Dr. D. Y. Patil Pratishthan's

Institute for Advanced Computing &Software Development

IACSD

ETHICAL HACKING

INDEX

Ethical Hacking Introduction

Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is what we call **Ethical Hacking**.

A computer expert who does the act of hacking is called a "Hacker". Hackers are those who seek knowledge, to understand how systems operate, how they are designed, and then attempt to play with these systems.

Types of Hacking

We can segregate hacking into different categories, based on what is being hacked. Here is a set of examples −

- **Website Hacking** − Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.
- **Network Hacking** − Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.
- **Email Hacking** − It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.
- **Ethical Hacking** − Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.
- **Password Hacking** − This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.

- **Computer Hacking** − This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Advantages of Hacking

Hacking is quite useful in the following scenarios −

- To recover lost information, especially in case you lost your password.
- To perform penetration testing to strengthen computer and network security.
- To put adequate preventative measures in place to prevent security breaches.
- To have a computer system that prevents malicious hackers from gaining access.

Disadvantages of Hacking

Hacking is quite dangerous if it is done with harmful intent. It can cause −

- Massive security breach.
- Unauthorized system access on private information.
- Privacy violation.
- Hampering system operation.
- Denial of service attacks.
- Malicious attack on the system.

Purpose of Hacking

There could be various positive and negative intentions behind performing hacking activities. Here is a list of some probable reasons why people indulge in hacking activities −

- Just for fun

- Show-off
- Steal important information
- Damaging the system
- Hampering privacy
- Money extortion
- System security testing
- To break policy compliance

Hacker Types

White Hat Hackers

White Hat hackers are also known as **Ethical Hackers**. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.

Black Hat Hackers

Black Hat hackers, also known as **crackers**, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information.

Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

Grey Hat Hackers

Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or knowledge.

Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

Miscellaneous Hackers

Apart from the above well-known classes of hackers, we have the following categories of hackers based on what they hack and how they do it −

Red Hat Hackers

Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

Blue Hat Hackers

A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term **BlueHat** to represent a series of security briefing events.

Elite Hackers

This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

Script Kiddie

A script kiddie is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, hence the term **Kiddie**.

Neophyte

A neophyte, "n00b", or "newbie" or "Green Hat Hacker" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology and hacking.

Hacktivist

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denialof-service attacks.

Ethical Hacking – Terminologies

Following is a list of important terms used in the field of hacking.

- **Adware** − Adware is software designed to force pre-chosen ads to display on your system.
- **Attack** − An attack is an action that is done on a system to get its access and extract sensitive data.
- **Back door** − A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections.
- **Bot** − A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. For example, sending HTTP, FTP or Telnet at a higher rate or calling script to create objects at a higher rate.
- **Botnet** − A botnet, also known as zombie army, is a group of computers controlled without their owners' knowledge. Botnets are used to send spam or make denial of service attacks.
- **Brute force attack** − A brute force attack is an automated and the simplest kind of method to gain access to a system or website. It tries different combination of usernames and passwords, over and over again, until it gets in.
- **Buffer Overflow** − Buffer Overflow is a flaw that occurs when more data is written to a block of memory, or buffer, than the buffer is allocated to hold.

- **Clone phishing** − Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.
- **Cracker** − A cracker is one who modifies the software to access the features which are considered undesirable by the person cracking the software, especially copy protection features.
- **Denial of service attack (DoS)** − A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.
- **DDoS** − Distributed denial of service attack.
- **Exploit Kit** − An exploit kit is software system designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it and exploiting discovered vulnerabilities to upload and execute malicious code on the client.
- **Exploit** − Exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to compromise the security of a computer or network system.
- **Firewall** − A firewall is a filter designed to keep unwanted intruders outside a computer system or network while allowing safe communication between systems and users on the inside of the firewall.
- **Keystroke logging** − Keystroke logging is the process of tracking the keys which are pressed on a computer (and which touchscreen points are used). It is simply the map of a computer/human interface. It is used by gray and black hat hackers to record login IDs and passwords. Keyloggers are usually secreted onto a device using a Trojan delivered by a phishing email.
- **Logic bomb** − A virus secreted into a system that triggers a malicious action when certain conditions are met. The most common version is the time bomb.

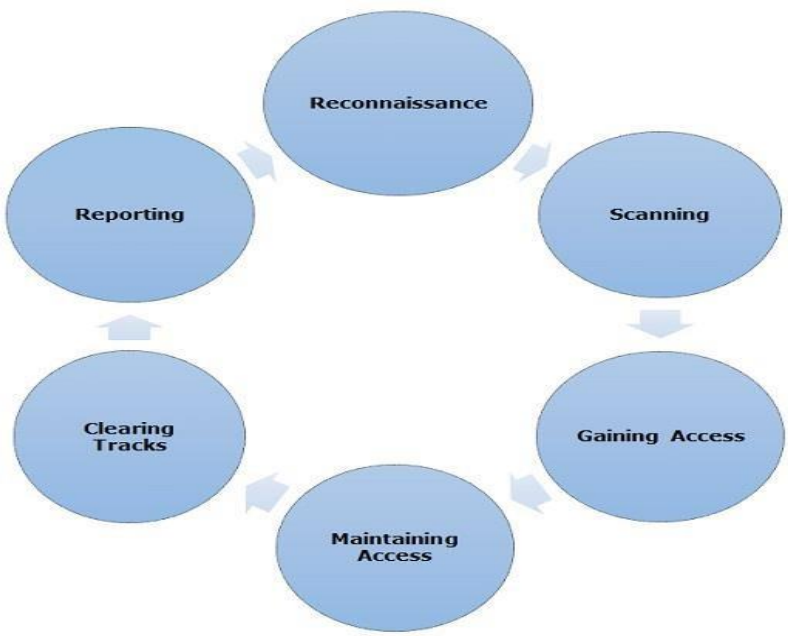
- **Malware** − Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.
- **Master Program** − A master program is the program a black hat hacker uses to remotely transmit commands to infected zombie drones, normally to carry out Denial of Service attacks or spam attacks.
- **Phishing** − Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking emails, in an attempt to gather personal and financial information from recipients.
- **Phreaker** − Phreakers are considered the original computer hackers and they are those who break into the telephone network illegally, typically to make free longdistance phone calls or to tap phone lines.
- **Rootkit** − Rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.
- **Shrink Wrap code** − A Shrink Wrap code attack is an act of exploiting holes in unpatched or poorly configured software.
- **Social engineering** − Social engineering implies deceiving someone with the purpose of acquiring sensitive and personal information, like credit card details or user names and passwords.
- **Spam** − A Spam is simply an unsolicited email, also known as junk email, sent to a large number of recipients without their consent.
- **Spoofing** − Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

- **Spyware** − Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.
- **SQL Injection** − SQL injection is an SQL code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- **Threat** − A threat is a possible danger that can exploit an existing bug or vulnerability to compromise the security of a computer or network system.
- **Trojan** − A Trojan, or Trojan Horse, is a malicious program disguised to look like a valid program, making it difficult to distinguish from programs that are supposed to be there designed with an intention to destroy files, alter information, steal passwords or other information.
- **Virus** − A virus is a malicious program or a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.
- **Vulnerability** − A vulnerability is a weakness which allows a hacker to compromise the security of a computer or network system.
- **Worms** − A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.
- **Cross-site Scripting** − Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users.
- **Zombie Drone** − A Zombie Drone is defined as a hi-jacked computer that is being used anonymously as a soldier or 'drone' for malicious activity, for example, distributing unwanted spam e-mails.

Ethical Hacking Process

Like all good projects, ethical hacking too has a set of distinct phases. It helps hackers to make a structured ethical hacking attack.

Different security training manuals explain the process of ethical hacking in different ways, but for me as a Certified Ethical Hacker, the entire process can be categorized into the following six phases.



Reconnaissance

Reconnaissance is the phase where the attacker gathers information about a target using active or passive means. The tools that are widely used in this process are NMAP, Hping, Maltego, and Google Dorks.

Scanning

In this process, the attacker begins to actively probe a target machine or network for vulnerabilities that can be exploited. The tools used in this process are Nessus, Nexpose, and NMAP.

Gaining Access

In this process, the vulnerability is located and you attempt to exploit it in order to enter into the system. The primary tool that is used in this process is Metasploit.

Maintaining Access

It is the process where the hacker has already gained access into a system. After gaining access, the hacker installs some backdoors in order to enter into the system when he needs access in this owned system in future. Metasploit is the preferred tool in this process.

Clearing Tracks

This process is actually an unethical activity. It has to do with the deletion of logs of all the activities that take place during the hacking process.

Reporting

Reporting is the last step of finishing the ethical hacking process. Here the Ethical Hacker compiles a report with his findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

Reconnaissance

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

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

- Gather initial information
- Determine the network range
- Identify active machines
- Discover open ports and access points
- Fingerprint the operating system
- Uncover services on ports
- Map the network

We will discuss in detail all these steps in the subsequent chapters of this tutorial. Reconnaissance takes place in two parts − **Active Reconnaissance** and **Passive Reconnaissance**.

Active Reconnaissance

In this process, you will directly interact with the computer system to gain information. This information can be relevant and accurate. But there is a risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then system admin can take severe action against you and trail your subsequent activities.

Passive Reconnaissance

In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

Footprinting

Footprinting is a part of reconnaissance process which is used for gathering possible information about a target computer system or network. Footprinting could be both **passive** and **active**. Reviewing a company's website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.

Footprinting is basically the first step where hacker gathers as much information as possible to find ways to intrude into a target system or at least decide what type of attacks will be more suitable for the target.

During this phase, a hacker can collect the following information −

- Domain name
- IP Addresses
- Namespaces
- Employee information
- Phone numbers
- E-mails
- Job Information

In the following section, we will discuss how to extract the basic and easily accessible information about any computer system or network that is linked to the Internet.

Domain Name Information

You can use http://www.whois.com/whois website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.

Note - It's always recommended to keep your domain name profile a private one which should hide the above-mentioned information from potential hackers.

Finding IP Address

You can use **ping** command at your prompt. This command is available on Windows as well as on Linux OS. Following is the example to find out the IP address of tutorialspoint.com

$ping tutorialspoint.com

It will produce the following result −

PING test.com (66.135.33.172) 56(84) bytes of data.
64 bytes from 66.135.33.172: icmp_seq = 1 ttl = 64 time = 0.028 ms
64 bytes from 66.135.33.172: icmp_seq = 2 ttl = 64 time = 0.021 ms
64 bytes from 66.135.33.172: icmp_seq = 3 ttl = 64 time = 0.021 ms
64 bytes from 66.135.33.172: icmp_seq = 4 ttl = 64 time = 0.021 ms

Finding Hosting Company

Once you have the website address, you can get further detail by using ip2location.com website. Following is the example to find out the details of an IP address −

	Field Name	Value
	IP Address	49.205.122.168
☑	Country	India
☐	Region & City	Kukatpalli, Telangana
☐	Latitude & Longitude	17.48333, 78.41667
☐	ZIP Code	508126
☐	ISP	Beam Telecom Pvt Ltd
☐	Domain	beamtele.com
☐	Time Zone	+05:30

Here the ISP row gives you the detail about the hosting company because IP addresses are usually provided by hosting companies only.

Note

If a computer system or network is linked with the Internet directly, then you cannot hide the IP address and the related information such as the hosting company, its location, ISP, etc. If you have a server containing very sensitive data, then it is recommended to keep it behind a secure proxy so that hackers cannot get the exact details of your actual server. This way, it will be difficult for any potential hacker to reach your server directly.

Another effective way of hiding your system IP and ultimately all the associated information is to go through a Virtual Private Network (VPN). If you configure a VPN,

then the whole traffic routes through the VPN network, so your true IP address assigned by your ISP is always hidden.

IP Address Ranges

Small sites may have a single IP address associated with them, but larger websites usually have multiple IP addresses serving different domains and sub-domains.

You can obtain a range of IP addresses assigned to a particular company using American Registry for Internet Numbers (ARIN).

You can enter company name in the highlighted search box to find out a list of all the assigned IP addresses to that company.

History of the Website

It is very easy to get a complete history of any website using www.archive.org.

You can enter a domain name in the search box to find out how the website was looking at a given point of time and what were the pages available on the website on different dates.

Note

Though there are some advantages of keeping your website in an archive database, but if you do not like anybody to see how your website progressed through different stages, then you can request archive.org to delete the history of your website.

Fingerprinting

The term OS fingerprinting in Ethical Hacking refers to any method used to determine what operating system is running on a remote computer. This could be −

- **Active Fingerprinting** − Active fingerprinting is accomplished by sending specially crafted packets to a target machine and then noting down its response and analyzing the gathered information to determine the target OS. In the following section, we have given an example to explain how you can use NMAP tool to detect the OS of a target domain.
- **Passive Fingerprinting** − Passive fingerprinting is based on sniffer traces from the remote system. Based on the sniffer traces (such as Wireshark) of the packets, you can determine the operating system of the remote host.

We have the following four important elements that we will look at to determine the operating system −

- **TTL** − What the operating system sets the **Time-To-Live** on the outbound packet.
- **Window Size** − What the operating system sets the Window Size at.
- **DF** − Does the operating system set the **Don't Fragment** bit.
- **TOS** − Does the operating system set the **Type of Service**, and if so, at what.

By analyzing these factors of a packet, you may be able to determine the remote operating system. This system is not 100% accurate, and works better for some operating systems than others.

Basic Steps

Before attacking a system, it is required that you know what operating system is hosting a website. Once a target OS is known, then it becomes easy to determine which vulnerabilities might be present to exploit the target system.

Below is a simple **nmap** command which can be used to identify the operating system serving a website and all the opened ports associated with the domain name, i.e., the IP address.

$nmap -O -v test.com

It will show you the following sensitive information about the given domain name or IP address −

Starting Nmap 5.51 (http://nmap.org) at 2015-10-04 09:57 CDT
Initiating Parallel DNS resolution of 1 host. at 09:57
Completed Parallel DNS resolution of 1 host. at 09:57, 0.00s elapsed
Initiating SYN Stealth Scan at 09:57
Scanning test.com(66.135.33.172) [1000 ports]
Discovered open port 22/tcp on 66.135.33.172
Discovered open port 3306/tcp on 66.135.33.172
Discovered open port 80/tcp on 66.135.33.172
Discovered open port 443/tcp on 66.135.33.172
Completed SYN Stealth Scan at 09:57, 0.04s elapsed (1000 total ports)
Initiating OS detection (try #1) against test.com(66.135.33.172)
Retrying OS detection (try #2) against test.com(66.135.33.172)
Retrying OS detection (try #3) against test.com(66.135.33.172)
Retrying OS detection (try #4) against test.com(66.135.33.172)

```
Retrying OS detection (try #5) against test.com(66.135.33.172)
Nmap scan report for test.com(66.135.33.172)
Host is up (0.000038s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open ssh
80/tcp   open http
443/tcp open https
3306/tcp open  mysql
```

You can go through **nmap** command in detail to check and understand the different features associated with a system and secure it against malicious attacks.

Note

You can hide your main system behind a secure proxy server or a VPN so that your complete identity is safe and ultimately your main system remains safe.

