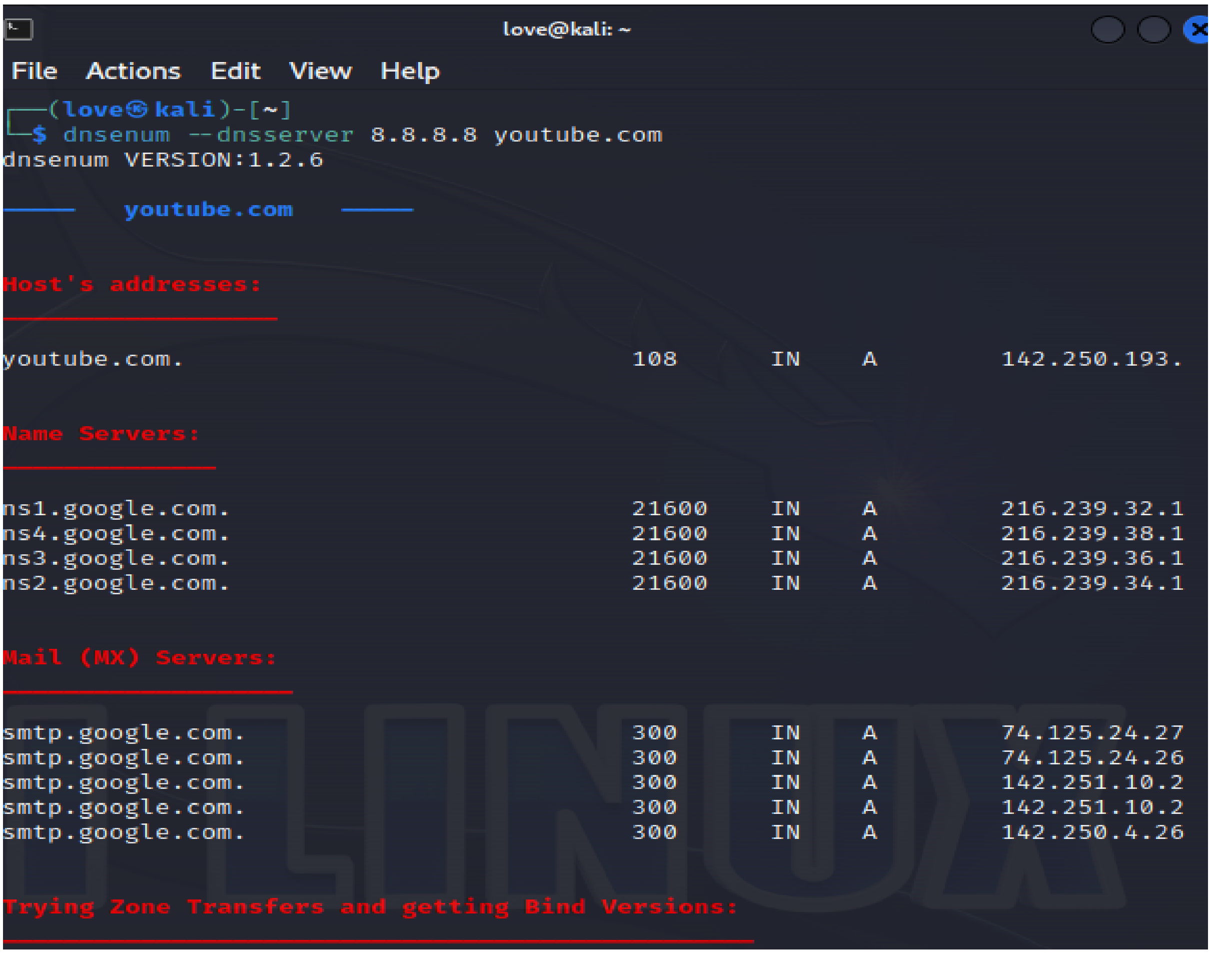
Assignment #2

Kali-linux tools

01) Information Gathering - DNS Analysis - DNSENUM

DNS enumeration, often performed using tools like `dnsenum`, is an important step in the information gathering phase of ethical hacking, penetration testing, or cybersecurity assessments. It involves querying DNS (Domain Name System) servers to gather valuable information about a target domain or network. The goal is to discover as much information as possible about the target's DNS infrastructure, which can help in identifying potential vulnerabilities and attack vectors



```
┌──(love㉿kali)-[~]
└─$ dnsenum --dnsserver 8.8.8.8 youtube.com
dnsenum VERSION:1.2.6

─────   youtube.com   ─────


Host's addresses:
__________________

youtube.com.                              108      IN    A        142.250.193.


Name Servers:
______________

ns1.google.com.                           21600    IN    A        216.239.32.1
ns4.google.com.                           21600    IN    A        216.239.38.1
ns3.google.com.                           21600    IN    A        216.239.36.1
ns2.google.com.                           21600    IN    A        216.239.34.1


Mail (MX) Servers:
___________________

smtp.google.com.                          300      IN    A        74.125.24.27
smtp.google.com.                          300      IN    A        74.125.24.26
smtp.google.com.                          300      IN    A        142.251.10.2
