Introduction to Ethical Hacking

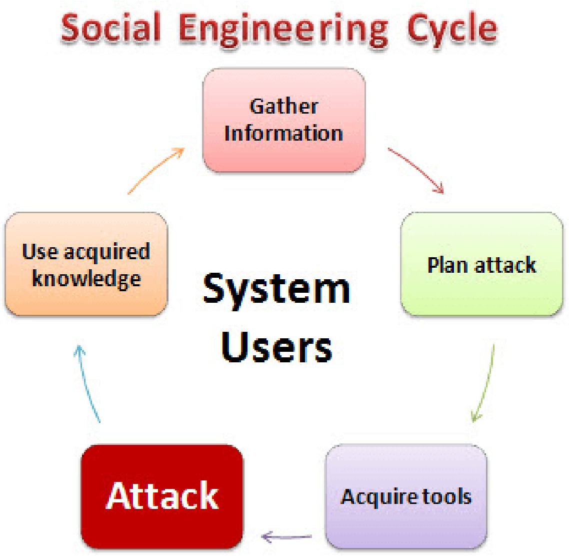
Ethical Hacking, also referred to as “white hat hacking,” “Pen Testing,” or simply “ethical hacking,” plays a critical role in maintaining the security and integrity of computer systems and networks. It involves cyber security practices that use hacking tools and techniques to identify vulnerabilities and weaknesses in computer systems and networks with the primary objective of preventing unauthorized access to systems and sensitive data, protecting against cyber-attacks, and ensuring the security of an organization’s assets.

Social engineering

Social engineering is the art of manipulating users of a computing system into revealing confidential information that can be used to gain unauthorized access to a computer system. The term can also include activities such as exploiting human kindness, greed, and curiosity to gain access to restricted access buildings or getting the users to installing backdoor software.

Knowing the tricks used by hackers to trick users into releasing vital login information among others is fundamental in protecting computer systems

In this tutorial, we will introduce you to the common social engineering techniques and how you can come up with security measures to counter them.



HERE,

Gather Information: This is the first stage, the learns as much as he can about the intended victim. The information is gathered from company websites, other publications and sometimes by talking to the users of the target system.

Plan Attack: The attackers outline how he/she intends to execute the attack
Acquire Tools: These include computer programs that an attacker will use when launching the attack.

Attack: Exploit the weaknesses in the target system.
Use Acquired Knowledge: Information gathered during the social engineering tactics such as pet names,

birthdates of the organization founders, etc. is used in attacks such as password guessing.

Types of Social Engineering Attacks

Social engineering techniques can take many forms. The following is the list of the commonly used techniques.

Familiarity Exploit:

Users are less suspicious of people they are familiar with. An attacker can familiarize him/herself with the users of the target system prior to the social engineering attack. The attacker may interact with users during meals, when users are smoking he may join, on social events, etc. This makes the attacker familiar to the users. Let’s suppose that the user works in a building that requires an access code or card to gain access; the attacker may follow the users as they enter such places. The users are most like to hold the door open for the attacker to go in as they are familiar with them. The attacker can also ask for answers to questions such as where you met your spouse, the name of your high school math teacher, etc. The users are most likely to reveal answers as they trust the familiar face. This information could be used to hack email accounts and other accounts that ask similar questions if one forgets their password.

Intimidating Circumstances:

People tend to avoid people who intimidate others around them. Using this technique, the attacker may pretend to have a heated argument on the phone or with an accomplice in the scheme. The attacker may then ask users for information which would be used to compromise the security of the users’ system. The users are most likely give the correct answers just to avoid having a confrontation with the attacker. This technique can also be used to avoid been checked at a security check point.

Phishing:

This technique uses trickery and deceit to obtain private data from users. The social engineer may try to impersonate a genuine website such as Yahoo and then ask the unsuspecting user to confirm their account name and password. This technique could also be used to get credit card information or any other valuable personal data.

Tailgating:

This technique involves following users behind as they enter restricted areas. As a human courtesy, the user is most likely to let the social engineer inside the restricted area.

Exploiting Human Curiosity:

Using this technique, the social engineer may deliberately drop a virus infected flash disk in an area where the users can easily pick it up. The user will most likely plug the flash disk into the computer. The flash disk may auto run the virus, or the user may be tempted to open a file with a name such as Employees Revaluation Report 2013.docx which may actually be an infected file.

Exploiting Human Greed:

Using this technique, the social engineer may lure the user with promises of making a lot of money online by filling in a form and confirm their details using credit card details, etc.

