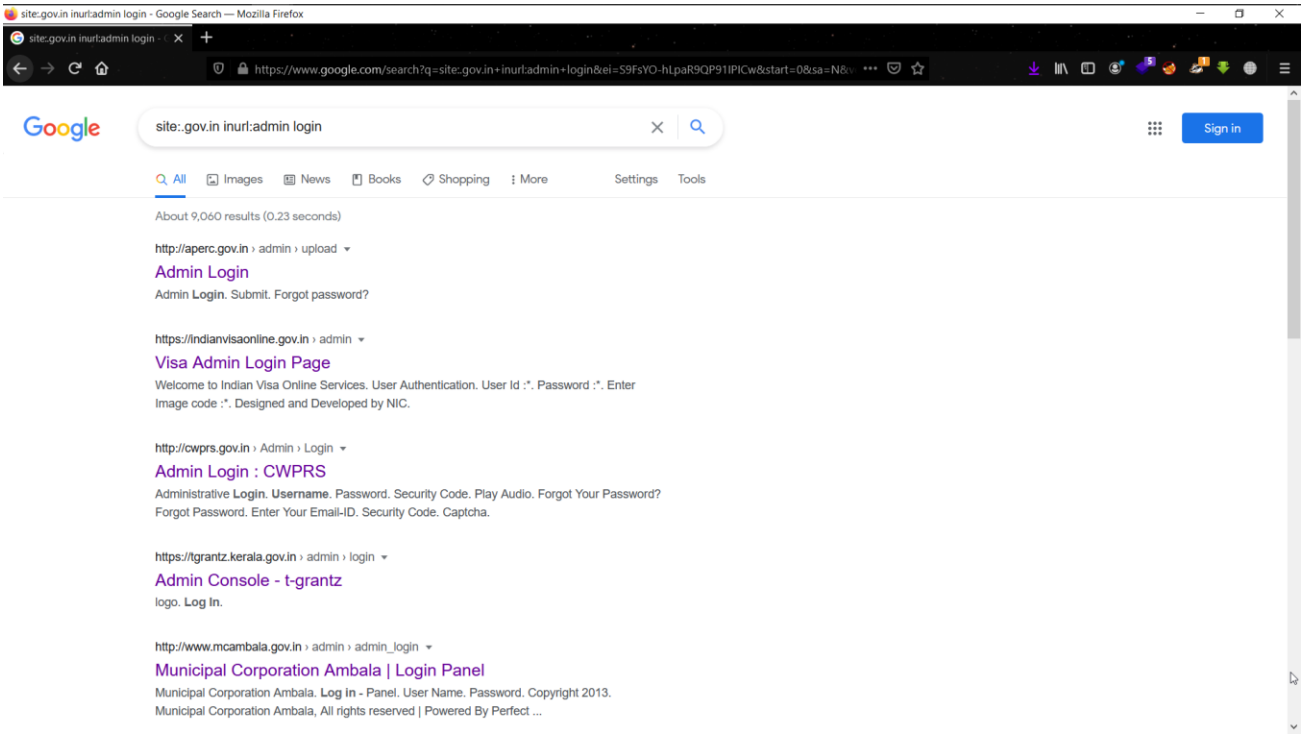
There are several numbers of tools to use together the information about the targets/hosts.
The most popular and powerful methods and tools for hacking we used were ***GHDB, MALTEGO, INTELX.IO, PHONEBOOK.CZ, HUNTER.IO.***

GOOGLE HACKING DATABASE (GHDB) –

Google hacking database is an index of google dorks which made the searching faster and accurate for expected results.