Port Scanning

We have just seen information given by **nmap** command. This command lists down all the open ports on a given server.

```
PORT      STATE   SERVICE
22/tcp    open    ssh
80/tcp    open    http
443/tcp   open    https
3306/tcp  open    mysql
```

You can also check if a particular port is opened or not using the following command –

```
$nmap -sT -p 443 test.com
```

It will produce the following result −

```
Starting Nmap 5.51 ( http://nmap.org ) at 2015-10-04 10:19 CDT
Nmap scan report for test.com(66.135.33.172)
Host is up (0.000067s latency).
PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

Once a hacker knows about open ports, then he can plan different attack techniques through the open ports.

Note

It is always recommended to check and close all the unwanted ports to safeguard the system from malicious attacks.

Ping Sweep

A ping sweep is a network scanning technique that you can use to determine which IP address from a range of IP addresses map to live hosts. Ping Sweep is also known as **ICMP sweep**.

You can use **fping** command for ping sweep. This command is a ping-like program which uses the Internet Control Message Protocol (ICMP) echo request to determine if a host is up.

fping is different from **ping** in that you can specify any number of hosts on the command line, or specify a file containing the lists of hosts to ping. If a host does not respond within a certain time limit and/or retry limit, it will be considered unreachable.

Note

To disable ping sweeps on a network, you can block ICMP ECHO requests from outside sources. This can be done using the following command which will create a firewall rule in **iptable**.

$iptables -A OUTPUT -p icmp --icmp-type echo-request -j DROP

DNS Enumeration

Domain Name Server (DNS) is like a map or an address book. In fact, it is like a distributed database which is used to translate an IP address 192.111.1.120 to a name www.example.com and vice versa.

DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. The idea is to gather as much interesting details as possible about your target before initiating an attack.

You can use **nslookup** command available on Linux to get DNS and host-related information. In addition, you can use the following **DNSenum** script to get detailed information about a domain −

DNSenum.pl

DNSenum script can perform the following important operations −

- Get the host's addresses
- Get the nameservers
- Get the MX record
- Perform **axfr** queries on nameservers
- Get extra names and subdomains via **Google scraping**

- Brute force subdomains from file can also perform recursion on subdomain that has NS records
- Calculate C class domain network ranges and perform **whois** queries on them
- Perform **reverse lookups** on **netranges**

Note

DNS Enumeration does not have a Note and it is really beyond the scope of this tutorial. Preventing DNS Enumeration is a big challenge.

If your DNS is not configured in a secure way, it is possible that lots of sensitive information about the network and organization can go outside and an untrusted Internet user can perform a DNS zone transfer.

Sniffing

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of "tapping phone wires" and get to know about the conversation. It is also called **wiretapping** applied to the computer networks.

There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.

In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

What can be sniffed?

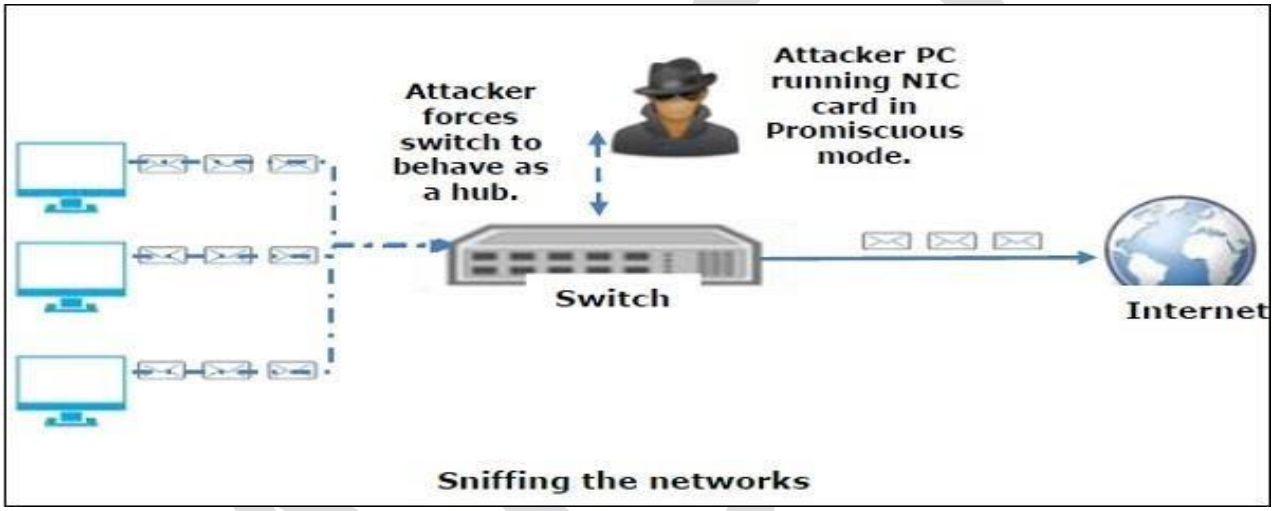
One can sniff the following sensitive information from a network −

- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

How it works

A sniffer normally turns the NIC of the system to the **promiscuous mode** so that it listens to all the data transmitted on its segment.

Promiscuous mode refers to the unique way of Ethernet hardware, in particular, network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.



A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

Types of Sniffing

Sniffing can be either Active or Passive in nature.

Passive Sniffing

In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

The good news is that hubs are almost obsolete no1wadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

Active Sniffing

In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting **address resolution packets** (ARP) into a target network to flood on the switch **content addressable memory** (CAM) table. CAM keeps track of which host is connected to which port.

Following are the Active Sniffing Techniques −

- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Spoofing Attacks
- ARP Poisoning

Protocols which are affected

Protocols such as the tried and true TCP/IP were never designed with security in mind and therefore do not offer much resistance to potential intruders. Several rules lend themselves to easy sniffing −

- **HTTP** − It is used to send information in the clear text without any encryption and thus a real target.
- **SMTP** (Simple Mail Transfer Protocol) − SMTP is basically utilized in the transfer of emails. This protocol is efficient, but it does not include any protection against sniffing.
- **NNTP** (Network News Transfer Protocol)− It is used for all types of communications, but its main drawback is that data and even passwords are sent over the network as clear text.

- **POP** (Post Office Protocol) − POP is strictly used to receive emails from the servers. This protocol does not include protection against sniffing because it can be trapped.
- **FTP** (File Transfer Protocol) − FTP is used to send and receive files, but it does not offer any security features. All the data is sent as clear text that can be easily sniffed.
- **IMAP** (Internet Message Access Protocol) − IMAP is same as SMTP in its functions, but it is highly vulnerable to sniffing.
- **Telnet** − Telnet sends everything (usernames, passwords, keystrokes) over the network as clear text and hence, it can be easily sniffed.

Sniffers are not the dumb utilities that allow you to view only live traffic. If you really want to analyze each packet, save the capture and review it whenever time allows.

Hardware Protocol Analyzers

Before we go into further details of sniffers, it is important that we discuss about **hardware protocol analyzers**. These devices plug into the network at the hardware level and can monitor traffic without manipulating it.

- Hardware protocol analyzers are used to monitor and identify malicious network traffic generated by hacking software installed in the system.
- They capture a data packet, decode it, and analyze its content according to certain rules.
- Hardware protocol analyzers allow attackers to see individual data bytes of each packet passing through the cable.

These hardware devices are not readily available to most ethical hackers due to their enormous cost in many cases.

Lawful Interception

Lawful Interception (LI) is defined as legally sanctioned access to communications network data such as telephone calls or email messages. LI must always be in pursuance of a lawful authority for the purpose of analysis or evidence. Therefore, LI is a security process in which a network operator or service provider gives law enforcement officials permission to access private communications of individuals or organizations.

Almost all countries have drafted and enacted legislation to regulate lawful interception procedures; standardization groups are creating LI technology specifications. Usually, LI activities are taken for the purpose of infrastructure protection and cyber security. However, operators of private network infrastructures can maintain LI capabilities within their own networks as an inherent right, unless otherwise prohibited.

LI was formerly known as **wiretapping** and has existed since the inception of electronic communications.

Sniffing Tools

There are so many tools available to perform sniffing over a network, and they all have their own features to help a hacker analyze traffic and dissect the information. Sniffing tools are extremely common applications. We have listed here some of the interesting ones −

- **BetterCAP** − BetterCAP is a powerful, flexible and portable tool created to perform various types of MITM attacks against a network, manipulate HTTP, HTTPS and TCP traffic in real-time, sniff for credentials, and much more.
- **Ettercap** − Ettercap is a comprehensive suite for man-in-the-middle attacks. It features sniffing of live connections, content filtering on the fly and many other

interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

- **Wireshark** − It is one of the most widely known and used packet sniffers. It offers a tremendous number of features designed to assist in the dissection and analysis of traffic.
- **Tcpdump** − It is a well-known command-line packet analyzer. It provides the ability to intercept and observe TCP/IP and other packets during transmission over the network. Available at www.tcpdump.org.
- **WinDump** − A Windows port of the popular Linux packet sniffer tcpdump, which is a command-line tool that is perfect for displaying header information.
- **OmniPeek** − Manufactured by WildPackets, OmniPeek is a commercial product that is the evolution of the product EtherPeek.
- **Dsniff** − A suite of tools designed to perform sniffing with different protocols with the intent of intercepting and revealing passwords. Dsniff is designed for Unix and Linux platforms and does not have a full equivalent on the Windows platform.
- **EtherApe** − It is a Linux/Unix tool designed to display graphically a system's incoming and outgoing connections.
- **MSN Sniffer** − It is a sniffing utility specifically designed for sniffing traffic generated by the MSN Messenger application.
- **NetWitness NextGen** − It includes a hardware-based sniffer, along with other features, designed to monitor and analyze all traffic on a network. This tool is used by the FBI and other law enforcement agencies.

A potential hacker can use any of these sniffing tools to analyze traffic on a network and dissect information.

ARP Poisoning

Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine MAC addresses. All network devices that need to communicate on the network broadcast ARP queries in the system to find out other machines' MAC addresses. ARP Poisoning is also known as **ARP Spoofing**.

Here is how ARP works −

- When one machine needs to communicate with another, it looks up its ARP table.
- If the MAC address is not found in the table, the **ARP_request** is broadcasted over the network.
- All machines on the network will compare this IP address to MAC address.
- If one of the machines in the network identifies this address, then it will respond to the **ARP_request** with its IP and MAC address.
- The requesting computer will store the address pair in its ARP table and communication will take place.

What is ARP Spoofing?

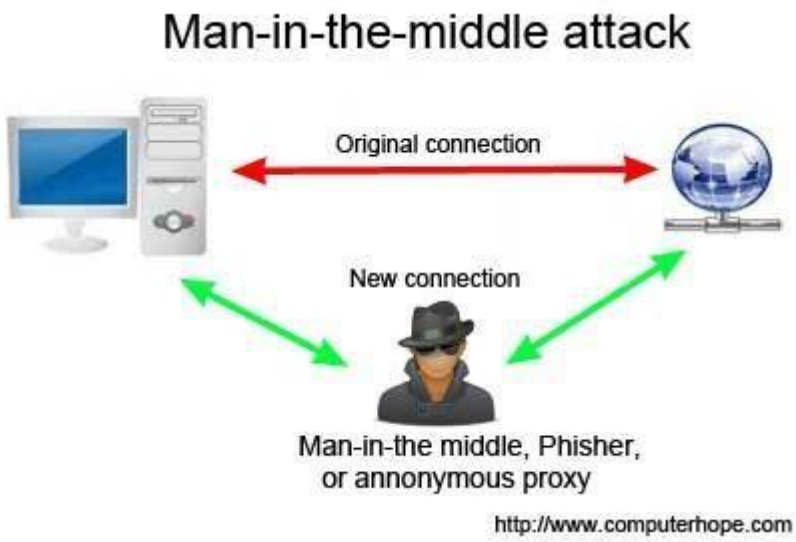
ARP packets can be forged to send data to the attacker's machine.

- ARP spoofing constructs a large number of forged ARP request and reply packets to overload the switch.
- The switch is set in **forwarding mode** and after the **ARP table** is flooded with spoofed ARP responses, the attackers can sniff all network packets.

Attackers flood a target computer ARP cache with forged entries, which is also known as **poisoning**. ARP poisoning uses Man-in-the-Middle access to poison the network.

What is MITM?

The Man-in-the-Middle attack (abbreviated MITM, MitM, MIM, MiM, MITMA) implies an active attack where the adversary impersonates the user by creating a connection between the victims and sends messages between them. In this case, the victims think that they are communicating with each other, but in reality, the malicious actor controls the communication.



A third person exists to control and monitor the traffic of communication between two parties. Some protocols such as **SSL** serve to prevent this type of attack.

ARP Poisoning − Exercise

In this exercise, we have used **BetterCAP** to perform ARP poisoning in LAN environment using VMware workstation in which we have installed **Kali** Linux and **Ettercap** tool to sniff the local traffic in LAN.

For this exercise, you would need the following tools −

- VMware workstation
- Kali Linux or Linux Operating system
- Ettercap Tool

- LAN connection

Note − This attack is possible in wired and wireless networks. You can perform this attack in local LAN.

Step 1 − Install the VMware workstation and install the Kali Linux operating system.

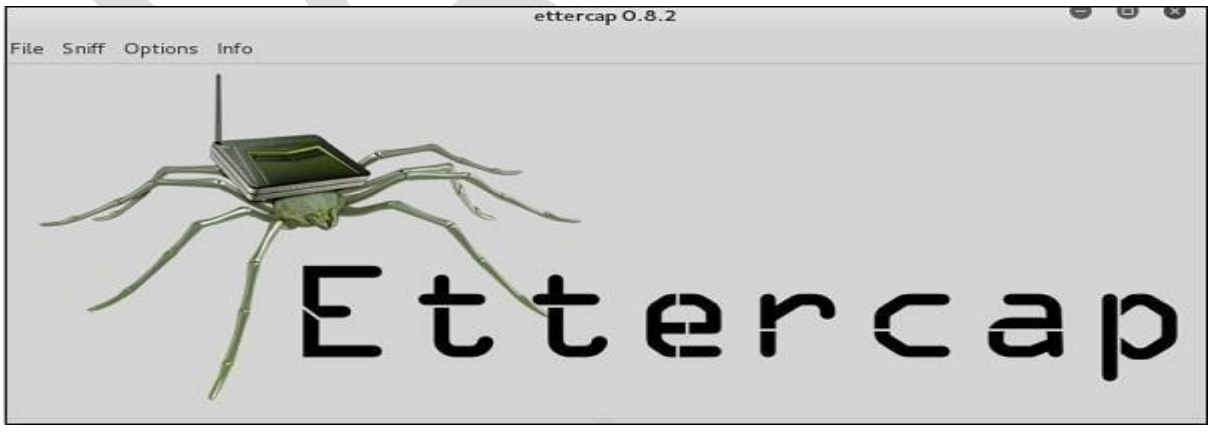
Step 2 − Login into the Kali Linux using username pass "root, toor".

Step 3 − Make sure you are connected to local LAN and check the IP address by typing the command **ifconfig** in the terminal.

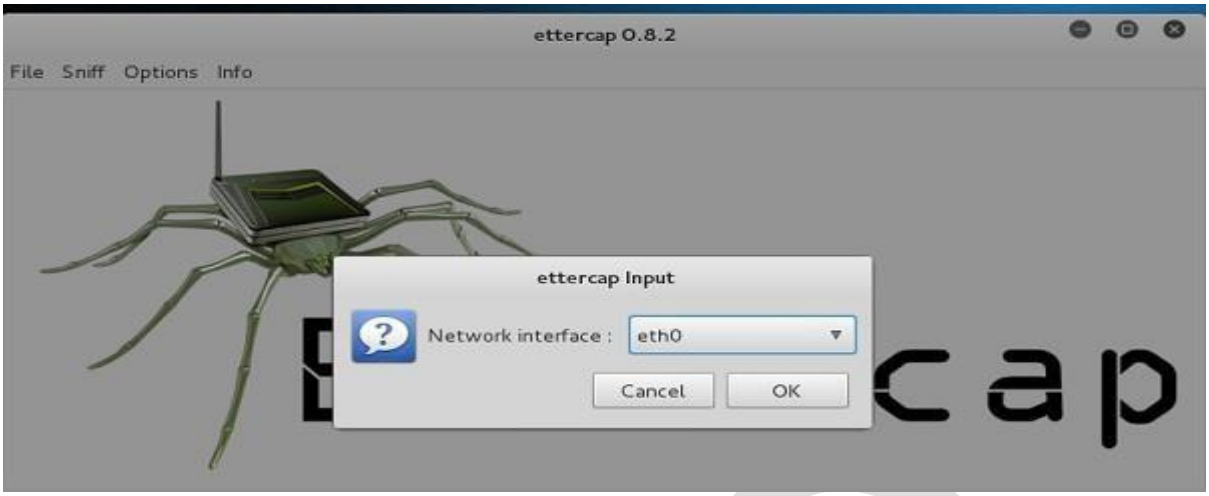
```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:cf:f8:e7
          inet addr:192.168.121.128  Bcast:192.168.121.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fecf:f8e7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:70 errors:0 dropped:0 overruns:0 frame:0
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4963 (4.8 KiB)  TX bytes:8868 (8.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:960 (960.0 B)  TX bytes:960 (960.0 B)
```

Step 4 − Open up the terminal and type "Ettercap –G" to start the graphical version of Ettercap.

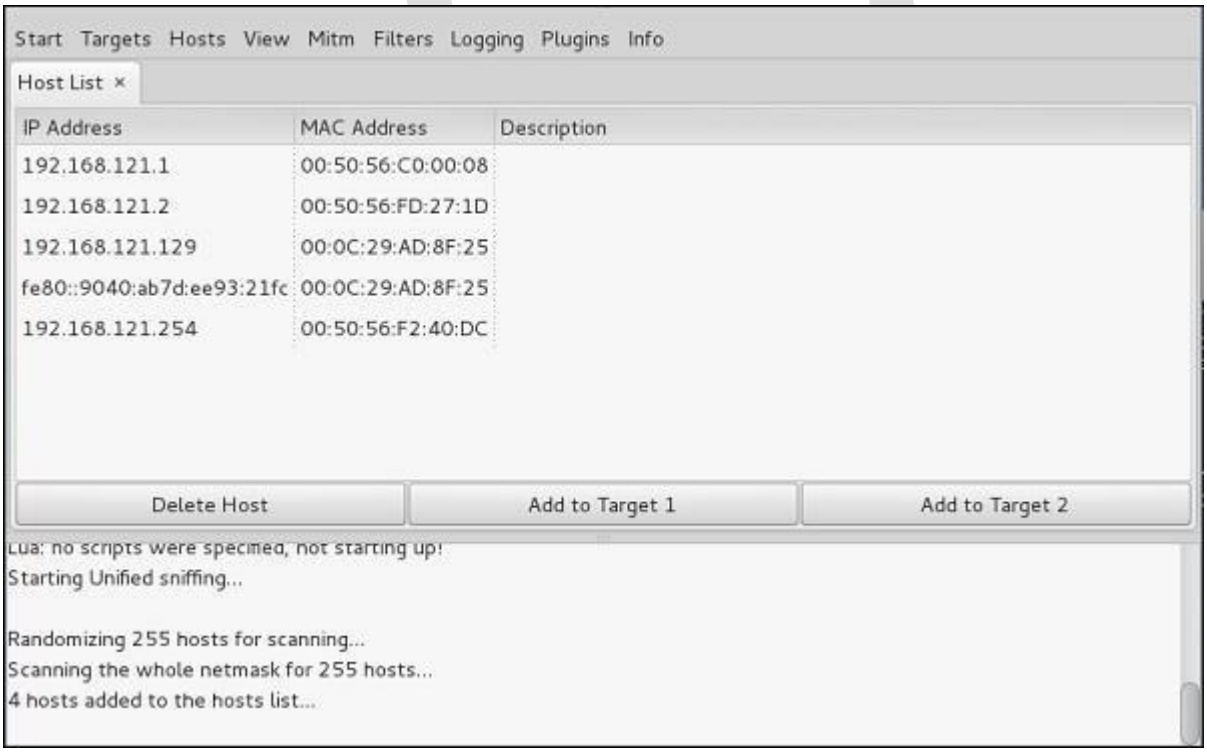


Step 5 − Now click the tab "sniff" in the menu bar and select "unified sniffing" and click OK to select the interface. We are going to use "eth0" which means Ethernet connection.



Step 6 − Now click the "hosts" tab in the menu bar and click "scan for hosts". It will start scanning the whole network for the alive hosts.

Step 7 − Next, click the "hosts" tab and select "hosts list" to see the number of hosts available in the network. This list also includes the default gateway address. We have to be careful when we select the targets.

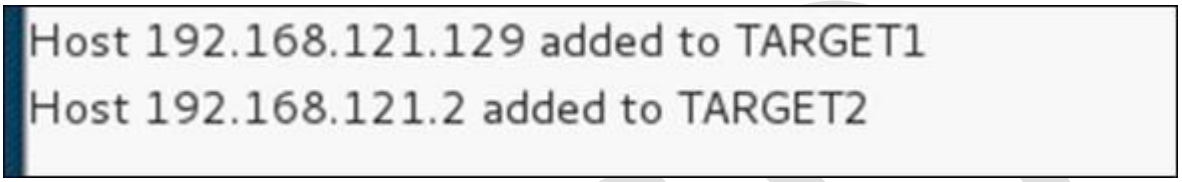


Step 8 − Now we have to choose the targets. In MITM, our target is the host machine, and the route will be the router address to forward the traffic. In an MITM attack, the

attacker intercepts the network and sniffs the packets. So, we will add the victim as "target 1" and the router address as "target 2."

In VMware environment, the default gateway will always end with "2" because "1" is assigned to the physical machine.

Step 9 − In this scenario, our target is "192.168.121.129" and the router is "192.168.121.2". So we will add target 1 as **victim IP** and target 2 as **router IP**.



Step 10 − Now click on "MITM" and click "ARP poisoning". Thereafter, check the option "Sniff remote connections" and click OK.

Step 11 − Click "start" and select "start sniffing". This will start ARP poisoning in the network which means we have enabled our network card in "promiscuous mode" and now the local traffic can be sniffed.

Note − We have allowed only HTTP sniffing with Ettercap, so don't expect HTTPS packets to be sniffed with this process.

Step 12 − Now it's time to see the results; if our victim logged into some websites. You can see the results in the toolbar of Ettercap.

This is how sniffing works. You must have understood how easy it is to get the HTTP credentials just by enabling ARP poisoning.

ARP Poisoning has the potential to cause huge losses in company environments. This is the place where ethical hackers are appointed to secure the networks.

Like ARP poisoning, there are other attacks such as MAC flooding, MAC spoofing, DNS poisoning, ICMP poisoning, etc. that can cause significant loss to a network.

In the next chapter, we will discuss another type of attack known as **DNS poisoning**.

DNS Poisoning

DNS Poisoning is a technique that tricks a DNS server into believing that it has received authentic information when, in reality, it has not. It results in the substitution of false IP address at the DNS level where web addresses are converted into numeric IP addresses. It allows an attacker to replace IP address entries for a target site on a given DNS server with IP address of the server controls. An attacker can create fake DNS entries for the server which may contain malicious content with the same name.

For instance, a user types www.google.com, but the user is sent to another fraud site instead of being directed to Google's servers. As we understand, DNS poisoning is used to redirect the users to fake pages which are managed by the attackers.

DNS Poisoning − Exercise

Let's do an exercise on DNS poisoning using the same tool, **Ettercap**.

DNS Poisoning is quite similar to ARP Poisoning. To initiate DNS poisoning, you have to start with ARP poisoning, which we have already discussed in the previous chapter. We will use **DNS spoof** plugin which is already there in Ettercap.

Step 1 − Open up the terminal and type "nano etter.dns". This file contains all entries for DNS addresses which is used by Ettercap to resolve the domain name addresses. In this file, we will add a fake entry of "Facebook". If someone wants to open Facebook, he will be redirected to another website.