Prevent Social Engineering Attacks

Here are some important ways to protect against all types of social engineering attacks:

- Avoid plugging an unknown USB into your computer.
- Never click on links in any emails or messages.
- Use strong passwords (and a password manager).
- Use multi-factor authentication.
- Be very cautious of building online-only friendships.
- Keep all your software updated.
- Secure your computing devices.
- Purchase anti-virus software.
- Back up your data regularly.
- Destroy sensitive documents regularly.
- Use a VPN.
- Lock your laptop

Social Engineering Counter Measures

Most techniques employed by social engineers involve manipulating human biases. To counter such techniques, an organization can;

- **To counter the familiarity exploit**, the users must be trained to not substitute familiarity with security measures. Even the people that they are familiar with must prove that they have the authorization to access certain areas and information.
- **To counter intimidating circumstances attacks,** users must be trained to identify social engineering techniques that fish for sensitive information and politely say no.
- **To counter phishing techniques**, most sites such as Yahoo use secure connections to encrypt data and prove that they are who they claim to be. **Checking the URL may help you spot fake sites**. **Avoid responding to emails that request you to provide personal information**.
- **To counter tailgating attacks,** users must be trained not to let others use their security clearance to gain access to restricted areas. Each user must use their own access clearance.
- **To counter human curiosity**, it's better to submit picked up flash disks to **system administrators who should scan them for viruses or other infection** preferably on an isolated machine.
- **To counter techniques that exploit human greed**, employees must be **trained** on the dangers of falling for such scams.

The ideology of hacking

Modern day information risk has evolved from amateur script kiddies, locked in their bedrooms at home seeking to outsmart their friends, to a highly organised and professional criminal activity.

To truly understand the threat you have to understand why a company could become a target. Why does the hacktivist community, even though their numbers swell and they become ever more organised in their operations, remain focused on targeting specific companies? Indeed, historic analysis suggests that there may be a number of indicators that point to why hacktivists undertake attacks on those specific companies and that, in many cases, it could be argued that the company itself is to blame.

The approach of the information security team or the lack of investment by the overall business in cyber security defences, but the link between a businesses' operating methods, its client-facing posture, and how these can make that business a possible target.

Hackers with a cause

Many members of the hacktivist community are quite ideological in their stance and target companies not because they think it is a challenge to do so, but because they fundamentally believe it is the right thing to do.

Hacktivism is fuelled by individuals who believe in a cause: Freedom of speech, eradication of poverty, religion, fair trade. While many companies have actively taken steps to promote their responsible behaviour towards all these issues, how many of these have actually taken steps to implement this through the overall culture of their business and down to the grass roots of their approach to risk and incident management?

Open source reporting claims that two of the most renowned hacking incidents of 2011 were undertaken by Anonymous with retribution against their victims in mind.

Reduce your risk of cyber attack

In today's cyber connected world, where the effects of bad information security practices can affect not just the technology that runs the company, but also its financial performance, share price, customer loyalty and brand, has the evolution of cyber risk reached a position where business leaders must examine an ideological approach to business management?.

Hackers

Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system. These different terms come from old Spaghetti Westerns, where the bad guy wears a black cowboy hat and the good guy wears a white hat.

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.

Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for 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 denial of-service attacks.

Sniffing Attacks

Sniffing attacks refer to data thefts caused by capturing network traffic through packet sniffers that can unlawfully access and read the data which is not encrypted. The data packets are captured when they flow through a computer network. The packet sniffers are the devices or media used to do this sniffing attack and capture the network data packets. They are called network protocol analyzers. Unless the packets are encrypted with strong network security, hackers will be able to steal and access the data. There are different packet sniffers such as Wireshark, Dsniff, Etherpeek, etc.

Examples of Sniffing Attacks

Some of the examples of Sniffing attacks are:

- Spoofing attacks
- DHCP attacks
- DNS poisoning
- JavaScript card sniffing attacks

Types of Sniffing Attacks

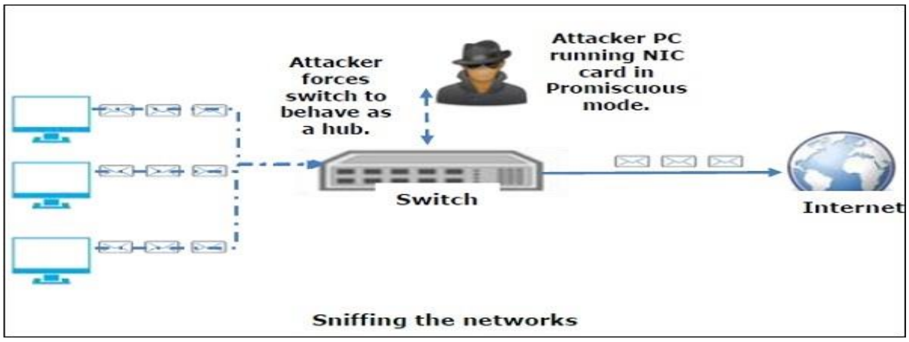
Broadly, sniffing attacks are classified into 2 categories:

Active Sniffing attacks

Active sniffing attacks majorly refer to attacks triggered by injecting Address Resolution Protocols (ARPs) into a network to flood the Switch Content address memory (CAM) table. The redirected legitimate traffic finally allows the attacker to perform the sniffing of the traffic from the switch.

