UNIT - IV

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 HOSTA and HOSTB or simply client and server. Sniffing is one of the important techniques and plays a major role in the penetration testing.

→ Sniffing is simply refers to stealing the Senstive Information or data over a network. The data may be passwords, login details, texts, files, etc.

→ In this, attackers 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, attackers analyse the packets to gain Sensitive Information.

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. The hardware works on layers of OSI model either on level 2 or level 3.

Mainly for 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.

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 incoming and outgoing packets are analysed. From packet analysis information is gained.

Sometimes, 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 most powerful packet analyser tool.

* Packet Analysis:-

Packet Analysis is itself a big topic to study. 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.

*Types of Sniffing :-

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 to poisan 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.

2. Passive Sniffing - In the passive sniffing, sniffing is done through HUB. An attacker directly gets connected to the hub and starts sniffing. It is difficult to detect the sniffing and there are less chances of being caught. passive sniffing is quite easy as compared to active sniffing.

In this, hub acts as intermediate. the packets are interapted easily and analysis process became smooth.

*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. In the process, the switch is bombed with fake mac addresses resulting into the flooding of switch.

+ 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.

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.

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 a: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.

Tods 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 abel 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 configure toolbar and configure the network device. Now open up the sniffer tab and click on start sniffer icon.
6. Click on 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.

9. See the screenshots below for the reference.

* 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. It is supported on windows and unix based systems.

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 blw source and destination.

7. Various display filters are used to filter the traffic for particular analysis. for ex: "dns" filter will only show the dns traffic.

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. The filter string will be used to input any filter in wireshark.

Wireshark filter cheat sheet is also available online which can be used as a reference.

*Tshark:

Tshark is a Command line based network sniffing and packet analyser tool. It is also one of the powerful sniffing tools. It captures the data from live network.

Using Tshark:

a. Open terminal in kali linux. Now to check manual or help screen of the tshark type "man tshark" and manual screen will be shown up. Here everything about tshark is mentioned. There are various commands are also described.

b. Now start tshark by typing "tshark" in terminal.

c. To check the working of tshark, generate some traffic using nmap or any other tool.

d. Now tshark will capture all the packets and show it in the following format:

1. Timestamp
2. Source
3. Destination
4. protocol
5. Port
6. PTR Record.

e. Tshark cheat sheet is available online, just like wireshark, tshark also supports filters. Apply the specific filters at the beginning and tshark will only capture specified packets.

* 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 the 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 b/w two hosts, this is known as TCP session hijacking.

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.

2. Passive:

In the passive session hijacking, an attacker sits between two communicating host and analyse their communication packets traffic. After getting the session id or valid cookie, attacker hijacks the session but doesn't perform any exploit.

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 Hijacking Tools:

Hamster:

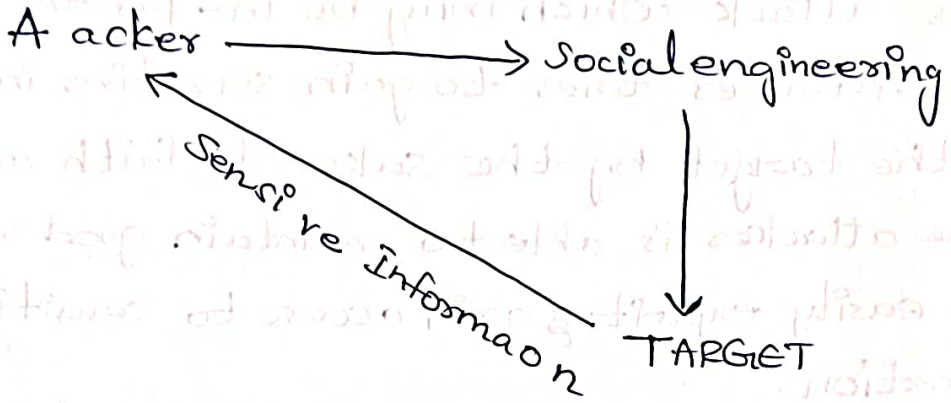
Hamster is a powerful side-jacking-tool. Hamster comes pre-installed in kali linux.

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.
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.
7. In the very first step, click on adapter menu and click on start sniffing.
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 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.

* Social Engineering :-

Social engineering is an art of human exploitation. Exploiting the human itself to gets senstive information. Social engineering play very big role in the hacking and penetration testing. A good needs to be a good Social engineering. It is a vast topic itself. If a hacker is good at Social engineering, hacking a thing is not a big deal for him.



* 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 to analyse the human behaviour of employees & officers. Once the attacker successfully analyse and finds a vulnerable target, attacker can successfully perform the attack.

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 position of that person is higher.

3. Maintain relationship:

Once attacker knows his target, he tries to make good relationship with the target. Directly or indirectly attacker 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.

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 & gain access to sensitive information.

*Identity Theft:

Identify 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. Identify theft is generally done when attacker is engaged in cases of fraud.

Fake identities are generally used by the fraudsters to commit fraud. 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:-

a. phone Call:

A phone call is used for social engineering an attacker owns a false 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.

b. Messages

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

c. Dumpster Diving:

Looking for sensitive information in garbage or dumps is known as dumpster diving.

d. Shoulder Surfing:

Looking at shoulder or guessing the password by viewing a person typing or indirectly seeking into his hand movement to get password.

e. Eavesdropping:

An attacker can look for the information without the permission and knowledge of the target.

*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.

2. Ads and Pop-up Screens:

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 feel and gain their personal information.

3. Phishing:

phishing is one of the oldest but working techniques of social engineering. In this generally an attacker creates a fake webpage or fake login page which looks exactly same as the original page.

* 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 succesful 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 localhost attacker register for a fake domain and fake hosting provided fake information. Attacker tries to keep the domain look similar to the original one.

3. Once the phising site is live, now attacker targets the users and spend phising 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 & destinatic Attacker monitors and sniffs the activities of the target and tries to get credentials. MITM can be performed over http as well as https.

2. Cross site Scripting (XSS):

XSS attack is generally performed by injecting code injection in the url parameters or input data field.

3. URL Redirection:

Attacker shares a link to the target user which on opening redirects to the phishing page.

4. Site cloning:

Site cloning is generally performed directly by the Social engineering toolkit (SET) which comes pre-installed in kali linux.

5. Keylogger or Malware Based:

Attacker can inject malware into the target system by the means of email or any methods or installs the keylogger which tracks every activity of the target and anonymous sends the data record attacker when target system goes online

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

1. Fake Search Engine
2. client Side Attack
3. DNS Redirection Attack.

*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.

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 kind 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 shownup 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:

1. Run kali linux and search social engineering toolkit.
2. Open social engineering toolkit and agree the licence aggreement
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 (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.

* 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 employee. 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. Dont open attachment emails coming from unknown source.
5. Try to keep your identity as much private as possible
6. Dont visit links which are detected by browser as harmful
7. Be aware of popups and ads.
8. Think twice before reacting.