

INFORMATION GATHERING

**The Initial Phase For Every Hacker**

## Under The Guidance: Dr. Kumar Debasis

Contents

* Introduction
* What are the objectives of information gathering in cybersecurity?
* Types, techniques, and methods of Information Gathering
* Tools we use to perform information gathering
* Using **Wireshark** to gather information from inside the network
* Using **N-map** for information gathering
* Using **Whois** lookup for information gathering (BRIEF)
* Conclusion

# INTRODUCTION

Information Gathering means gathering different kinds of information about the target. It is basically, the first step or the beginning stage of Ethical Hacking, where the penetration testers or hackers (both black hat or white hat) tries to gather all the information about the target, to use it for Hacking. To obtain more relevant results, we have to gather more information about the target to increase the probability of a successful attack.

It is a method used by analysts to determine the needs of customers and users. Techniques that provide safety, utility, usability, learnability, etc. for collaborators result in their collaboration, commitment, and honesty. Various tools and techniques are available, including public sources such as Whois, nslookup which can help hackers to gather user information.



# What are the objectives of information gathering in cybersecurity?

Any basic cybersecurity information gathering process often includes these two types of data collection goals:

* Collecting network data: Such as public, private and associated domain names, network hosts, public and private IP blocks, routing tables, TCP and UDP running services, SSL certificates, open ports, and more.
* Collecting system-related information: This includes user enumeration, system groups, OS hostnames, OS system type (probably by fingerprinting), system banners (as seen in the banner grabbing blog post), etc.

But there’s a lot more involved. Let’s learn about it, by exploring the most popular techniques used during this phase.

# Types, techniques, and methods of Information Gathering

There are many different ways to gain access to information on an organization or individual. Some of these options require technical skills while others require the soft skills of human hacking. Some options are fine to use from any location with internet access. While others can only be done in-person at a specific location. There are options that require no more equipment than a voice, options that only require a phone, and still others that require sophisticated gadgets.

Ethical hackers use a big variety of techniques and tools to get this precious information about their targets, as well as locations and data collection software they’ll be using towards the information gathering goal.

**Social engineering:** This includes in-person chat, phone conversations and email spoofing attacks. What all these methods have in common is the psychology of human weakness, needed to get maximum data about the target.

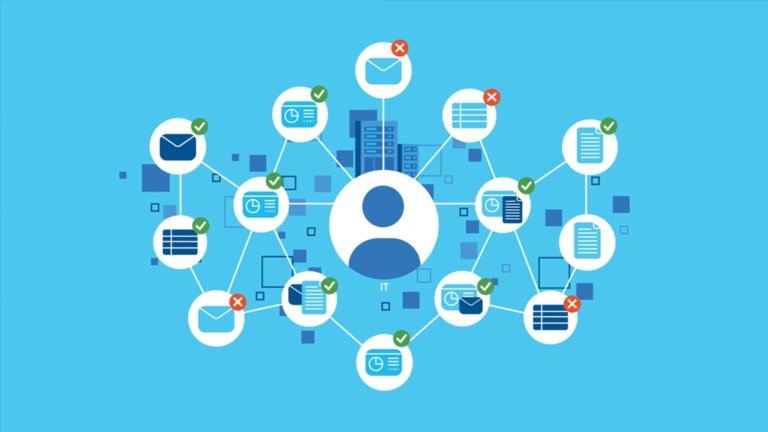
**Search engines:** Web crawlers can be used to fetch information about anything, and this includes companies, persons, services, and even real hacks, as seen in our previous article about Google Hacking.

**Social networks:** Facebook, Twitter, LinkedIn and other social networks are great sources of information to build a profile, especially when targeting individuals.

**Domain names:** These are registered by organizations, governments, public and private agencies, and people. Therefore, they’re a great starting point when you want to investigate someone. Personal information, associated domains, projects, services and technologies can be found by inspecting domain name information.

**Internet servers:** authoritative DNS servers are a great source of information, as they often include every single surface point exposed to the Internet—which means a direct link to related services such as HTTP, email, etc. In our previous article about passive DNS, we analyzed the importance of DNS servers, and especially passive DNS-recon services, such as the ones we offer here at SecurityTrails.

All these techniques are really useful when combined with enterprise security tools. Keep reading to discover how to maximize your information gathering results by using some really cool infosec utilities.



# Tools we use to perform information gathering



To complete an information-gathering exercise, you need to strategically plan what kind of information you want to collect about a target system.

Kali Linux is a powerful operating system that contains many tools for various tasks related to information gathering.

Below is the topmost powerful tools that come with Kali Linux which you can use for gathering information.

**Wireshark:** Wireshark is one of the most well-known and often used packet sniffing tools available today. It is used by cybersecurity professionals, network administrators and hackers to collect information from networks. Network packets contain a wealth of information, and Wireshark captures this data for later analysis. Learning how to use Wireshark is essential if you wish to conduct information gathering on a network.

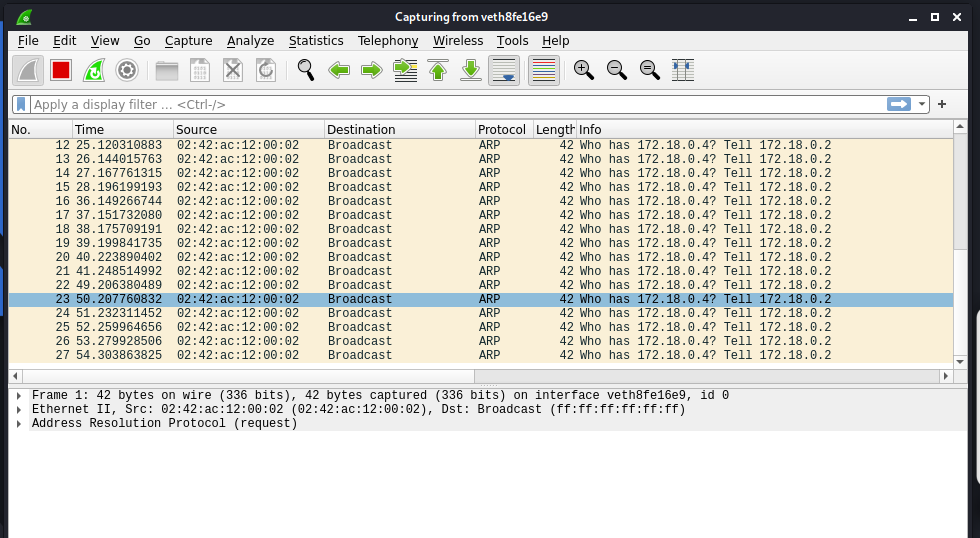
**N-map:** With Nmap, security professionals can find live hosts on a network and perform port scanning. This app is helpful for many reasons such as identifying open ports which are vulnerable to attack by hackers, or finding the operating system in use so that vulnerabilities may be exploited.

