IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 3, March 2024

A Brief Overview of Whitehat Hacking and Its Techniques

Ms. Shiwani Ujal[1], **Mrs. Akshata Chavan**[2], **Mrs. Pooja Devrukhkar**[3]

Student[1], M.Sc.IT., I.C.S. College, Khed,
Assistant Professor, Department of I.T[2,3]
I.C.S. College, Khed, Ratnagiri

Abstract: *My theme is white cap hacking but I fair need to present you approximately hacking but in right heading this right course of hacking is called white cap hacking. Here we are going ponder approximately what is hacking and moral hacking essentially moral hacking is the only white hat hacking so here we are going think about that in case any programmer needs to hack any target at that point which steps he use to total his point since to catch a cheat we have to be think like a cheat so we'll study how programmers collect information's and why they are not caught by others and we are going ponder each step by which able to protect our self when we'll know how they enter in our framework and how they control any network then we will halt them so fundamental point is white cap programmer is for cyber security but in case we'll ensure our self at that point able to moreover gotten to be like a white cap programmer not at a tall level but we'll able to secure our self so we are going see it one by one at a fundamental level..*

Keywords: hacking

I. INTRODUCTION

In basic words hacking implies “stealing”. Hacking word is related to computer and its cruel is taking but this sort of taking will be conceivable when man who needs to take something must be imaginative and profoundly brilliantly since as it were that individual can hack any computer framework that has more information in computer range than other individual. In my point of see the meaning of hacking is –

“Hacking may be a creation by any individual who found or made a unused thing by which he can do anything concurring to his possess wish.Hacking may be legitimate or unlawful. When a man (Programmer) who needs to hack something for his claim advantage and don't care almost misfortunes and don’t care almost future.

Programmer discover out a few botches and point where he can break the security. These sorts of botch which is made by others in unprepared makes a difference the programmers and after finding these sorts of botch, programmer assaults on that botch and gotten to be effective to steal some imperative data and due to this cyber security isn't secure. This sort of hacking is unlawful it is additionally known as cyber wrongdoing. Due to cyber wrongdoing we cannot say that hacking is not great for security no since in the event that one thing has a few positive focuses at that point this can be settle that same thing has a few negative focuses too. And we all have listened that press can be cut by as it were press so on the off chance that due to hacking cyber wrongdoing is expanding at that point this is often settle that only due to hacking cyber wrongdoing can be halted. This sort of hacking is known as lawful hacking or moral hacking.

II. ETHICAL HACKING

We all know that what is the meaning of moral in other words we are able say that we all are recognizable with this word. This implies lawfulness. On the off chance that we do something lawfully or which we are doing which is based on law and a few rules and control that's called moral. In straightforward words if we are doing any work to take after a few rules and control and law which isn’t hurtful for others that work is called moral work or lawful work and moral work continuously advances security and goodness. But here we are talking around moral hacking so usually clear that which hacking is done inside limits of a few rules and law is called moral hacking. Essentially moral hacking is to halt cyber crime and for cyber security. This can be too hacking not any extraordinary hacking but usually completely for security and security and done for great purposes and able to say that to halt cyber hoodlums we have to be think like them at that point we will halt them. This sort of programmer is prepared uncommonly for cyber security and they are certified programmer and they have permit for hacking in right direction.In moral hacking programmers hack any given target to know that where is the issue? In system or in arrange by which any other programmer can hack that framework or organize at that point moral programmer attempt to evacuate that blame. This work is given by any company or government to moral programmer to find that point where the framework and organize can be hacked.So we have seen that hacking is depend on programmers on the off chance that hacker goes in wrong course at that point that's called illicit hacking or cyber wrongdoing and in case same programmer goes in right direction at that point that's called moral hacking. So it is exceptionally essential to get it that who are the programmer and how numerous sorts of programmer is living in between us.

HACKER

Hacker may be a individual who appreciates the alterations which is done by him. Programmer has the capability to adjust any media gadget and any arrange or framework and can control those devices according to his claim wish and can run too. In my point of see programmer is –“A individual who can do anything in any media gadget or framework by making a few unused traps and techniques.

WHITE HATHACKING

White cap hacking is come to halt dark cap programmers. Presently a day numerous sorts of cyber wrongdoings are expanding day by day so we can say that nowadays we are not secure in other words able to say that our identity and our information’s are not secure. By and large we transfer our data and our information’s online on social organizing destinations and other data related to bank, company, etc on other destinations so some hackers can take our identity easily. Numerous companies misfortune their vital information’s and data because some sorts of saltines break security system and after that they can easily enter interior the company’s arrange and can steal anything. So this is often clear that nowadays we are not secure online usually as it were due to some dark cap programmers or cyber criminals and to ensure our self we need white cap hacking. White cap hacking is too a type of hacking but this hacking provides us security in other words we are able say that white cap hacking is protective. This sort of hacking is done by white cap programmers. White cap programmers ended up portion of any lawful organization and these are too known as cyber security master and white cap programmers have a permit to hack. In white cap hacking programmers utilize same instruments and aptitudes but in right heading. White cap hacker’s work is same as dark cap programmers but white cap programmers discover out deduction and make strides that finding instead of crush that deduction like dark hat hackers. White cap hacking is additionally known as moral hacking and this is completely genuine that white cap hacking is today’s require for cyber security. For any type of hacking we should know a few terms and words which are utilized for hacking

VULNERABILITY

Vulnerability word is related to deductions. Lack of security in any framework or network is known as circle gap or defenselessness. Any hacker hack any system or media gadget by the assistance of these circle gaps. Dark cap programmers utilize these circle holes for hacking or by these circle gap dark cap hacker enters in security framework and crush the security system and steel a few important in arrangements but in other hand white cap hacker find these circle gaps and recoup these loop gaps to ensure same media gadget or framework from dark cap hackers.These programmers make a group by a great co-ordination with each other; this group is called ruddy group. This group may be group of dark cap programmers and white cap programmers. Dark cap programmers make ruddy group to hack anybody and white cap programmers make ruddy group to secure anybody.