GHDB

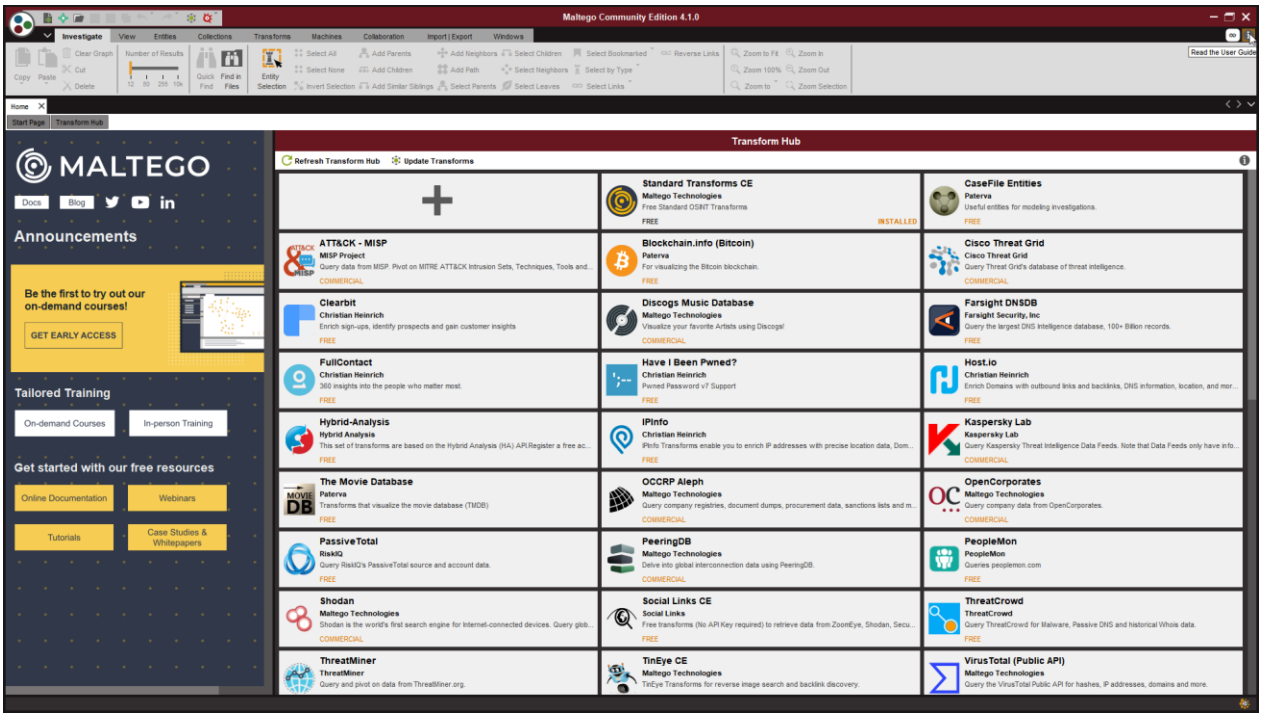


GHDB-POC

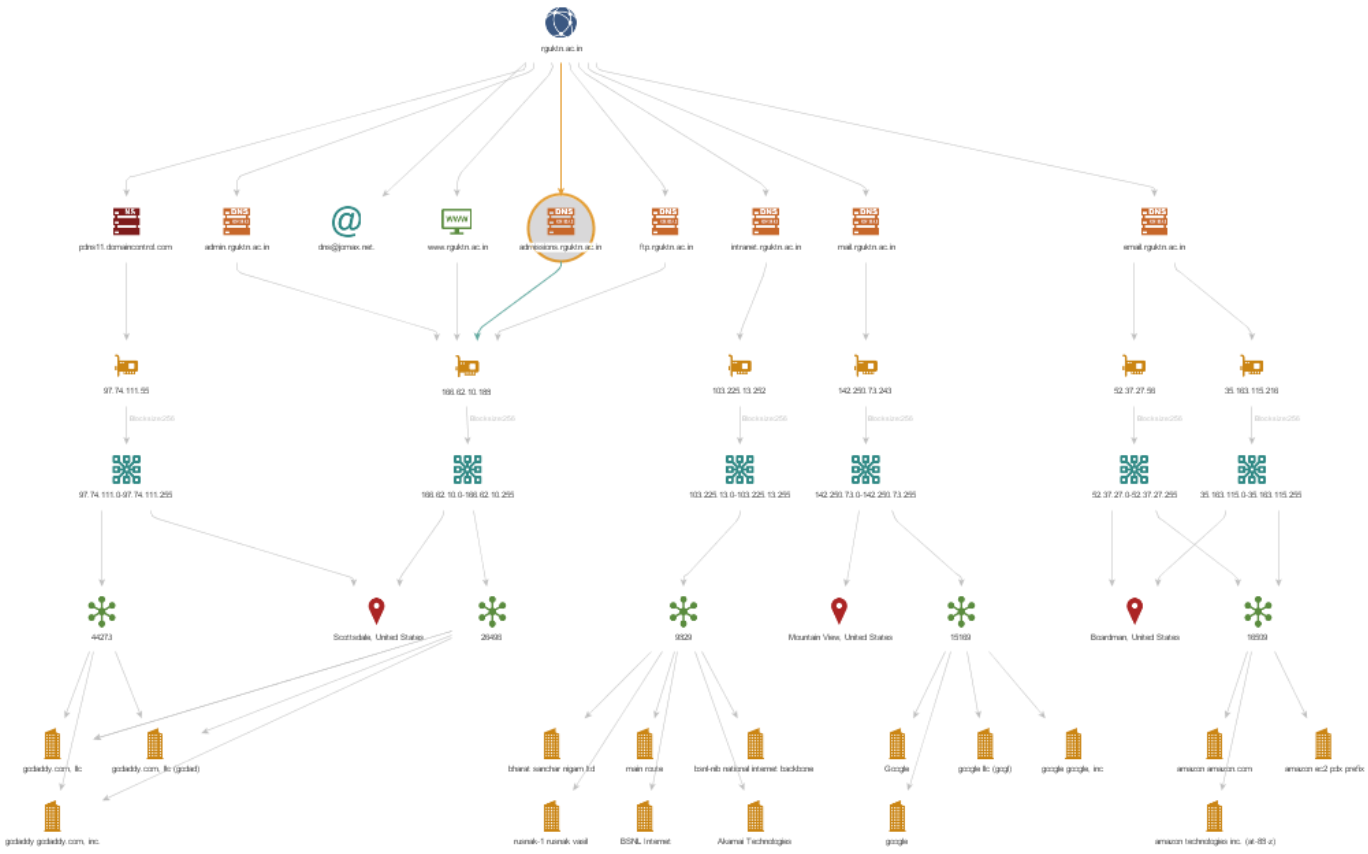
(Just a simple dork - ***site:.gov.in inurl:admin login***)

MALTEGO –

Maltego is a graphical analysis tool that is used to perform OSINT and forensics which is more useful for investigative tasks.