**Whois:** Whois is a simple, yet powerful, tool that allows you to see information about a specific domain name or IP address. You can use it to see things like contact information, nameservers, and domain registration information.

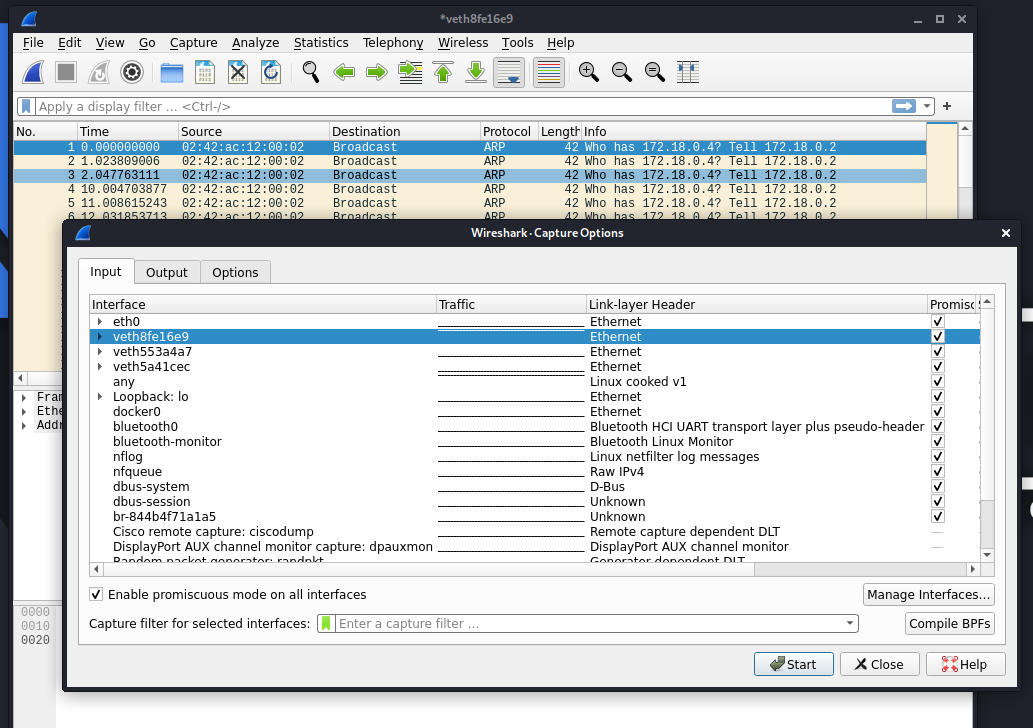
# Using Wireshark to gather information from inside the network

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.

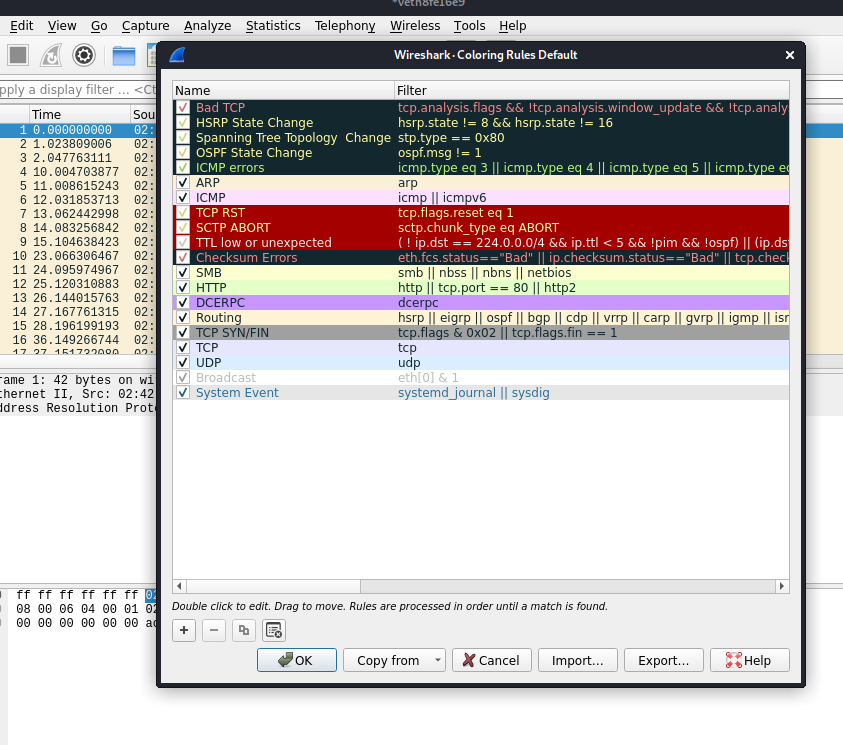
Now its in the state of capturing the packets in the network



We can get all the lists of interfaces that’s captured by clicking the capture button..