TARGET If any person’s framework has been hacked then that individual is called target or victim. For dark hat hackers target may be any person’s data or any company’s information or any mystery and for white cap programmers target may be to halt dark cap programmers or to find loop holes or conclusions of any system.

PATCH LEVEL After finding the circle gaps or vulnerability if we fulfill that circle gaps then that fulfillers is called fix level in simple words we can say that the method of evacuating the circle gaps or powerlessness is called patch level. Generally this is done by white cap programmers to ensure victim from cyber hoodlums.

ETHICAL HACKING

We all know that what is the meaning of ethical in other words we can say that we all are familiar with this word. This means legality. If we do something legally or which we are doing and that is based on law and some rules and regulation that is called ethical. In simple words if we are doing any work to follow some rules and regulation and law and that is not harmful for others that work is called ethical work or legal work and ethical work always promotes safety and goodness. But here we are talking about ethical hacking so this is clear that which hacking is done within limits of some rules and law is called ethical hacking. Basically ethical hacking is to stop cyber crime and for cyber security. This is also hacking not any special hacking but this is fully for security and safety and done for good purposes and we can say that to stop cyber criminals we have to think like them then we can stop them. This type of hacker is trained specially for cyber security and they are certified hacker and they have license for hacking in right direction.

In ethical hacking hackers hack any given target to know that where is the problem? In system or in network by which any other hacker can hack that system or network then ethical hacker try to remove that fault. This work is given by any company or government to ethical hacker to find that point where the system and network can be hacked.

So we have seen that hacking is depend on hackers if hacker goes in wrong direction then that is called illegal hacking or cyber crime and if same hacker goes in right direction then that is called ethical hacking. So it is very necessary to understand that who are the hacker and how many types of hacker is living in between us.

HACKER

Hacker is a person who enjoys the modifications which is done by him. Hacker has the capability to modify any media device and any network or system and can control those devices according to his own wish and can run also. In my point of view hacker is –

“A person who can do anything in any media device or system by creating some new tricks and techniques.”

WHITE HAT HACKING

White hat hacking is come to stop black hat hackers. Now a day many types of cyber crimes are increasing day by day so we can say that today we are not secure in other words we can say that our identity and our information’s are not safe. Generally we upload our data and our information’s online on social networking sites and other information related to bank, company, etc on other sites so some hackers can steal our identity easily. Many companies loss their important information’s and data because some types of crackers crack security system and then they can easily enter inside the company’s network and can steal anything. So this is clear that today we are not safe online this is only due to some black hat hackers or cyber criminals and to protect our self we need white hat hacking.

White hat hacking is also a type of hacking but this hacking provides us protection in other words we can say that white hat hacking is defensive. This type of hacking is done by white hat hackers. White hat hackers become part of any legal organization and these are also known as cyber security expert and white hat hackers have a license to hack. In white hat hacking hackers use same tools and skills but in right direction. White hat hacker’s work is same as black hat hackers but white hat hackers find out deduction and improve that deduction rather than destroy that deduction like black hat hackers.

White hat hacking is also known as ethical hacking and this is fully true that white hat hacking is today’s need for cyber safety. For any type of hacking we should know some terms and words which are used for hacking –

VULNERABILITY

Vulnerability word is related to deductions. Lack of security in any system or network is known as loop hole or vulnerability. Any hacker hack any system or media device by the help of these loop holes. Black hat hackers use these loop holes for hacking or by these loop hole black hat hacker enters in security system and destroy the security system and steel some important in formations but in other hand white hat hacker find these loop holes and recover these loop holes to protect same media device or system from black hat hackers.

These hackers make a team by a good co-ordination with each other; this team is called red team. This team may be team of black hat hackers and white hat hackers. Black hat hackers make red team to hack anybody and white hat hackers make red team to protect anybody.

TARGET

If any person’s system has been hacked then that person is called target or victim. For black hat hackers target may be any person’s information or any company’s data or any secret and for white hat hackers target may be to stop black hat hackers or to find loop holes or deductions of any system.

PATCH LEVEL

After finding the loop holes or vulnerability if we fulfill that loop holes then that fulfillers is called patch level in simple words we can say that the process of removing the loop holes or vulnerability is called patch level. Generally this is done by white hat hackers to protect victim from cyber criminals.

HACKTIVISM

If hacking is done by any person due to political or social reason then that is called hacktivism. It comes for revenge if any person is exploited by any political agenda then feelings and views of that person is changed for that political party then he always wants to take revenge for his own satisfaction and for this he use some wrong ways and in these ways one way is hacktivism.