```
root@kali:~# locate etter.dns
/etc/ettercap/etter.dns
root@kali:~# nano /etc/ettercap/etter.dns
```

Step 2 − Now insert the entries under the words "Redirect it to www.linux.org". See the following example −

```
# redirect it to www.linux.org
#
www.facebook.com    A    216.58.199.174
*.facebook.com      A    216.58.199.174
www.facebook.com    PTR  216.58.199.174

microsoft.com       A    107.170.40.56
*.microsoft.com     A    107.170.40.56
www.microsoft.com   PTR  107.170.40.56      # Wildcards in PTR are not allowed
```

Step 3 − Now save this file and exit by saving the file. Use "ctrl+x" to save the file.

Step 4 − After this, the whole process is same to start ARP poisoning. After starting ARP poisoning, click on "plugins" in the menu bar and select "dns_spoof" plugin.

Host List × Plugins ×

	Name	Version	Info
	arp_cop	1.1	Report suspicious ARP activity
	autoadd	1.2	Automatically add new victims in the target range
	chk_poison	1.1	Check if the poisoning had success
*	dns_spoof	1.2	Sends spoofed dns replies
	dos_attack	1.0	Run a d.o.s. attack against an IP address
	dummy	3.0	A plugin template (for developers)
	find_conn	1.0	Search connections on a switched LAN
	find_ettercap	2.0	Try to find ettercap activity
	find_ip	1.0	Search an unused IP address in the subnet

Step 5 − After activating the DNS_spoof, you will see in the results that facebook.com will start spoofed to Google IP whenever someone types it in his browser.