Passive Sniffing attacks

This kind of sniffing usually occurs at the hub. Contrary to active sniffing, here the hub can be directly injected with a sniffing device to easily extract the data packets. However, hubs hardly are used these days and hence passive sniffing attacks are barely reported.


Attacker forces switch to behave as a hub.
Attacker PC running NIC card in Promiscuous mode.
Switch
Internet
Sniffing the networks

There are various types of sniffing attacks such as

- **LAN Sniff** – The sniffer attacks the internal LAN and scans the entire IP gaining access to live hosts, open ports, server inventory, etc. A port-specific vulnerability attack happens in LAN sniffing.
- **Protocol Sniff** – The sniffer attacks occur based on the network protocol used. Different protocols such as **ICMP**, UDP, Telnet, PPP, DNS, etc., or other protocols might be used.
- **ARP Sniff** – ARP Poisoning attacks or packet spoofing attacks occur based on the data captured to create a map of IP addresses and associated MAC addresses.
- **TCP Session stealing** – TCP session stealing is used to monitor and acquire traffic details between the source & destination IP address. All details such as port number, service type, TCP sequence numbers, data are stolen by the hackers.
- **Application-level sniffing** – Applications running on the server are attacked to plan an application-specific attack.
- **Web password sniffing** – HTTP sessions created by users are stolen by sniffers to get the user ID, password, and other sensitive information.

Tools used for Packet Sniffing

Various sniffing tools used currently and widely in the industry –

Wireshark

These are open-sourced and widely used packet analyzers that are utilized for network troubleshooting, analysis, software, and communications protocol development. Wireshark is cross-platform and is extensively used to monitor network and packet flows in the network.

Tcpdump

Usually running under a command user interface, Tcpdump allows users to display TCP/IP and other packets being transmitted or being received over an attacked computer network. It has lesser security risk and requires few resources only. In Windows, it runs as WinDump.

Dsniff

Dsniff was developed to parse different protocols and extract relevant information. It is a set of password sniffing and network traffic analysis tools, used to sniff different protocols in UNIX and Linux systems only.

NetworkMiner

It is an open-source NFAT for Windows. NetworkMiner is one of the most commonly used tools that make network analysis simple, to detect host and open ports through packet sniffing. It can operate offline too.

Kismet

Specifically used to sniff in wireless networks, even from hidden networks and SSIDs. In simpler terms, Kismet is a network detector, packet sniffer, and intrusion detection system. KisMac is used for MAC and OSX environments and works with any wireless card which supports raw monitoring mode.

There are various other packet sniffing tools such as **EtherApe**, Fiddler, **OmniPeek, PRTG Network** monitor, and so on.

Hardware Protocol Analyzer:

A protocol analyzer usually captures, analyzes the signal and data traffic in a network channel. These devices can attach themselves at the hardware level and are used to monitor traffic. It is used to capture data packet, decodes and analyzes the data. It is a hardware device that enables the hacker to see individual data bytes in the network.

MAC attacks & Flooding Switches

MAC attacks are also known as CAM table overflow attacks, here the attacker does not attack the host machine directly, but he attacks the network switches. A network switch is used to connect the devices together in the same computer network. MAC flooding compromises the security of the network switches by flooding the switches with fake address/port mapping. The switch cannot save a lot of MAC addresses; hence it enters into a fail-open mode and so it starts broadcasting all the incoming data to the ports. So the attacker gains access to the victim’s data packets.

To prevent a MAC flooding attack, we need to use Port Security (Cisco Switches), Authentication With AAA servers, Security measures to prevent ARP or IP spoofing, and Implementing IEEE 802.1X Suites.

Sniffing Detection

Detecting sniffers can be quite tedious since they are mostly passive (collect data only) especially in a Shared Ethernet. When the user is functioning on a switched Ethernet network segment,

It is easier to detect the sniffing using the following techniques:–

Ping Method

Sending a ping request of the IP address of the affected machine, the sniffer machine might respond to the ping if the suspect machine is still running. It is not a strongly reliable method.

ARP method

Machines always capture and cache ARP. Upon sending a non-broadcast ARP, the sniffer/promiscuous machine will cache the ARP and it will respond to our broadcast ping

On Local Host

Logs can be used to find if the machine is running on a sniffer attack or not.

Latency method

Ping time is used to detect the sniffing, the time is generally short. If the load is heavy by the sniffer, it takes a long time to reply to pings.

ARP Watch

Used to trigger alarms when it sees a duplicate cache of the ARP.

Using IDS

Intrusion detection systems monitor for ARP spoofing in the network. It records packets on networks with spoofed ARP addresses.