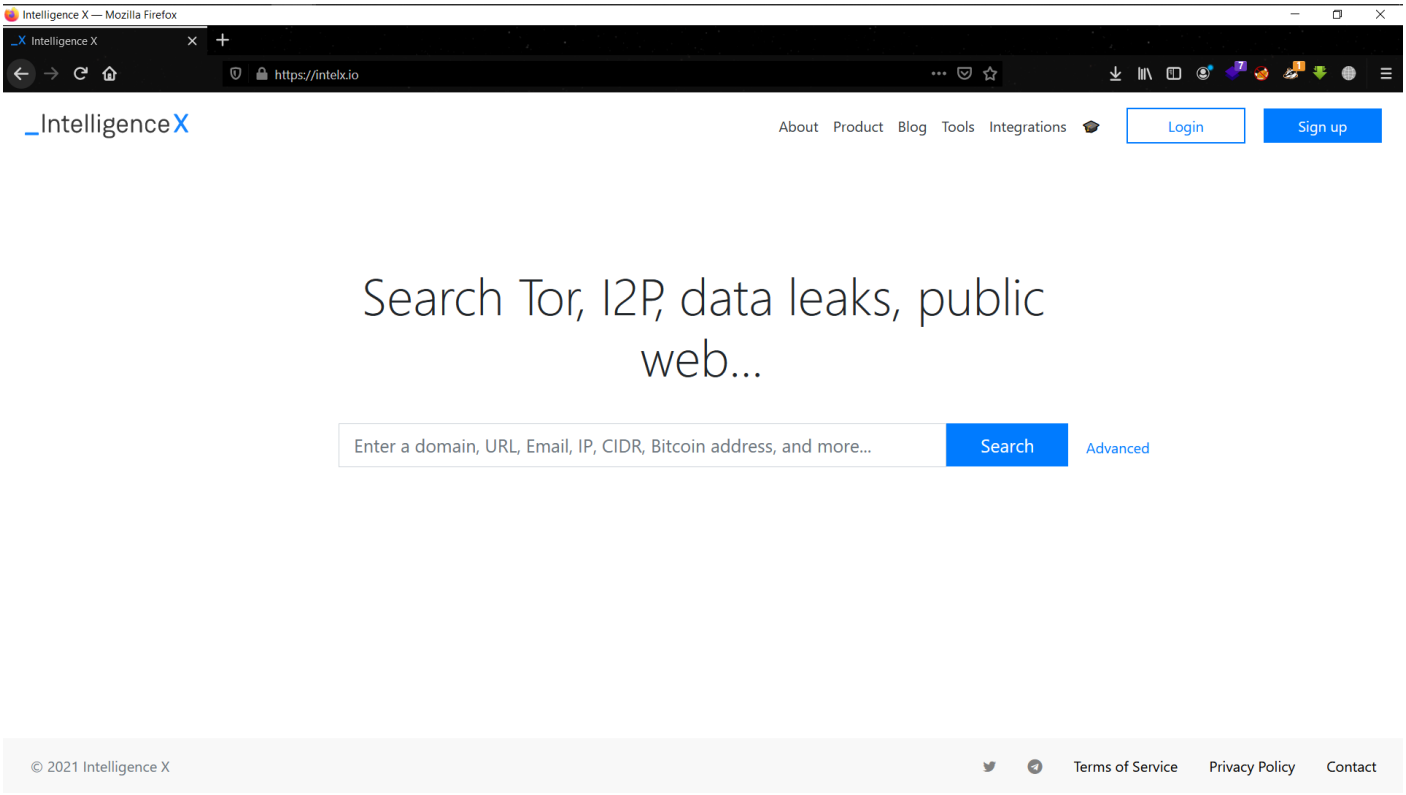
MALTEGO-INTERFACE



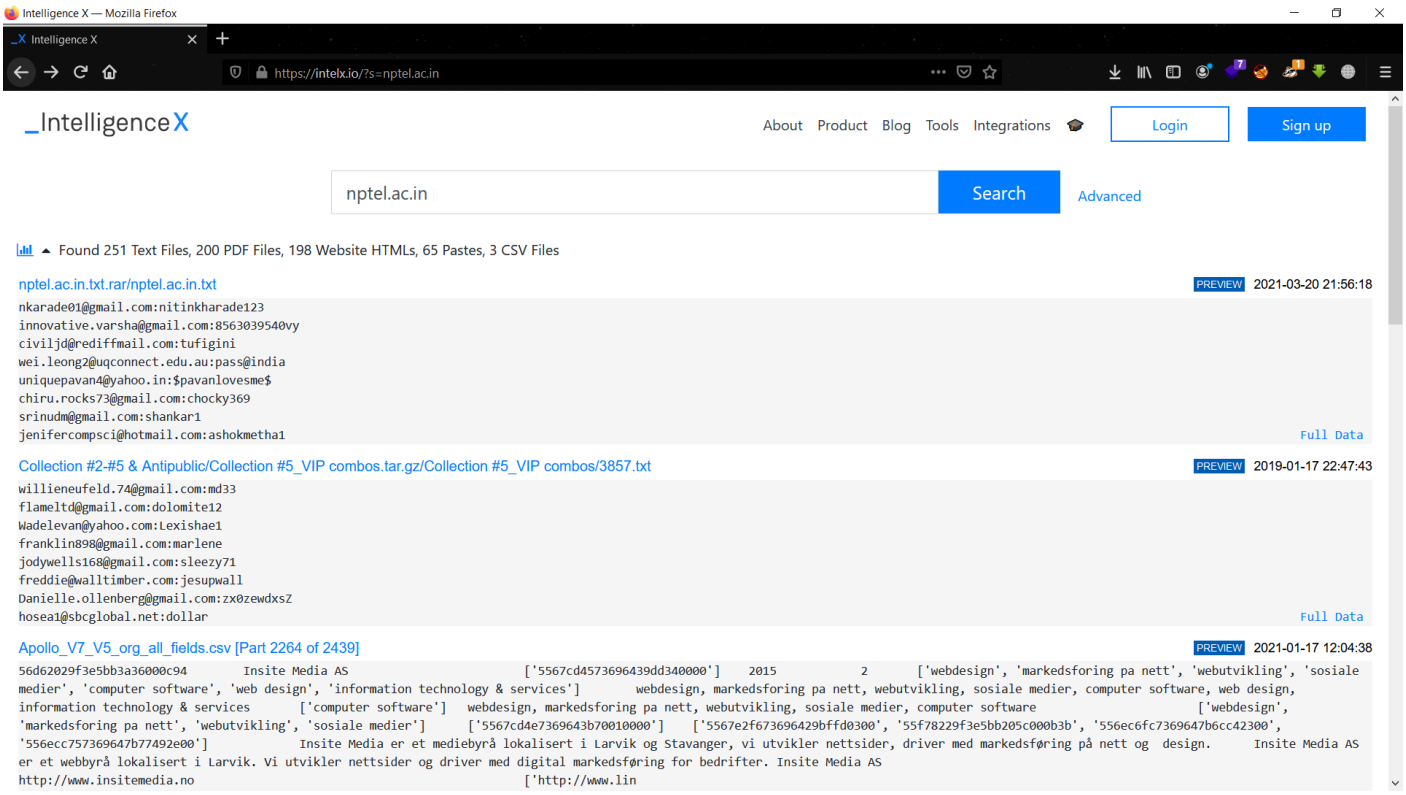
MLATEGO-POC

INTELX.IO –

Intelligence X is a search engine in which we can look for the information of a target which might have been leaked in data breaches or might be available in the internet publicly. We can search for emails, domains, CIDR, bitcoin address, I2P and many more.



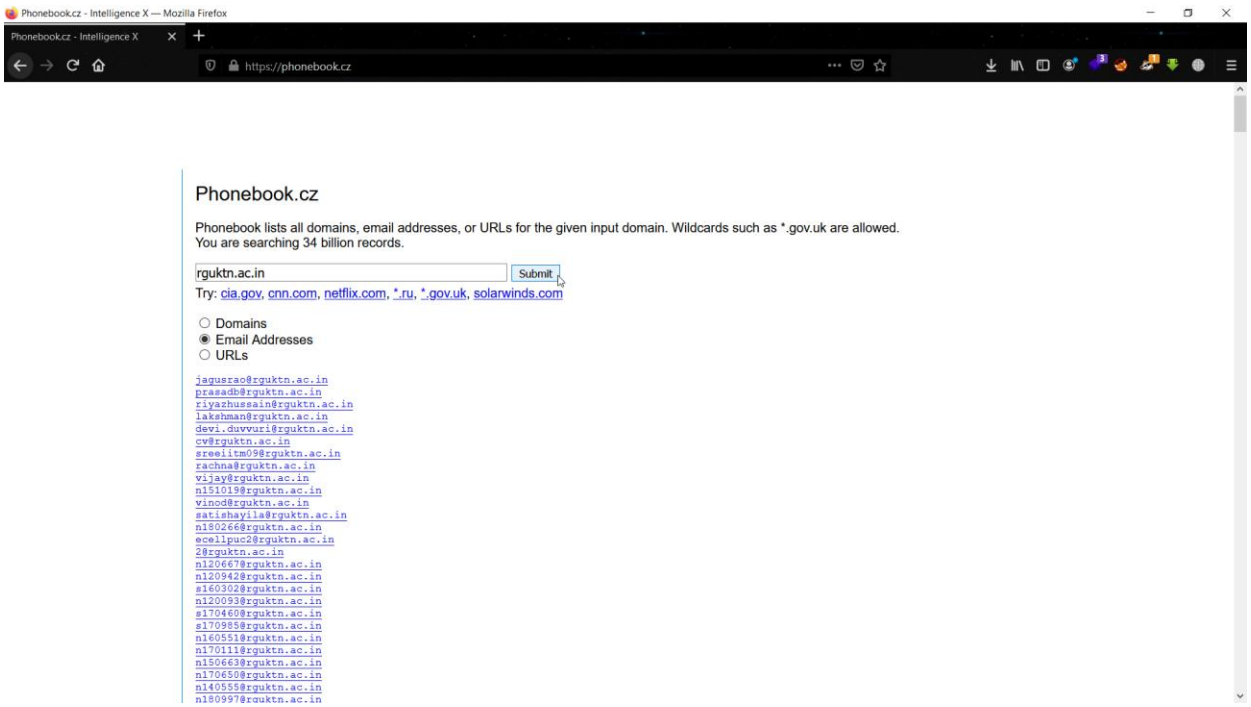
intelx.io interface



intelx.io-POC-showing results for the domain(nptel.ac.in)