These are some words which are generally used for hacking but to understand complete hacking whether black hat hacking or white hat hacking we have to study all steps of hacking one by one because there are a complete module of hacking so to understand complete hacking we have to study all steps which completes whole module of hacking. White hat hacking is not any special hacking in this hacking hackers use same tools and technology but in right sense that’s why this is called white hat hacking or ethical hacking. In simple words to catch a thief we have to think like a thief.

We can understand the process of white hat hacking by this example –

“If we want to recover whole road and want to make same road free from all holes and damages then we have to start moving on that road from starting point of that road and then we have to find the all damages and holes by which road is not safe and then we can improve those damage and other hand there is same work for

White hat hackers that mean white hat hackers will have to move on same way like black hat hackers to find that holes which are made by black hat hackers.”

So now we will study whole process of hacking in steps and these steps are –

FOOTPRINTING
SCANNING
ENUMERATION
SYSTEM HACKING
TROJANS
VIRUS & WORMS
SNIFFING
SESSION HIJACKING
WEB HACKING
CRYPTOGRAPHY
WIRELESS NETWORK HACKING

FOOTPRINTING

Foot printing is the first step of any hacker. We have read already that if any hacker hacks any target or system without knowing target system’s information is called suicide hacking. So this is very necessary to collect all information about target like how many security systems and what is Ip address of that system and which operating system is used by target what is domain name etc. We have read already also that any cyber security expert thinks like a hacker so collection of all information is the first step of any white hat hacker or any hacker. In my point of view definition of foot printing is –

“The way of gathering all information about target system in safe mode is called foot printing.”

Foot printing is divided in two parts or you may say that there are two way to collect all information of any target –

Active foot printing
Passive foot printing

ACTIVE FOOTPRINTING

By active foot printing we can know all active information of target like target is live or not and if we got a e-mail and we want to know all information about that system by which e-mail was send then by active foot printing we can do this and to find loop holes of any website we use some tools so there are some process of active foot printing that are following –

MIRRORING WEBSITE

Mirroring website is a process in which we can download all available contents for offline analysis of any website. After download the contents we can find vulnerability and loop holes in that website and white hat hacker used this to check loop holes by copy whole website contents by using some tools. These tools are –
Track web site copier
iMiser
Teleport Pro

SERVER VERIFICATION –

If we want to hack any system then we have to check that system is live or not, server reachable or not and to check connectivity with target system is called server verification and this checking is very necessary for any hacker and for this we use “PING” command. To enumerate network path from attacker to target we use some command and tools. If we are going to hack any target then we have to know about all those routers or paths by which we want to connect target system and for this we use “TRACERT” command and there are also some tools by which we can done server verification these tools are –
Visual Traceroute
Sam Spade
TCR Trace Route

PASSIVE FOOTPRINTING –

In passive foot printing hacker does not make any contact with target system in other word by passive foot printing hackers collect all information of target system without target system’s knowledge. This type of information is collected by hacker by some tools and from there where all information are available already like –
-Google search
Whois queries
DNS lookup
Social networking site
Google search is used by hacker to collect sensitive or hidden information’s by search engine or browser. If anybody wants to block Google queries then this is impossible because nobody can stop hackers to hack Google data base because they find easily loop holes and vulnerability in target system. For Google hacking some specific words or keywords are used because there are a specific criteria of Google hacking and these words are used with (:) and these words are –
inurl:
intitle:
site:
filetype:
By the help of whois queries and DNS lookup hacker find the website’s Ip address and owner name and registration date and expiry date of that website and many more and after collecting these information hacker search vulnerability with the help of these information and for some personal information hacker use social networking sites because now a day’severybody upload personal details in their profile and hacker take benefit through these information’s.

There are some websites which have already hacked Google's data base like –
www.hackersforcharity.org
www.exploit-db.com
There is a website which provides all details of any website –
- website.informer.com
There is a website which shows any website's past or history –
www.archive.org

SCANNING

We have learned that by foot printing we can get target system's information but this is true that by foot printing we cannot get all information because some information are hidden in target system so to get hidden information's we use scanning in other words we can say that to get further information's after foot printing like which is operating system and how many services are running in target system ant how many open ports etc, we use a different technique and this technique is called foot printing. In my point of view definition of scanning is –

"To know that what is running in the target system currently is called scanning."

Scanning is very important for both attacker or hacker and white hat hacker or ethical hacker because if any organization or company take or choose any certified hacker (white hat hacker) for cyber security then first of all white hat hacker starts scanning in that company's system to find that how many ports or services are open by which any attacker can hack that system, after scanning white hat hacker close the all open ports and services to save from hacker. There are three types of scanning and every type of scanning gives us different types of information related to the target system –
PORT SCANNING
NETWORKING SCANNING
VULNERABILITY SCANNING

PORT SCANNING

Through port scanning any attacker search that how many ports or services are open in target system and these open ports and services are called vulnerability and by these vulnerability attacker enters in target system and then attacker can steal database and other important information's by these vulnerabilities

PORT

Port is a logical connection by which we can send data from one computer to another computer directly. Till now 65,536 ports are available and 1024 (0-1023) are well known ports which are used commonly like for website we use "http". On open these ports hacker hacks system and server because these ports are become boon for hackers to hack any system.