The better way to prevent sniffing is the usage of encryption tools, adding MAC address of gateway Permanently to ARP cache, switching to SSH, HTTPS instead of HTTP, and so on.

Precautionary Measures on Sniffing Attacks

Some of the sniffing prevention techniques can be:

Anti-virus tools

Installing an updated anti-virus program may prove to be beneficial in tackling sniffing.

Data Encryption

Encrypting your data with a VPN is considered one of the most feasible options in securing data from sniffing.

Unencrypted websites

Website URLs with HTTPS are secure while the ones with just HTTP don't guarantee that nobody will be watching your activities and the data. Visiting unsecured websites should be prevented to avoid exposure to sniffing attacks.

Unencrypted messaging apps

Usage of such messaging apps should also be prevented in order to reduce the risk of sniffing attacks.

Internet Security Suite

Adopting a full-fledged internet security suite for your organizations or personal systems is one of the most trusted solutions to prevent cyber attacks.

Training

It is advisable to train the staff of the organization to thoroughly check the links and e-mail addresses before clicking on them and mails. Keeping the employees informed about cybersecurity threats, modes and precautions by conducting training sessions has become crucial nowadays.

Endpoint Protection

There are networks that are remotely bridged to devices. Laptops, computers, and mobile devices are Connected to corporate networks paving the way for security threats. Such paths need endpoint protection software.

Firewall

Installing a firewall has been proven to have defied major cyber-attacks. Firewalls tend to block any brute force attacks meant for the computer system before they could damage the network or files.

Footprinting in Ethical Hacking

In ethical hacking, footprinting means gathering as much information as possible about a target system, network, or infrastructure. The aim is to identify vulnerabilities and opportunities to penetrate the system and safeguard it against different types of hacking attacks.

The footprinting process involves profiling organizations and collecting data about hosts, networks, and third-party partners. The information includes firewalls, IP addresses, URLs, operating systems, virtual private networks, network maps, email addresses, domain name system information, etc.

Different Types of Footprinting in Ethical Hacking

Now that you know what is footprinting, let’s know about its types. So, there are two types of footprinting:

Active Footprinting

In active footprinting, the hackers use certain techniques and tools to connect with the target machine. It can include the use of ping sweep or commands.

Passive Footprinting

On the other hand, passive footprinting includes a collection of the target's information and data that is publicly available. For instance, gathering information through the website, social media handles, etc.

Uses and Roles of Footprinting

Following are the roles and applications of footprinting in ethical hacking:

1. Get an Overview of the Security Framework

It allows hackers to know about the security practices and stance of the target. They find whether the network uses a firewall, what security configurations are in place for the apps, etc.

2. Find Vulnerabilities

Footprinting helps find the vulnerabilities and loopholes in the systems, computers, networks, etc. An ethical hacker can access sensitive data or breach the system to **determine vulnerabilities** and **types of attacks** a system is prone to.

3. Specify the Attack Area

Hackers can find specific target areas in a system or **network** and focus on those areas only. It narrows down the wide area of target systems.

4. Create a Network Map

Footprinting also helps in creating a map of all the networks used by the target. It can include routers, servers, topology, etc.

Information Gathering in Footprinting

An ethical hacker can collect different types of information using footprinting, and there are several sources to gather information.

Types of Information That Can be gathered with Footprinting Techniques

- IP address
- Network map
- Firewall
- Email id
- Password
- URLs
- VPN

- Server configurations
- Operating system of the target device
- Security configurations of the target device

Sources to Collect Information with Footprinting Techniques

Different sources used to obtain information are:

Social Media

As most people share their details online, hackers may use fake accounts to connect with someone on social media and seek sensitive data about them. They can appear genuine, become online friends or follow accounts to get information.

Social Engineering

Social engineering includes two major techniques:

Eavesdropping: An attacker may record the personal conversation of the victim or target person. They eavesdrop on the conversation held over the phone or in person.

Shoulder Surfing: This involves obtaining personal information, such as the email id and password of the target victims, by peeking over their shoulders while they are typing or writing these details for some work.

“Whois” Site

The **whois.com** website is often used by hackers to achieve their purposes. The website traces information, such as domain name, email id, domain owner, and more, and hackers use the data for personal benefit. This also paves the way for website footprinting.

Job Websites

Companies often share confidential or sensitive data on various job websites while writing job descriptions. Hackers can extract detail they want and use them for malicious activities.

NeoTrace

NeoTrace is a GUI router tracer program. It is a commonly-used tool to collect path information. The graphical representation highlights the path between you and the remote website, intermediate nodes, and their related details, such as contact information, IP address, and location.

Google

Google is one of the most powerful tools used by hackers to perform extensive searches. It can give you details that you can’t ever imagine. Hence, used by hackers for Google hacking.

They combine **basic search techniques** with cutting-edge operators to cause some serious damage. Moreover, the platform is used by attackers to find sensitive information that should never be revealed.