```
Activating dns_spoof plugin...
dns_spoof: A [staticxx.facebook.com] spoofed to [216.58.199.174]
dns_spoof: A [www.facebook.com] spoofed to [216.58.199.174]
dns_spoof: A [pixel.facebook.com] spoofed to [216.58.199.174]
```

It means the user gets the Google page instead of facebook.com on their browser.

In this exercise, we saw how network traffic can be sniffed through different tools and methods. Here a company needs an ethical hacker to provide network security to stop all these attacks. Let's see what an ethical hacker can do to prevent DNS Poisoning.

Defenses against DNS Poisoning

As an ethical hacker, your work could very likely put you in a position of prevention rather than pen testing. What you know as an attacker can help you prevent the very techniques you employ from the outside.

Here are defenses against the attacks we just covered from a pen tester's perspective −

- Use a hardware-switched network for the most sensitive portions of your network in an effort to isolate traffic to a single segment or collision domain.
- Implement IP DHCP Snooping on switches to prevent ARP poisoning and spoofing attacks.
- Implement policies to prevent promiscuous mode on network adapters.
- Be careful when deploying wireless access points, knowing that all traffic on the wireless network is subject to sniffing.
- Encrypt your sensitive traffic using an encrypting protocol such as SSH or IPsec.
- Port security is used by switches that have the ability to be programmed to allow only specific MAC addresses to send and receive data on each port.
- IPv6 has security benefits and options that IPv4 does not have.
- Replacing protocols such as FTP and Telnet with SSH is an effective defense against sniffing. If SSH is not a viable solution, consider protecting older legacy protocols with IPsec.
- Virtual Private Networks (VPNs) can provide an effective defense against sniffing due to their encryption aspect.

- SSL is a great defense along with IPsec.

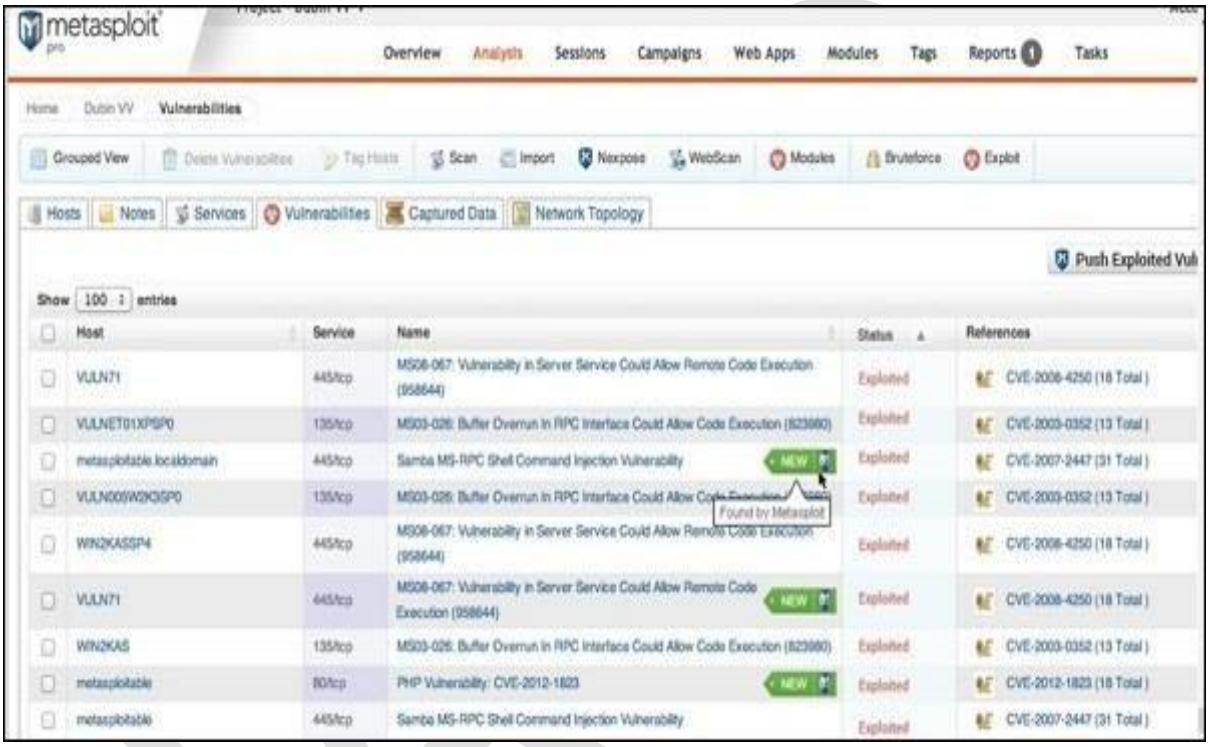
Summary

In this chapter, we discussed how attackers can capture and analyze all the traffic by placing a packet sniffer in a network. With a real-time example, we saw how easy it is to get the credentials of a victim from a given network. Attackers use MAC attacks, ARP and DNS poisoning attacks to sniff the network traffic and get hold of sensitive information such as email conversations and passwords.

Exploitation

Exploitation is a piece of programmed software or script which can allow hackers to take control over a system, exploiting its vulnerabilities. Hackers normally use vulnerability scanners like Nessus, Nexpose, OpenVAS, etc. to find these vulnerabilities.

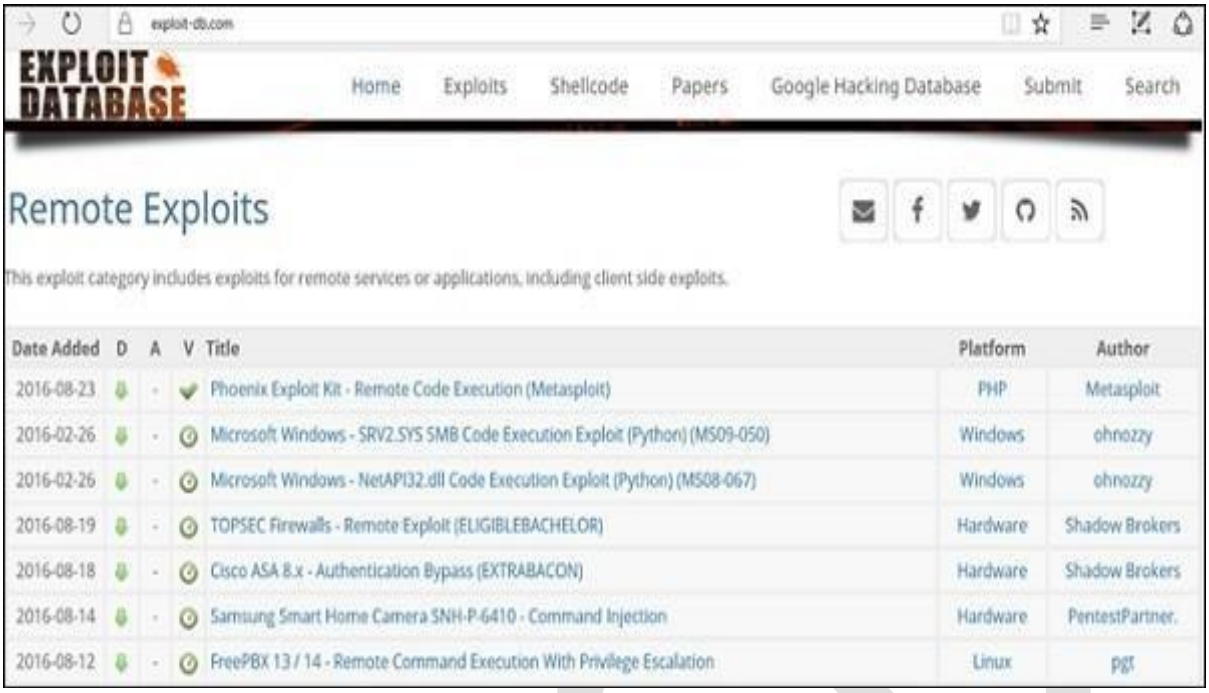
Metasploit is a powerful tool to locate vulnerabilities in a system.



Based on the vulnerabilities, we find exploits. Here, we will discuss some of the best vulnerability search engines that you can use.

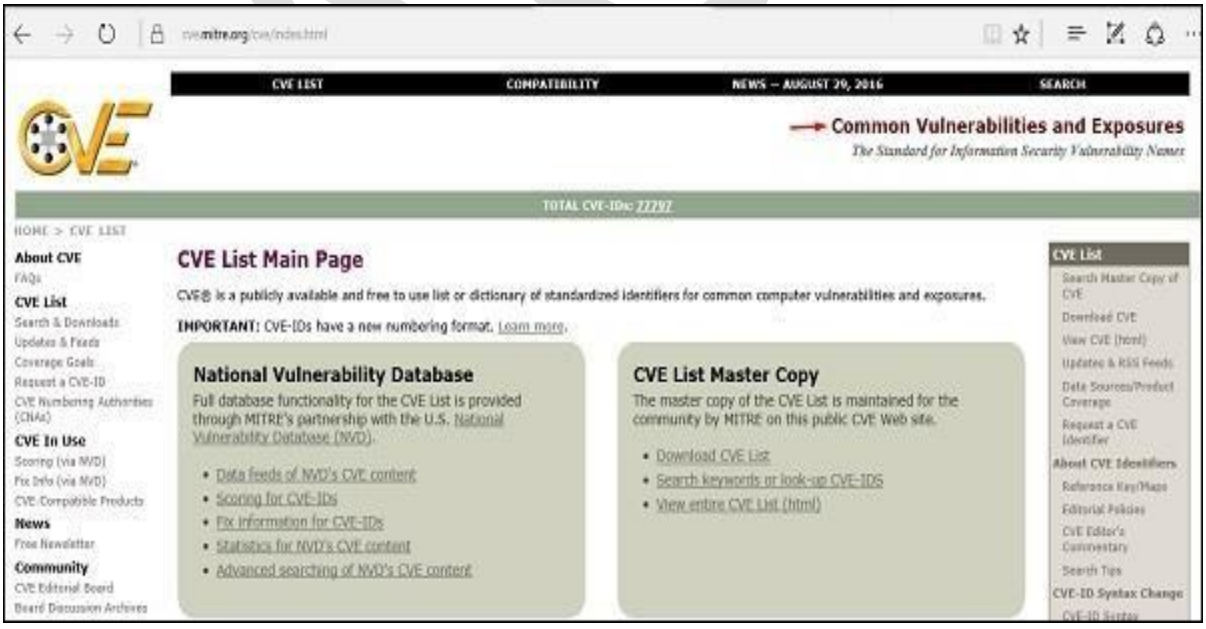
Exploit Database

www.exploit-db.com is the place where you can find all the exploits related to a vulnerability.



Common Vulnerabilities and Exposures

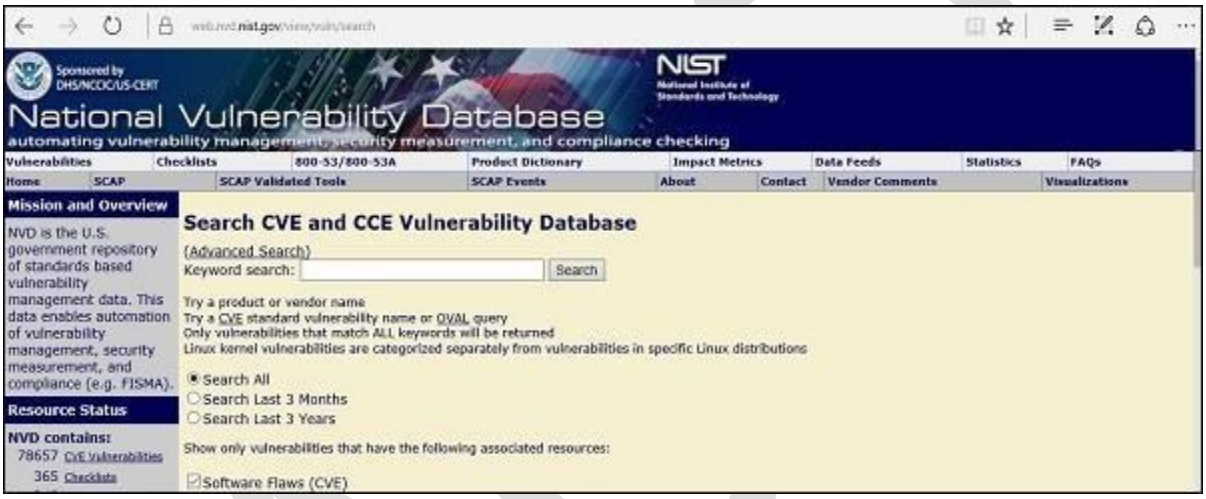
Common Vulnerabilities and Exposures (CVE) is the standard for information security vulnerability names. CVE is a dictionary of publicly known information security vulnerabilities and exposures. It's free for public use. https://cve.mitre.org



National Vulnerability Database

National Vulnerability Database (NVD) is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance. You can locate this database at − https://nvd.nist.gov

NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.



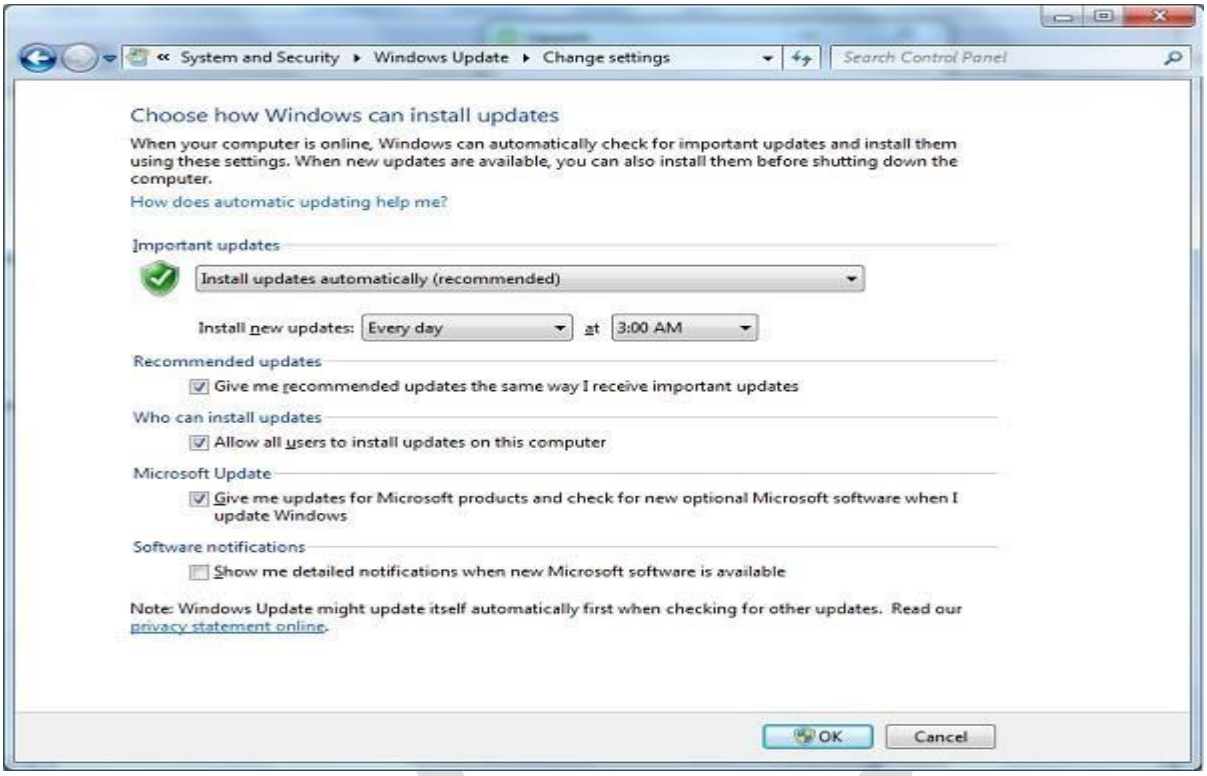
In general, you will see that there are two types of exploits −

- **Remote Exploits** − These are the type of exploits where you don't have access to a remote system or network. Hackers use remote exploits to gain access to systems that are located at remote places.
- **Local Exploits** − Local exploits are generally used by a system user having access to a local system, but who wants to overpass his rights.

Note

Vulnerabilities generally arise due to missing updates, so it is recommended that you update your system on a regular basis, for example, once a week.

In Windows environment, you can activate automatic updates by using the options available in the Control Panel → System and Security → Windows Updates.



Enumeration

Enumeration belongs to the first phase of Ethical Hacking, i.e., “Information Gathering”. This is a process where the attacker establishes an active connection with the victim and try to discover as much attack vectors as possible, which can be used to exploit the systems further.

Enumeration can be used to gain information on −

- Network shares
- SNMP data, if they are not secured properly
- IP tables
- Usernames of different systems
- Passwords policies lists

Enumerations depend on the services that the systems offer. They can be −

- DNS enumeration
- NTP enumeration
- SNMP enumeration
- Linux/Windows enumeration
- SMB enumeration

Let us now discuss some of the tools that are widely used for Enumeration.

NTP Suite

NTP Suite is used for NTP enumeration. This is important because in a network environment, you can find other primary servers that help the hosts to update their times and you can do it without authenticating the system.

Take a look at the following example.

ntpdate 192.168.1.100 01 Sept 12:50:49 ntpdate[627]:

adjust time server 192.168.1.100 offset 0.005030 sec

or

ntpdc [-ilnps] [-c command] [hostname/IP_address]

root@test]# ntpdc -c sysinfo 192.168.1.100

***Warning changing to older implementation

***Warning changing the request packet size from 160 to 48

system peer: 192.168.1.101

system peer mode: client

leap indicator: 00

stratum: 5

precision: -15

root distance: 0.00107 s

root dispersion: 0.02306 s

reference ID: [192.168.1.101]

reference time: f66s4f45.f633e130, Sept 01 2016 22:06:23.458

system flags: monitor ntp stats calibrate

jitter: 0.000000 s

stability: 4.256 ppm

broadcastdelay: 0.003875 s

authdelay: 0.000107 s

enum4linux

enum4linux is used to enumerate Linux systems. Take a look at the following screenshot and observe how we have found the usernames present in a target host.

```
root@kali:~# enum4linux -U -o 192.168.1.200
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ )

 ==========================
|    Target Information    |
 ==========================
Target ..... 192.168.1.200
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 =====================================================
|    Enumerating Workgroup/Domain on 192.168.1.200    |
 =====================================================
```

smtp-user-enum

smtp-user-enum tries to guess usernames by using SMTP service. Take a look at the following screenshot to understand how it does so.