PHONEBOOK.CZ –

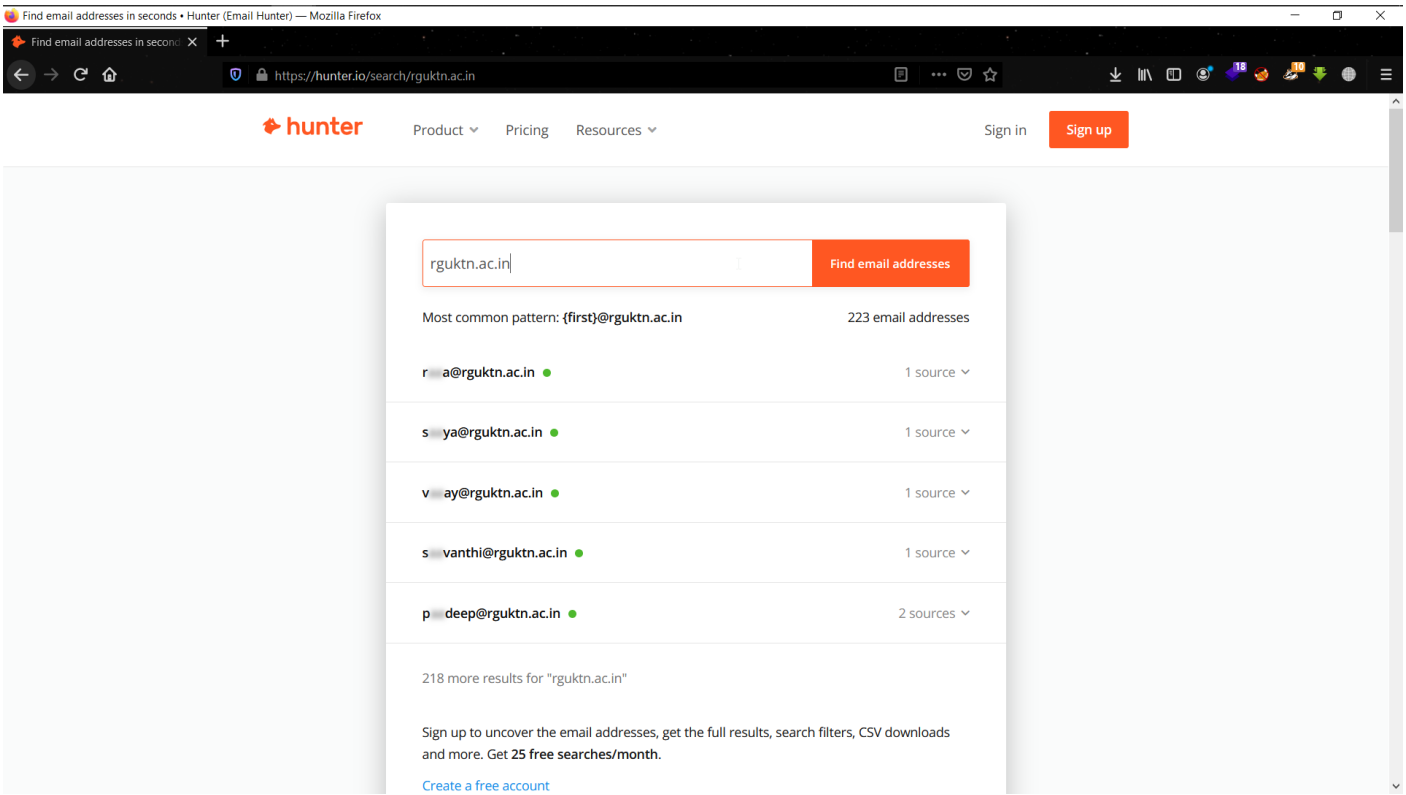
Phonebook.cz is also a search engine in where we can search for domains, email addresses, URLs.



phonebook.cz-POC

HUNTER.IO –

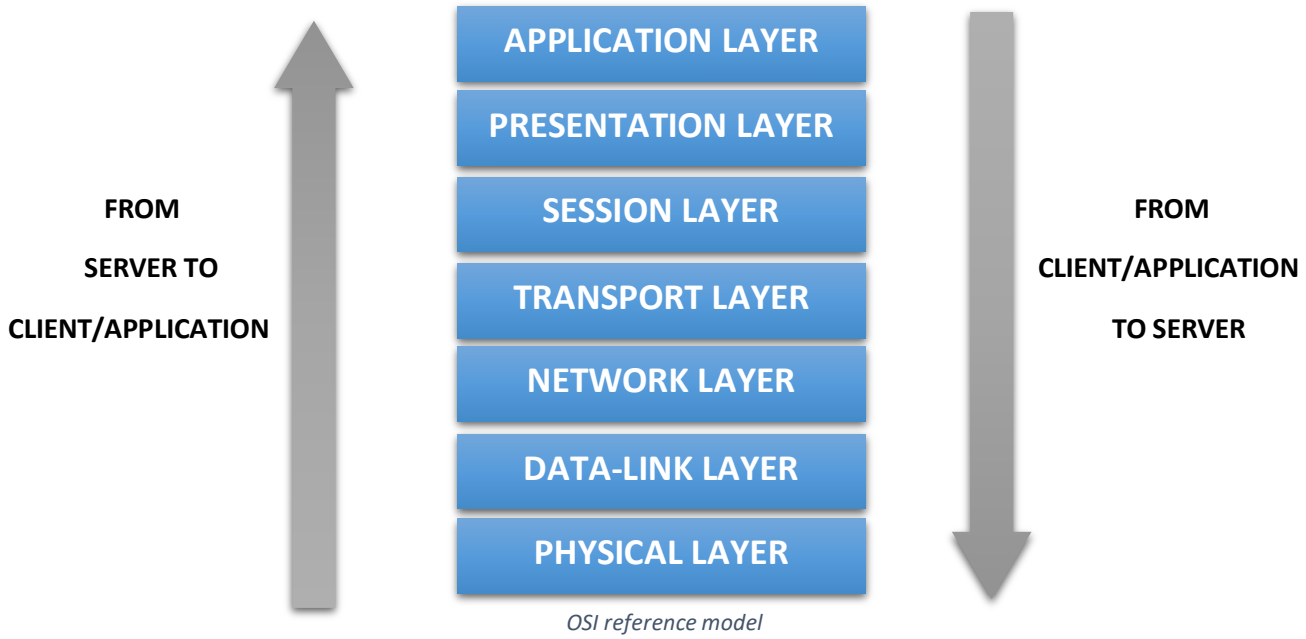
Hunter.io is an effective tool to verify the email address either valid or not. Hunter.io provides most appreciable results in reconnaissance. We have to sign up to hunter.io to see more results using this tool.



