

NARASARAOPETA INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering ETHICAL HACKING (IV - CSE) – I SEM

UNIT IV

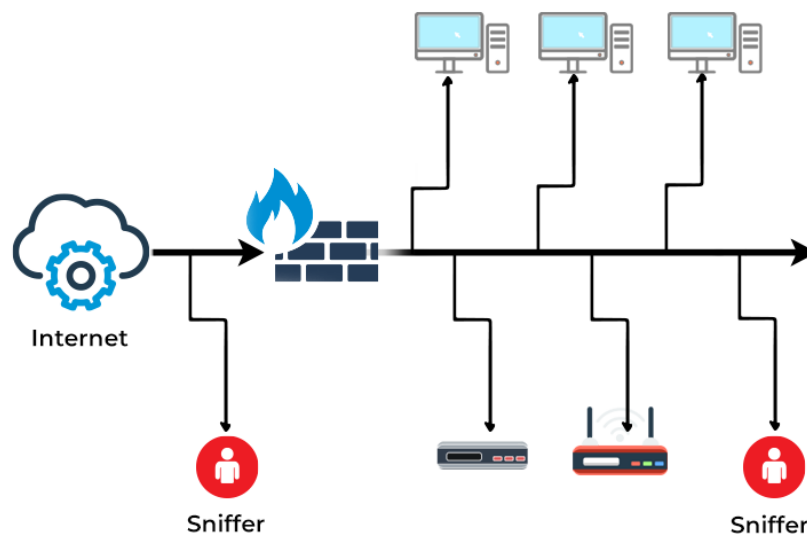
Sniffing, Packet Analysis & Session Hijacking: Sniffing, Packet Analysis, Types of Sniffing, Active and Passive Sniffing Techniques, Session Hijacking, Social Engineering: Social Engineering, Process, Identity Theft, Human and Computer Based Social Engineering Techniques, Phishing Process, Types of Phishing Attacks, Social Engineering Toolkit (SET).

SNIFFING

Sniffing is the process of intercepting the exchange of information between two hosts. In sniffing, attacker intercepts the information which is exchanged in the form of packets from the communication between HOST A and HOST B or simply client and server.

Sniffing is one of the important techniques and plays a major role in the penetration testing. Sniffing simply refers to stealing the sensitive information or data over a network. The data may be passwords, login details, texts, files, etc. In the sniffing, attacker setups man in the middle attack or packet sniffers to intercept the packets which are used to transfer the information between client and server.

Now, attacker analyse the packets to gain sensitive information. An attacker can manipulate and modify the packets to hack into the network. Also sniffing gives attacker an advantage to change the information of the original packet and send the fake packet to the receiver.

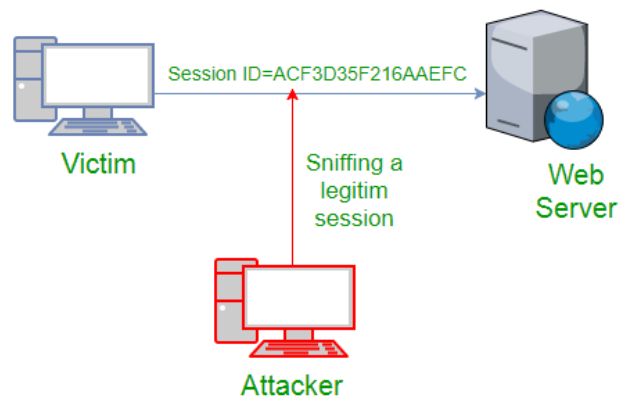


In the process of penetration testing, sniffing is one of the major techniques which professional uses. Sometimes, an attacker can sniff passwords or credentials over the wireless networks

which are generally not encrypted. Wireshark is one of the powerful packet analyser which is used for sniffing the network traffic and analysing the packets.

Network Sniffing in Ethical Hacking:

Ethical hackers use network sniffing tools to capture and examine data packets as they travel across a network. By analyzing these packets, they can uncover potential security issues such as unencrypted sensitive information, unauthorized access attempts, and potential vulnerabilities in network protocols or configurations.



Ethical hackers perform network sniffing to achieve several goals:

1. **ulnerability Assessment:** By analyzing network traffic, ethical hackers can identify vulnerabilities in network configurations or applications that could potentially be exploited by malicious hackers.
2. **Intrusion Detection:** Sniffing can help detect unauthorized or suspicious activities within a network. This is especially important for identifying potential security breaches.
3. **Traffic Analysis:** Ethical hackers can study the flow of network traffic to understand how data moves through a network. This analysis can reveal patterns that could indicate irregular or malicious behavior.
4. **Encryption Assessment:** Sniffing can help assess the effectiveness of encryption mechanisms. Ethical hackers can determine whether sensitive data is transmitted securely or if there are weaknesses in encryption implementations.

Tools which are used for sniffing are known as Sniffers.

There are two types of sniffers:

1. **Hardware Sniffers :**

Like hardware keyloggers, hardware sniffers are the physical tools which are used to intercept the packets. A hardware tool is installs between the server and target. That hardware works on

layers of OSI model either on level 2 or level 3. Mainly for the sniffing software sniffers are used. Hardware sniffer stores the packets information into the log file or depending upon the hardware used.

- Hardware sniffer is basically installed when the wired connection is present between two hosts.
- Hardware sniffers are useless when it comes to the wireless sniffing.

Hardware Sniffer Example:

Fluke Networks OptiView XG (Hardware)

The Fluke Networks OptiView XG is an example of a hardware sniffer. It's a portable network analysis tool designed for diagnosing and troubleshooting complex network issues. It's a self-contained device with its own interface and display.

Here's how it works:

- You connect the OptiView XG to the network you want to analyze.
- The device captures network traffic and analyzes it in real-time.
- It provides detailed insights into the network's performance, identifies bottlenecks, and helps diagnose problems.
- The device's interface displays the results, allowing network administrators to take informed actions based on the analysis.

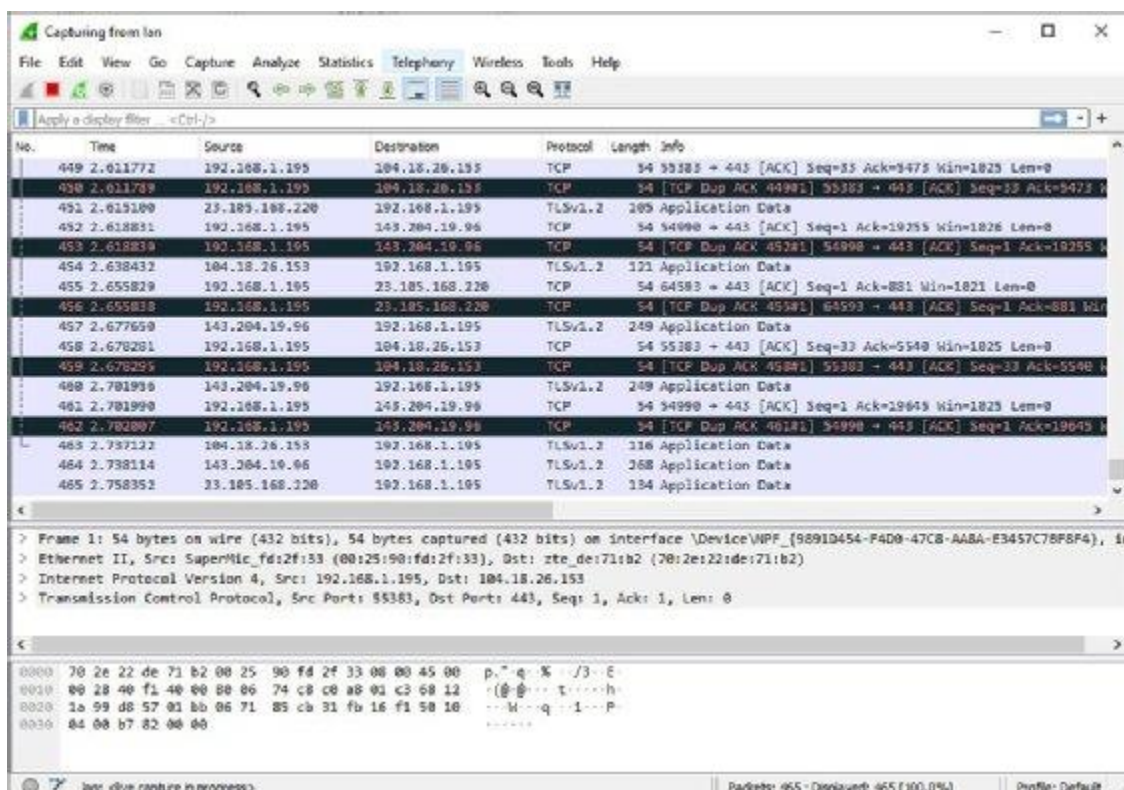


2. Software Sniffers :

- Software sniffers are known as packet analysers and are widely used for the sniffing traffic and packet analysis.
- Packet analysis is one of the important technique in which all the incoming and outgoing packets are analysed. From the packet analysis information is gained
- On the big levels, traffic monitoring is done regularly to avoid the threats coming to the network. Sometime, malwares or viruses can be packed into the packet and transferred by the attacker, so using the packet analysis, exploitation can be avoided.
- Wireshark is one of the most powerful packet analyser tools. Wireshark comes pre-installed in kali linux whereas it is available for download on its website.
- Along with wireshark, TcpDump and tShark are also used. tShark is command line based wireshark tool used for packet analysis.