```
root@kali:~# smtp-user-enum -M VRFY -u root -t 192.168.1.25
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............
```

Note

It is recommended to disable all services that you don't use. It reduces the possibilities of OS enumeration of the services that your systems are running.

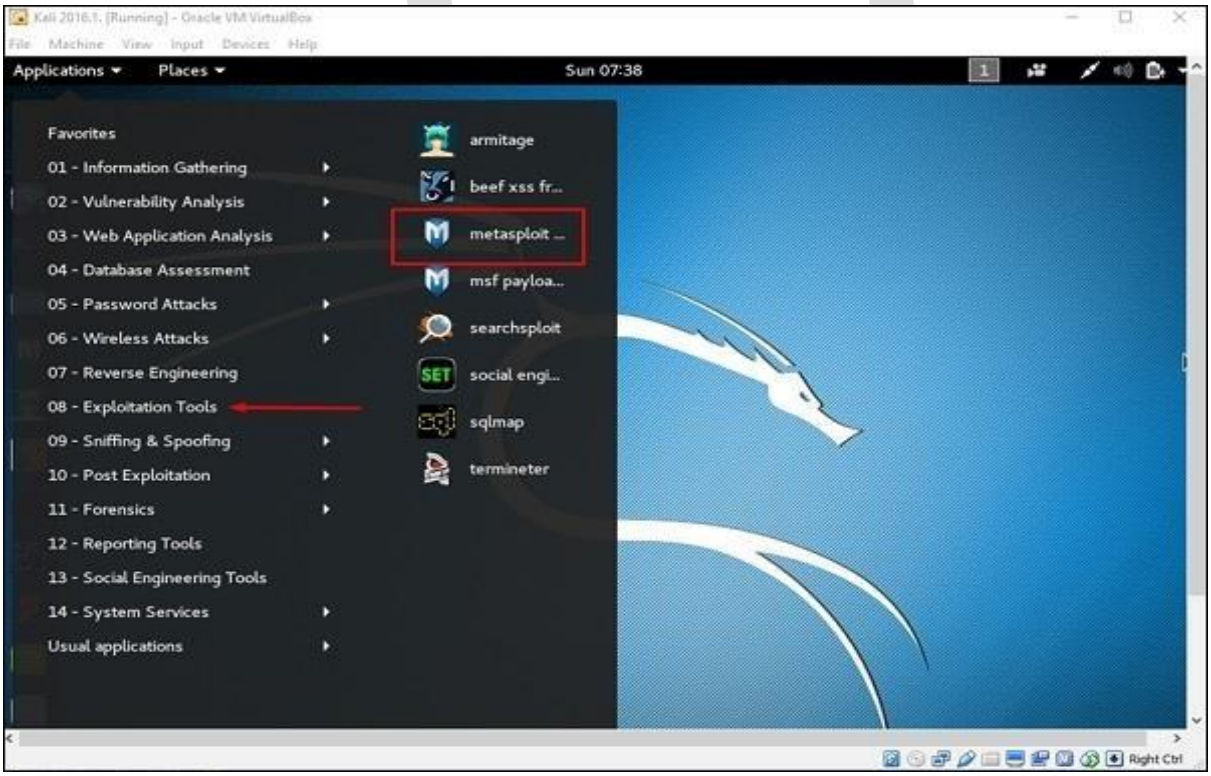
Metasploit

Metasploit is one of the most powerful exploit tools. Most of its resources can be found at: https://www.metasploit.com. It comes in two versions − **commercial** and **free edition**. There are no major differences in the two versions, so in this tutorial, we will be mostly using the Community version (free) of Metasploit.

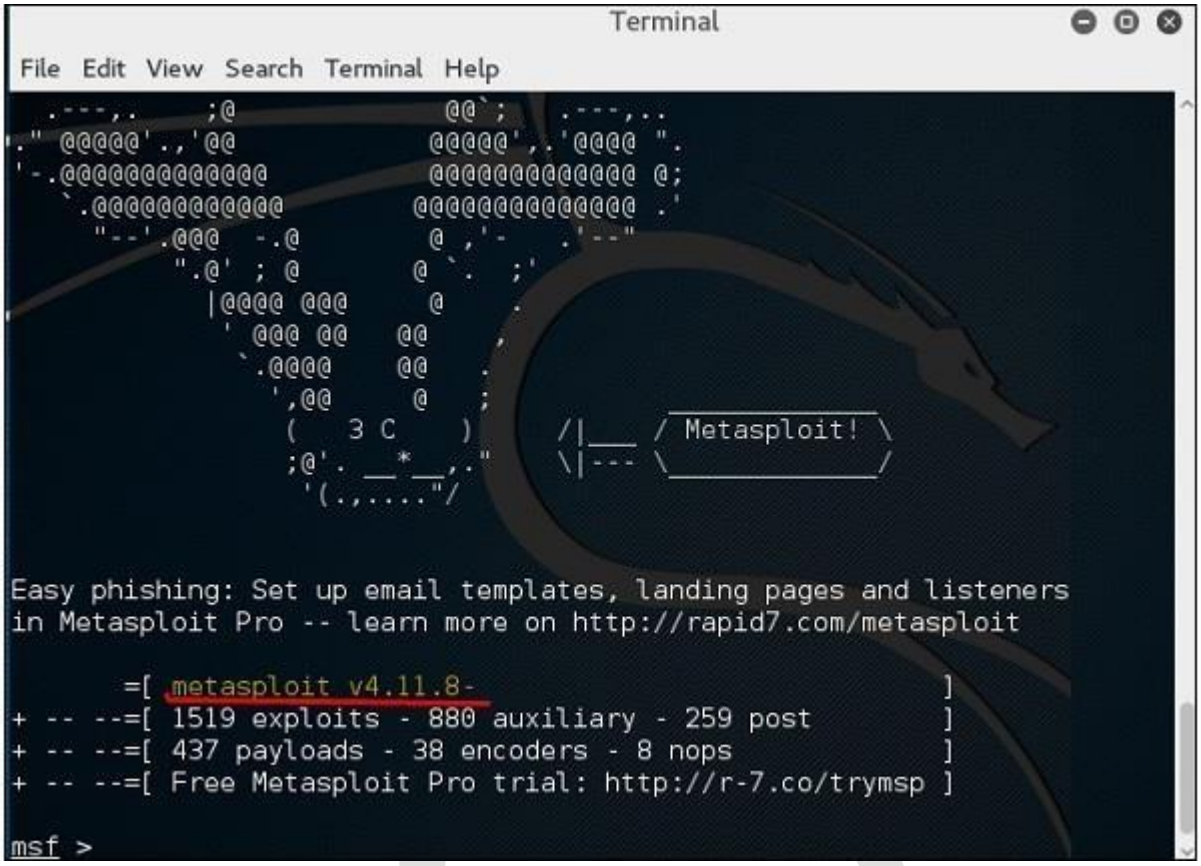
As an Ethical Hacker, you will be using "Kali Distribution" which has the Metasploit community version embedded in it along with other ethical hacking tools. But if you want to install Metasploit as a separate tool, you can easily do so on systems that run on Linux, Windows, or Mac OS X.

Matasploit can be used either with command prompt or with Web UI.

To open in Kali, go to Applications → Exploitation Tools → metasploit.



After Metasploit starts, you will see the following screen. Highlighted in red underline is the version of Metasploit.



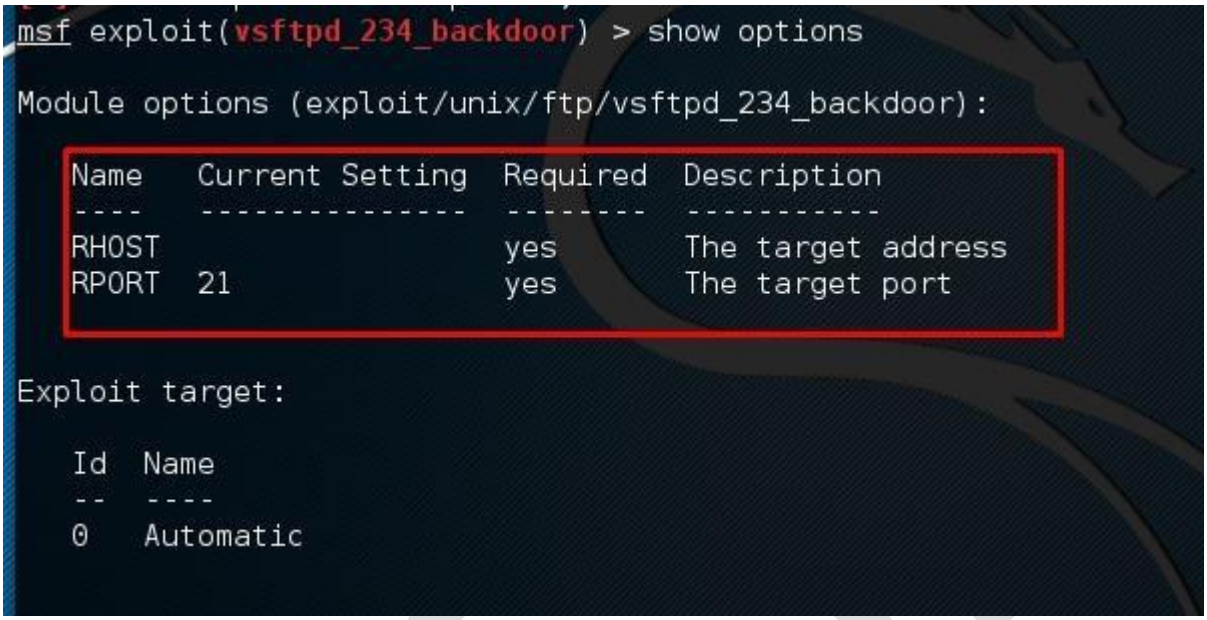
Exploits of Metasploit

From Vulnerability Scanner, we found that the Linux machine that we have for test is vulnerable to FTP service. Now, we will use the exploit that can work for us. The command is −

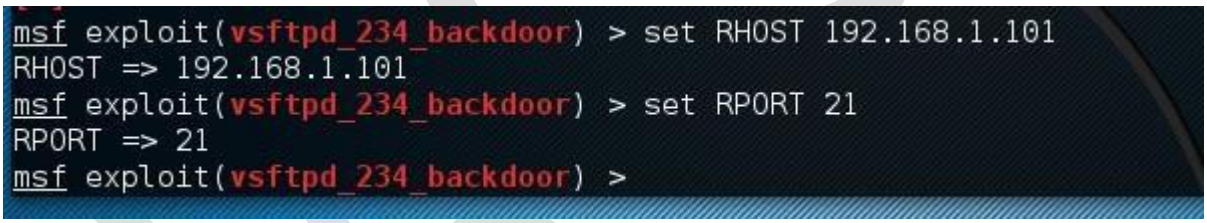
use “exploit path”

The screen will appear as follows −

Then type **mfs> show options** in order to see what parameters you have to set in order to make it functional. As shown in the following screenshot, we have to set RHOST as the "target IP".



We type **msf> set RHOST 192.168.1.101 and msf>set RPORT 21**



Then, type **mfs>run**. If the exploit is successful, then it will open one session that you can interact with, as shown in the following screenshot.

Metasploit Payloads

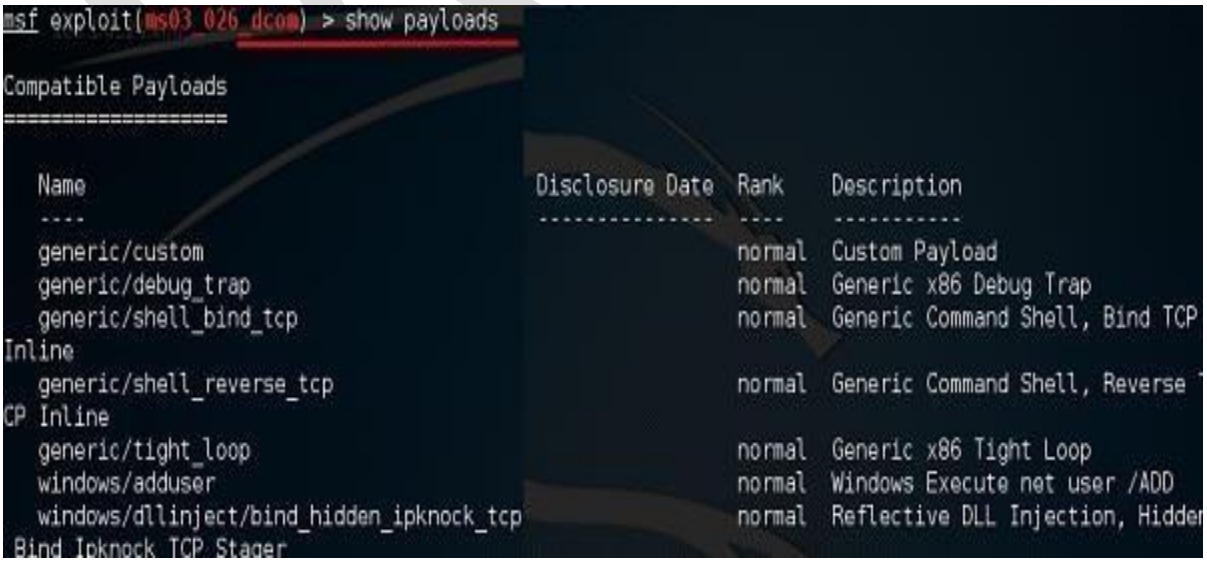
Payload, in simple terms, are simple scripts that the hackers utilize to interact with a hacked system. Using payloads, they can transfer data to a victim system.

Metasploit payloads can be of three types −

- **Singles** − Singles are very small and designed to create some kind of communication, then move to the next stage. For example, just creating a user.
- **Staged** − It is a payload that an attacker can use to upload a bigger file onto a victim system.
- **Stages** − Stages are payload components that are downloaded by Stagers modules. The various payload stages provide advanced features with no size limits such as Meterpreter and VNC Injection.

Payload Usage − Example

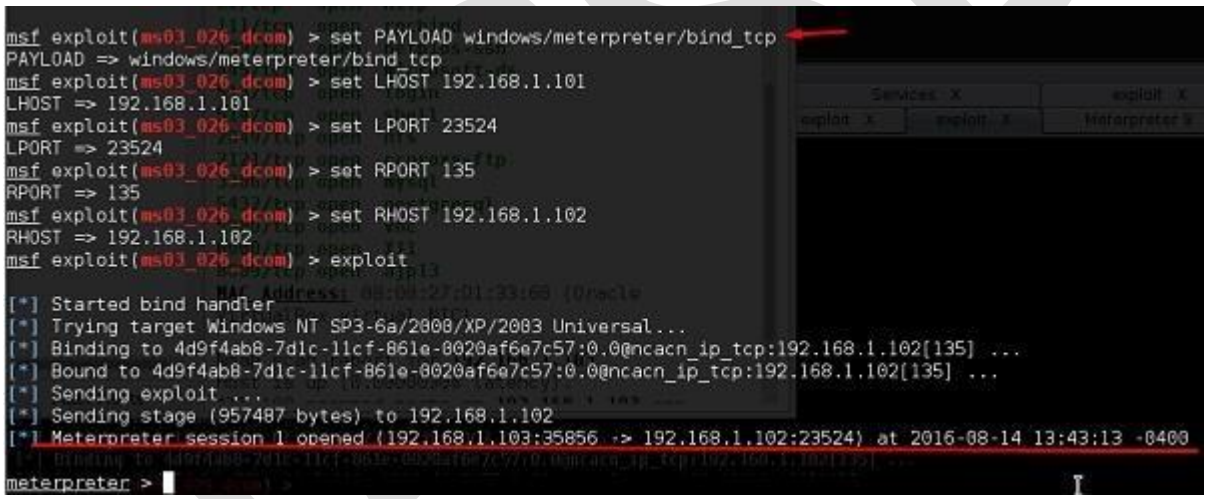
We use the command **show payloads**. With this exploit, we can see the payloads that we can use, and it will also show the payloads that will help us upload /execute files onto a victim system.



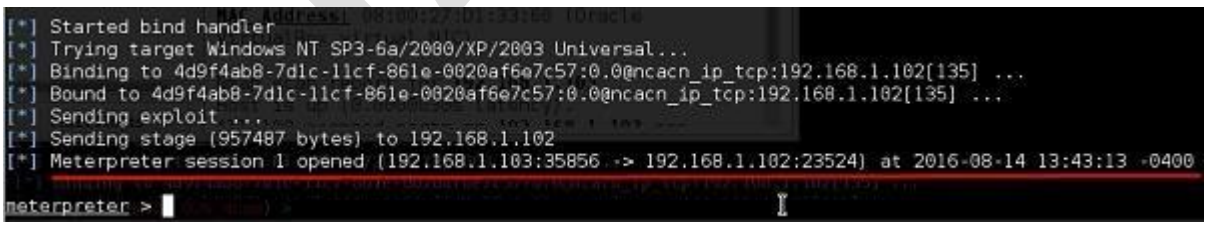
To set the payload that we want, we will use the following command −

set PAYLOAD payload/path

Set the listen host and listen port (LHOST, LPORT) which are the **attacker IP** and **port**. Then set remote host and port (RPORT, LHOST) which are the **victim IP** and **port**.



Type “exploit”. It will create a session as shown below −



Now we can play with the system according to the settings that this payload offers.

Trojan Attacks

Trojans are non-replication programs; they don't reproduce their own codes by attaching themselves to other executable codes. They operate without the permissions or knowledge of the computer users.

Trojans hide themselves in healthy processes. However we should underline that Trojans infect outside machines only with the assistance of a computer user, like clicking a file that comes attached with email from an unknown person, plugging USB without scanning, opening unsafe URLs.

Trojans have several malicious functions −

- They create backdoors to a system. Hackers can use these backdoors to access a victim system and its files. A hacker can use Trojans to edit and delete the files present on a victim system, or to observe the activities of the victim.
- Trojans can steal all your financial data like bank accounts, transaction details, PayPal related information, etc. These are called **Trojan-Banker**.
- Trojans can use the victim computer to attack other systems using Denial of Services.
- Trojans can encrypt all your files and the hacker may thereafter demand money to decrypt them. These are **Ransomware Trojans**.
- They can use your phones to send SMS to third parties. These are called **SMS Trojans**.

Trojan Information

If you have found a virus and want to investigate further regarding its function, then we will recommend that you have a look at the following virus databases, which are offered generally by antivirus vendors.

- **Kaspersky Virus database** − https://www.kaspersky.com

- **F-secure** − https://www.f-secure.com
- **Symantec – Virus Encyclopedia** − https://www.symantec.com

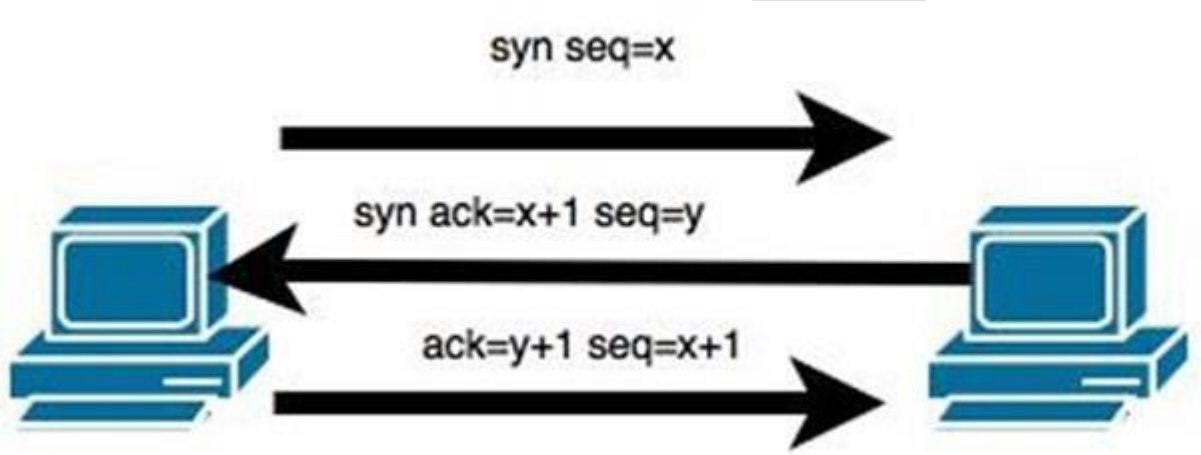
Quick Tips

- Install a good antivirus and keep it updated.
- Don’t open email attachments coming from unknown sources.
- Don’t accept invitation from unknown people in social media.
- Don’t open URLs sent by unknown people or URLs that are in weird form.

TCP/IP Hijacking

TCP/IP Hijacking is when an authorized user gains access to a genuine network connection of another user. It is done in order to bypass the password authentication which is normally the start of a session.

In theory, a TCP/IP connection is established as shown below −



To hijack this connection, there are two possibilities −

- Find the **seq** which is a number that increases by 1, but there is no chance to predict it.
- The second possibility is to use the Man-in-the-Middle attack which, in simple words, is a type of **network sniffing**. For sniffing, we use tools like **Wireshark** or **Ethercap**.

Example

An attacker monitors the data transmission over a network and discovers the IP's of two devices that participate in a connection.

When the hacker discovers the IP of one of the users, he can put down the connection of the other user by DoS attack and then resume communication by spoofing the IP of the disconnected user.

Quick Tip

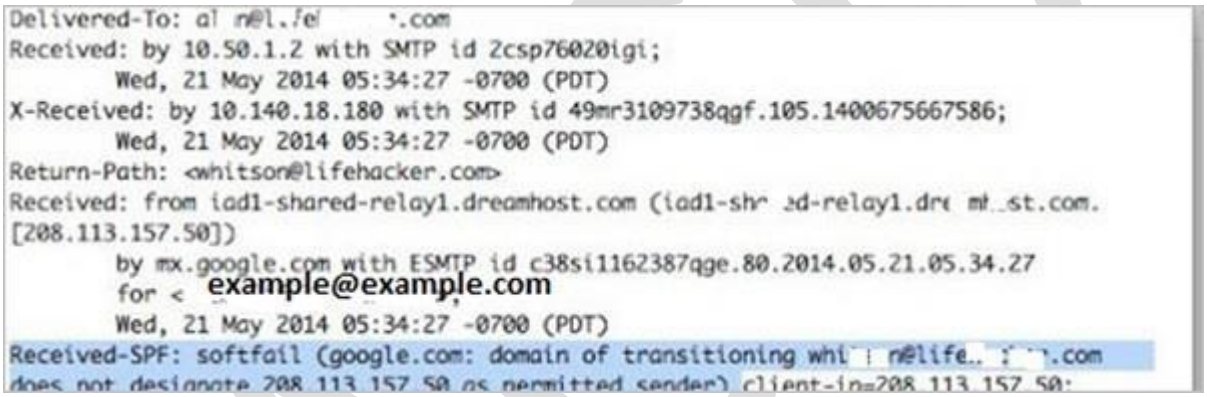
All unencrypted sessions are vulnerable to TCP/IP session hijacking, so you should be using encrypted protocols as much as possible. Or, you should use double authentication techniques to keep the session secured.

Email Hijacking

Email Hijacking, or email hacking, is a widespread menace nowadays. It works by using the following three techniques which are email spoofing, social engineering tools, or inserting viruses in a user computer.

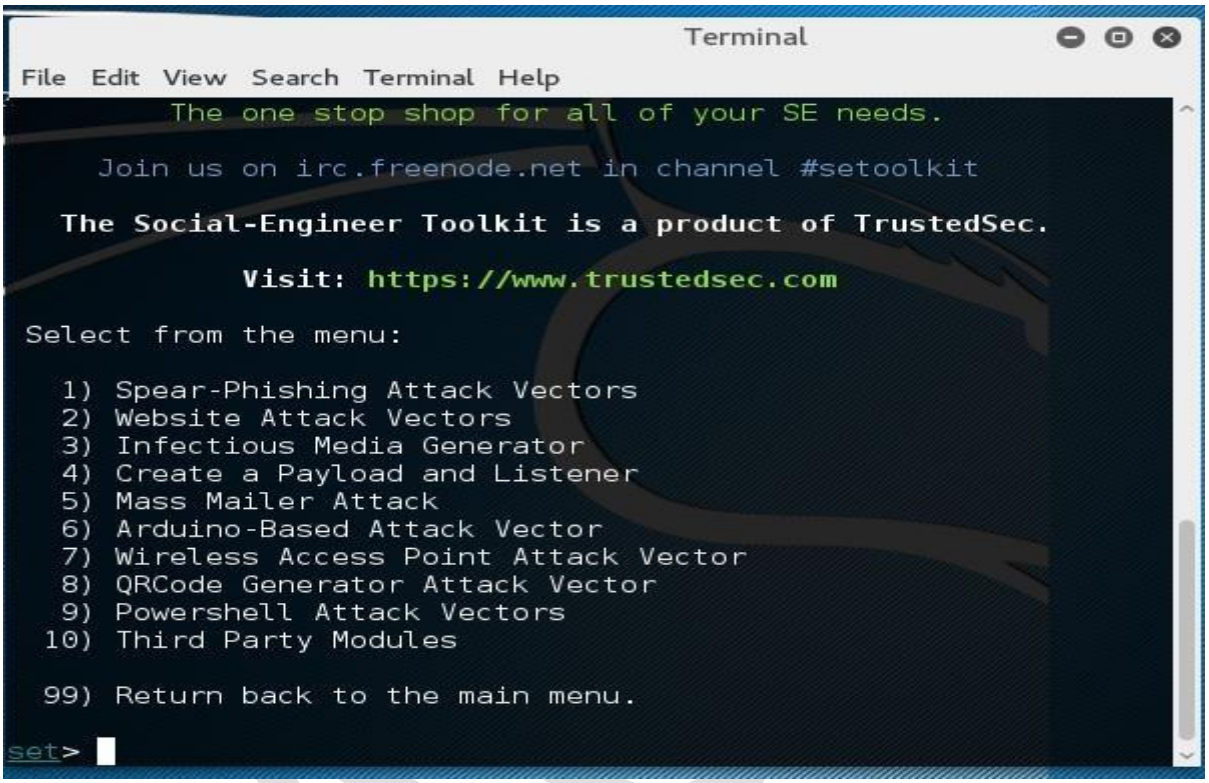
Email Spoofing

In email spoofing, the spammer sends emails from a known domain, so the receiver thinks that he knows this person and opens the mail. Such mails normally contain suspicious links, doubtful content, requests to transfer money, etc.



Social Engineering

Spammers send promotional mails to different users, offering huge discount and tricking them to fill their personal data. You have tools available in Kali that can drive you to hijack an email.



Email hacking can also be done by **phishing techniques**. See the following screenshot.

The links in the email may install malware on the user's system or redirect the user to a malicious website and trick them into divulging personal and financial information, such as passwords, account IDs or credit card details.

Phishing attacks are widely used by cybercriminals, as it is far easier to trick someone into clicking a malicious links in the email than trying to break through a computer's defenses.

Inserting Viruses in a User System

The third technique by which a hacker can hijack your email account is by infecting your system with a virus or any other kind of malware. With the help of a virus, a hacker can take all your passwords.

How to detect if your email has been hijacked?

- The recipients of spam emails include a bunch of people you know.
- You try to access your account and the password no longer works.