Organization’s Website

This is the best and easiest way to look for open-source data freely provided to customers or the general public.

Reconnaissance in Ethical Hacking

Footprinting is a part of a more extensive process called Reconnaissance. It is a critical data-gathering stage in the initial ethical hacking process. The information collected can be about network infrastructure, employee contact details, target flaws, and vulnerabilities used for penetration testing and at the beginning of data breaches. The aim of reconnaissance is to determine potential attack vectors.

Data collected from reconnaissance include:

Security Policies

Uncovering an organisation’s security policies can also help you find vulnerabilities and weaknesses in its system.

- Password change frequency
- Password complexity requirements
- Firewalls
- Expired or disabled account retention
- Intrusion detection systems
- Physical security, such as access badges or door locks.

Network Infrastructure

Hackers extract this information to know the type of network the target system is using, such as WAN, LAN, or MAN.

- Subnet mast
- IP address range
- Domain names
- **Network topology**

Employee Details

Used for social engineering attacks.

- Designations

- Email addresses
- Social media accounts
- Computer skills
- Phone number

Host Information

Details about the specific host to find weaknesses.

- User names
- Group names
- Operating system and version
- Architecture type
- TCP and UDP services with versions

Difference between Footprinting vs Reconnaissance

A tricky question that people who go through our Ethical Hacking Tutorial for Beginners often ask is: "What is the difference between footprinting and reconnaissance?"

Well, you can say that reconnaissance is a broad term covering footprinting and everything else involved in information gathering of a target system, website, network, etc. So, footprinting is a part of reconnaissance.

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 paruluniversity.ac.in
```

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 paruluniversity.ac.in
```

It will produce the following result −

```
Starting Nmap 5.51 ( http://nmap.org ) at 2015-10-04 10:19 CDT
Nmap scan report for tutorialspoint.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.

Quick Fix

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.

Quick Fix

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**

Quick Fix

DNS Enumeration does not have a quick fix 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.

ARP Poisoning

ARP is the acronym for Address Resolution Protocol. It is used to convert IP address to physical addresses [MAC address] on a switch. The host sends an ARP broadcast on the network, and the recipient computer responds with its physical address [MAC Address]. The resolved IP/MAC address is then used to communicate. ARP poisoning is sending fake MAC addresses to the switch so that it can associate the fake MAC addresses with the IP address of a genuine computer on a network and hijack the traffic.

Types of ARP Poisoning Attacks

- Man in the Middle Attacks
- Traffic Interception
- Denial of Service (DoS) attacks

How to Prevent ARP Poisoning Attacks

Static ARP entries: these can be defined in the local ARP cache and the switch configured to ignore all auto ARP reply packets. The disadvantage of this method is, it’s difficult to maintain on large networks. IP/MAC address mapping has to be distributed to all the computers on the network.

ARP poisoning detection software: these systems can be used to cross check the IP/MAC address resolution and certify them if they are authenticated. Uncertified IP/MAC address resolutions can then be blocked.

Operating System Security: this measure is dependent on the operating system been used. The following are the basic techniques used by various operating systems.

- Linux based: these work by ignoring unsolicited ARP reply packets.
- Microsoft Windows: the ARP cache behavior can be configured via the registry. The following list includes some of the software that can be used to protect networks against sniffing;
- AntiARP– provides protection against both passive and active sniffing
- Agnitum Outpost Firewall–provides protection against passive sniffing
- XArp– provides protection against both passive and active sniffing
- Mac OS: ArpGuard can be used to provide protection. It protects against both active and passive sniffing.

Hacking Activity: Configure ARP Entries in Windows

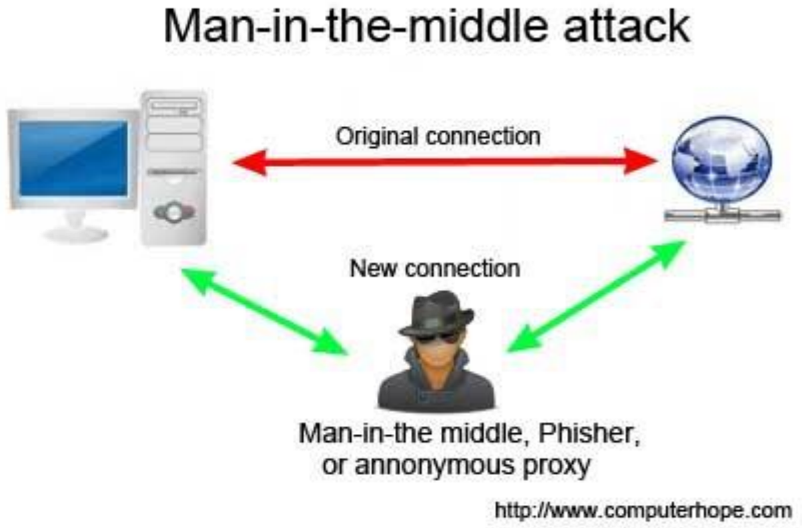
We are using Windows 7 for this exercise, but the commands should be able to work on other versions of windows as well.

Open the command prompt and enter the following command