Coloring rules of wireshark @ view -> coloring rules

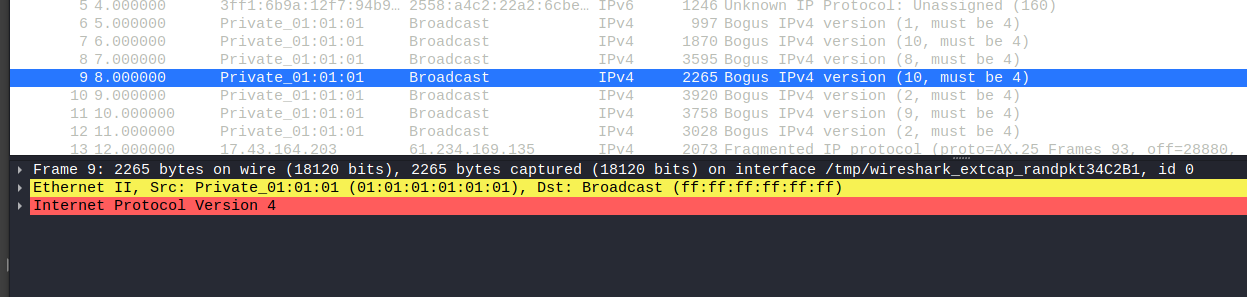


File -> objects contained -> http

This gives the objects travelled through the http protocol



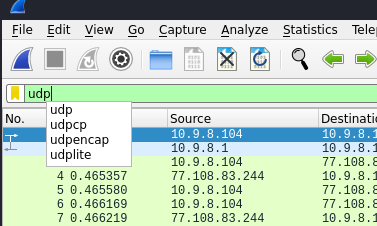
You can info about the packets travelled, and protocol used and also time date, ip address of hosts and destination.



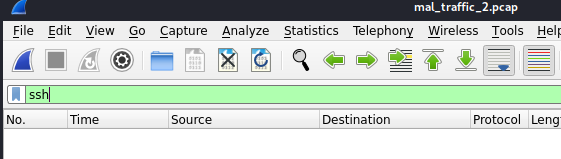
There are two types of filters in Wireshark:

1. Display Filter
2. Capture Filter

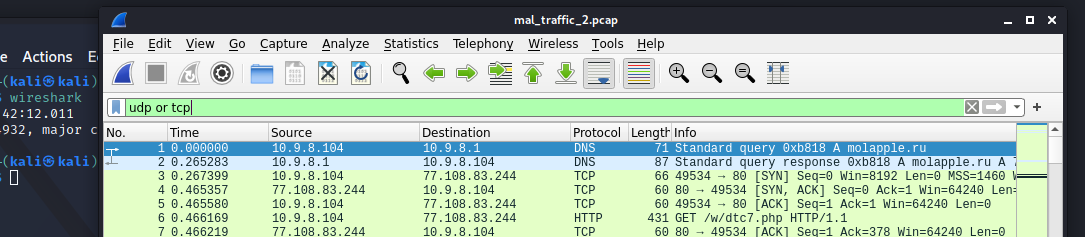
UDP – Filter, shows the traffic from UDP ports



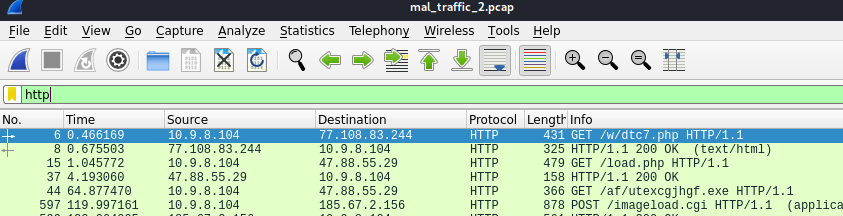
SSH – Filter, shows the traffic from ssh protocol



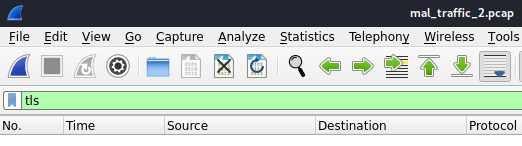
UDP OR TCP



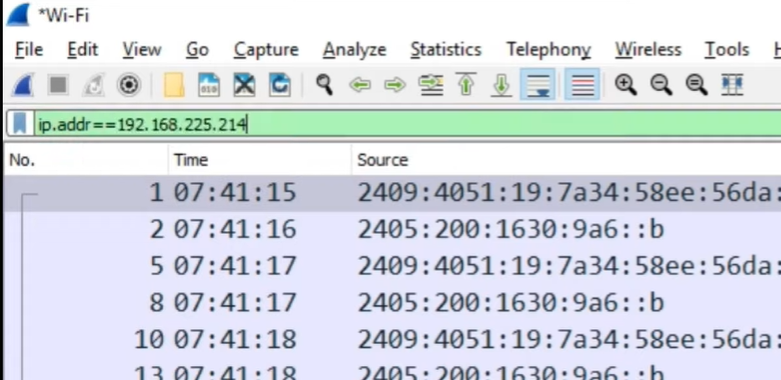
HTTP – shows all the connections through http protocol



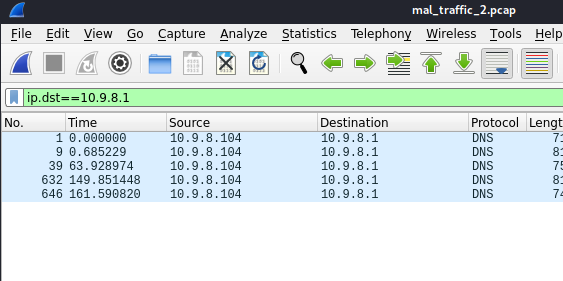
Tls – filter shows the connections form tls encoded



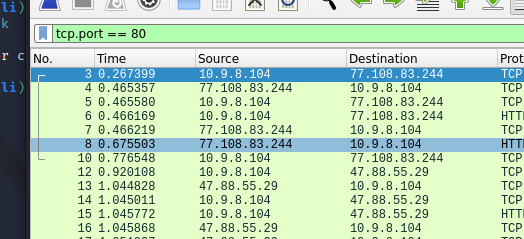
Ip.addr == 192,168.255.214 shows the connections travelled from this address