- You try to access the "Forgot Password" link and it does not go to the expected email.
- Your Sent Items folder contains a bunch of spams you are not aware of sending.

Quick tips

In case you think that your email got hijacked, then you need to take the following actions −

- Change the passwords immediately.
- Notify your friends not to open links that they receive from your email account.
- Contact the authorities and report that your account has been hacked.
- Install a good antivirus on your computer and update it.
- Set up double authentication password if it is supported.

Password Hacking

We have passwords for emails, databases, computer systems, servers, bank accounts, and virtually everything that we want to protect. Passwords are in general the keys to get access into a system or an account.

In general, people tend to set passwords that are easy to remember, such as their date of birth, names of family members, mobile numbers, etc. This is what makes the passwords weak and prone to easy hacking.

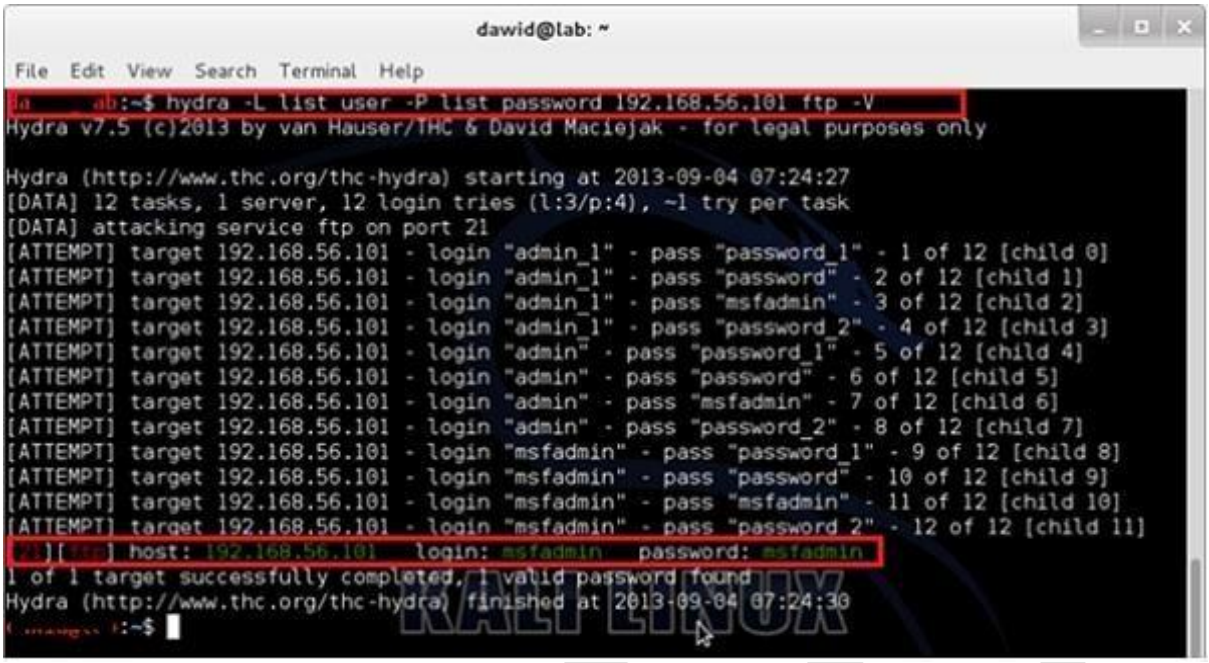
One should always take care to have a strong password to defend their accounts from potential hackers. A strong password has the following attributes −

- Contains at least 8 characters.
- A mix of letters, numbers, and special characters.
- A combination of small and capital letters.

Dictionary Attack

In a dictionary attack, the hacker uses a predefined list of words from a dictionary to try and guess the password. If the set password is weak, then a dictionary attack can decode it quite fast.

Hydra is a popular tool that is widely used for dictionary attacks. Take a look at the following screenshot and observe how we have used Hydra to find out the password of an FTP service.



Hybrid Dictionary Attack

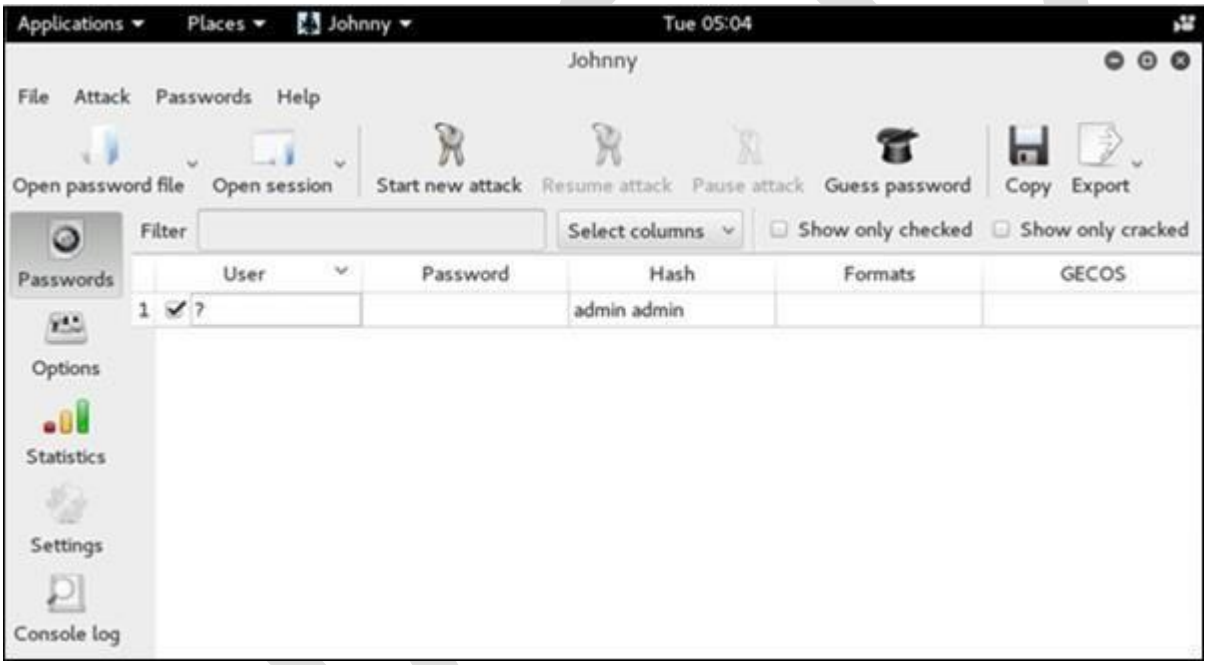
Hybrid dictionary attack uses a set of dictionary words combined with extensions. For example, we have the word “admin” and combine it with number extensions such as “admin123”, “admin147”, etc.

Crunch is a wordlist generator where you can specify a standard character set or a character set. **Crunch** can generate all possible combinations and permutations. This tool comes bundled with the Kali distribution of Linux.

Brute-Force Attack

In a brute-force attack, the hacker uses all possible combinations of letters, numbers, special characters, and small and capital letters to break the password. This type of attack has a high probability of success, but it requires an enormous amount of time to process all the combinations. A brute-force attack is slow and the hacker might require a system with high processing power to perform all those permutations and combinations faster.

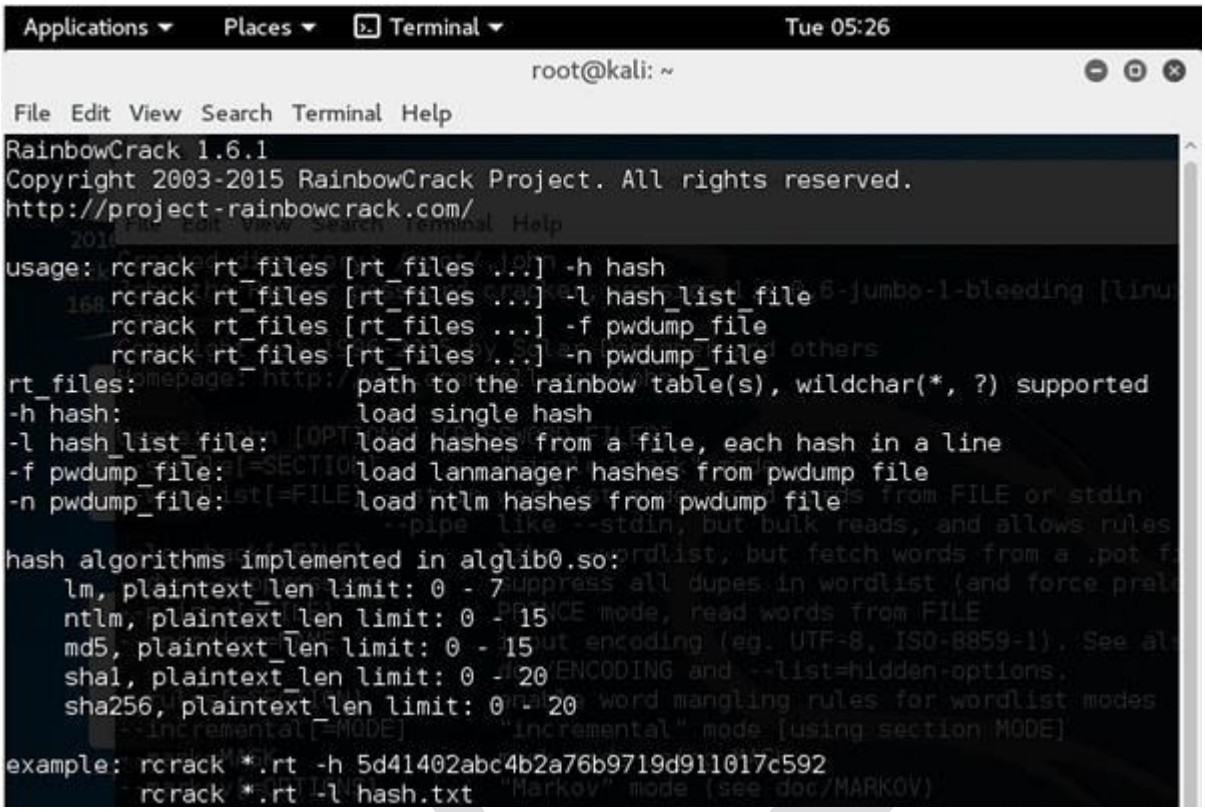
John the Ripper or **Johnny** is one of the powerful tools to set a brute-force attack and it comes bundled with the Kali distribution of Linux.



Rainbow Tables

A rainbow table contains a set of predefined passwords that are hashed. It is a lookup table used especially in recovering plain passwords from a cipher text. During the process of password recovery, it just looks at the pre-calculated hash table to crack the password. The tables can be downloaded from http://project-rainbowcrack.com/table.htm

RainbowCrack 1.6.1 is the tool to use the rainbow tables. It is available again in Kali distribution.



Quick Tips

- Don’t note down the passwords anywhere, just memorize them.
- Set strong passwords that are difficult to crack.
- Use a combination of alphabets, digits, symbols, and capital and small letters.
- Don’t set passwords that are similar to their usernames.

Wireless Hacking

A wireless network is a set of two or more devices connected with each other via radio waves within a limited space range. The devices in a wireless network have the freedom to be in motion, but be in connection with the network and share data with other devices in the network. One of the most crucial point that they are so spread is that their installation cost is very cheap and fast than the wire networks.

Wireless networks are widely used and it is quite easy to set them up. They use IEEE 802.11 standards. A **wireless router** is the most important device in a wireless network that connects the users with the Internet.

A Wireless Router

In a wireless network, we have **Access Points** which are extensions of wireless ranges that behave as logical switches.

Although wireless networks offer great flexibility, they have their security problems. A hacker can sniff the network packets without having to be in the same building where the network is located. As wireless networks communicate through radio waves, a hacker can easily sniff the network from a nearby location.

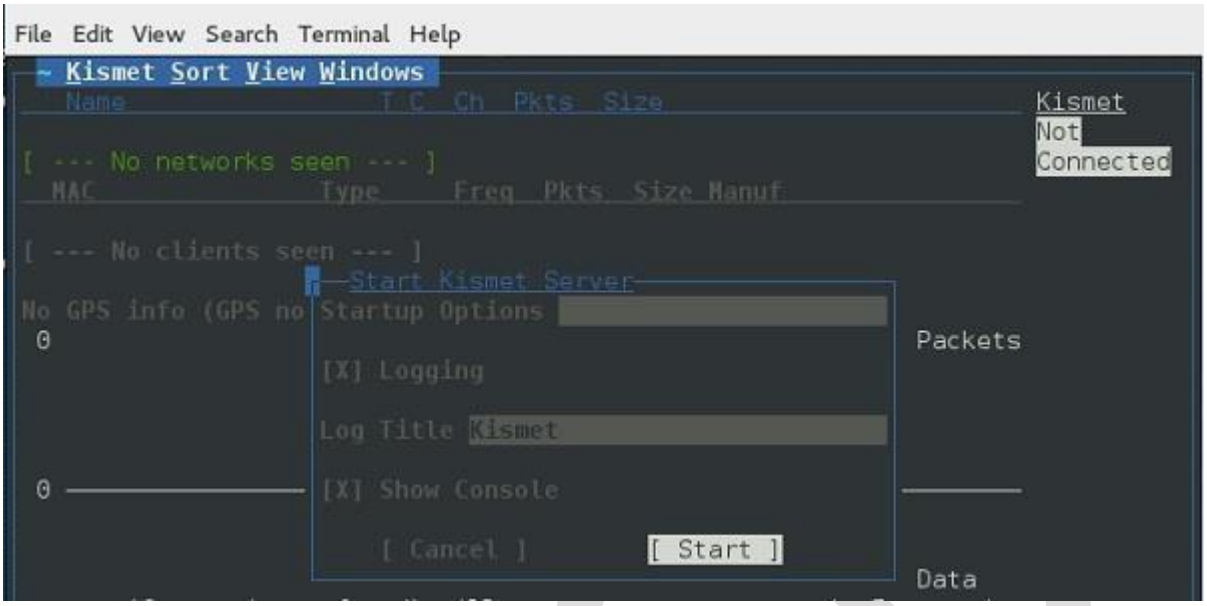
Most attackers use network sniffing to find the SSID and hack a wireless network. When our wireless cards are converted in sniffing modes, they are called **monitor mode**.

Kismet

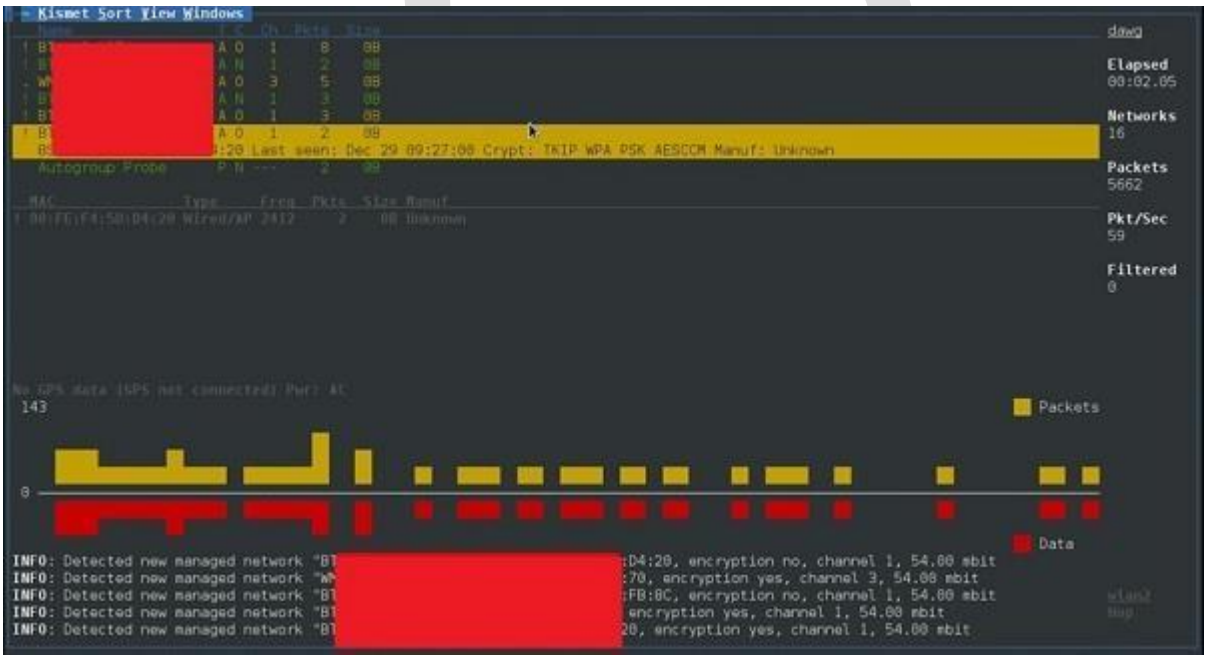
Kismet is a powerful tool for wireless sniffing that is found in Kali distribution. It can also be downloaded from its official webpage − https://www.kismetwireless.net

Let's see how it works. First of all, open a terminal and type **kismet**. Start the Kismet Server and click Yes, as shown in the following screenshot.

As shown here, click the Start button.



Now, Kismet will start to capture data. The following screenshot shows how it would appear −



Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is a security protocol that was invented to secure wireless networks and keep them private. It utilizes encryption at the data link layer which forbids unauthorized access to the network.

The key is used to encrypt the packets before transmission begins. An **integrity check mechanism** checks that the packets are not altered after transmission.

Note that WEP is not entirely immune to security problems. It suffers from the following issues −

- CRC32 is not sufficient to ensure complete cryptographic integrity of a packet.
- It is vulnerable to dictionary attacks.
- WEP is vulnerable to Denial of Services attacks too.

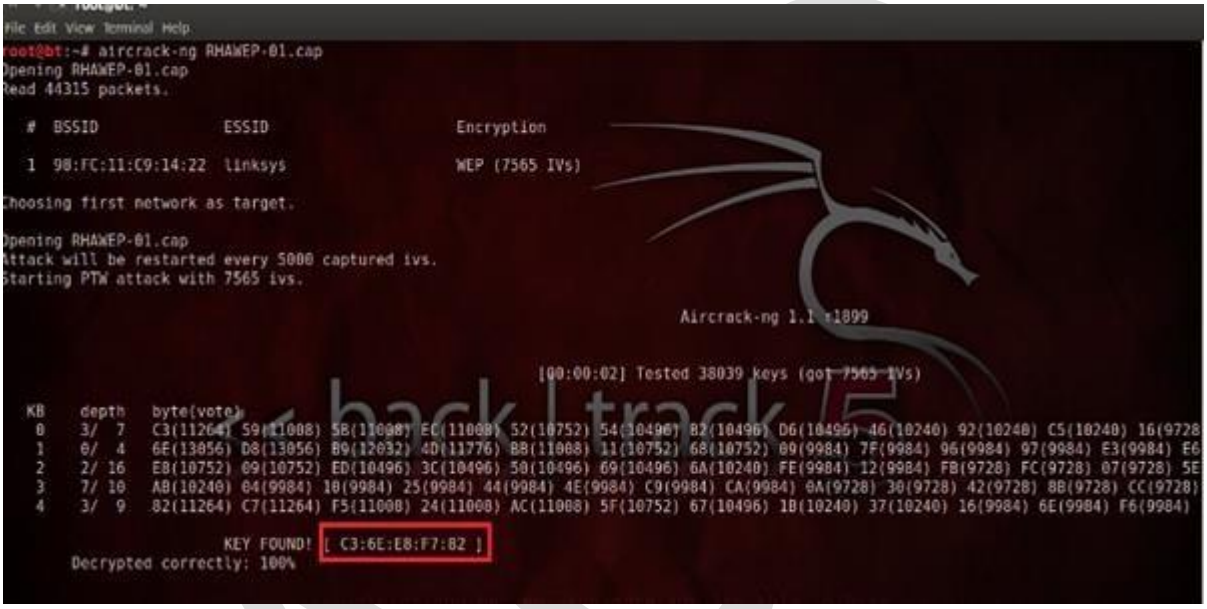
WEPcrack

WEPcrack is a popular tool to crack WEP passwords. It can be downloaded from − https://sourceforge.net/projects/wepcrack/

Aircrack-ng

Aircrak-ng is another popular tool for cracking WEP passwords. It can be found in the Kali distribution of Linux.

The following screenshot shows how we have sniffed a wireless network and collected packets and created a file RHAWEP-01.cap. Then we run it with aircrack-ng to decrypt the cypher.



Wireless DoS Attacks

In a wireless environment, an attacker can attack a network from a distance and therefore, it is sometimes difficult to collect evidences against the attacker.

The first type of DoS is **Physical Attack**. This type of attack is very basic and it is in the base of radio interferences which can be created even from cordless phones that operate in 2.4 GHz range.

Another type is **Network DoS Attack**. As the Wireless Access Point creates a shared medium, it offers the possibility to flood the traffic of this medium toward the AP which will make its processing more slow toward the clients that attempt to connect. Such attacks can be created just by a **ping flood DoS attack**.

Pyloris is a popular DoS tool that you can download from − https://sourceforge.net/projects/pyloris/

Low Orbit Ion Cannon (LOIC) is another popular tool for DoS attacks.

Quick Tips

To secure a wireless network, you should keep the following points in mind −

- Change the SSID and the network password regularly.
- Change the default password of access points.
- Don’t use WEP encryption.
- Turn off guest networking.
- Update the firmware of your wireless device.

Social Engineering

Example 1

You must have noticed old company documents being thrown into dustbins as garbage. These documents might contain sensitive information such as Names, Phone Numbers, Account Numbers, Social Security Numbers, Addresses, etc. Many companies still use carbon paper in their fax machines and once the roll is over, its carbon goes into dustbin which may have traces of sensitive data. Although it sounds improbable, but attackers can easily retrieve information from the company dumpsters by pilfering through the garbage.

Example 2