hunter.io-POC

OSI reference model –

OPEN SYSTEM INTERCONNECTION is reference model that describes how the transmission of data takes place from the application/browser to the server which is sitting up there through the physical medium.
To explain the transmission of data, OSI reference model consists of seven layers where each layer performs its own network function.



OSI reference model

The order of the layers from top to bottom or bottom to top is distinguished by the flow of data either from client to server or server to client respectively.

Each layer has its own network functioning.

PHYSICAL LAYER converts the data from one form to another (i.e., original file form to binary) and sends it through the physical medium such as cables. Physical layer is the cause for the data moving from one host to another host.

DATA-LINK LAYER provides the media accessing and physical addressing by using hardware addresses. Network devices such as Switches/Hubs and MAC Addresses were involved in this layer of OSI reference model.

NETWORK LAYER provides the path determination for the destination to where the data will be sent. It uses the logical addressing to assign addresses and then determines the path. Routers and IP addresses comes under this layer.

TRANSPORT LAYER determines the method/protocol to share the data according to the type of data that is going to be sent. This layer provides end to end connections and also reliable/unreliable data delivery and flow control by using TCP or UDP transport protocols to share the data or to make the connection.

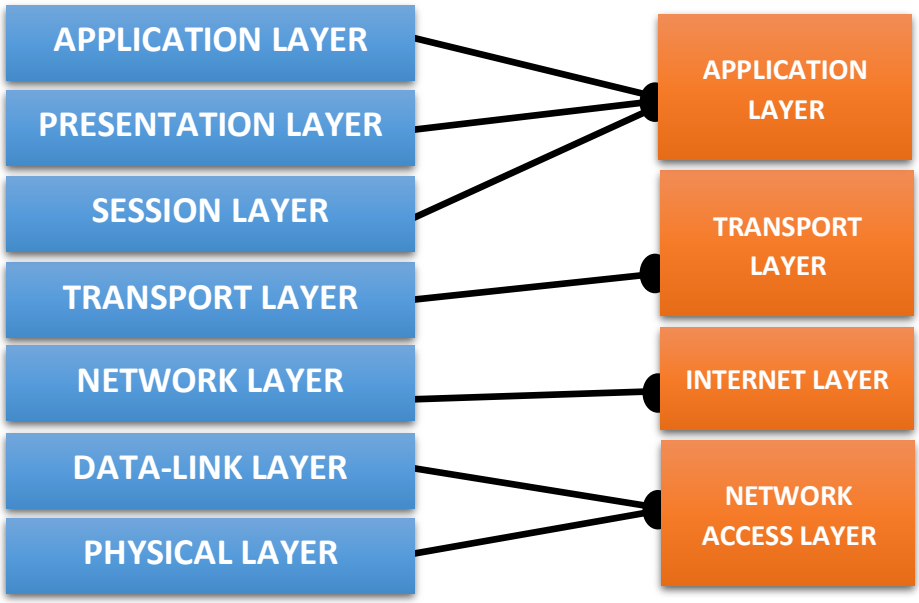
SESSION LAYER creates sessions between the devices to make them connected/communicate further. This layer handles the connection control between hosts and clients and maintains distinction between the data of various applications that runs on the machine.

PRESENTATION LAYER presents the data to the user. This layer handles the encryption & decryption, compression & extraction of the data to secure the data on the network.

APPLICATION LAYER provides the user an interface to access the data that has been sharing over the internet. Protocols were concerned in this layer. The data transfer starts from this layer when considered from client to server and ends with this layer when considered from server to client.

TCP/IP model –

TCP/IP model is mostly used model of networking which is made to be a prior to the OSI reference model. It is conceptually designed into 4 layers (sometime described as 5) and functions the same way as OSI.

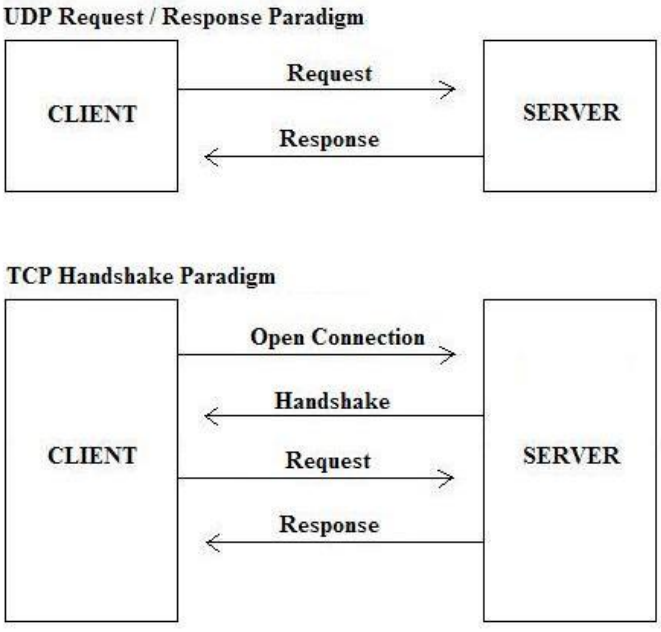


OSI reference model *TCP/IP model*

TCP& UDP architecture –

Transport Control Protocol is a standard connection-oriented communication protocol which is used to transmit the data from one system/device to another system/device. TCP connection is reliable connection and thus no data loss will happen. TCP uses a three-way handshake method for making a connection with a host.

User Datagram Protocol is connectionless communication protocol in which the data might usually lost sometimes, but UDP transfers the data faster than TCP connection since UDP doesn't use a three-way handshake.