SERVICE

Benefit may be a prepare that runs in computer without any client interaction and these administrations make appropriate working of computer working framework and other related applications. These administrations are as of now built with working framework like –
telnet
ftp
If these administrations are gotten by programmer in target's working framework at that point programmer can hack that framework effortlessly and tries to remotely get to of that framework.

NETWORKING SCANNING

In organizing filtering programmer finds data like every network's Ip address, live have and framework design.

VULNERABILITY SCANNING

In case any programmer is gotten to be victory to know that which computer program is utilized by target framework and which form of that computer program are utilized at that point he tries to discover powerlessness and circle gaps in that computer program in case he is gotten to be victory to discover the powerlessness at that point he tries to control entirety server and after that he runs that server agreeing to claim wish. So to discover this sort of helplessness is called helplessness checking and in case programmer is ended up victory any day to discover any unused powerlessness at that point that day is called "0-day".

O-DAY

On the off chance that any programmer finds any modern defenselessness and no one knows almost that powerlessness at that point that day is called 0-day. This sort of powerlessness is looked by any white cap programmers to shut that circle gap or by any capable programmer to hack somebody. Denial-of-Service (DoS) and Buffer over Stream (BoF) are two vulnerabilities by which o-day created.

For filtering we ought to take after a few steps one by one and these steps are

– CHECK FOR LIVE Framework (To hack any framework typically exceptionally fundamental that framework ought to be on. So to check this assailant doe's ping or ping clear of target framework and for ping or ping clear we utilize a few devices like – irate Ip scanner).

If the attacker has access to the system, they can find out how many ports are open and which services are available. To protect the system from the attacker, we can check the number of ports and services that are open in the system and close them. We can use "currports" tool or follow the path to the target system (e.g. windows, system32, drivers, etc.) and hacker can use "zenmap" tool to check the open ports in the target system. We can also use " id serve " tool to check the number of banners that are being banner grabbed.

PREPARE PROXY (If any hacker doesn't know that how to use proxy that type hacker is called suicide hacker and proxy is very important step for any hacker.)

SCAN FOR VULNERABILITY (After preparing proxy hackers scan or search loop holes and vulnerability and for this we use "nexpose" tool.)

DRAW NETWORK DIAGRAM (This is not any important step for hackers but some hackers use this if they feel that there is need to draw network diagram.)

PROXY

We know that what proxy is because we have used this in classroom for our friends but this is new thing that proxy is used in hacking or in other words proxy is used by hackers but this is true that proxy is used by hackers. To hide their identity hackers use proxy servers. When we open any website in our pc then first of all our pc sends its Ip address to that website then website sends us webpage so this is the point that if hackers will hack any website then they will caught by that website's server because that server knows hacker's Ip address which is send by hacker's pc. So to hide their identity hackers use proxy Ip address and nobody can caught them because if victim will try to find that Ip by which victim's system hacked then he will get that Ip which is used by hacker as a proxy not real Ip address. So in my point of view the definition of proxy in hacking is –

In order to mask the identity of the attacker, proxy servers are used as a mask between the attacker and the target. These servers reveal the attacker's identity other than the real face, and the entire system by which the hacker hides themselves is called a proxy server.

ATTACKER ---------- PROXY SERVER ---------- TARGET

There are two way to use proxy –

LOGGED PROXY –

Logged proxy is a way for hackers to hide their identity by using a single proxy server. They can use any website's IP address or any server's proxy. For this type of proxy, you can use websites like hide.me/proxy, www.hidemyass, etc. You can also use the "proxy switcher" tool to switch between the two, and you can use proxy bouncing to make sure the hacker's location shows different times.

HAINING PROXY

Hackers use proxy chaining to hide their identity and hack into any website or system they want. This type of proxy is used by skilled hackers, so we need to find the server's IP addresses that are active. To do this, we use websites like Proxylist, Hidemyass, and Xroxy. Once we find the IP address, we use the "proxifier" tool to hide our identity. If we visit any website, different IP addresses and locations will show up on the server, so we're safe.

ENUMERATION

We've seen that when we're printing and scanning, we can gather all the info we need using certain tools and commands. But when we're doing this, we weren't really connecting with the target system. We were collecting all the info from the outside to the inside, and then once we had all the info we needed, we could connect with the target system or create an active connection. This active connection is what we call enumeration. Basically, enumeration is the process of making an active connection to or within the target system.

There are five types of enumeration by which we can make an active connection with target system and this are-