```
arp -a
```

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.


Man-in-the-middle attack
Original connection
New connection
Man-in-the middle, Phisher, or annonymous proxy
http://www.computerhope.com

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 −

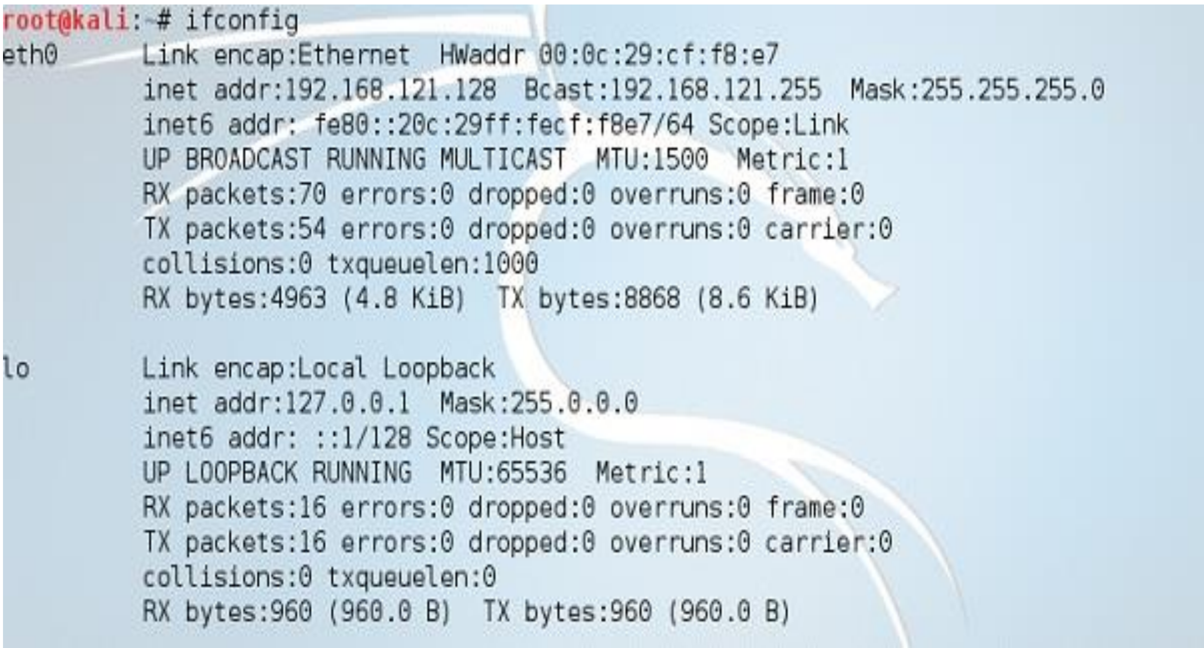
- VMware workstation
- Kali Linux or Linux Operating system
- Ettercap Tool
- LAN connection

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”.

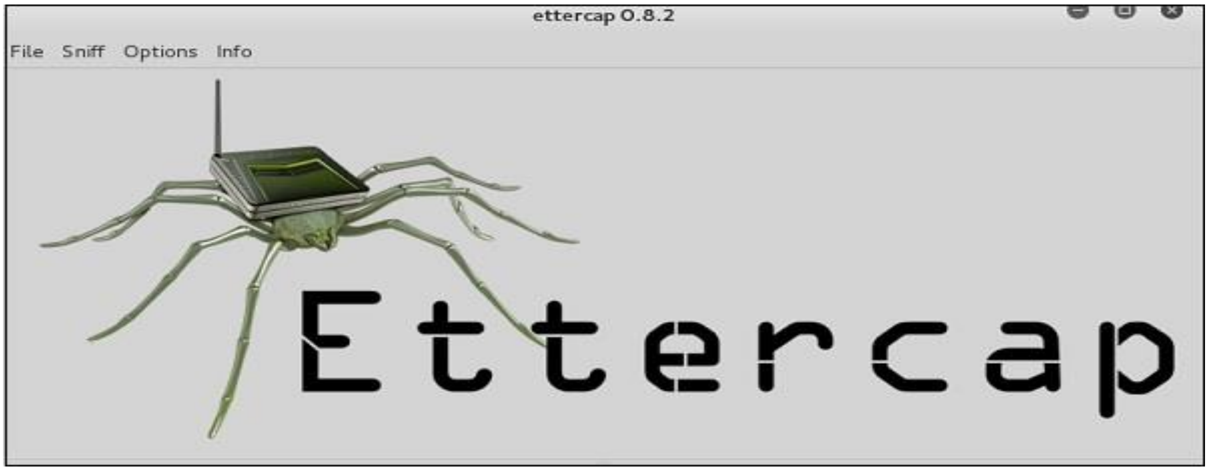
Step 3 − Make sure you are connected to local LAN and check the IP address by typing the command **ifconfig** in the terminal.



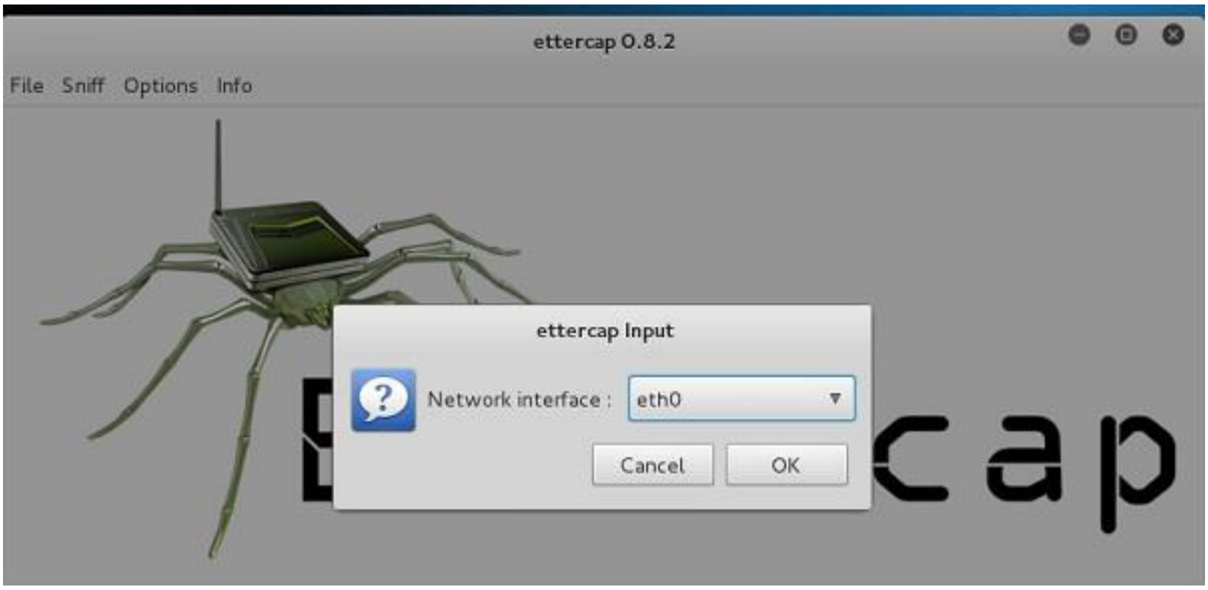
```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:cf:f8:e7
          inet addr:192.168.121.128  Bcast:192.168.121.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fecf:f8e7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:70 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.