Wireshark in Promiscuous Mode (Software)

Wireshark is a popular open-source software sniffer that allows you to capture and analyze network traffic. It can be installed on your computer and used to intercept data packets on the local network interface. While Wireshark itself is a software application, it's a great example of a software sniffer in action.

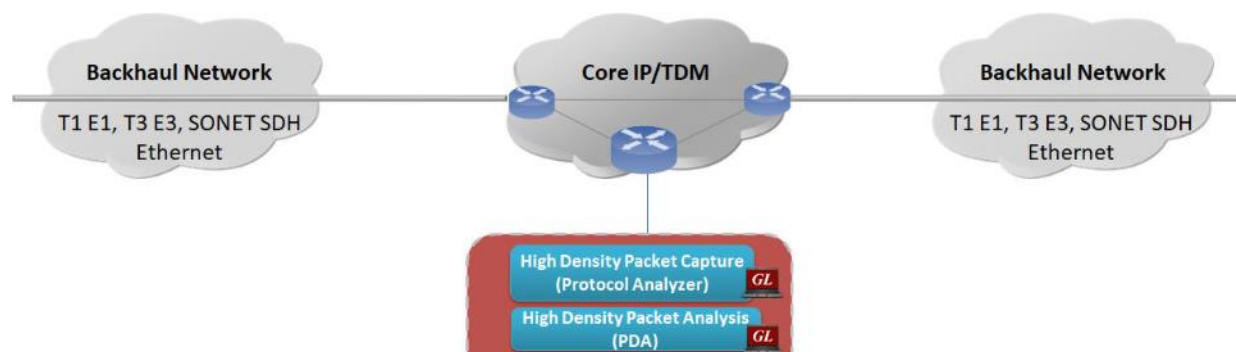


Here's how it works:

- You install Wireshark on your computer.
- You run Wireshark and select the network interface you want to capture traffic from.
- You put the selected network interface into promiscuous mode, which allows it to capture all network traffic passing through, not just traffic meant for your machine.
- Wireshark captures the packets and presents them to you in a human-readable format for analysis.

PACKET ANALYSIS:

Traffic monitoring and packet analysis is widely adopted by corporates to stay away from security threats. Sometimes, packets transferred are infected or contains malicious information.



In this case monitoring each and every incoming and outgoing packet is necessary.

1. **Capture:** Packet capture involves intercepting data packets as they travel through a network. This can be done using hardware or software tools, such as network analyzers, packet sniffers, or intrusion detection systems. These tools can be set up to capture packets on specific network interfaces or segments.
2. **Inspection:** Once captured, the individual packets are inspected to gather information about their contents. This includes details such as source and destination IP addresses, source and destination port numbers, protocol used (e.g., TCP, UDP), payload data, and more.
3. **Analysis:** The captured packet data is analyzed to gain insights into network activity, performance, and potential issues. Network administrators, security analysts, and researchers use packet analysis to identify patterns, anomalies, and potential threats. They can also use it to troubleshoot network problems, optimize network performance, and ensure compliance with network policies.
4. **Diagnosis and Troubleshooting:** Packet analysis can help diagnose network issues such as latency, packet loss, and connection problems. By examining the sequence of packets exchanged between devices, analysts can pinpoint the source of problems and take corrective actions.

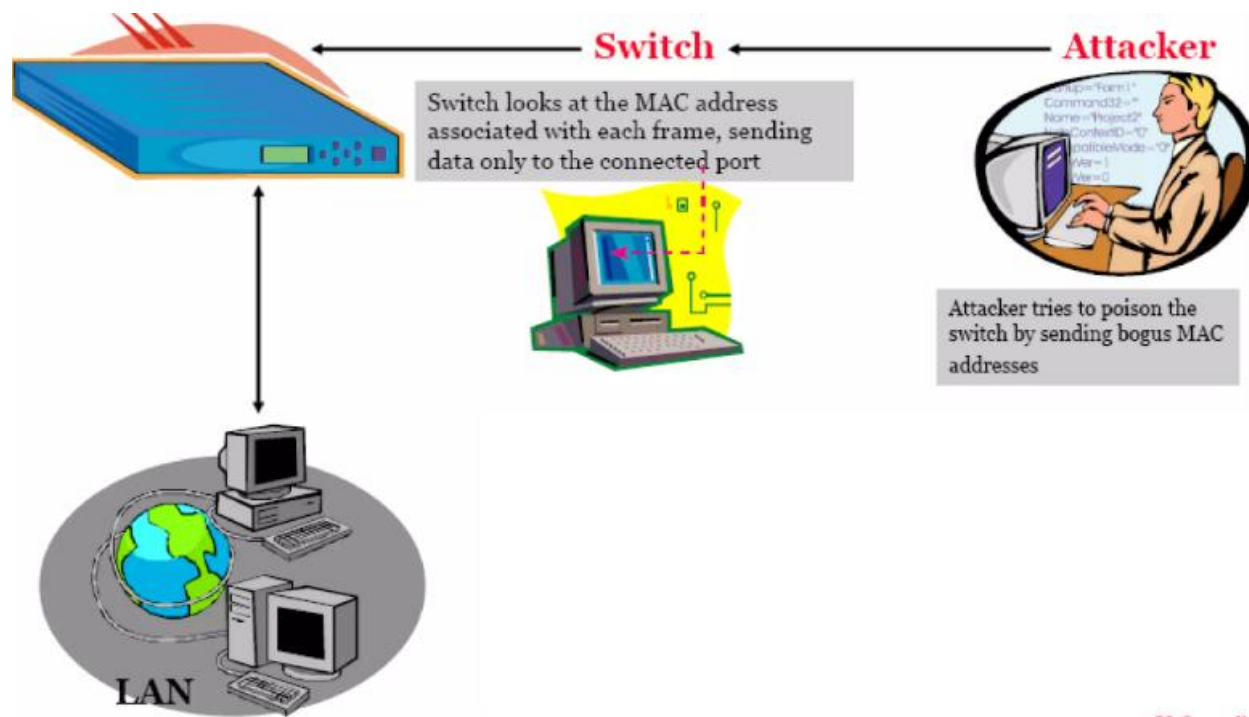
5. **Security Monitoring:** Packet analysis is a crucial tool for monitoring network security. It allows security professionals to detect suspicious activities, such as unauthorized access attempts or data exfiltration, by examining the content and patterns of network traffic.
6. **Forensics:** In the event of a security breach or network incident, packet analysis can be used for forensic investigation. Analysts can reconstruct the sequence of events leading up to an incident by examining captured packets.
7. **Performance Optimization:** Network engineers can use packet analysis to optimize network performance by identifying bandwidth-intensive applications, network bottlenecks, and inefficient communication patterns.
8. **Protocol Analysis:** Packet analysis helps in understanding how different network protocols are being used. It's especially useful when diagnosing issues related to specific protocols, like HTTP, DNS, or VoIP.

TYPES OF SNIFFING

Sniffing refers to the practice of intercepting and inspecting data as it travels across a network. Sniffing the traffic and packet analysis can be done in following two ways:

1. Active Sniffing :

In the active sniffing, sniffing is done through switch. An attacker tries to poison the switch using fake or spoofed mac address. The ultimate aim is to poison the switch and intercept every packets passing through it. In this, switch acts as intermediate. Now the switch looks each and every mac address and sends the information on the connected ports.

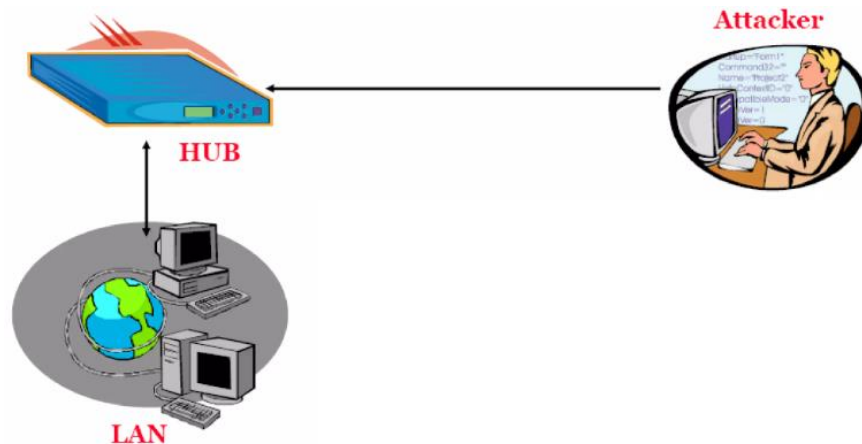


1. Packet Injection
2. Detection Risk
3. Use in Network Troubleshooting
4. Security Analysis
5. Malicious Use
6. Promiscuous Mode

Though sniffing took place using switch it is difficult to sniff the packets and there are great chances of being caught. Active sniffing may get detected easily and hence it is not efficient way of sniffing.

2. Passive Sniffing :

In the passive sniffing, sniffing is done through HUB. An attacker directly gets connected to the hub and starts sniffing. This type of sniffing is often used for network analysis, troubleshooting, and monitoring purposes. As the attacker is directly connected to the hub, it is difficult to detect the sniffing and there are less chances of being caught. Passive sniffing is quite easy as compared to the active sniffing.



In the passive sniffing, hub acts as an intermediate. The packets are intercepted easily and analysis process became smooth.

Observation without Participation:

Passive sniffers do not actively inject any packets into the network; instead, they passively listen to the traffic that is already present on the network.

Use in Network Troubleshooting:

Network administrators commonly use passive sniffing tools, also known as network analyzers or protocol analyzers, to troubleshoot network issues. By analyzing the existing traffic, they can identify problems such as bottlenecks, errors, or abnormal patterns.