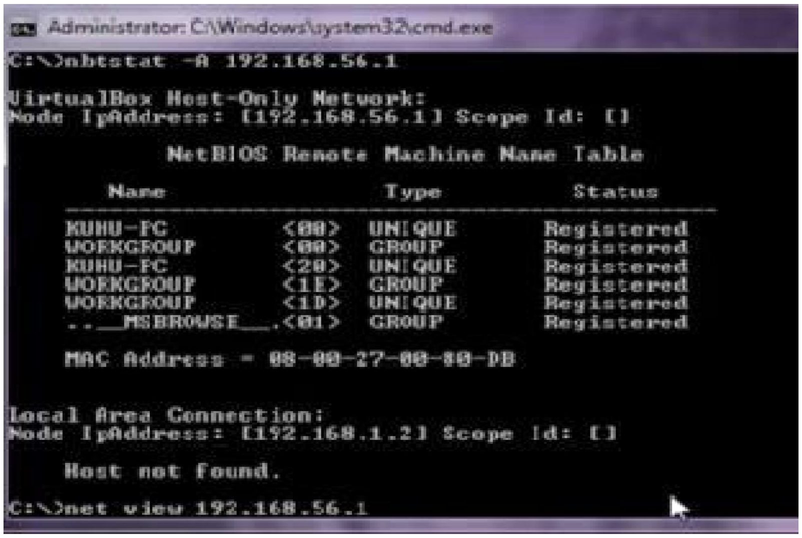
Net Bios
SNMP
LDAP
NTP
DNS

We can use Net Bios to make an active connection to the target system, but most hackers use Net Bios because it's vulnerable and gives them more advantages. Net Bios has an open port that makes it easy for hackers to make active connections. If the port is open, it means the target system is sharing files and printers, which is known as Network Basic Input Output System. Net Bios can work on these open ports. – 445,137,138,139.

If we starts scanning and if we get any port (445 or 137 or 138 or 139) is open then this means that file and printer sharing is on in target system and we can remotely access of this target system. To remotely access any target system we have to follow some steps and these steps are –

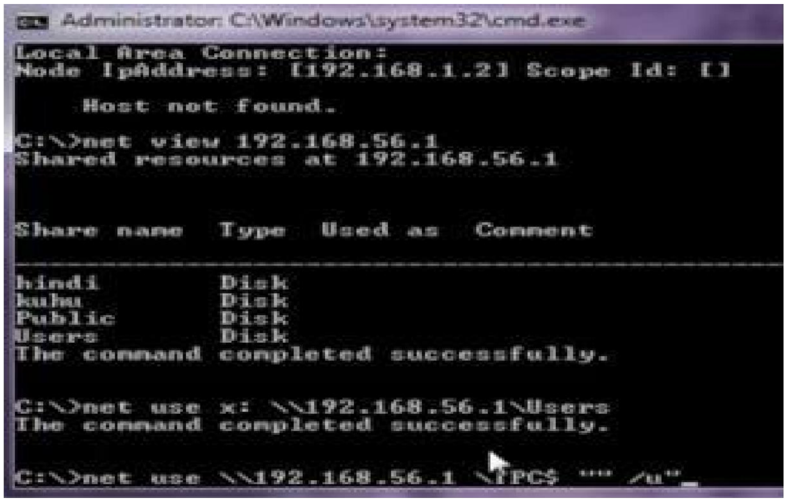
Firstly we will open cmd and then we will type "nbtstat –A (Ip address)" if after pressing enter hex code "<20>" is appear then its mean file and printer sharing is on….and

Then we will type "net view (Ip address)"



```
C:\>nbtstat -A 192.168.56.1

VirtualBox Host-Only Network:
Node IpAddress: [192.168.56.1] Scope Id: []

                NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    KUHU-PC          <00>  UNIQUE      Registered
    WORKGROUP        <00>  GROUP       Registered
    KUHU-PC          <20>  UNIQUE      Registered
    WORKGROUP        <1E>  GROUP       Registered
    WORKGROUP        <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered

    MAC Address = 08-00-27-00-80-DB


Local Area Connection:
Node IpAddress: [192.168.1.2] Scope Id: []

    Host not found.

C:\>net view 192.168.56.1
```

then after pressing enter we will know that how many and which folder is sharing and then we will type "net use x: \\(ip address)\folder name" and if after pressing enter this message will appear "the command was completed successfully" that's mean we can remotely access target system and only we have to type last command "net use \\(ipaddress) \IPC$ "" /u" ".



```
Local Area Connection:
Node IpAddress: [192.168.1.2] Scope Id: []

    Host not found.

C:\>net view 192.168.56.1
Shared resources at 192.168.56.1


Share name   Type   Used as   Comment

-------------------------------------------------------------------------------
hindi        Disk
kuhu         Disk
Public       Disk
Users        Disk
The command completed successfully.


C:\>net use x: \\192.168.56.1\Users
The command completed successfully.


C:\>net use \\192.168.56.1 \IPC$ "" /u"_
```

SYSTEM HACKING

In system hacking this is very necessary to know about windows and password hacking by which we can hack any target system through target's operating system, so to hack any system we have to know that how to hack any window and how to crack it's password.

WINDOWS HACKING –

Any attacker or hacker knows very well about all operating system and that's why attackers are easily entered in our systems and they know about every loop hole and vulnerabilities by which they can create back door for them to enter in our systems and after that they can change our pc's settings and they can also block our important folders and also control panels and we are become unable to access our system and then we have only one option to format our system but if we will know about windows hacking then we do not have to format our system. That's why for any white hat hacker or ethical hacker it is very necessary to know about windows hacking. There are two options or editor present in every operating system by which we can manage our system according to our self and we can protect our operating system by some editing to save our system from attackers by these editor we can control whole operating system that is what we have to show at the place of start button and we can block control panel and everything which we see in our operating system. These two editors are –

Registry

Gpedit

REGISTRY –

Registry is collection of all data by which our operating system run and Microsoft don't Want that anybody know about this data and by this data we can control our operating and We can change everything by this data. In other words we can say that through registry we Can change everything and we can make our operating system according to our self. To Open registry we have to go in run option and there we have to type "regedit" and then Press ok button after pressing ok button a window will open in which two columns will Appear and in this window left side five "HKEY" are present these five keys are called "Hives". If we open any hkey then many subkeys of that hkey will open. These hkey are –

HKEY CLASSES ROOT (to hack or change file types, file name and extensions and similar information's).