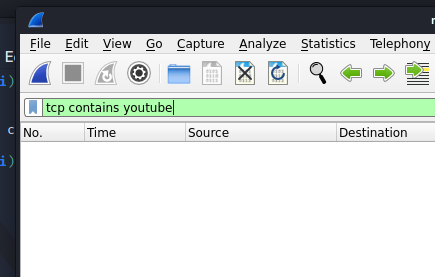
This command shows the packets received from this destination



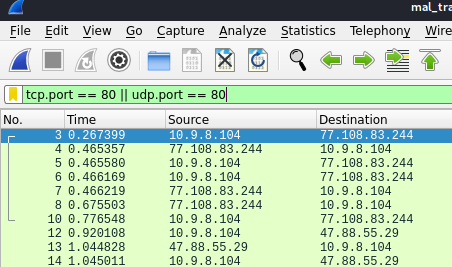
This shows the packets transferred from the port number “80”



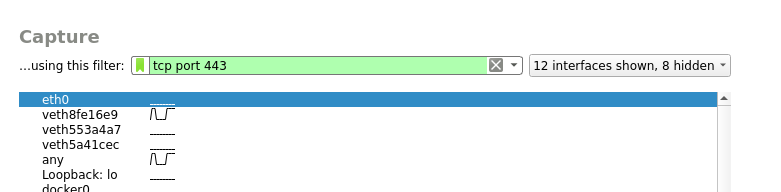
This filter enables shows the connections from the domain name



This shows the connections from UDP and TCP ports



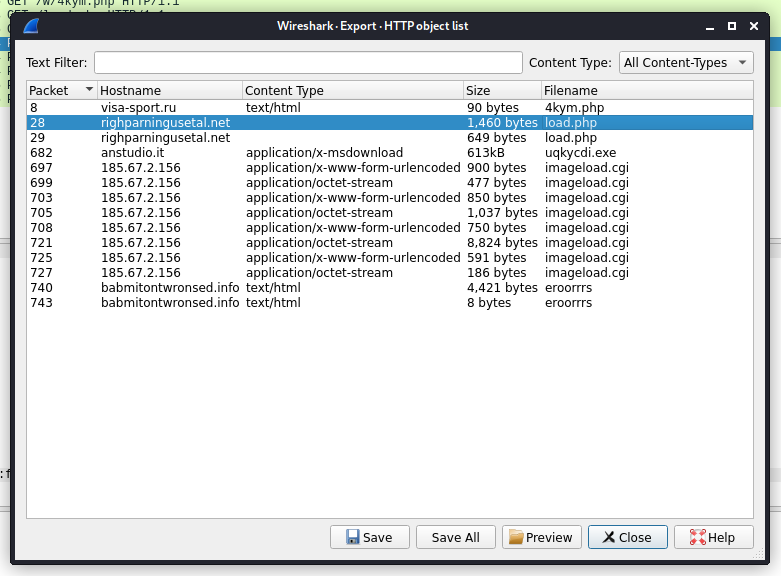
This shows the connections from port number 443



## Now let’s put this to test by analyzing the Pcap files of Wireshark to achieve the following information

* Find the objects (.exe, .html, .php or any other format)
* Export the found objects
* Note down the subdomains or other communicated domains
* Compromised site
* Port number communicated
* Protocol used for communication (TCP/UDP)
* Associated domains
* Any other domains, if any?
* Find the gateway address.
* Find the LAN segment broadcast
* Find the domain name of the infected host.
* OS the infected host runs?
* IP address of the infected Windows host?
* MAC address of the infected Windows host?
* Host name of the infected Windows host?
* Identify the infected URL which has Windows executable file?
* Generate SHA256 hashes of the Windows executable files sent to the infected Windows host?
* Indicator of Compromise
* What was the date and time the malicious traffic started?

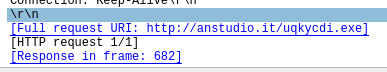
Objects contained:

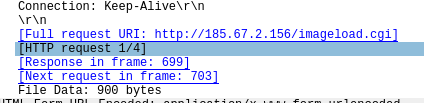


Communicated domains: , Compromised sites

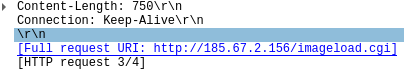










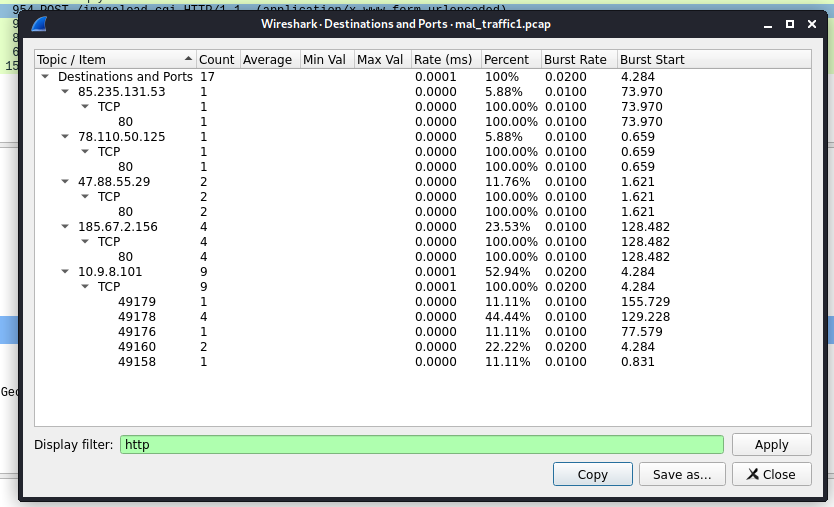






Protocol used : TCP

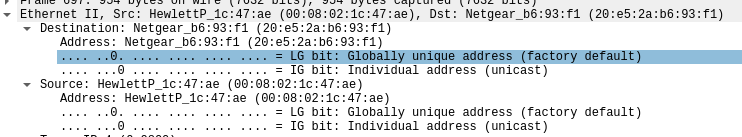
Ports Communicated:



OS the infected host runs: Windows

Ip address of the infected host: 10.9.8.101

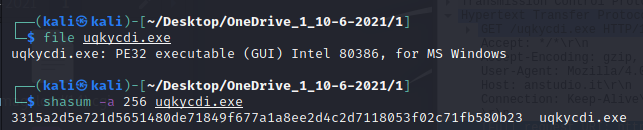
MAC address of the infected host and Host Name:



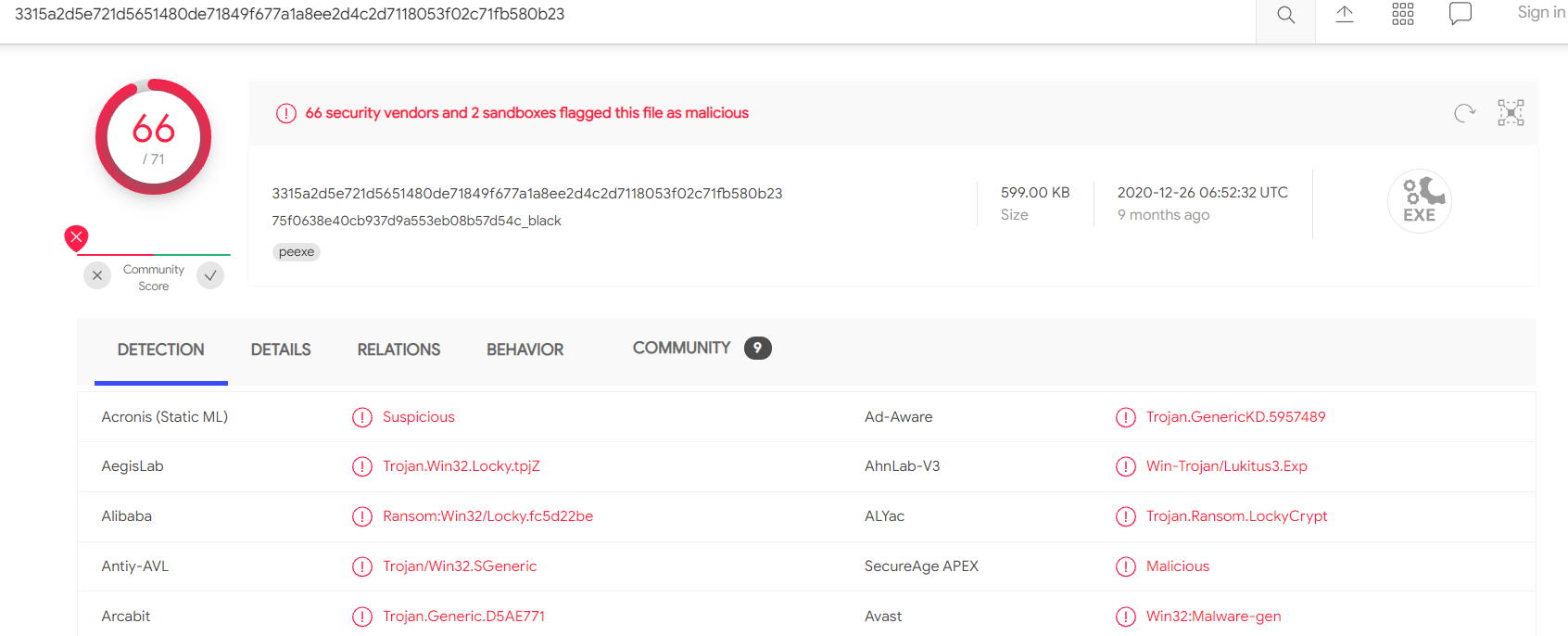
Infected URl containg exe file:

http://anstudio.it/uqkycdi.exe

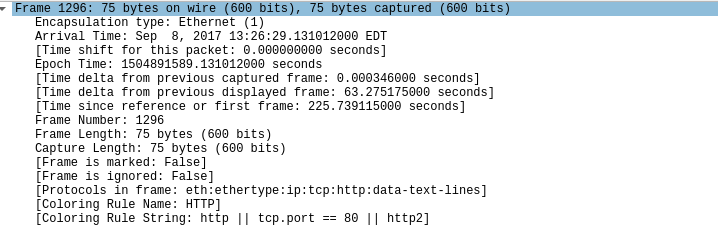
Generating SHA256 hashes for the exe file



Type of malware: Trojan



Time and Date of Attack:

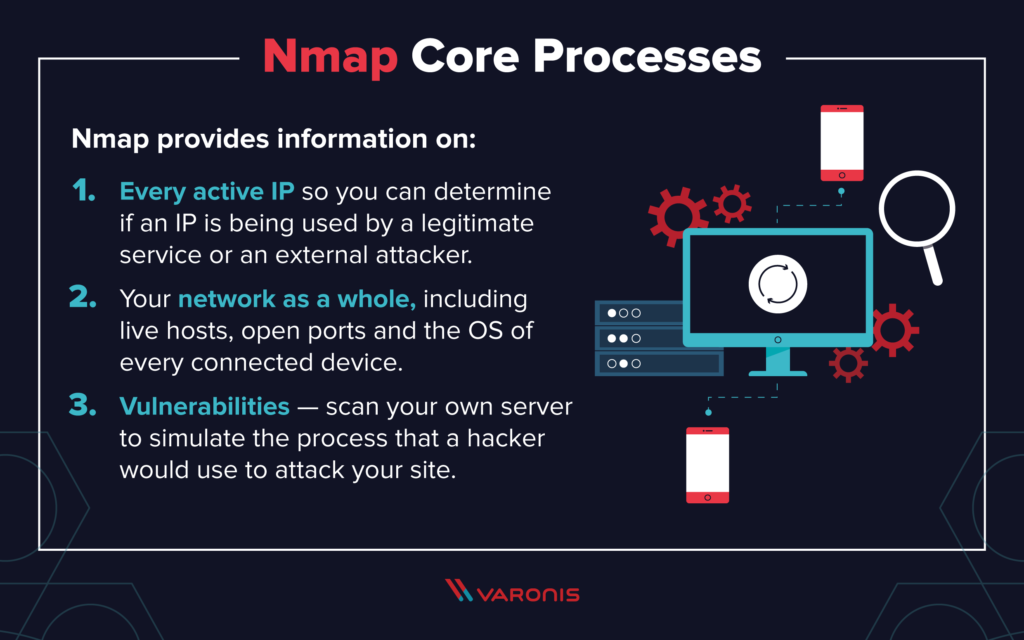


# Using N-map For Information Gathering

Before getting started on using the N-map tool to gather information let’s see how to install it so that even if we don’t have the tool pre-installed in the operating system we can install the tool and get the information needed.

The process for installing Nmap is easy but varies according to your operating system. The Windows, Mac, and Linux versions of the program can be [downloaded here](https://nmap.org/download.html).

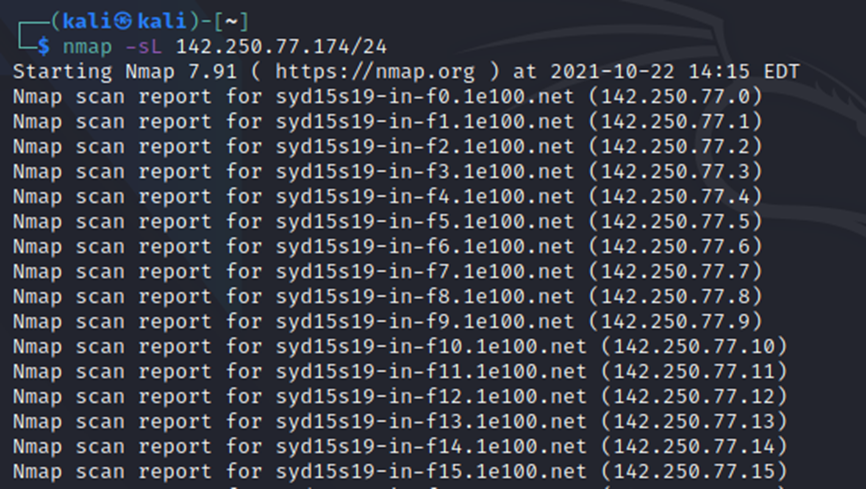
* For Windows, Nmap comes with a custom installer (namp<version>setup.exe). Download and run this installer, and it automatically configures Nmap on your system.
* On Mac, Nmap also comes with a dedicated installer. Run the Nmap-<version>mpkg file to start this installer. On some recent versions of macOS, you might see a warning that Nmap is an “unidentified developer”, but you can ignore this warning.
* Linux users can either compile Nmap from the source or use their chosen package manager. To use apt, for instance, you can run Nmap –version to check if Nmap is installed, and sudo apt-get install Nmap to install it.



## How To Run A Host Scan

A more powerful way to scan your networks is to use Nmap to perform a host scan. Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts connected to your network. Each host then responds to this packet with another ARP packet containing its status and MAC address.

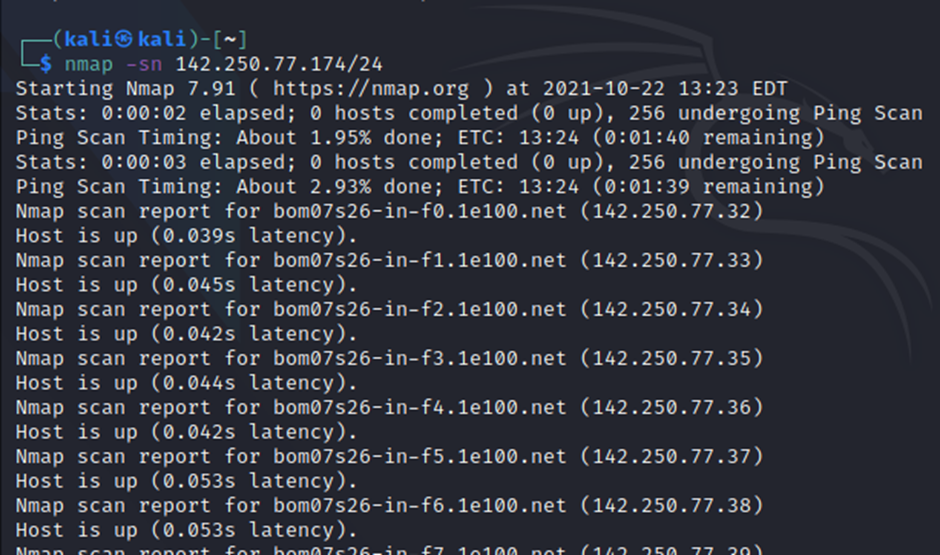
To run a host scan, use the following command: -sL: List Scan - simply list targets to scan



## How To Run A Ping Scan

One of the most basic functions of Nmap is to identify active hosts on your network. Nmap does this by using a ping scan. This identifies all of the IP addresses that are currently online without sending any packers to these hosts.