An attacker may befriend a company personnel and establish good relationship with him over a period of time. This relationship can be established online through social networks, chatting rooms, or offline at a coffee table, in a playground, or through any other means. The attacker takes the office personnel in confidence and finally digs out the required sensitive information without giving a clue.

Example 3

A social engineer may pretend to be an employee or a valid user or an VIP by faking an identification card or simply by convincing employees of his position in the company. Such an attacker can gain physical access to restricted areas, thus providing further opportunities for attacks.

Example 4

It happens in most of the cases that an attacker might be around you and can do **shoulder surfing** while you are typing sensitive information like user ID and password, account PIN, etc.

Phishing Attack

A phishing attack is a computer-based social engineering, where an attacker crafts an email that appears legitimate. Such emails have the same look and feel as those received from the original site, but they might contain links to fake websites. If you are not smart enough, then you will type your user ID and password and will try to login which will result in failure and by that time, the attacker will have your ID and password to attack your original account.

Note

- You should enforce a good security policy in your organization and conduct required trainings to make all the employees aware of the possible Social Engineering attacks and their consequences.
- Document shredding should be a mandatory activity in your company.
- Make double sure that any links that you receive in your email is coming from authentic sources and that they point to correct websites. Otherwise you might end up as a victim of Phishing.
- Be professional and never share your ID and password with anybody else in any case.

DDOS Attacks

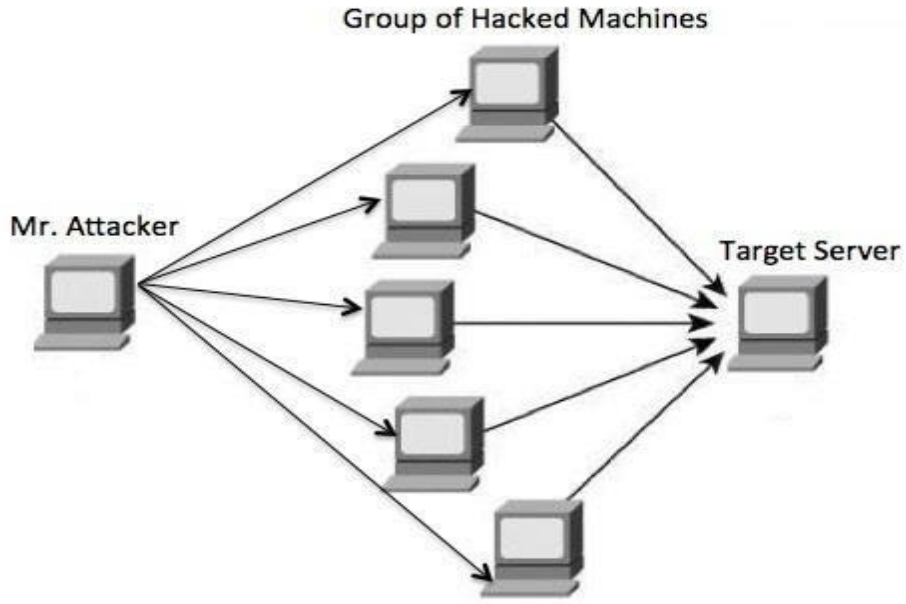
A Distributed Denial of Service (DDoS) attack is an attempt to make an online service or a website unavailable by overloading it with huge floods of traffic generated from multiple sources.

Unlike a Denial of Service (DoS) attack, in which one computer and one Internet connection is used to flood a targeted resource with packets, a DDoS attack uses many computers and many Internet connections, often distributed globally in what is referred to as a **botnet**.

A large scale volumetric DDoS attack can generate a traffic measured in tens of Gigabits (and even hundreds of Gigabits) per second. We are sure your normal network will not be able to handle such traffic.

What are Botnets?

Attackers build a network of hacked machines which are known as **botnets**, by spreading malicious piece of code through emails, websites, and social media. Once these computers are infected, they can be controlled remotely, without their owners' knowledge, and used like an army to launch an attack against any target.



A DDoS flood can be generated in multiple ways. For example −

- Botnets can be used for sending more number of connection requests than a server can handle at a time.
- Attackers can have computers send a victim resource huge amounts of random data to use up the target's bandwidth.

Due to the distributed nature of these machines, they can be used to generate distributed high traffic which may be difficult to handle. It finally results in a complete blockage of a service.

Types of DDoS Attacks

DDoS attacks can be broadly categorized into three categories −

- Volume-based Attacks
- Protocol Attacks
- Application Layer Attacks

Volume-Based Attacks

Volume-based attacks include TCP floods, UDP floods, ICMP floods, and other spoofedpacket floods. These are also called **Layer 3 & 4 Attacks**. Here, an attacker tries to saturate the bandwidth of the target site. The attack magnitude is measured in **Bits per Second** (bps).

- **UDP Flood** − A UDP flood is used to flood random ports on a remote host with numerous UDP packets, more specifically port number 53. Specialized firewalls can be used to filter out or block malicious UDP packets.
- **ICMP Flood** − This is similar to UDP flood and used to flood a remote host with numerous ICMP Echo Requests. This type of attack can consume both outgoing and incoming bandwidth and a high volume of ping requests will result in overall system slowdown.

- **HTTP Flood** − The attacker sends HTTP GET and POST requests to a targeted web server in a large volume which cannot be handled by the server and leads to denial of additional connections from legitimate clients.
- **Amplification Attack** − The attacker makes a request that generates a large response which includes DNS requests for large TXT records and HTTP GET requests for large files like images, PDFs, or any other data files.

Protocol Attacks

Protocol attacks include SYN floods, Ping of Death, fragmented packet attacks, Smurf DDoS, etc. This type of attack consumes actual server resources and other resources like firewalls and load balancers. The attack magnitude is measured in **Packets per Second**.

- **DNS Flood** − DNS floods are used for attacking both the infrastructure and a DNS application to overwhelm a target system and consume all its available network bandwidth.
- **SYN Flood** − The attacker sends TCP connection requests faster than the targeted machine can process them, causing network saturation. Administrators can tweak TCP stacks to mitigate the effect of SYN floods. To reduce the effect of SYN floods, you can reduce the timeout until a stack frees memory allocated to a connection, or selectively dropping incoming connections using a firewall or **iptables**.
- **Ping of Death** − The attacker sends malformed or oversized packets using a simple ping command. IP allows sending 65,535 bytes packets but sending a ping packet larger than 65,535 bytes violates the Internet Protocol and could cause memory overflow on the target system and finally crash the system. To avoid Ping of Death attacks and its variants, many sites block ICMP ping messages altogether at their firewalls.

Application Layer Attacks

Application Layer Attacks include Slowloris, Zero-day DDoS attacks, DDoS attacks that target Apache, Windows or OpenBSD vulnerabilities and more. Here the goal is to crash the web server. The attack magnitude is measured in **Requests per Second**.

- **Application Attack** − This is also called **Layer 7 Attack**, where the attacker makes excessive log-in, database-lookup, or search requests to overload the application. It is really difficult to detect Layer 7 attacks because they resemble legitimate website traffic.
- **Slowloris** − The attacker sends huge number of HTTP headers to a targeted web server, but never completes a request. The targeted server keeps each of these false connections open and eventually overflows the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients.
- **NTP Amplification** − The attacker exploits publically-accessible Network Time Protocol (NTP) servers to overwhelm the targeted server with User Datagram Protocol (UDP) traffic.
- **Zero-day DDoS Attacks** − A zero-day vulnerability is a system or application flaw previously unknown to the vendor, and has not been fixed or patched. These are new type of attacks coming into existence day by day, for example, exploiting vulnerabilities for which no patch has yet been released.

How to Fix a DDoS Attack

There are quite a few DDoS protection options which you can apply depending on the type of DDoS attack.

Your DDoS protection starts from identifying and closing all the possible OS and application level vulnerabilities in your system, closing all the possible ports, removing unnecessary access from the system and hiding your server behind a proxy or CDN system.

If you see a low magnitude of the DDoS, then you can find many firewall-based solutions which can help you in filtering out DDoS based traffic. But if you have high volume of DDoS attack like in gigabits or even more, then you should take the help of a DDoS protection service provider that offers a more holistic, proactive and genuine approach.

You must be careful while approaching and selecting a DDoS protection service provider. There are number of service providers who want to take advantage of your situation. If you inform them that you are under DDoS attack, then they will start offering you a variety of services at unreasonably high costs.