Security Monitoring:

Passive sniffing can be used for security monitoring to detect and analyze network anomalies. Security professionals may use passive sniffers to identify potential security threats or unauthorized activities on the network.

ACTIVE SNIFFING TECHNIQUES:

1. MAC Flooding :

Mac flooding is technique used for flooding the SWITCH by sending huge amount of requests. The switch gets flooded by huge number of mac requests.

A switch contains limited memory to map the mac address on the physical ports. By sending the numerous amount of request the limited gets over. In the process, the switch is bombed with fake mac addresses resulting into the flooding of switch.

Once the switch is get flooded, now it acts as hub because of the flooding switch messed up. Now, due to behaviour shown by switch is like a hub, packets are transferred to all the devices on the network and hence the attacker can easily perform the sniffing.

A. Macof

Macof is one of the powerful tools used for MAC Flooding. Macof is pre-installed with kali linux. It simply floods the local random mac address resulting into failure of the switch to open in repeating mode and hence enables sniffing with ease.

Using Macof :

1. Open the terminal into kali linux.
2. Type “macof /?” to open the help screen of the macof tool.
3. Syntax for flooding is :

macof [-i interface] [-s source] [-d destination] [-e tha] [-x sport] [-y dport] [-n times].

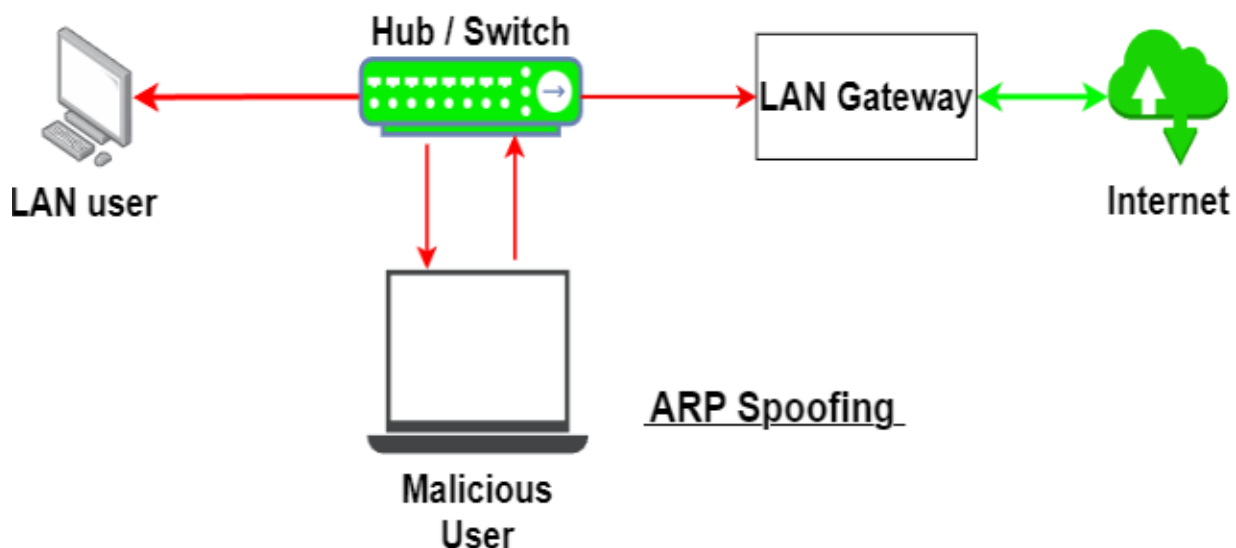
4. Attacker can simply change the syntax according to his needs.
5. Macof floods the switch with random mac address.