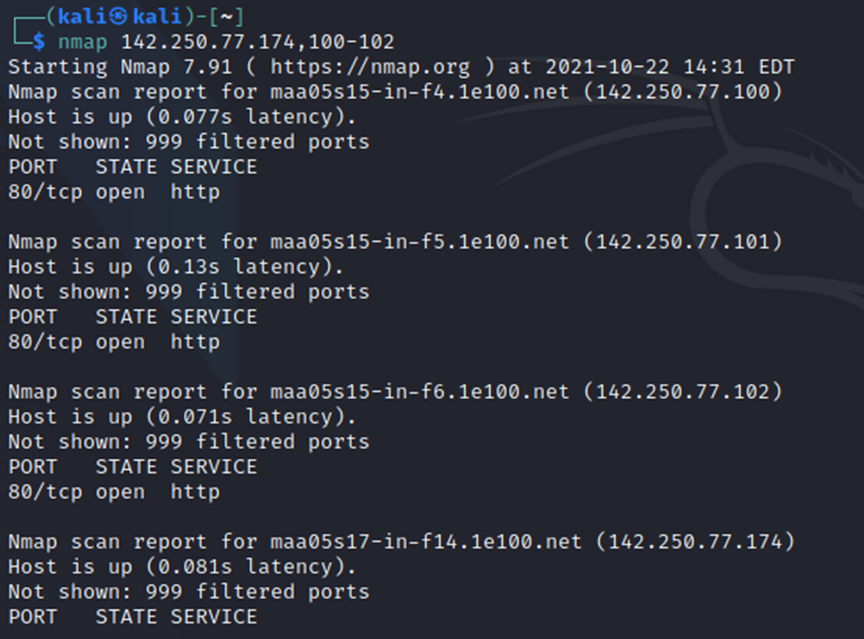
To run a ping scan, run the following command: -sn: Ping Scan - disable port scan



## How to Find Open Ports

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

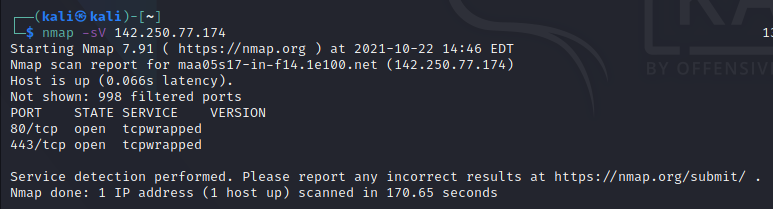
To find open ports across a network command is: nmap <ipaddress>, <port numbers range>



Find Services Listening on Ports on host Kali machine:

SERVICE/VERSION DETECTION:

-sV: Probe open ports to determine service/version info



This gives the information the state, version of the machine you using and the service running on the machine.

## Find Anonymous FTP Logins on Hosts:

CRYPT SCAN:

-sC: equivalent to --script=default

--script=<Lua scripts>: <Lua scripts> is a comma separated list of

directories, script-files or script-categories

--script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts

--script-args-file=filename: provide NSE script args in a file

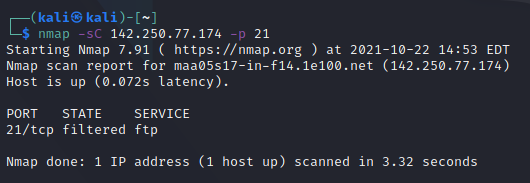
--script-trace: Show all data sent and received

--script-updatedb: Update the script database.

--script-help=<Lua scripts>: Show help about scripts.

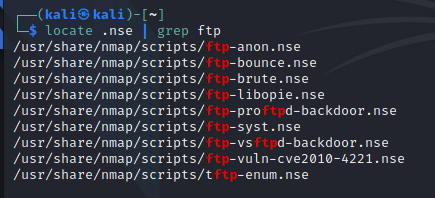
<Lua scripts> is a comma-separated list of script-files or

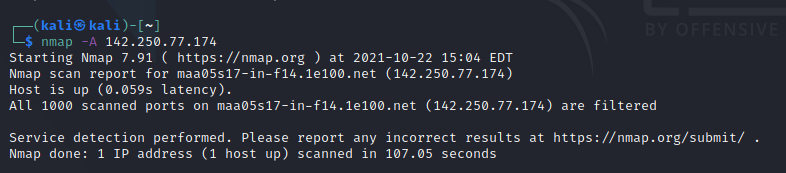
script-categories.

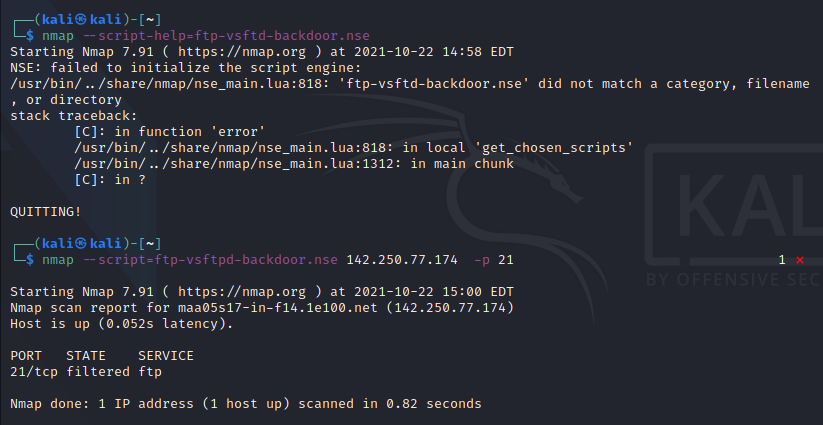


## Check for Vulnerabilities on Hosts:

Vulnerabilities are like gateways for hackers which helps them to gain control of your system without getting notified, to fine these vulnerabilities through nmap in a network use the following code.