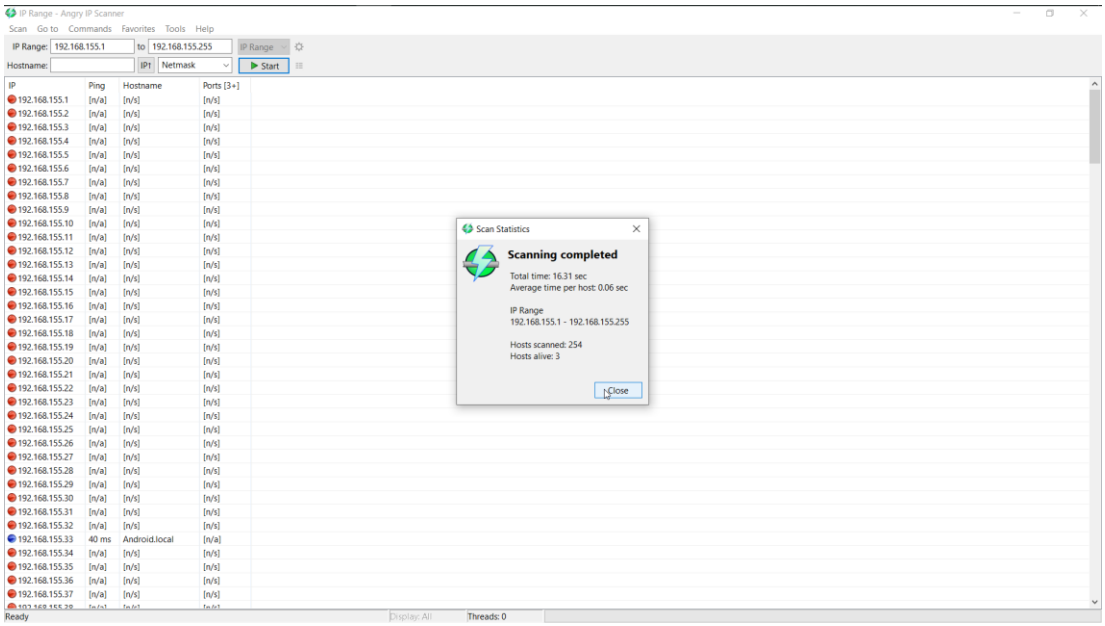
TCP and UDP communication architecture

TCP flags –

TCP flags are used to identify the connection state of the host or additional information about the host while making the connection. TCP flags were kept inside the TCP packets of the data that is being transferred. There are six flags and they are **SYN, ACK, SYNACK, FIN, RST, UNIQUE POINTER.**

Angry IP Tool –

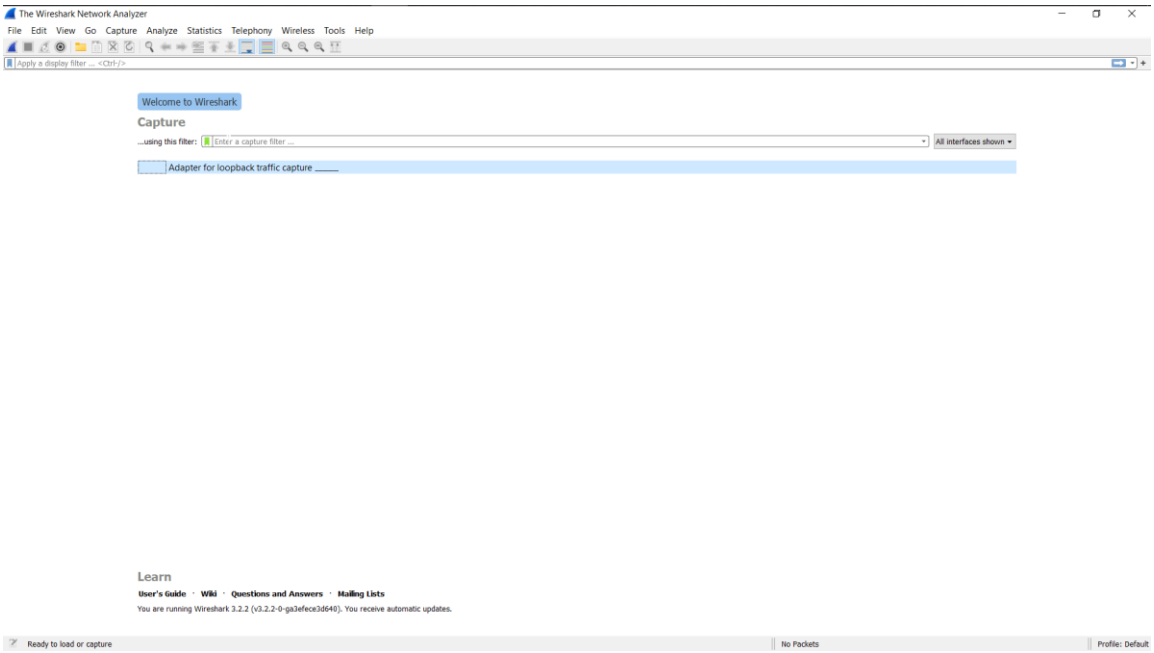
Angry IP tool is a network scanner. It can scan IP addresses of any range and can also scan the ports of the target.