smtp.google.com.                          300      IN    A        142.251.10.2
smtp.google.com.                          300      IN    A        142.250.4.26


Trying Zone Transfers and getting Bind Versions:
_________________________________________________
```

02) Vulnerability analysis

Vulnerability analysis is the process of identifying and assessing security vulnerabilities in a system, network, application or any other digital asset. The main objective of vulnerability analysis is to identify weaknesses that could be exploited by attackers to gain unauthorized access, steal data, or cause damage to the system.

Discovery: This step involves identifying the assets that need to be analyzed, including the hardware, software, and data,

Scanning: This step involves using automated tools to scan the assets for known vulnerabilities, such as outdated software, open ports, weak passwords, and unsecured configurations.

Analysis: This step involves manually reviewing the results of the scanning process and identifying any potential vulnerabilities that were not detected by the automated tools.

Prioritizatiorg This step involves ranking the identified vulnerabilities based on their severity and the potential impact on the system.

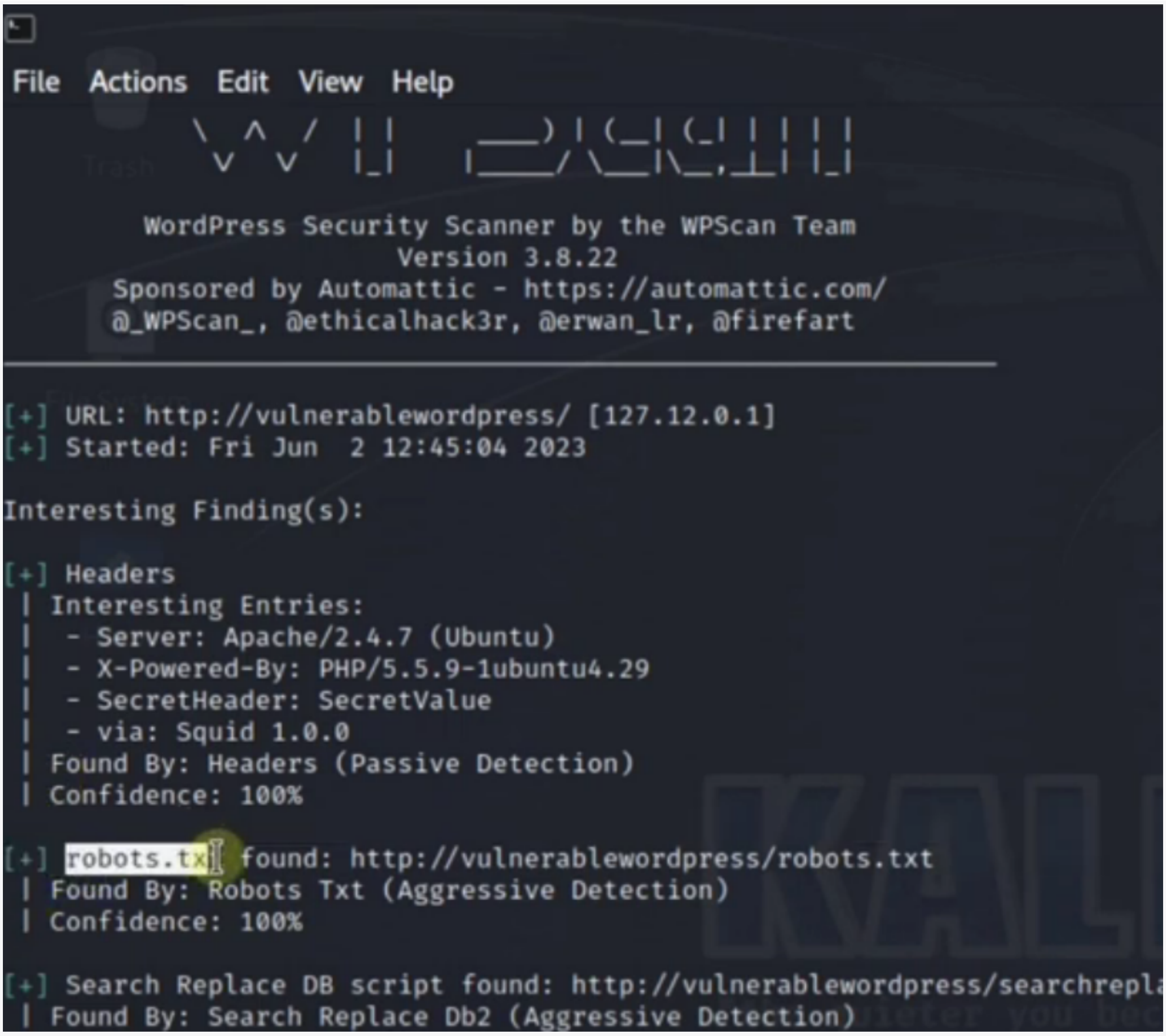
Remediation: This step involves addressing the identified vulnerabilities by applying patches, updating software, reconfiguring systems, or implementing additional security measures.