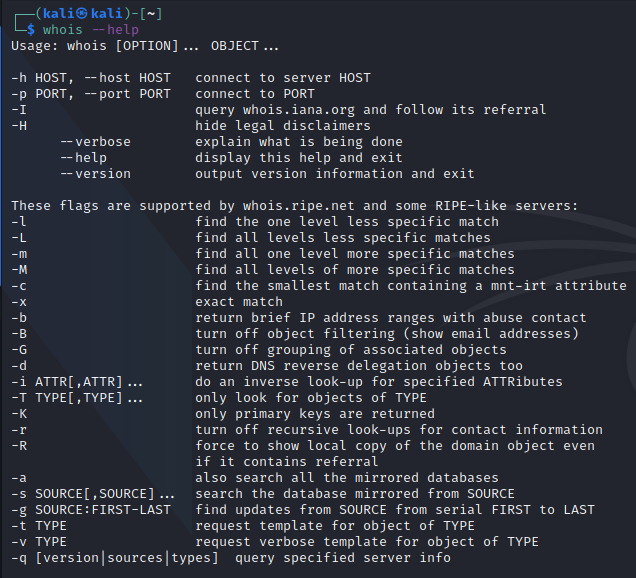


# Using Whois lookup for information gathering (BRIEF)

A whois Kali linux command is a utility as a part of the information gathering used in all of the Linux-based operating systems. this tool is part of information security assessment, and one of information gathering techniques. there are a lot of information gathering strategies. It is used to identify domain information and more.

This package provides a command line client for the WHOIS (RFC 3912) protocol, which queries online servers for information such as contact details for domains and IP address assignments. It can intelligently select the appropriate WHOIS server for most queries.

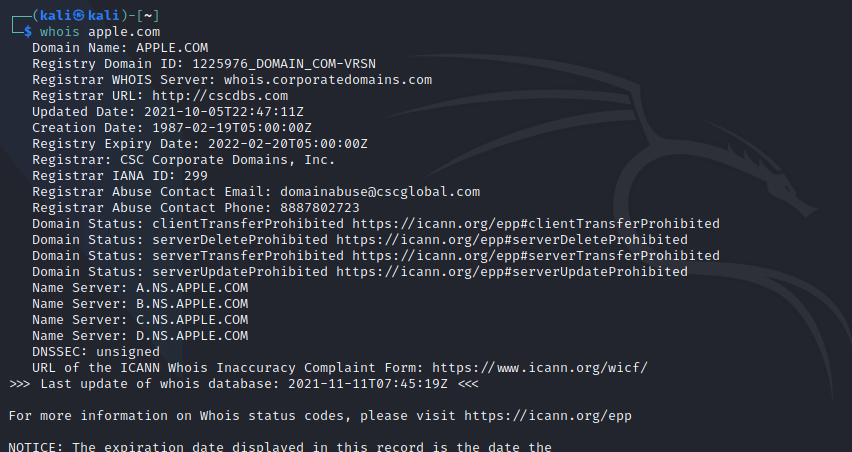
whois –help : Gives you all the ways WHOIS tool can be used..



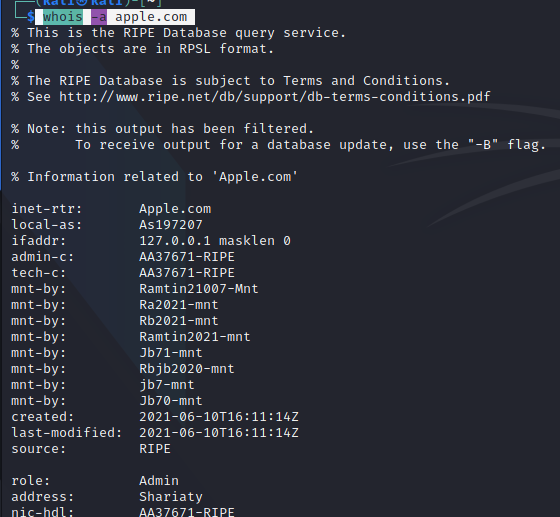
Whois [ip address] : This gives the info of the Ip address like registered date, location etc..



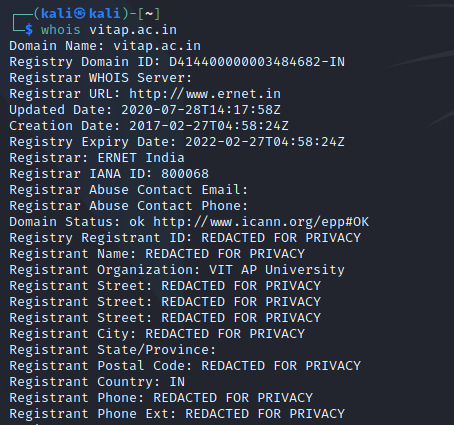
Whois [hostname] : gives the details of that website



whois -a apple.com : Searches for all the mirrored databases



Getting info on VITAP hostname



# CONCLUSION

Kali Linux has around 600 penetration-testing programs (tools), including Armitage (a graphical cyber-attack management tool), Nmap (a port scanner), Wireshark (a packet analyzer), metasploit (penetration testing framework), John the Ripper (a password cracker), sqlmap (automatic SQL injection and database takeover tool), Aircrack-ng (a software suite for penetration-testing wireless LANs), Burp suite and OWASP ZAP web application security scanners, etc.

Sometimes we have to automate our tasks while performing penetration testing or hacking as there could be thousands of conditions and payloads to test and testing them manually is a difficult task, So to increase the time efficiency we use tools that come pre-packed with Kali Linux. These tools not only saves our time but also captures accurate data and output the specific result.

# REFERENCES

* <https://www.geeksforgeeks.org/top-10-kali-linux-tools-for-hacking/>
* <https://www.kali.org/tools/nmap/>
* <https://www.kali.org/tools/wireshark/>
* <https://www.kali.org/tools/whois/>
* <https://en.wikipedia.org/wiki/Kali_Linux>
* <https://www.cyberpratibha.com/blog/using-whois-a-command-for-information-gathering/>
* <https://www.malware-traffic-analysis.net/>
* <https://www.bleepingcomputer.com/news/security/packettotal-a-useful-site-for-analyzing-pcap-files/?__cf_chl_rt_tk=x9eEakqnaLik.VeXAhAAYMJgmz1tmvTW1qmdqtIBCZ0-1637608167-0-gaNycGzNCNE>
* <http://www.securityidiots.com/Web-Pentest/Information-Gathering/Part-3-information-Gathering-with-nmap.html>