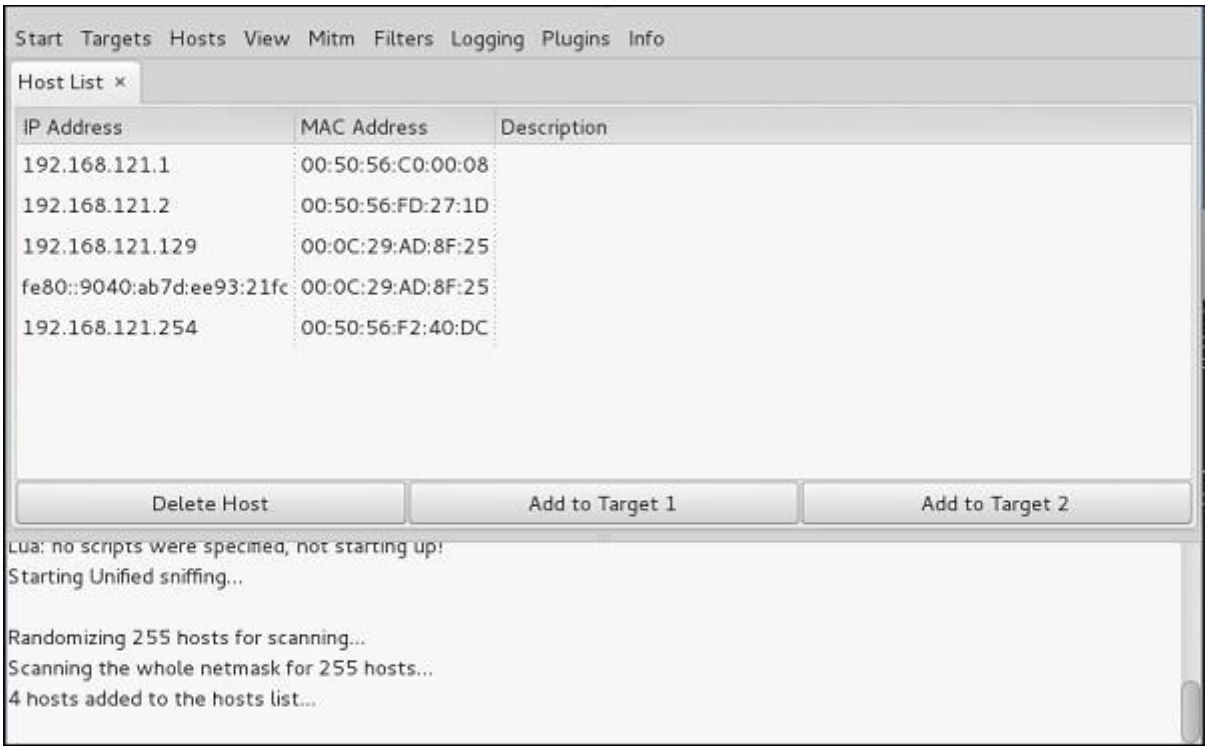
Step 5 − Now click the tab “sniff” in the menu bar and select “unified sniffing” and click OK to select the interface. We are going to use “eth0” which means Ethernet connection.