Validation: This step involves verifying that the vulnerabilities have been effectively addressed and that the system is now more secure.

‘Vulnerability analysis is an important component of an overall security strategy, as it helps organizations to proactively identify and address security weaknesses before they can be exploited by attackers

03) Web Application Analysis-CMS and Framework identification -wpscan vulnerability scanner

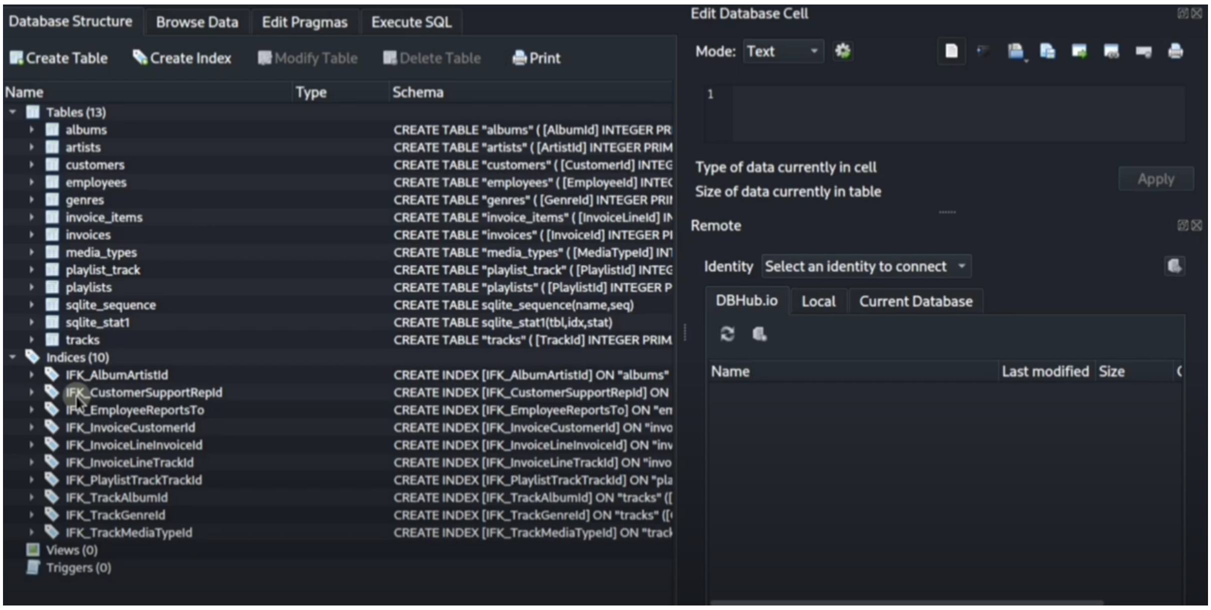
Web application analysis involves identifying the content management system (CMS) and framework used for a website. One tool that can help with this task is WPScan, which is primarily designed for WordPress CMS but can also provide some information about other CMSs and frameworks. Here's a step-by-step guide on how to use WPScan for CMS and framework identification and vulnerability scanning