HKEY CURRENT USER (to hack or change system setup of the user that is currently logged on.)

HKEY LOCAL MACHINE (to hack or change computer's settings and operating system's settings and all hardware's settings like – keyboard, printer ports, mouse etc.)

HKEY USERS (to hack or change every user's profile settings on the system.)

HKEY CURRENT CONFIG (to hack or change hardware configuration that is currently running on the system.)

To control registry there are some data types and values and we have to set these data types and values in right panel to control registry. These data types of values are –
REG_SZ (string value – in this we use plain text and numbers.)
REG_MULTI_SZ (string array value – in this we use strings of plain text and numbers.)
REG_EXPAND_SZ (expanded string value – in this some variables are used to point the location of files.)
REG_BINARY (binary values – in this we use binary number 0 and 1.)
REG_DWORD (dword values – in this we use binary number and some other numbers also like 456.)
Now we know that we can manage our operating system by our self but there are more than 3000 thousand registries in every operating system so we cannot change all registries but it's not mean that we cannot do this we can but for it more time and knowledge is required. So there are some registry and their path by which we can change some basics settings of any operating system by some editing in that registry –
To remove right-click menu items from files and folders we will follow this path to reach exact registry for editing (HKEY_CLASSES_ROOT*\SHELLEX\CONTEXT MENU HANDLERS) and then we have to select removing item and then in right column we have to press right click at default folder and then a box will open then we have to add a "-" in the starting of the given value and then we will restart our pc and that setting will apply.
- To add legal notice we will follow this path
(HKEY_LOCAL_MACHINE\SOFT\MICRO\ WIN\CV\POLICIES\SYSTEM) and then in right column we will double click at the legal notice caption and a box will appear and in this box we will type that name by which we want to show this notice and then we will press enter and then we will double click at the legal notice text and in this box we will type that message which we want to show as a legal notice and then we will restart our pc then we will see that a legal notice will appear that will be for fun but hacker use this as weapon but if we know about this then there is no need to fear we can close this by same way.
To remove control panel or clock or run or search option we will follow this path (HKEY_ CURRENT_USER\SOFT\MICRO\WIN\CV\POLICIES\EXPLORER) and then in right column we will right click and then we will go in new and then we will ok at the DWORD value and then a folder will appear in right column and in this we will type that name which we want to remove like this – "NoControlPanel" or "NoRun" or "NoFind" and then we will double click at this folder and we will change binary number if 0 is present then we will replace it by 1 and then we will press enter and then we will restart and that setting will apply.

GPEDIT –

In gpedit we can also change or set our operating system according to our self but in gpedit it is easy to edit or change something compare to registry because in gpedit every where mentioned all related information's we have no need to find or search to change something. To edit or change something in gpedit we have to open run and we have to type "gpedit.msc" and after pressing enter a screen will appear and this screen is also divided into two parts left part and right part and in left part both types of settings user settings and computer settings are available and then we can select any option which we want to change and after selection in right panel we have to select an individual option which we want to edit and then we will click at the appropriate option after clicking a screen will appear and then in that screen we have to mark "enable" button to execute that change then we will press ok button. In gpedit there is no need to restart the computer for applying that change only we will refresh the system and that change will apply this is the good point in gpedit.

PASSWORD HACKING -

To know about password hacking this is very necessary to know about what is password? In my point of view –
"Password is collection of words, numbers and symbols which is arranged according to the users in any system or any website or any social networking site by which at the time running time system could recognize that who wants to enter in system which is true user or any other user."
But we know that this is not necessary that only true user can access the right password because by some tools and tricks any other person can also access the right password that person is called attacker and this stealing way of password is called password hacking. So this is very necessary to know that which tricks and tools helps somebody to

steal our password then we can protect our system and other password from attackers. For protection of password we should follow these steps by which we can make a strong password –

When we make a password then we should set a good length of password.

We should use both small and capital laters.

We should use special characters.

We should also use numerical words.

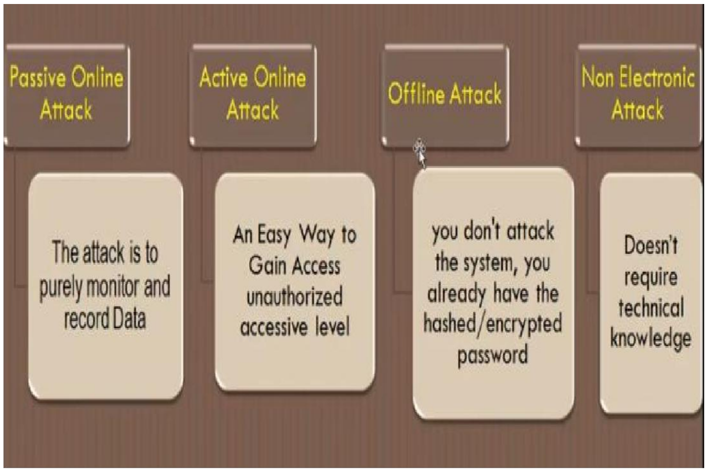
This is very necessary to follow these steps because a normal password can be broken easily by the software but to break a proper password any software takes minimum two months.