Angry IP-POC

Wireshark –

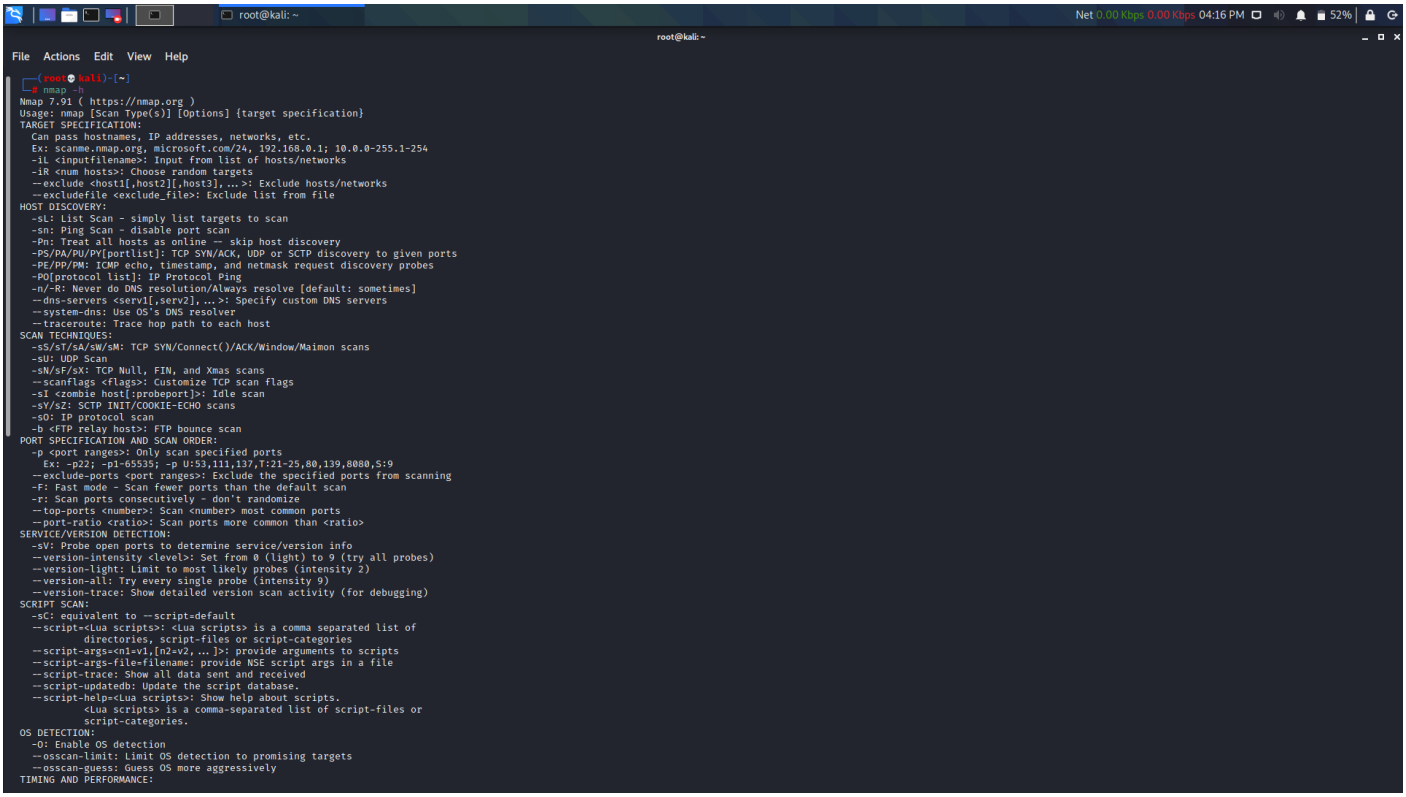
Wireshark is an open-sourced packet analyser tool which is more popularly known for network sniffing and interception.