6. Example of macof command is shown in screenshot

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# macof -i eth0 -n 15  
ca:92:9f:63:cd:c9 e9:7:8e:6f:a1:49 0.0.0.0.3677 > 0.0.0.0.63148: S 392094569:392  
3d:45:20:21:1b:e6 99:e1:72:54:fe:c6 0.0.0.0.54206 > 0.0.0.0.11843: S 1459372484:  
a8:ea:4d:16:8f:6a b4:5f:38:56:33:80 0.0.0.0.35475 > 0.0.0.0.11499: S 1252574726:  
97:a8:2b:2b:19:87 a3:6e:b4:3:3a:cb 0.0.0.0.5290 > 0.0.0.0.57111: S 311973068:311  
61:91:80:d:c1:cd 7e:44:10:31:ee:d4 0.0.0.0.24501 > 0.0.0.0.59519: S 1393648417:1  
be:48:8a:2e:28:b7 d9:a4:2b:3e:35:ad 0.0.0.0.35607 > 0.0.0.0.16879: S 1711281500:  
a6:9f:d2:4a:1e:cf 5c:73:84:2f:d0:5c 0.0.0.0.52615 > 0.0.0.0.44803: S 1311016079:  
d8:dd:9d:60:95:71 5b:68:53:1a:4:34 0.0.0.0.48115 > 0.0.0.0.9786: S 8519533:85195  
a6:1a:9:4:38:77 ac:51:a3:57:b5:1 0.0.0.0.53284 > 0.0.0.0.44933: S 1988733969:198  
ae:5f:9e:6b:13:8d cb:84:d5:15:2c:ee 0.0.0.0.57800 > 0.0.0.0.14188: S 1011689393:  
d8:a1:80:4a:74:22 14:6e:fd:37:8:6f 0.0.0.0.34423 > 0.0.0.0.4716: S 1793632231:17  
82:cc:f:38:7f:31 37:c8:68:35:e1:2d 0.0.0.0.3725 > 0.0.0.0.33625: S 1402600953:14  
60:fa:79:54:e0:9c 3c:f3:fe:4a:7a:e9 0.0.0.0.40565 > 0.0.0.0.27862: S 1053302980:  
6b:5c:e7:44:e4:cb a5:9f:42:5:65:47 0.0.0.0.13307 > 0.0.0.0.49509: S 2108133412:2  
79:cd:53:7a:5d:92 f4:2b:55:4c:6c:c5 0.0.0.0.26490 > 0.0.0.0.52940: S 1296818571:
```

2. ARP Spoofing :

ARP is the Address Resolution Protocol which is used to convert ip address into mac address. Arp packets are intercepted to send the data to attacker's machine. Working of ARP is discussed in the previous chapters. An attacker can exploit arp poisoning in order to intercept or perform sniffing attack in a network. When the switch is flooded using mac flooding the arp tables can be spoofed, due to flooding the switch is in forward mode so that sniffing can be performed easily.

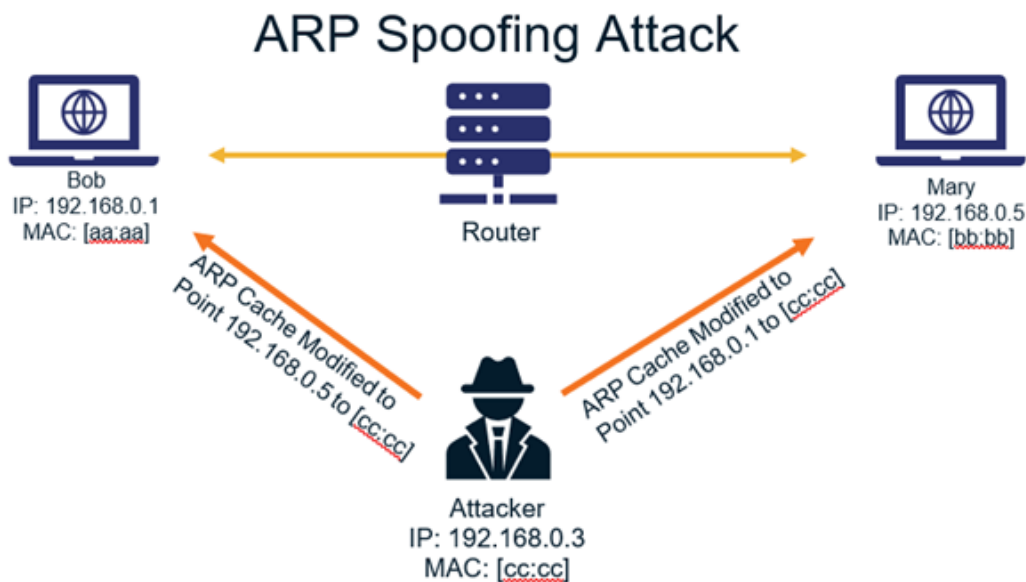


3. Arp Poisoning :

In the arp poisoning, the attacker steals the arp information and spoofs the mac address of the target to itself. Now, switch sends all the information to the spoofed mac address i.e. to the attacker.

ARP Poisoning took place in following steps:

1. User A sends Arp request to the switch asking about the ip address. The query of ip address is processed by switch. For ex ip address is 42.45.56.45.
2. Now User B having the same ip address will reply to the switch with its mac address. For ex, mac address is x:y:z:a:b . now here is role of attacker.
3. Attacker will eavesdrop on the arp request and will spoof the mac address of target and sends its mac address to the User A which is a:b:x:y:z .
4. Now all the information or the queries of the ip address 42.45.56.45 will be sent to the attacker's machine.



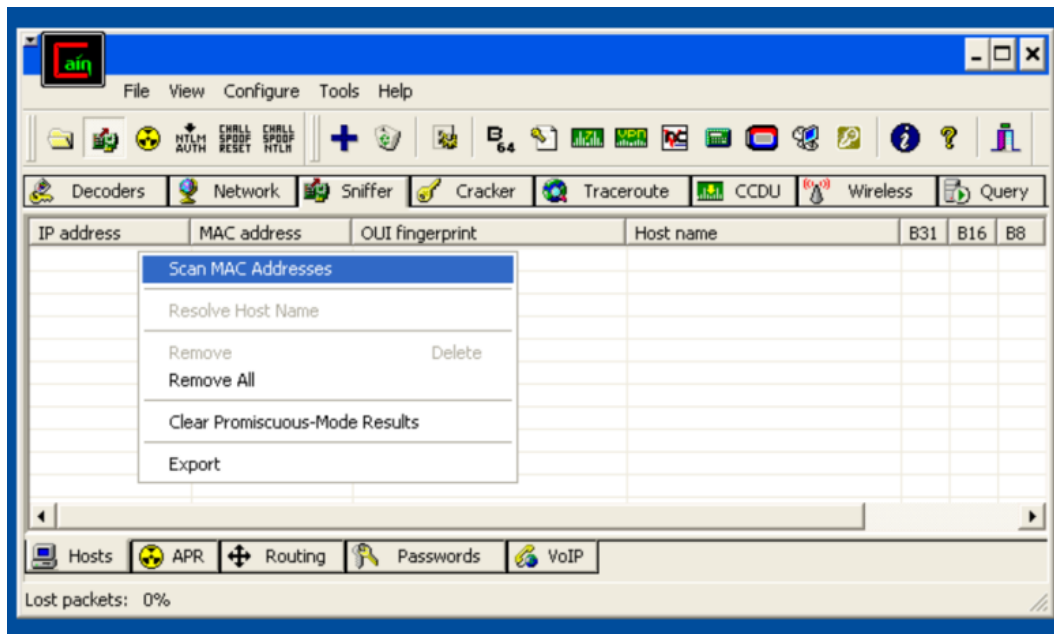
Tools used for ARP Poisoning:

Generally Cain and Abel, ettercap, etc. are used for arp poisoning. In this book, cain and abel is discussed.

1. Cain and Abel :

Cain and able is powerful password recovery tool which is also used for sniffing and various purposes. It allows password recovery using brute force, sniffing, dictionary attacks and by

various methods. It takes advantages of weakness present in a particular protocol's authentication mechanism.



Some of the important features of cain and abel are:

1. MS-CACHE hash dictionary attacker and brute force cracker.
2. Offline processing of captured file.
3. SIP-MD5 hash dictionary attacker and brute force cracker.
4. Sniffer can extract audio communication and save them in .wav format.
5. Remote register editor and VoIP sniffer.
6. AirPcap TX capability automatic recognition.
7. And much more.

Using Cain and Abel :

1. You can download it for windows and other unix systems.
2. Download and install cain and abel (for windows).
3. Open Cain and Abel.
4. Before performing arp spoofing, configure the tool on your network. Target and attacker need to have on same network.
5. Click on the configure toolbar and configure the network device. Now open up the sniffer tab and click on start sniffer icon.
6. Click on the plus (+) icon to add the hosts. When the new window will open confirm that all hosts have same subnet as of the attacker.
7. Check that the target is listed before performing arp spoof. Now click on a yellow circle icon in the toolbar to start attack.
8. Once you start attacking, the status will be changed to poisoning and the bottom panel will start having traffic.

Passive Sniffing Techniques:

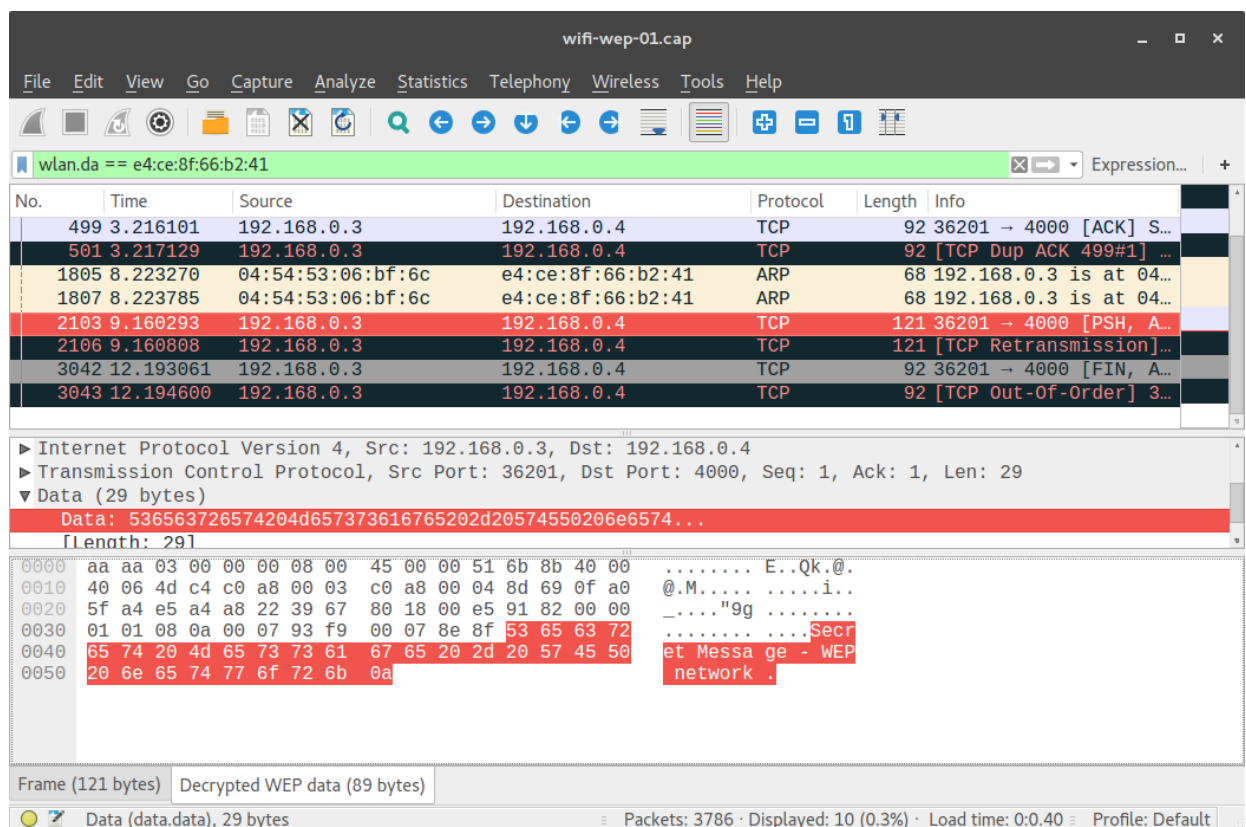
Passive sniffing techniques are widely used because in passive sniffing, attacker can directly intercept the packets due to presence of hub.

Some tools used for performing Passive Sniffing:

1. Wireshark :

- Wireshark is a powerful packet analyser tool. Wireshark is generally used for capturing the network traffic, packet analysis and sniffing the information.
- Wireshark comes pre-installed in kali linux and it is also available for download.
- Wireshark is supported on windows and unix based systems. Wireshark allows a user to live capture the network traffic and perform analysis. Display filters are used in wireshark to view particular packets or sets of data.

Download : www.wireshark.org



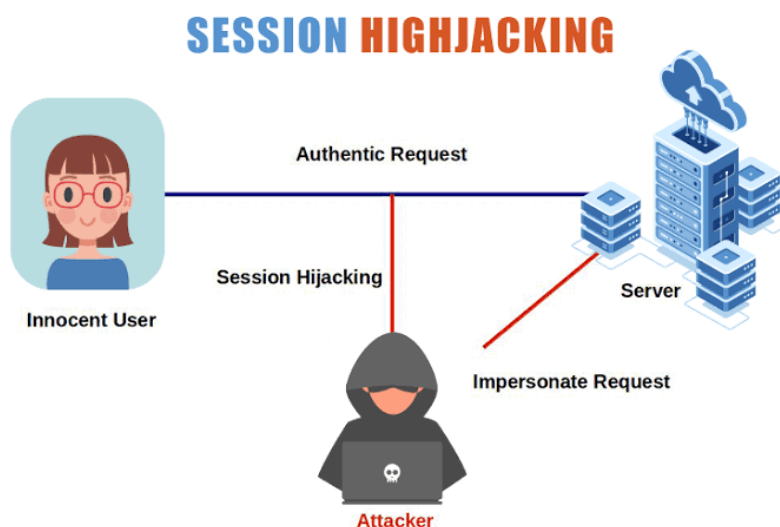
Using Wireshark :

1. Download wireshark on windows system or open wireshark from kali linux.
2. Choose the interface from which the network traffic is to be captured. User can select multiple interfaces like wireless network, Ethernet, etc.

3. Click on start capture to start capturing the traffic. Once there will be some traffic on the network, packets will be shown in wireshark (shown in screenshot).
4. There are many display filters are available in the wireshark to shortlist the particular data.
For ex: `ip.addr==127.0.0.1` will filter all the packets which are transferred to or from this ip address.
5. Colour coding is used in wireshark, different colour indicates different traffic. Green colour indicates tcp traffic whereas light blue indicates udp traffic.
6. Right click on any packet and click on follow tcp streams to check the full conversation between source and destination (shown in screenshot).
7. Various display filters are used to filter the traffic for particular analysis. for ex : “dns” filter will only show the dns traffic (shown in screenshot).
8. There are variety of filters are available. Go to capture menu and click on capture filters. It will show all the available filters. Click on any filter name and at the bottom it will show filter string.