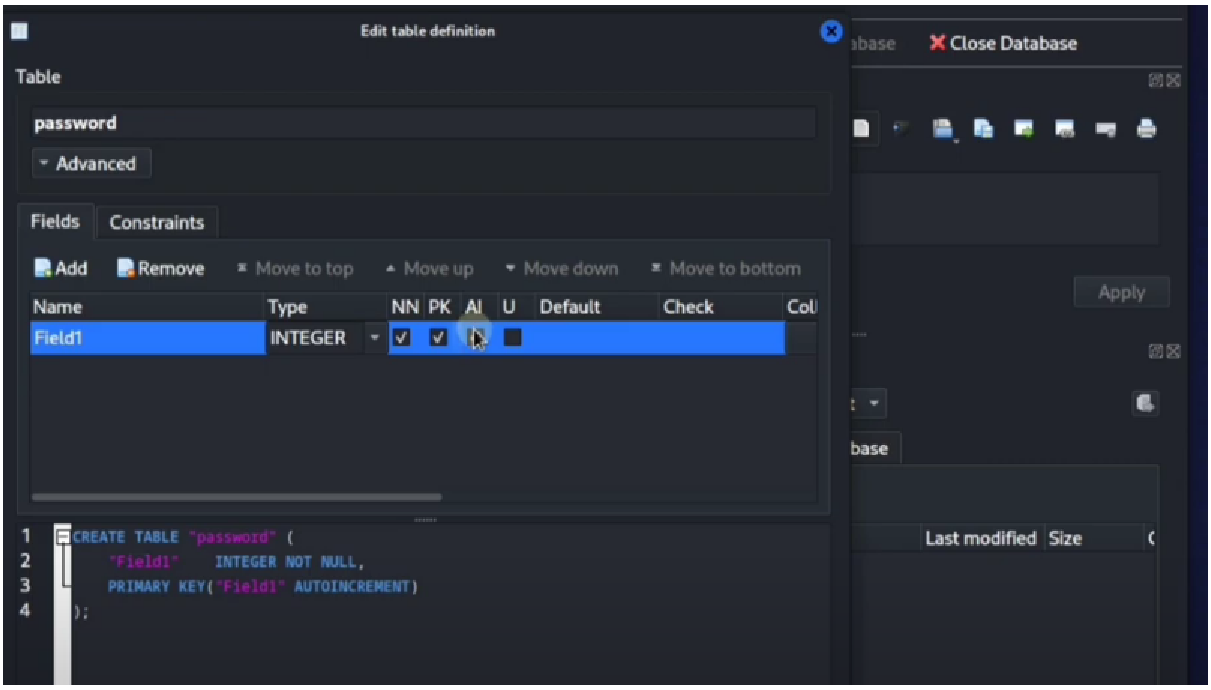
```
         \ /\ /  | |    ___) | (__| (_| | | | |
          V  V   |_|   |____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.22
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://vulnerablewordpress/ [127.12.0.1]
[+] Started: Fri Jun  2 12:45:04 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.7 (Ubuntu)
 |  - X-Powered-By: PHP/5.5.9-1ubuntu4.29
 |  - SecretHeader: SecretValue
 |  - via: Squid 1.0.0
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://vulnerablewordpress/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] Search Replace DB script found: http://vulnerablewordpress/searchrepla
 | Found By: Search Replace Db2 (Aggressive Detection)
```

04) Database assessment-SQLite DB Browser

SQLite Database Browser is a graphical tool that allows you to assess and manage SQLite databases. Here's a step-by-step guide on how to perform a database assessment using SQLite Database Browser:



Name	Type	Schema
Tables (13)		
albums		CREATE TABLE "albums" ([AlbumId] INTEGER PR
artists		CREATE TABLE "artists" ([ArtistId] INTEGER PRIM
customers		CREATE TABLE "customers" ([CustomerId] INTEG
employees		CREATE TABLE "employees" ([EmployeeId] INTEC
genres		CREATE TABLE "genres" ([GenreId] INTEGER PRII
invoice_items		CREATE TABLE "invoice_items" ([InvoiceLineId] IN
invoices		CREATE TABLE "invoices" ([InvoiceId] INTEGER PI
media_types		CREATE TABLE "media_types" ([MediaTypeId] INT
playlist_track		CREATE TABLE "playlist_track" ([PlaylistId] INTEG
playlists		CREATE TABLE "playlists" ([PlaylistId] INTEGER P
sqlite_sequence		CREATE TABLE sqlite_sequence(name,seq)
sqlite_stat1		CREATE TABLE sqlite_stat1(tbl,idx,stat)
tracks		CREATE TABLE "tracks" ([TrackId] INTEGER PRIM
Indices (10)		
IFK_AlbumArtistId		CREATE INDEX [IFK_AlbumArtistId] ON "albums"
IFK_CustomerSupportRepId		CREATE INDEX [IFK_CustomerSupportRepId] ON
IFK_EmployeeReportsTo		CREATE INDEX [IFK_EmployeeReportsTo] ON "em
IFK_InvoiceCustomerId		CREATE INDEX [IFK_InvoiceCustomerId] ON "invo
IFK_InvoiceLineInvoiceId		CREATE INDEX [IFK_InvoiceLineInvoiceId] ON "inv
IFK_InvoiceLineTrackId		CREATE INDEX [IFK_InvoiceLineTrackId] ON "invo
IFK_PlaylistTrackTrackId		CREATE INDEX [IFK_PlaylistTrackTrackId] ON "pla
IFK_TrackAlbumId		CREATE INDEX [IFK_TrackAlbumId] ON "tracks" ([
IFK_TrackGenreId		CREATE INDEX [IFK_TrackGenreId] ON "tracks" ([
IFK_TrackMediaTypeId		CREATE INDEX [IFK_TrackMediaTypeId] ON "track
Views (0)		
Triggers (0)		