At the making time of making password this is also very necessary that that password should be easy to learn. But sometimes users forget the password like –

syskey password

administrator password

So there are some types of password techniques by which users can find their password or to access their password if users forget their password. But attackers also have some techniques by which they find our password and can access our system without our permission.


Passive Online Attack
Active Online Attack
Offline Attack
Non Electronic Attack
The attack is to purely monitor and record Data
An Easy Way to Gain Access unauthorized accessive level
you don't attack the system, you already have the hashed/encrypted password
Doesn't require technical knowledge

TYPES OF PASSWORD CRACKING TECHNIQUES

Basically password cracking techniques are for legal users. If they forget their password then some techniques by which they can access their system or regenerate the password. We can see password cracking techniques in this figure –

TYPES OF PASSWORD ATTACK

Password attack is basically done by hackers to hack password and hackers can hack password by four ways and these four ways are

TYPES OF SYSTEM PASSWORD

In system password we can crack syskey or administrative password of any operating system like –

SYSKEY PASSWORD –

To crack syskey password we need "Hiren's boot CD" if we forget our syskey password then we will insert hiren's boot CD and then again we will restart the computer then automatically CD will start its work and only we have to follow that instructions. First of all we will choose "offline password changer" then we will press enter then boot option will appear then again we have to press enter to boot the CD. After that CD will scan all partition of the system and then "candidate windows partition no." will appear if 1 then we have to type 1 and we will press enter then CD will find path from registry and only we have to press enter then we will select "password reset" option and we will press enter and then we will select 2nd option "syskey status and change" and we will press enter and then system will ask to disable the syskey password then we will type "y" mean yes we want and then we will type "q" to quit from there and in last system will ask about to right files then to make that password change completely we will type “y” and after that system will again ask for any rechange then we will type “n” because we have type everything right. After that we will take out CD and then we will restart our pc and at the time of starting system will not ask syskey password.

ADMINISTRATIVE PASSWORD

To remove or recover administrative password we will directly switch off the system then we will select “launch startup repair” after that we will select first option and we will press next button and then we will choose command prompt and then we will type in cmd “C:” because in c drive windows are installed this may be d or e we will choose according to that and then we will type “cd windows” cd is for to change directory and then we will type “cd system32” and then we have to rename “utilman.exe” because this allows user to enter in the system to change password we will have to rename it for this we will type “ren utilman.exe (other name)” other name means that name which we want to replace at the place of utilman.exe this may be like –“ nexture.exe” and then we will copy cmd in place of utilman because at the time of starting we can open cmd in place of utilman by cmd we can change password for this we will type “copy cmd.exe utilman.exe” and then to come out we will type “exit” and then we will restart our system. When password window will be appeared then we will press “window key + U” and cmd will open and we will type “net user” and then we will press enter and then we will type “net user (user name) password (new)” and then we will come out and in password box we can type new password to enter in the system.

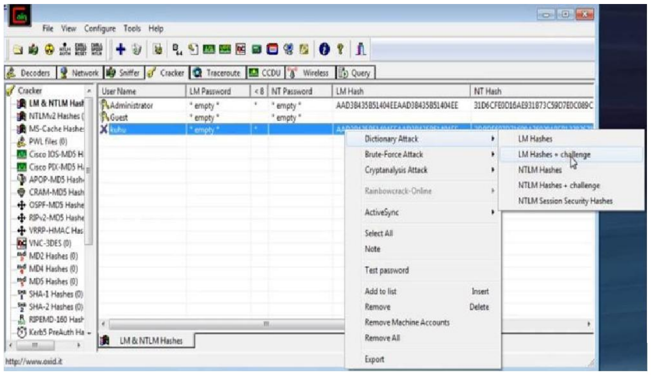
CRACKING OF PASSWORD THROUGH HASHES VALUE –

When we set a password then that password is store in encrypted form that encrypted form of real password is called hashes value and these value is stored in SAM file but nobody can copy or access of this SAM file to copy this SAM file we have to write a program in batch file programming language which is used in hacking or as a hacking language. We will write this program in notepad and we will save it “----.bat” extension.

Program is –

```
“@echo off
Reg SAVE HKLM\SAM C:\SAM
Reg SAVE HKLM\SYSTEM C:\SYSTEM
Exit”
```

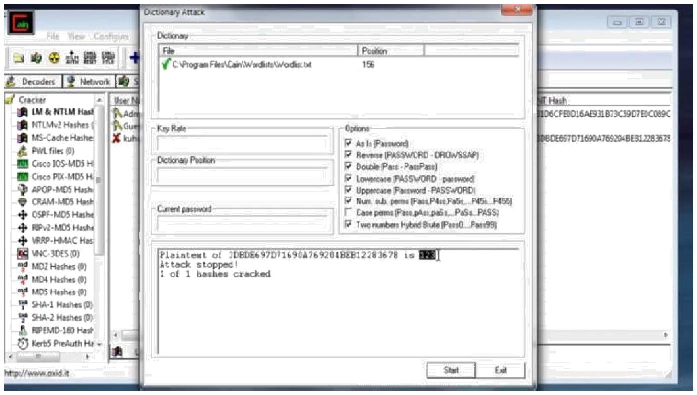
After saving it in .bat extension when we will open it then automatically it will be saved in c drive as a SAM file and a SYSTEM file and now we can copy this file and can access. In SAM file password is present in encrypted form and in SYSTEM file boot hash key is present which used to gain password. To make plane password from encrypted password we use “cain and abel” tool. We will open this tool and then we will click at the “cracker” tab and then we click at “+” tab then a window will appear if we want to crack password in same system then we will choose “import hashes from local system” if we want to crack password in other system then we will choose “import hashes from a sam database” and then we will browse SAM file and then we will browse boot key (SYSTEM file) and we will copy this key and then we will paste it in boot key option. After that we will right click at the encrypted value and then a box will appear to crack password we can choose any attack and any hashes from this box like –