SESSION HIJACKING

An attacker tries to access the remote session of a target by stealing the session id of the target. If the attacker is able to get the valid session id of target system, he can easily access the active remote session of target. Using a session id, an attacker can get access into the target system and take over the data.



- Session hijacking can be done from various types. When the attacker is able to steal the tcp sessions between two hosts, this is known as TCP Session Hijacking.

- Most of the ports and protocols use TCP connections so that intercepting an initiating tcp session id help an attacker to access the target system.
- An attacker can access into machine and perform exploit. It can be complete takeover of the target host.
- Spoofing and session hijacking both are different. In the spoofing, an attacker spoofs and pretended to be another user and performs the attack using that.
- In spoofing, an attacker does not take part actively. In session hijacking, an attacker actively participates in attack.
- Target host needs to be actively connected to the server. An attacker takes over the active session and manages to steal the credentials using that.

Types of Session Hijacking:

1. Active :

In active session hijacking, an attacker is able to manage stealing active and valid session id of the target user. Attacker disconnects the target from the active session and takes over that active session.

Generally the attacker needs to intercept the packets and analysis them in order to get valid cookies or session id information. Before that takeover of an active session are quite complex and difficult.



How active session hijacking typically works:

Session Token or Cookie- When a user logs into a system or a website, they are often assigned a session token or cookie.

Interception- The attacker intercepts the session token or cookie.

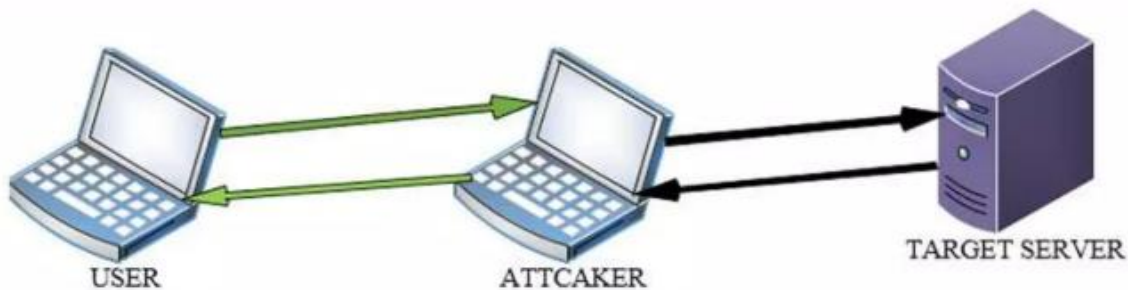
Use of Stolen Token- Once the attacker has the session token, they use it to impersonate the legitimate user.

Unauthorized Access- With the stolen session, the attacker can perform actions on behalf of the victim, such as making changes to their account settings, accessing sensitive information, or conducting transactions.

2. Passive :

- In the passive session hijacking, an attacker sits between two communicating host and analyse their communication packets traffic.
- Passive session hijacking, also known as session eavesdropping, is an attack in which an unauthorized party monitors and intercepts communication between two entities without actively manipulating the data during transmission.
- After getting the session id or valid cookie, attacker hijacks the session but doesn't perform any exploit.

Attacker simply analyse all the packet communication which are going in forward request and tries to communicate using the fake identity in order to get highly sensitive information from the other side.



How passive session hijacking typically occurs:

1. Monitoring Communication:

The attacker secretly monitors the communication between a user and a system, such as a website or an application.

2. Capturing Session Data:

The attacker captures data exchanged during the session, including session tokens, cookies, or other authentication credentials.

3. Analyzing Captured Data:

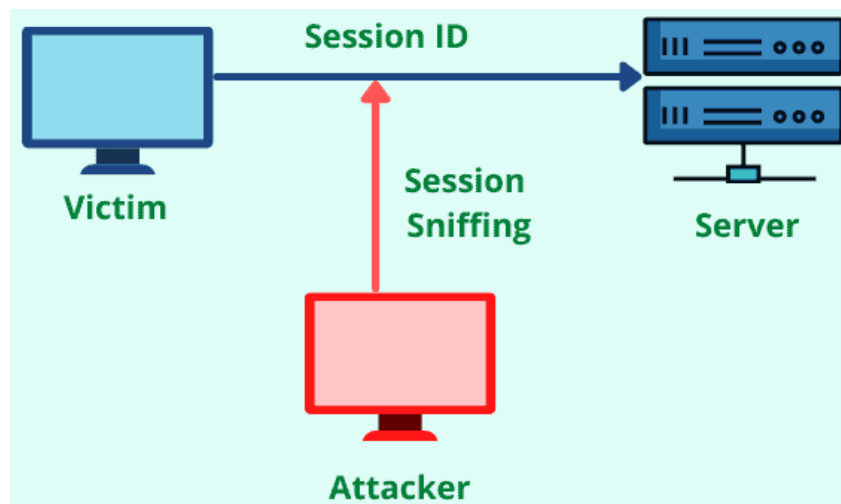
Once the data is captured, the attacker analyzes it to extract sensitive information, such as session identifiers or authentication tokens.

4. Unauthorized Access:

With the information obtained through passive session hijacking, the attacker may gain unauthorized access to the user's account or system.

Steps Involved in Session Hijacking:

1. An attacker sits between the two communicating hosts, i.e. tries to sniff the communication packets.
2. Attacker intercepts the packets and analyse every packet.
3. Now attacker exploits the target's active session once he analysed and found required tcp packets.
4. Attacker disconnects the target from its current session and takes over the session of the target host.
5. Now attacker tries to exploit the target host by injecting the infected packets into the target host.



Methods of Session Hijacking:

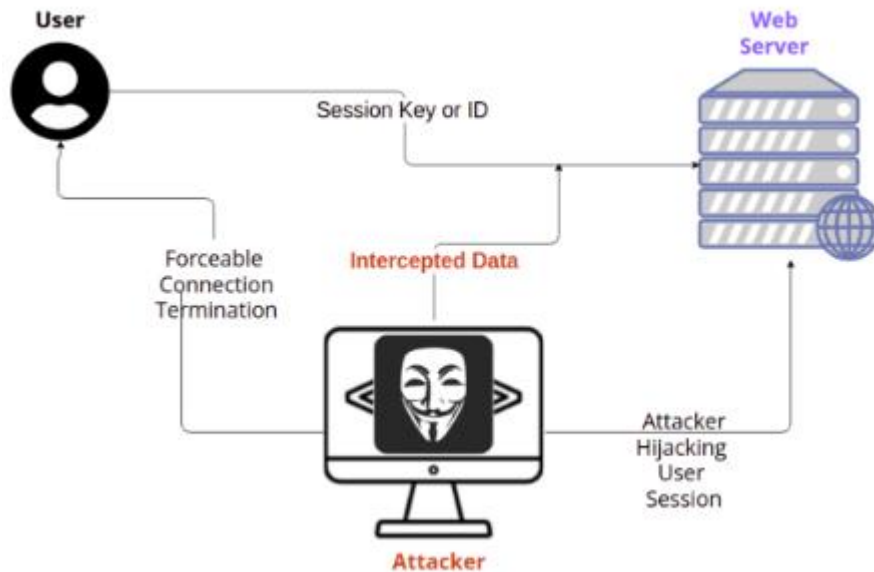
Session Hijacking can be done from following ways :

1. Network Side Session Hijacking :

In the network side session hijacking, an attacker sits between two communicating hosts and tries to intercept all the communication packets to get the valid cookies and session IDs. Generally it is done when the communication between two hosts is TCP or UDP based.

Network side session hijacking can be done in following ways :

1. Exploiting TCP/IP Communication.
2. Exploiting 3-Way Handshake.
3. Exploiting UDP Communication.
4. Man in the Middle Attack (MITM).
5. IP Spoofing.



2. Application Side Session Hijacking :

In application side session hijacking, an attacker tries to get the valid session ids of the target user in-order to get access of the active session and sometimes due to presence of critical vulnerability attacker can even create an unauthorised new session.

Session Ids might be present in the URL of web application which is reflected result of HTTP GET request. Also user tries to intercept the valid session cookies of the target user and tries to hijack the session. Generally, Brute Force is used in guessing for the session ids. An attacker uses the brute force to get the session id of the target user.

SESSION HIJACKING TOOLS :

Hamster :

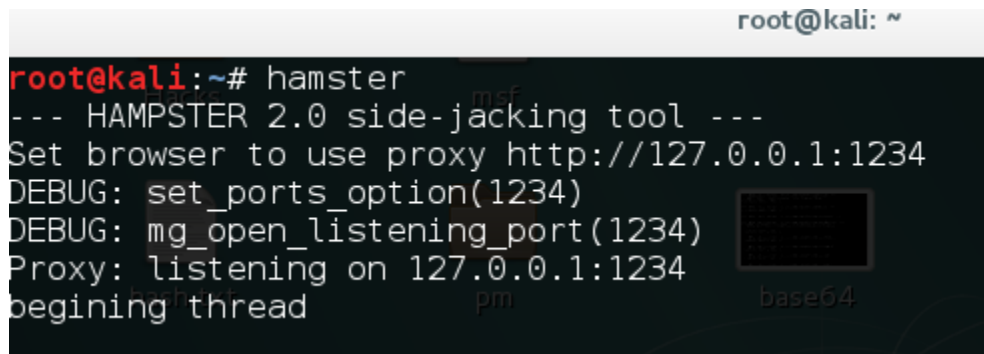
Hamster is a powerful side-jacking tool.

Hamster comes preinstalled in kali linux. Session Hijacking Using Hamster:

1. Run Kali Linux.
2. Navigate to applications > Sniffing & Spoofing and open Hamster.
3. Hamster will start and it will show the proxy listing details (shown in first screenshot).
4. Open a new terminal and type “ apt-get install ferret”, to install the ferret.
5. Now open the browser and visit to the ip –address along with the configured port.

For ex : 127.0.0.1:1234

6. Hamster configuration window will open. Now there are some steps given to configure the hamster for side jacking (shown in second screenshot).
7. In the very first step, click on adapter menu and click on start sniffing (shown in third screenshot).
8. Wait for few seconds and check whether packets are receiving or not.
9. Now wait till the target appears. Once the target appears click on the clone its session to perform the cookie stealing.