Table

password

Name	Type	NN	PK	AI	U	Default	Check	Col
Field1	INTEGER	☑	☑	☑	□			

```
CREATE TABLE "password" (
    "Field1"    INTEGER NOT NULL,
    PRIMARY KEY("Field1" AUTOINCREMENT)
);
```

05) Password Attacks-Offline Password Attack-Chntpw

Chntpw is a utility for resetting or removing Windows passwords on local user accounts. It is especially useful when you have physical access to a Windows machine and need to recover or reset a forgotten password. Here's how it works:

1. Download and Prepare Chntpw:

- You can download Chntpw from its official website or from various Linux distributions' repositories, as it's commonly included in many Linux distributions.
- After downloading, you may need to compile it or install it based on your specific distribution.

2. Create a Bootable USB or CD:

- Chntpw is often used as part of a bootable CD or USB drive, like a live Linux distribution. You'll need to create a bootable medium containing Chntpw.

3. Boot from the Bootable Medium:

- Insert the bootable CD or USB drive into the target Windows machine.
- Boot the Windows machine from the bootable medium (you may need to change the boot order in BIOS/UEFI settings).

4. Use Chntpw:

- Once booted into the live environment with Chntpw, you can access the Windows registry and reset or remove Windows passwords for local user accounts.
- Run the `chntpw` command followed by the path to the Windows registry hive file where user credentials are stored. Typically, this is located in the `C:\Windows\System32\config` directory and named "SAM."
- Chntpw will display a list of user accounts. You can choose a specific user account to reset or remove the password.

5. Reset or Remove Passwords:

- Chntpw provides options to reset the password, clear the password (blank), or promote a standard user account to an administrator account.
- Follow the on-screen instructions to make the desired changes to the user account.

6. Save Changes and Exit:

- After making the changes, save the modifications to the Windows registry.
- Reboot the Windows system without the bootable medium, and the password changes should take effect.

It's important to note that Chntpw is meant for legal and legitimate purposes, such as recovering lost passwords on systems where you have authorization. Unauthorized use of this tool to gain access to systems or accounts that you do not own or have permission to access is illegal and unethical.

Always use password recovery and reset tools responsibly and only on systems or accounts where you have explicit authorization. Unauthorized use can lead to legal consequences.

07) Reverse engineering

Reverse engineering is the process of deconstructing and analyzing an existing product, system, or software in order to understand how it works, how it was built, and what its components and functions are. The goal of reverse engineering is often to gain insights into the design and functionality of a system, identify vulnerabilities, create compatible or interoperable alternatives, or modify the system for specific purposes. This process can be applied to a wide range of fields, including software, hardware, and mechanical systems.

apktool	It is a tool for reengineering Android apk files that can decode resources to the nearly original form and rebuild them after the modification.

dex2jar	It converts jar to dex by invoking dx.
diStorm3	It is a lightweight, easy to use and fast decomposer library.
edb-debugger	It is a modular and cross platform debugger.
jad	It is a java de-compiler.
javasnoop	It attaches itself to an existing process and instantly begin tampering with method calls, run custom code, or just analyse the processing of the system.
JD-GUI	It is a graphical utility that displays java source codes of ".class" files.
OllyDbg	It is a 32-bit assembler level analysing debugger for Microsoft Windows.
smali	It is an assembler /disassembler for the dex file used by dalvik.
Valgrind	It is a tool for debugging and profiling Linux programs.
YARA	Using YARA, you can create a description of malware based on textual or binary patterns.