User Name	LM Password	< 8	NT Password	LM Hash	NT Hash
Administrator	* empty *	*	* empty *	AAD3B435B51404EEAAD3B435B51404EE	31D6CFE0D16AE931B73C59D7E0C089C
Guest	* empty *		* empty *		
kuhu	* empty *	*		[illegible]	[illegible]

After choosing an option a new window will open and in this window we have to right click in dictionary file and we will select "add to list" and then we have to open "wordlists" from "cain" which is present in (c drive\ program files\ cain\ wordlists) and then we will choose appropriate option to crack password then we will click at the start button and real password will open like this –

If in one trial password is not coming in real form then we have to choose different – different option until password is not found. After success in white box password will be appeared in real form.



Dictionary Attack

Dictionary

File	Position
C:\Program Files\Cain\Wordlists\Wordlist.txt	156

Key Rate

Dictionary Position

Current password

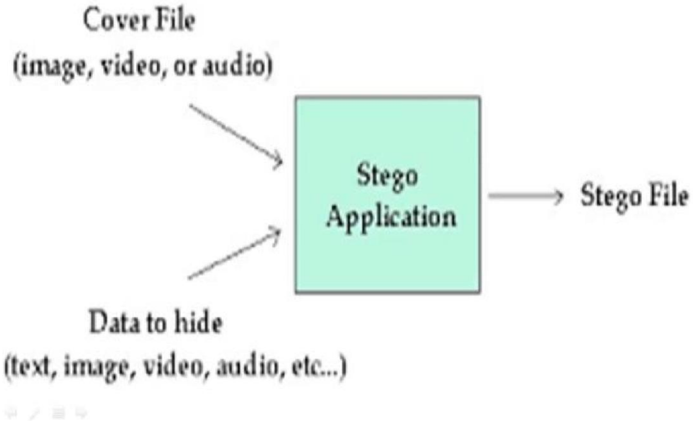
Options

- ☑ As Is (Password)
- ☑ Reverse (PASSWORD - DROWSSAP)
- ☑ Double (Pass - PassPass)
- ☑ Lowercase (PASSWORD - password)
- ☑ Uppercase (Password - PASSWORD)
- ☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- ☐ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- ☑ Two numbers Hybrid Brute (Pass0...Pass99)

```
Plaintext of 3DBDE697D71690A769204BEB12283678 is 123
Attack stopped!
1 of 1 hashes cracked
```

STEGANOGRAPHY

Steganography word is made by two Greek word "stegano" and "graphy" stegano means covering and graphy means writing so we can say that steganography means send something in hidden form. Steganography is mostly used by black hat hacker and these black hat hackers create a hidden file in which target can see only cover file that may be image, any audio, video and hacker write any message or hidden data which is merged with cover file that cannot be seen by target system and if white hat hacker knows that how to break hidden information then that can save their system from this steganography and black hat hacker send viruses from this steganography and that send to us by email or in any other format when we will open this type of file then we will see only cover file and hidden data internally will be installed in our pc and then hacker can control our system so this is very necessary to know that how to break this type of steganography to save our pc but in other hand this steganography is used by white hat hacker to send some important information's which can be access only by that person who know the password of that stegano. The process of steganography can be understood by this outline –



So we can see by stego application we can merge cover file and hidden data and this stego application will make a stego file that can be send by attacker or hacker to the target system.

There are some types of steganography which are used –

TEXT STEGANOGRAPHY

ISSN 2581-9429 IJARSCT
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN SCIENCE, COMMUNICATION AND TECHNOLOGY

AUDIO STEGANOGRAPHY
VIDEO STEGANOGRAPHY
IMAGE STEGANOGRAPHY

To make a stego file we use “xiao steganography” software and if we want to use image steganography then this is very necessary that that image file must be in “bmp” format and which we want to hide in text format that must be written in notepad and we will open that software and we will click add files and then after selecting image file we will press next button and then we will add text file and then we will press next button and then we will set a password that no one could access this and then we will press next button and we will save this file. But if we want to read any stegano file then we will select extract files and then we will add stegano file and then we will enter password and then we will extract file and we will save it in the system and that file can be read easily.

To make a stego file we can make it through cmd also for it we have to open cmd and we will choose that directory where files are available by which we want to make a stego file like if my folder is pagan and it is present at desktop then we will give these commands –

```
Cd desktop      Press enter
Cdpagan         Press enter
```

Then we will copy files in image file for it we will type –

Copy /b (image file name like “sdf.jpg”) + (text file name like “sdf.rar”)
(New file name in “.jpg” format)

If we want to hide any video file by any image file then we will use “stealth files” software and then we will hide the file and then we will retrieve file and our file will save in c drive in stealth folder. In source file we will choose video file and in carrier file we will select image file.

So by these ways we can make a stego file