10. Follow all the steps shown in hamster configuration window to perform a successful side jacking attack.

A terminal window titled 'root@kali: ~' showing the execution of the 'hamster' tool. The output includes: '--- HAMPSTER 2.0 side-jacking tool ---', 'Set browser to use proxy http://127.0.0.1:1234', 'DEBUG: set_ports_option(1234)', 'DEBUG: mg_open_listening_port(1234)', 'Proxy: listening on 127.0.0.1:1234', and 'begining thread'. There is a small black square icon and the text 'base64' on the right side of the terminal output.

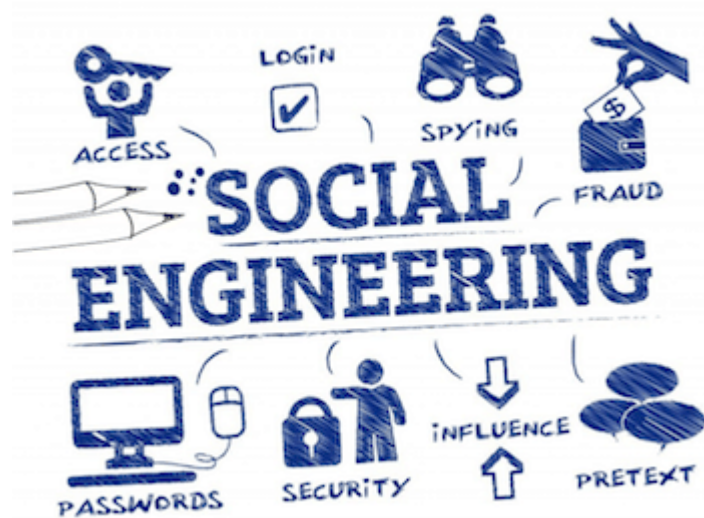
```
root@kali: ~  
root@kali:~# hamster  
--- HAMPSTER 2.0 side-jacking tool ---  
Set browser to use proxy http://127.0.0.1:1234  
DEBUG: set_ports_option(1234)  
DEBUG: mg_open_listening_port(1234)  
Proxy: listening on 127.0.0.1:1234  
begining thread
```

SOCIAL ENGINEERING

Social engineering is an art of human exploitation. Exploiting the human itself to gets sensitive information. Social engineering play very big role in the hacking and penetration testing. A good needs to be a good social engineering.

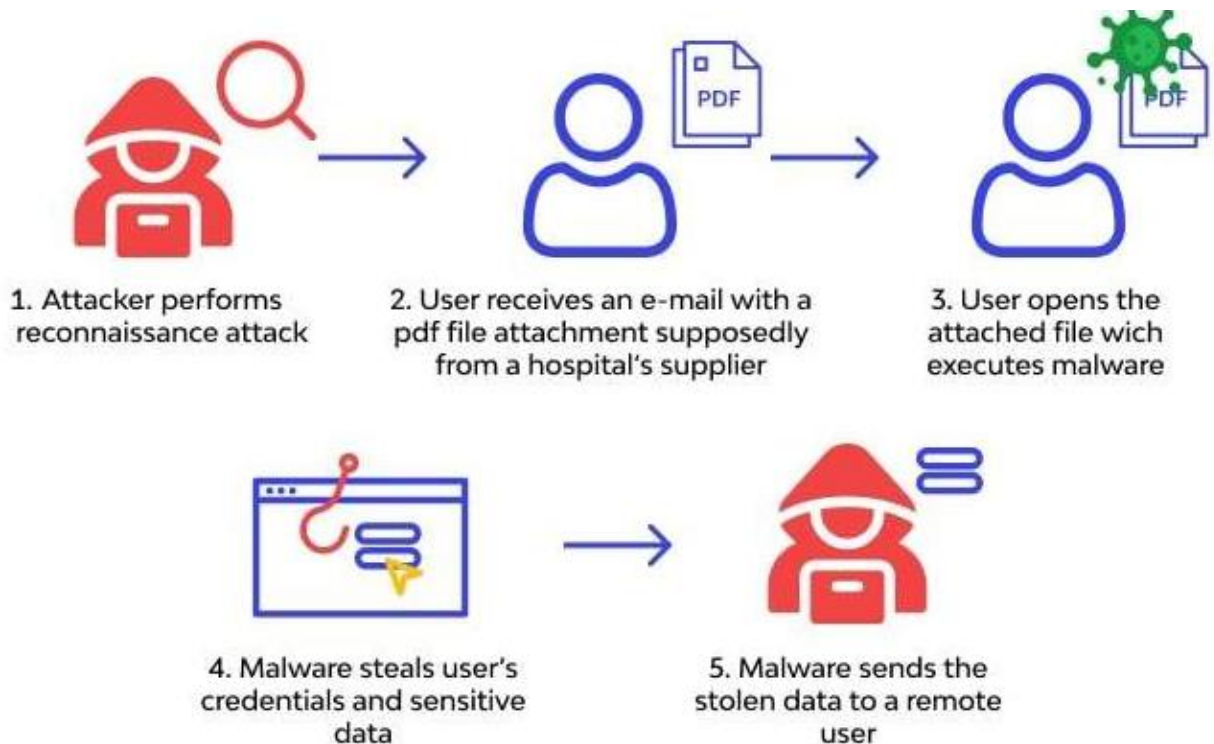
If a hacker is good at social engineering, hacking a thing is not a big deal for him. An attacker manipulates the user in order to get sensitive information using social engineering. Social engineering may be human based or tool based.

Both kind of social engineering plays an important role. If an attacker is able to manipulate the customer services or receptionist of a company, he can get some sort of sensitive information from there. Hence social engineering is a vast field, by which simply manipulate a target, an attacker can compromise and gain much of sensitive information to perform further hack.



Social engineering can be performed online or live in persons. Now a days, fake emails, fake mobile calls and messages, etc. are used to get the information from the target.

For ex, an attacker calls the target and says hello, I am from XYZ Company, you have won 50000 rupees in our lottery and many other manipulating things. They ask for your personal information in order to avail this money. Now, at last sometimes they give you a number to call and avail you lottery amount.



During this they already have performed social engineering attack and gained your personal information. Many times people get emails and messages as well. There are many scammers who try to thug a person to get benefited.

A human is the weakest part of any company. Exploiting the human by manipulating can give tons of sensitive information and sometimes even access to the network of company.

There is no solution to fix the level of human manipulation. Hence a human is always vulnerable to social engineering and hence the whole corporate network is vulnerable. Simply manipulating a person can provide huge information disclosure, the person may be directly or indirectly related to the company, may be the peon or clerk or maybe an officer at higher post.

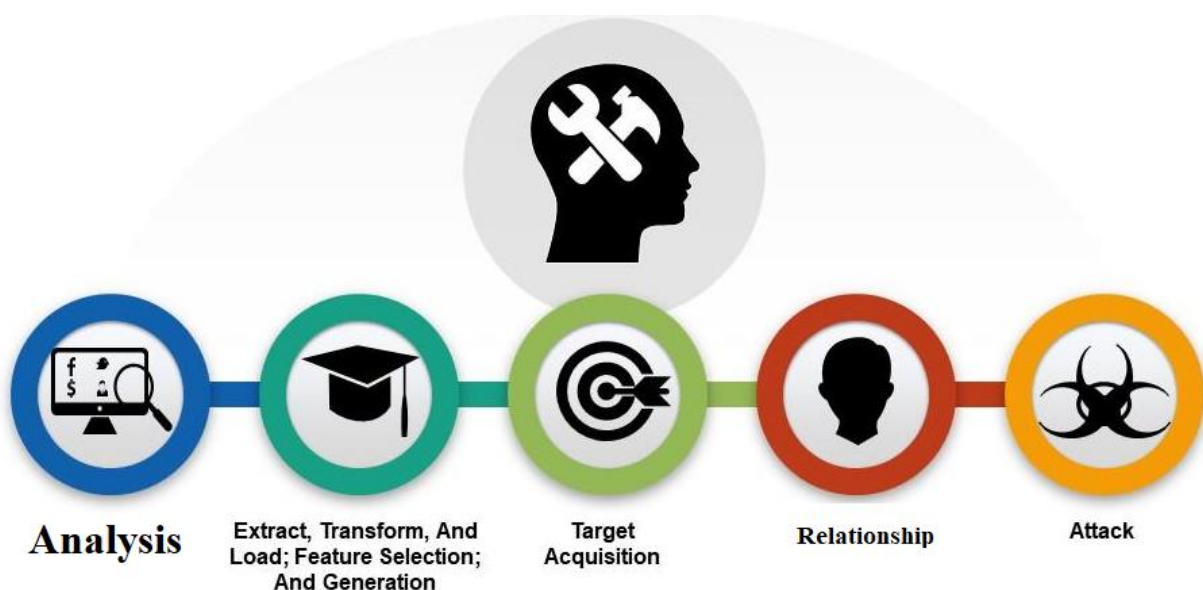
There is no such role of post in the social engineering. Social engineering totally depends upon the manipulating skills of an attacker, if he is good at manipulating or convincing a person, he can compromise into the whole network, without actually performing Hack.

Process of Social Engineering:

1. Analysis : Analysis is one of important factor at any stage of life as well as in penetration testing. If an attacker wants to perform social engineering attack at any corporate structure, first requirement is to analyse the human behaviour of employees and officers. Once the attacker successfully analyse and finds a vulnerable target, attacker can successfully perform the attack. Hence before targeting any random human, an attacker needs to analyse the whole target structure.

2. Selection :

After careful assessment, now attacker selects the most vulnerable human with which he can perform social engineering and can get some sensitive information. While selecting sometimes attacker choose medium or least vulnerable person if the position of that person is higher. Hence for successful attack, an attacker needs to choose the target person very carefully.



3. Maintain relationship :

Once attacker knows his target, he tries to make good relationship with the target. Directly or indirectly attackers comes into contact with the target and tries to take his faith and trust. In this phase, the motive of attacker is to gain trust of the target. Once target starts believing in attacker, it becomes quite easy to perform social engineering attacks.

4. Attack :

This is the ultimate phase, in this phase an attacker performs attack which may be in-person or live attack. Attacker tries to gain sensitive information from the target by the sake of faith and trust. If the attacker is able to maintain good relationship, he can easily exploit and gain access to the sensitive information.

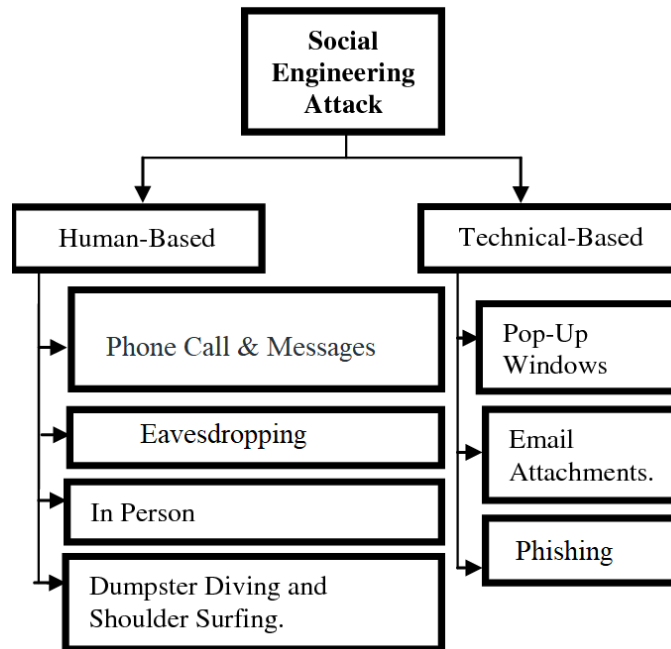
These are the simple process which is followed by an attacker while performing. A hacker never go off the track, he follow the process because if something got missed, there are chances of being caught.

Identity Theft :

- Identity theft is referred as making a fake identity of the same person in order to get benefit. If an attacker steals name and information of the target, this thing is known as identity theft.
- Identity theft is generally done when attacker is engaged in cases of fraud. Fake identities are generally used by the fraudsters to commit fraud.
- How an attacker steals the identity is quite interesting thing. Generally people throws off bills or other documents from which an attacker can gain information of the target. Sometimes an attacker stole your purse which contains your important documents.
 - for ex : if an attacker gets your identity card, now if he wants to use it to get fake passport, simply he will apply for a new passport stating the bills and saying that you have moved to new address.

Now this is the major threat where the fraudsters can do big scams and ultimately the target is victimised. Once the new identity cards are made, an attacker can also ask you bank to issue new cheque books or credit and debit cards by showing the fake identity and ultimately target is now also exploited financially. From the fake identity of the target, an attacker can do anything. He can issue new sim cards, bank accounts and much more fake scams on the name of the target. If the activities get caught, ultimately the target is victimised in first sight.