We can suggest you a simple and working solution which starts with a search for a good DNS solution provider who is flexible enough to configure A and CNAME records for your website. Second, you will need a good CDN provider that can handle big DDoS traffic and provide you DDoS protection service as a part of their CDN package.

Assume your server IP address is AAA.BBB.CCC.DDD. Then you should do the following DNS configuration −

- Create a **A Record** in DNS zone file as shown below with a DNS identifier, for example, **ARECORDID** and keep it secret from the outside world.
- Now ask your CDN provider to link the created DNS identifier with a URL, something like **cdn.someotherid.domain.com**.
- You will use the CDN URL cdn.someotherid.domain.com to create two CNAME records, the first one to point to **www** and the second record to point to @ as shown below.

You can take the help from your system administrator to understand these points and configure your DNS and CDN appropriately. Finally, you will have the following configuration at your DNS.

Type	TTL	Name	Value
A	3600	ARECORDID	AAA.BBB.CCC.DDD
CNAME	3600	www	cdn.someotherid.domain.com
CNAME	3600	@	cdn.someotherid.domain.com

Now, let the CDN provider handle all type of DDoS attacks and your system will remain safe. But here the condition is that you should not disclose your system's IP address or A record identifier to anyone; else direct attacks will start again.

Note

DDoS attacks have become more common than ever before, and unfortunately, there is no Note for this problem. However, if your system is under a DDoS attack, then don’t panic and start looking into the matter step by step.

Cross-Site Scripting

Cross-site scripting (XSS) is a code injection attack that allows an attacker to execute malicious JavaScript in another user's browser.

The attacker does not directly target his victim. Instead, he exploits a vulnerability in a website that the victim visits, in order to get the website to deliver the malicious JavaScript for him. To the victim's browser, the malicious JavaScript appears to be a legitimate part of the website, and the website has thus acted as an unintentional accomplice to the attacker. These attacks can be carried out using HTML, JavaScript, VBScript, ActiveX, Flash, but the most used XSS is malicious JavaScript.

These attacks also can gather data from account hijacking, changing of user settings, cookie theft/poisoning, or false advertising and create DoS attacks.

Types of XSS Attacks

XSS attacks are often divided into three types −

- **Persistent XSS,** where the malicious string originates from the website's database.
- **Reflected XSS,** where the malicious string originates from the victim's request.
- **DOM-based XSS,** where the vulnerability is in the client-side code rather than the server-side code.

Generally, cross-site scripting is found by **vulnerability scanners**

Burp Suite and **acunetix** are considered as the best vulnerability scanners.

Quick Tip

To prevent XSS attacks, keep the following points in mind −

- Check and validate all the form fields like hidden forms, headers, cookies, query strings.
- Implement a stringent security policy. Set character limitation in the input fields.

SQL Injection

SQL injection is a set of SQL commands that are placed in a URL string or in data structures in order to retrieve a response that we want from the databases that are connected with the web applications. This type of attacks generally takes place on webpages developed using PHP or ASP.NET.

An SQL injection attack can be done with the following intentions −

- To dump the whole database of a system,
- To modify the content of the databases, or
- To perform different queries that are not allowed by the application.

This type of attack works when the applications don't validate the inputs properly, before passing them to an SQL statement. Injections are normally placed put in address bars, search fields, or data fields.

The easiest way to detect if a web application is vulnerable to an SQL injection attack is to use the " ' " character in a string and see if you get any error.

Quick Tips

To prevent your web application from SQL injection attacks, you should keep the following points in mind −

- Unchecked user-input to database should not be allowed to pass through the application GUI.
- Every variable that passes into the application should be sanitized and validated.
- The user input which is passed into the database should be quoted.

Pen Testing

Penetration Testing is a method that many companies follow in order to minimize their security breaches. This is a controlled way of hiring a professional who will try to hack your system and show you the loopholes that you should fix.

Before doing a penetration test, it is mandatory to have an agreement that will explicitly mention the following parameters −

- what will be the time of penetration test,
- where will be the IP source of the attack, and
- what will be the penetration fields of the system.

Penetration testing is conducted by professional ethical hackers who mainly use commercial, open-source tools, automate tools and manual checks. There are no restrictions; the most important objective here is to uncover as many security flaws as possible.

Types of Penetration Testing

We have five types of penetration testing −

- **Black Box** − Here, the ethical hacker doesn't have any information regarding the infrastructure or the network of the organization that he is trying to penetrate. In black-box penetration testing, the hacker tries to find the information by his own means.
- **Grey Box** − It is a type of penetration testing where the ethical hacker has a partial knowledge of the infrastructure, like its domain name server.
- **White Box** − In white-box penetration testing, the ethical hacker is provided with all the necessary information about the infrastructure and the network of the organization that he needs to penetrate.

- **External Penetration Testing** − This type of penetration testing mainly focuses on network infrastructure or servers and their software operating under the infrastructure. In this case, the ethical hacker tries the attack using public networks through the Internet. The hacker attempts to hack the company infrastructure by attacking their webpages, webservers, public DNS servers, etc.
- **Internal Penetration Testing** − In this type of penetration testing, the ethical hacker is inside the network of the company and conducts his tests from there.

Penetration testing can also cause problems such as system malfunctioning, system crashing, or data loss. Therefore, a company should take calculated risks before going ahead with penetration testing. The risk is calculated as follows and it is a management risk.

RISK = Threat × Vulnerability

Example

You have an online e-commerce website that is in production. You want to do a penetration testing before making it live. Here, you have to weigh the pros and cons first. If you go ahead with penetration testing, it might cause interruption of service. On the contrary, if you do not wish to perform a penetration testing, then you can run the risk of having an unpatched vulnerability that will remain as a threat all the time.

Before doing a penetration test, it is recommended that you put down the scope of the project in writing. You should be clear about what is going to be tested. For example −

- Your company has a VPN or any other remote access techniques and you want to test that particular point.
- Your application has webservers with databases, so you might want to get it tested for SQL injection attacks which is one of the most crucial tests on a webserver. In addition, you can check if your webserver is immune to DoS attacks.

Quick Tips

Before going ahead with a penetration test, you should keep the following points in mind −

- First understand your requirements and evaluate all the risks.
- Hire a certified person to conduct penetration test because they are trained to apply all the possible methods and techniques to uncover possible loopholes in a network or web application.
- Always sign an agreement before doing a penetration test.