08) exploitation tools

Kali Linux is a popular distribution for penetration testing and ethical hacking, and it includes a wide range of exploitation tools that security professionals and researchers can use to test the security of systems, networks, and applications. These tools are intended for legal and ethical use with the proper authorization. Here are some of the exploitation tools available in Kali Linux:

Metasploit Framework: Metasploit is a powerful penetration testing tool that provides a wide range of exploits, payloads, and auxiliary modules for testing and exploiting vulnerabilities in systems, including web applications and network services.
Exploit Database (Exploit-DB): Kali Linux includes the Exploit-DB tool, which provides a vast collection of exploits and security vulnerability information for various applications and platforms.
Armitage: Armitage is a graphical user interface (GUI) for Metasploit. It simplifies the process of selecting and launching exploits, making it more user-friendly for penetration testers.
BeEF: The Browser Exploitation Framework (BeEF) is a tool for testing web browsers' security by exploiting client-side vulnerabilities. It focuses on browser-based attacks.
SQLMap: SQLMap is a tool for detecting and exploiting SQL injection vulnerabilities in web applications. It automates the process of identifying and exploiting database vulnerabilities.

09)sniffing and spoofing

Sniffing and spoofing are two common techniques used in network security and computer networking, but they can also be used for malicious purposes if not employed ethically and legally. Here's an overview of each:

1. Sniffing:

- Definition: Sniffing refers to the practice of intercepting and capturing data packets as they traverse a network. This can include capturing data transmitted over Wi-Fi, Ethernet, or other network protocols.
- Purpose: Network administrators and security professionals often use sniffing for legitimate purposes, such as monitoring network traffic for troubleshooting, security analysis, or network optimization.
- Tools: Wireshark is a popular network protocol analyzer tool that allows you to capture and inspect data packets in real-time. Tcpdump is another command-line tool commonly used for packet sniffing.
- Legitimate Use: Network administrators use sniffing to diagnose network issues, monitor bandwidth usage, and detect malicious activities. Ethical hackers also use sniffing to identify vulnerabilities and security weaknesses in a network.

2. Spoofing:

- Definition: Spoofing involves falsifying information in network packets or headers to impersonate a legitimate entity or device on a network. This can include IP spoofing, ARP spoofing, DNS spoofing, and more.
- Purpose: Legitimate uses of spoofing include network testing, security assessments, and some forms of load balancing. However, it is also commonly used in cyberattacks.
- Tools: There are various tools and techniques for different types of spoofing. For example, tools like ARPspoof and Ettercap can be used for ARP spoofing attacks.
- Legitimate Use: Network administrators may use spoofing for legitimate purposes like load balancing or testing network configurations. In penetration testing, ethical hackers may use spoofing to assess network security and discover vulnerabilities.

It's important to note that while these techniques have legitimate uses in network administration, security testing, and troubleshooting, they can also be maliciously employed. Unauthorized and malicious sniffing or spoofing can lead to various security risks, including data theft, man-in-the-middle attacks, and unauthorized access to network resources.

10) **post exploitation**

Post-exploitation is a phase in the cybersecurity field that occurs after an attacker has successfully compromised a system or network. During this phase, the attacker or penetration tester (in the case of ethical hacking) works on maintaining access to the compromised system, escalating privileges, exfiltrating data, and achieving their ultimate objectives. For ethical hackers, the goal is to identify vulnerabilities and weaknesses in a system's post-exploitation defenses.

Here are some common activities and considerations during the post-exploitation phase:

Maintaining Access: Once an attacker has gained access to a system, they often want to maintain that access for as long as possible. This may involve creating backdoors, establishing persistent connections, or exploiting vulnerabilities that allow for re-entry even if the initial entry point is patched or closed.

Privilege Escalation: Attackers typically seek to escalate their privileges within a compromised system or network. This means acquiring higher-level access rights or administrative privileges to gain more control over the system.

Data Exfiltration: One of the primary goals in post-exploitation is exfiltrating sensitive data. Attackers look for valuable information such as user credentials, financial data, intellectual property, or other proprietary information.

Lateral Movement: In larger networks, attackers may move laterally to compromise other systems or escalate privileges further. They may use stolen credentials, exploit vulnerabilities, or use other techniques to pivot within the network.

Covering Tracks: Attackers often attempt to cover their tracks by deleting logs, modifying system timestamps, and removing any evidence of their presence. This makes it harder for security analysts to detect their activities.