HUMAN BASED SOCIAL ENGINEERING TECHNIQUES:



1. Phone Call:

A phone call is used for social engineering, an attacker owns a fake identity and tries to get information from the target. An attacker behaves like or sounds in such a manner to gain trust of the target over phone call. Now once the attacker succeeds in manipulating the target, gaining information is not a big deal.

For Ex : Person A receive a phone call stating I am from XYZ University and this is to inform you that your documents are missing or misplaced by the staff. Please provide your following information to keep you admission secure.

Generally in this case, due to fear of losing the admission or having the faith that call is from university, A will provide the information asked. Now, actually the caller was owned a fake identity of university employee and manipulated A to give off the information. Hence before giving the information, ensure that the cause is genuine.

2. Message

Fake messages are sent to users to gain their personal and sensitive information. Those messages seem very real and trust worthy but actually there is a hand of attacker behind them.

For Ex:

Person A receive a message, stating thank you for being the customer of XYZ, you are our today's lucky customer and have won a prize. Please provide your information to confirm your prize. Now the person A thinks that the message is from company and there is now harm in providing the information and hence replies back with the asked information. In this case target

may be victimised of identity theft. Personal information of A might be used by fraudster for the fraud purposes.

3. Dumpster Diving

Looking for sensitive information in garbage or dumps is known as dumpster diving. Sometimes, attacker may find a piece of paper or some important documents from which sensitive information can be retrieved. When penetration testing or hacking is performed each and every possible aspect of gathering information is taken into consideration.

4. Shoulder Surfing :

Looking at shoulder or guessing the password by viewing a person typing or indirectly seeking into his hand movement to get password. Sometimes it provides quite sensitive information.

5. Eavesdropping :

An attacker can look for the information without the permission and knowledge of the target. Eavesdropping might be happened when someone is doing sort of transitions or at any possible area where the information can be obtained by simply looking secretly. Attacker sometime hears the verbal conversation of its target to gain some information.

COMPUTER BASED SOCIAL ENGINEERING:

1. E-Mail :

E-mails are widely used for the information exchange. Hence it is a major way by which social engineering can be done. An attacker can send malicious files like Trojans or viruses and which can exploit the target.

Generally spammers send infected emails or email containing infected files to the target. Once the target open the mail or attachment, virus or Trojan associated with it gets executed into the system of target and remotely spying the target system. Hence the attacker can gain the information of target from target's system.

For Ex : A receives an email with an attachment, now the email seems to be from a reputed company and hence A opens the mail. Now there is an attachment which is named x.docs or maybe of any type. A download and opens the attachment for viewing. In the background, a malicious application gets executed and now tracks every activity of A's system. Sometimes product sell emails are also sent to the users stating that get a particular product in 80% off or some other sort advertisement. User generally opens those links and register with their details. They won't get any product but their information has been disclosed and there are chances of identity theft.

2. Ads and Pop-up screen :

While surfing over internet, user generally sees some sort of ads like discount on cloths or mobiles. There are some strategies which are used to make user fool and gain their personal information. Usually the ads are related to recent search history of the user because of the tracking by search engine, websites and internet service provider.

While downloading or visiting a website, sometimes popup window occurs showing some interesting things which attract the user to follow the pop-up and ultimately they end up with giving their information to the attacker. More or less, again there is a huge chance of identity theft. Data collected is generally sold out at higher prices and this data is misused.

3. Phishing :

Phishing is one of the oldest but working techniques of social engineering. In the phishing generally an attacker creates a fake webpage or fake login page which looks exactly same as the original page. Now, once the page is made the attacker targets a user and manipulates him to login on that. Once user logs in, his credentials are recorded into the attacker's database.

Now-a-days, phishing has been extended. Phishing can be done by making fake pages, by fake e-mail or fake applications which resembles to the original one. Phishing can be easily identified by checking the URL. The phishing link will contain the url which will not resemble to the original URL.

For Ex :

A person receives an email that XYZ Company (reputed one) is launching an Application. Apply for the beta-tester of the application and there is a link present to login and download the application. User generally gets happy by seeing that he got a chance to test the application for everyone.

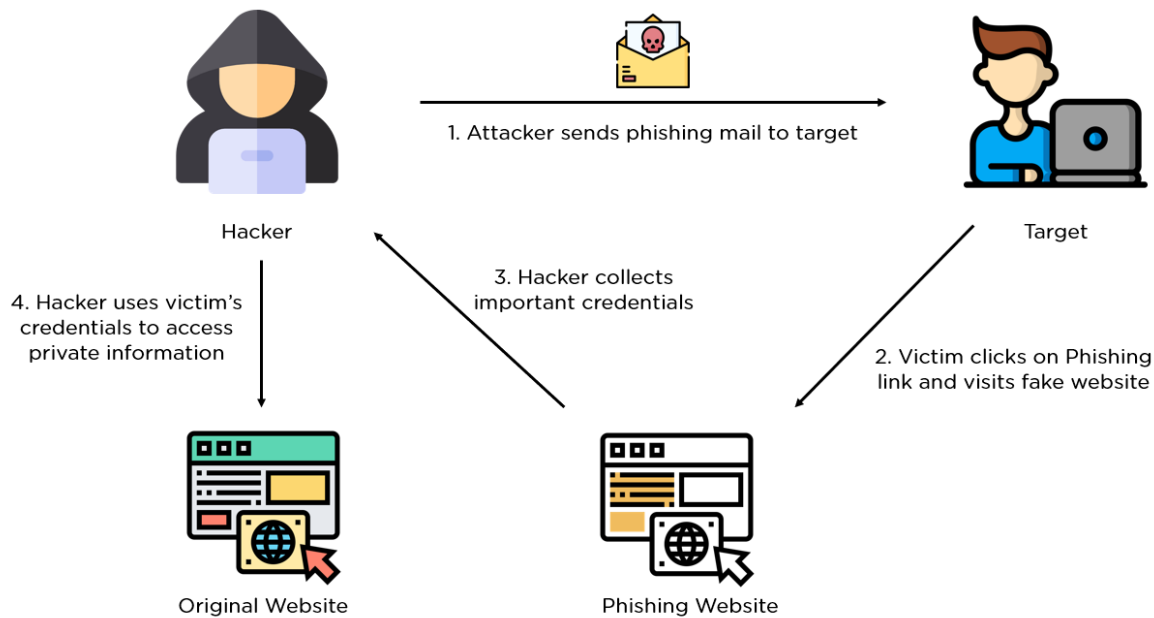
Now, once he opens the link and register successfully, the page shows some message like “oopps.. !! You missed the chance, We have already closed beta-tester application”. Generally user ignores and takes it as consequence but actually he is victimised of phishing and social engineering.

PHISHING PROCESS:

1. First an attacker creates the replica of original website and check whether there is anything which can be easily detected. After the successful creation, sometimes for the surety attacker runs the phishing site on local host using the software like “xampp”.

2. Once the phishing site runs with zero error on the local host, attacker register for a fake domain and fake hosting provided fake information. Attacker tries to keep the domain look similar to the original one.

For ex : original domain – xoxox.zxv . Now attacker tries to keep fake domain like : x0x0x.zxv etc. which is not easily noticed by the user.

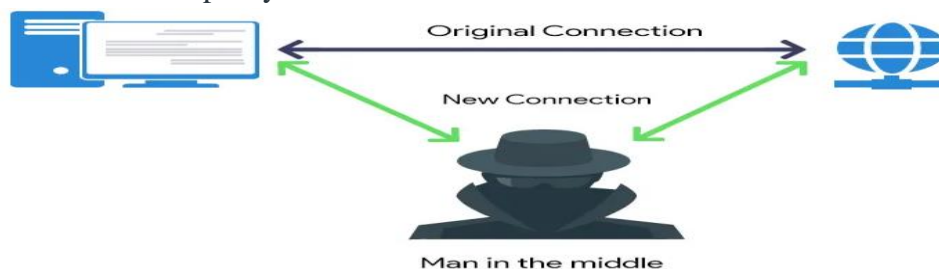