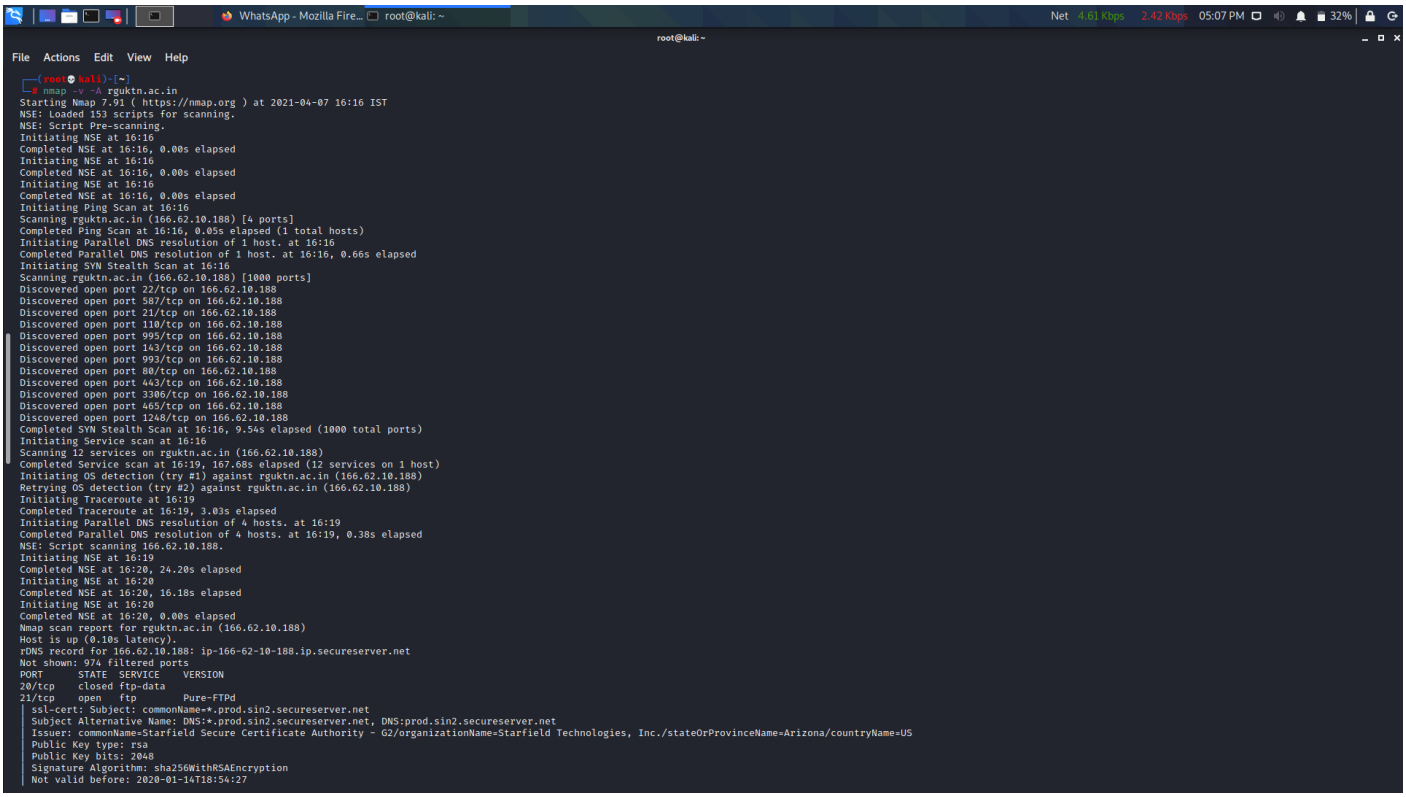
Wireshark-interface

NMAP tool –

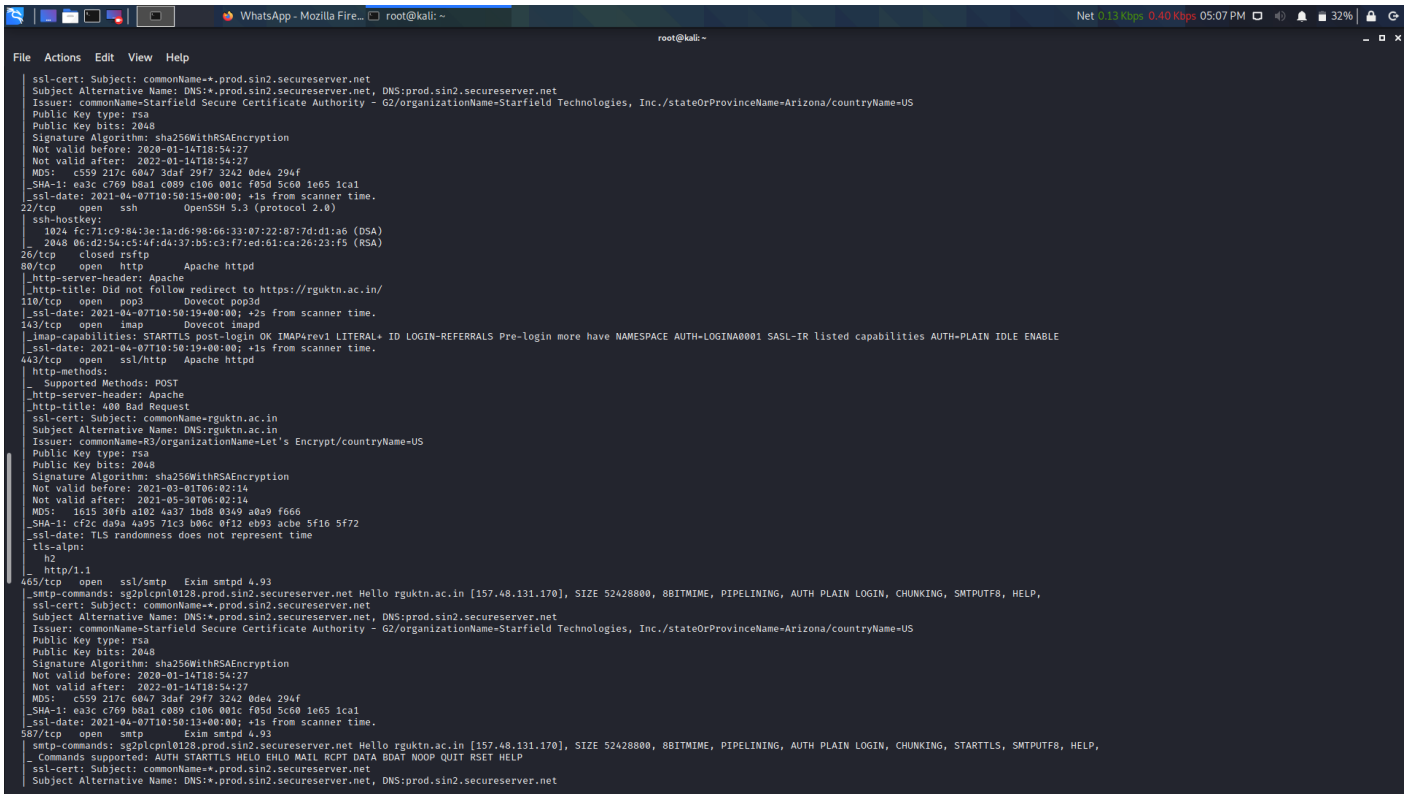
Network Mapper (NMAP) is an open-source utility for network discovery and security auditing. NMAP is mostly used to discover open ports, scan through the networks for network discovery. NMAP is a very powerful tool that it can even detect the operating systems and also can find vulnerabilities as well.



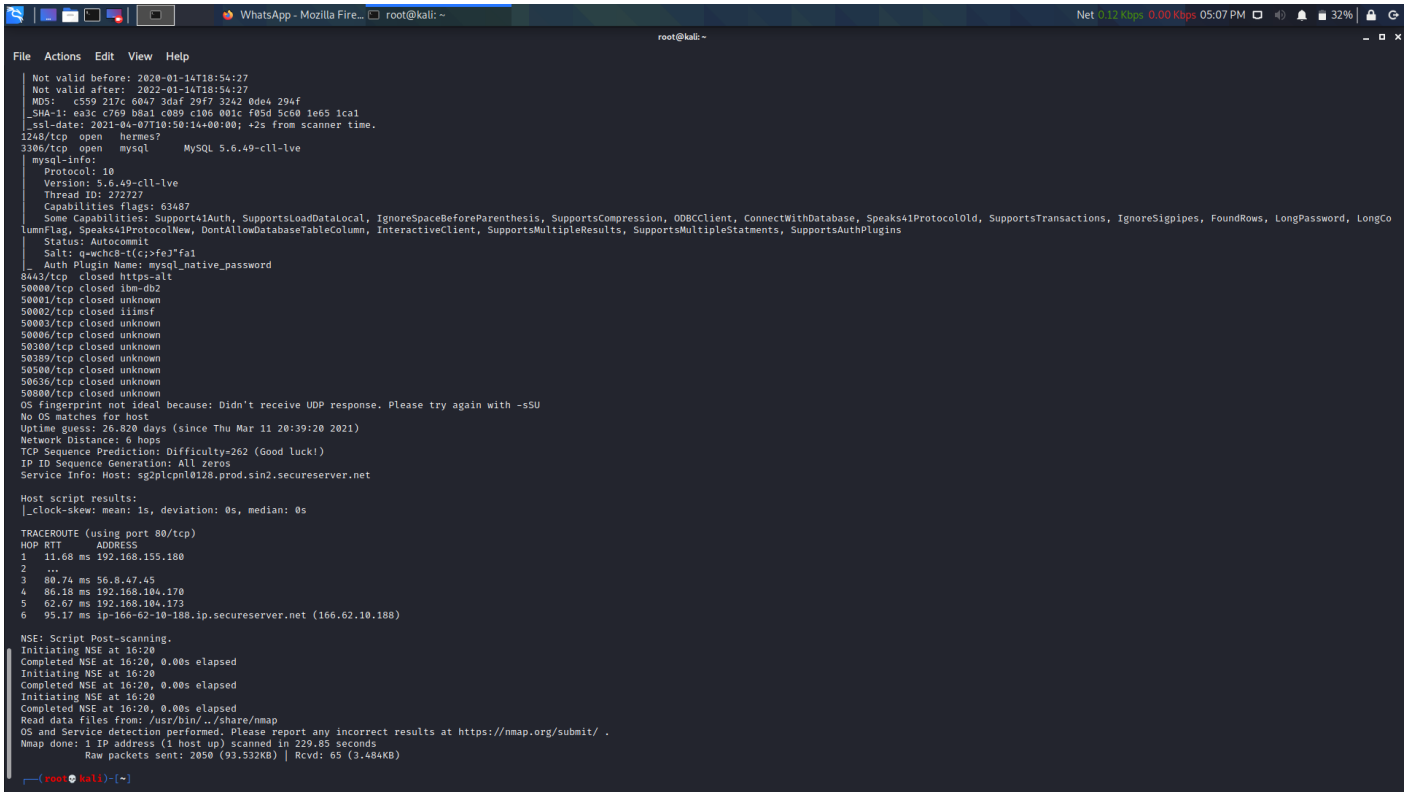
NMAP INTERFACE



NMAP-POC-1



NMAP-POC-2



NMAP-POC-3