Network interface : eth0

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.



IP Address	MAC Address	Description
192.168.121.1	00:50:56:C0:00:08	
192.168.121.2	00:50:56:FD:27:1D	
192.168.121.129	00:0C:29:AD:8F:25	
fe80::9040:ab7d:ee93:21fc	00:0C:29:AD:8F:25	
192.168.121.254	00:50:56:F2:40:DC	

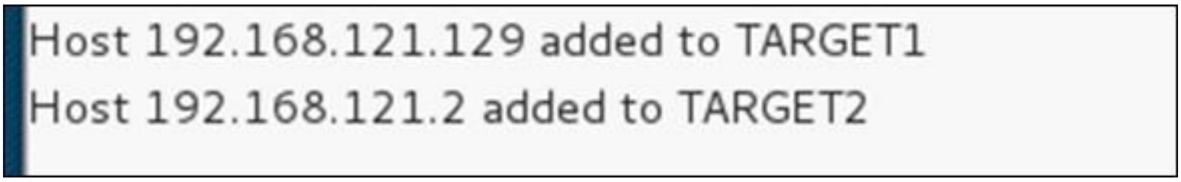
```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
```

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.”

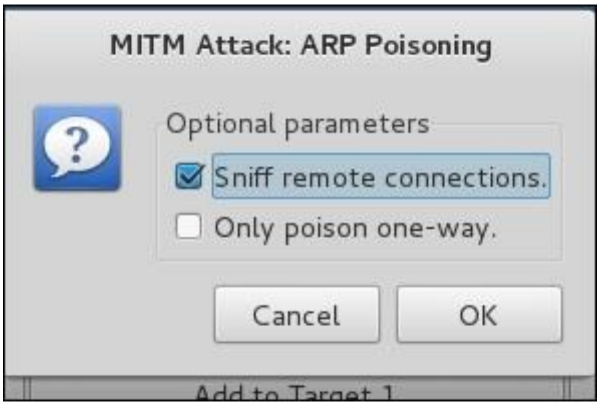
In VMware environment, the default gateway will always end with "2" because "1" is assigned to the physical machine.

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**.



```
Host 192.168.121.129 added to TARGET1
Host 192.168.121.2 added to TARGET2
```

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



MITM Attack: ARP Poisoning

Optional parameters

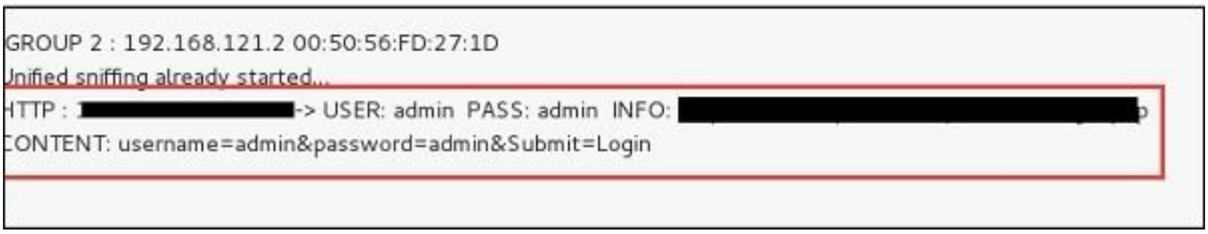
☑ Sniff remote connections.

☐ Only poison one-way.

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.



```
GROUP 2 : 192.168.121.2 00:50:56:FD:27:1D
Jnified sniffing already started...
HTTP : [redacted] -> USER: admin  PASS: admin  INFO: [redacted]
CONTENT: username=admin&password=admin&Submit=Login
```

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**.

All the Best