3. Once the phishing site is live, now attacker targets the users and send phishing link via mail or over the chats in such a way that user get manipulated and opens the link. Once user login to the link, his credentials are recorded.

Types of phishing Attacks:

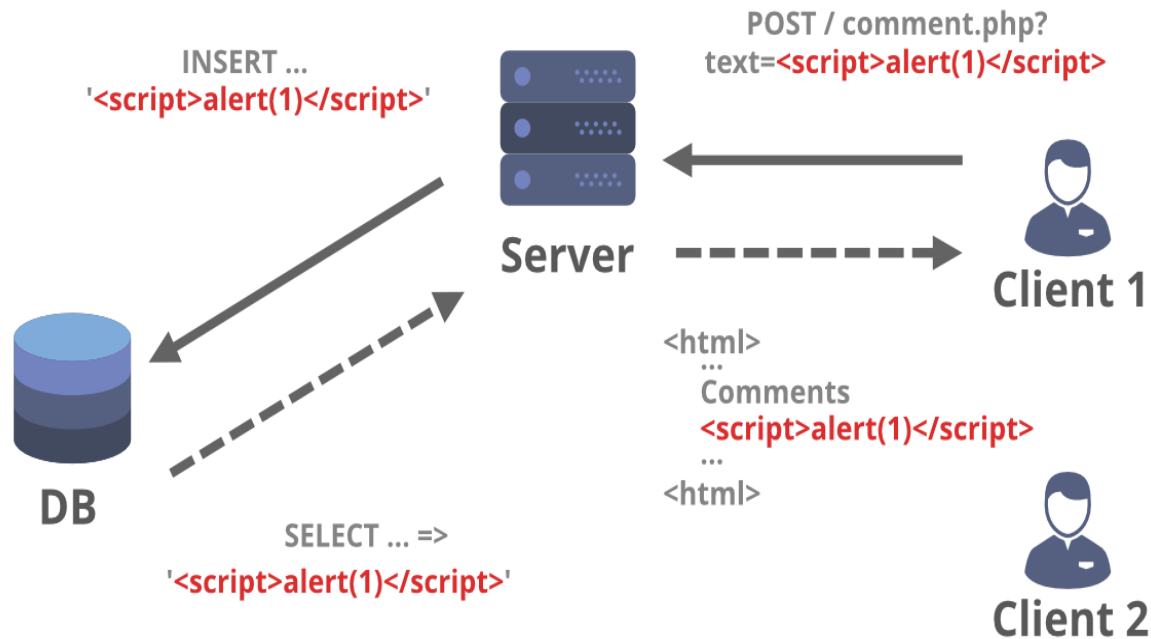
1. Man in the middle attack (MITM) :

In MITM, Attacker sits between the source and destination. Attacker monitors and sniffs the activities of the target and tries to get the credentials. MITM can be performed over http as well as https. Generally the user is redirected to a proxy server and real proxy is not used which makes this attack more successful. The proxy may be of any type but attacker avoids the user to use real proxy.



2. Cross site scripting (XSS) :

XSS attack is generally performed by injecting code injection in the url parameters or input data field. Generally xss is carried out by url formatting. Xss may be persistence or DOM based. XSS is counted in top 10 vulnerability list according to owasp top 10 2013.



3. URL Redirection :

Attacker shares a link to the target user which on opening redirects to the phishing page. Attacker tries to keep the link as similar as the original so that there are less chances of being caught. This is one of the traditional methods of performing the phishing attack. Generally user shares such links over personal chats or emails.

4. Site cloning :

Site cloning is generally performed directly by the Social Engineering Toolkit (SET) which comes pre-installed in kali linux. It creates the clone of site on the local ip of the attacker. When the target & attacker both share the same network, site cloning is useful.

5. Keylogger or Malware Based :

Attacker can inject malware into the target system by the means of e-mail or any method or installs the keylogger which tracks every activity of the target and anonymous sends the data record to the attacker when target system goes online.

Beside these attacks there are some other types of phishing attacks which also plays an important role. Some are:

Fake Search Engine:

A fake search engine is a malicious website designed to mimic a legitimate search engine, like Google or Bing, with the intention of deceiving users. Users may be directed to the fake search engine through phishing emails, malicious ads, or compromised websites.

Client-Side Attack:

A client-side attack targets vulnerabilities on the user's device or application rather than the server or network. This could involve exploiting weaknesses in web browsers, plugins, or other client-side software.

DNS Redirection Attack:

DNS (Domain Name System) redirection attacks involve manipulating the DNS resolution process to redirect users from a legitimate website to a malicious one. Attackers may compromise DNS servers or use techniques like DNS spoofing to achieve this redirection.

SOCIAL ENGINEERING TOOLKIT (SET):

Social engineering toolkit is one of the powerful packages which contain tons of social engineering tools. SET comes pre-installed in kali linux. Set can be downloaded into other operating systems too. SET is an open source framework which is freely available.

Social Engineering toolkit have ability to perform various attacks like tabnapping, site cloning, mass mailing, arduino based attacks and much more. Website attack vectors are generally used to perform phishing type attacks.

Site Cloning using Social Engineering Toolkit :

1. Run kali linux and search social engineering toolkit.
2. Open Social engineering toolkit and agree the licence agreement.
3. 6 options will be shown up illustrating various kind of attack methods.
4. Select (1) which is Social-Engineering Attacks.
5. 10 options will be shown up illustrating various kinds of attack vectors.
6. Select (2) which is Website Attack Vectors.
7. 8 options will be shown up illustrating various kinds of attack vectors.

8. Select (4) which is Tabnapping Attack Method.
9. 3 options will be shown up illustrating various kinds of attack vectors.
10. Select (2) which is Site Cloner.
11. It will ask for IP Address on which the Site will be cloned, Open a terminal and type “ifconfig” to check the ip address. Provide the ip address of kali machine.
12. Now, it will ask for the URL of the website to clone. Input the desired website.
13. This will take a little time and starts cloning. If the apache service is not on, it will ask for turning it on. Input with ‘y ‘ to turn on the apache service.
14. Now send the ”ip address” on which the site has been cloned. Remember, target and attacker needs to be on same network.
15. Passwords will stored in directory named “VAR/WWW “ in the log file.

MASS MAILER USING SOCIAL ENGINEERING TOOLKIT :

6. Select (5) which is Mass Mailer Attack.
7. To mass attack single email, select (1) option, else select (2) option.
8. Select (1) for bombing via own gmail account, else select (2) for creating own server or open relay.
9. (Own account is selected), input gmail account.
10. Input the name which will be seen to user.
11. Input the email password.
12. Set the priority. For high priority select 'yes' else 'no'.
13. Enter the email subject. Select the type of mail. For html input with 'h' and for plain input with 'p'.
14. Input the body of message and once the body is completed, end with using "END".
15. Now SET will send the emails.

```
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #settoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules

99) Return back to the main menu.

set> █
```

```
set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.

What do you want to do:

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer

99. Return to main menu.

set:mailer>1
set:phishing> Send email to:iamunknown0208@gmail.com

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing> 
```

Prevention of Social Engineering:

Social engineering inside the corporate is performed successfully due to lack of training of employees, inter-personal controversies or by the ex-employee. Social engineering can be prevented to a great extent if the proper training is given to the employees.

There are some prevention mechanisms for avoiding social engineering:

1. Checking the URL's before visiting.
2. Proper training.
3. Ensure about the received phone call or text message before giving information.
4. Don't open attachment e-mails coming from unknown source.
5. Try to keep your identity as much private as possible.
6. Don't visit the links which are detected by the browser as harmful.

