

MUFFAKHAM JAH COLLEGE OF ENGINEERING AND TECHNOLOGY

(Affiliated to OU)

Hyderabad – 500034



A MINI-PROJECT REPORT

ON

“Detection and Response”

Submitted by

Syed Khaja Ikramuddin

1604-18-733-017

Syed Ibrahim Shakir

1604-18-733-019

Mohd Safiuddin

1604-18-733-036

**Department of Computer Science & Engineering
Muffakham Jah College of Engineering and Technology**

2020-2021

CERTIFICATE

Certified that the mini-project work entitled “**Detection and Response**” is a bona fide work carried out by

Syed Khaja Ikramuddin

1604-18-733-017

Syed Ibrahim Shakir

1604-18-733-019

Mohd Safiuddin

1604-18-733-036

The report has been approved as it satisfies the academic requirements in respect of mini-project work prescribed for the course.

.....
Dr. Krishna Keerthi Chennam
Mini Project Coordinator CSE-A

ABSTRACT:

We are performing three different kind of cyber attacks.

A **denial of service** (DoS) event is a cyber attack in which hackers or cybercriminals seek to make a host machine, online service or network resource unavailable to its intended users. It is an attack where a computer is used to flood a server with TCP and UDP packets. We are using Low orbit ion cannon(LOIC) tool to perform DoS attack on a private aurl/server.

A **dictionary attack** is a systematic method of guessing a password by trying many common words and their simple variations. We preforming dictionary attack on wifi using aircrack-ng. Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs.

A **malware attack** executes unauthorized actions on the victim's system. The malicious software encompasses many specific types of attacks such as ransomware, spyware, command and control. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. We are using this tool to spyware on a android device or other OS if possible

.

TABLE OF CONTENTS:

1.INTRODUCTION	1
1.1. Objective	1
1.1.1 DoS attack	1
1.1.2 Dictionary attack	1
1.1.3 Malware attack	1
1.2. SYSTEM REQUIREMENTS	3
1.2.1. Kali Linux OS	3
1.2.2 Wireless Adapter Capable of Packet Injection	3
1.2.3 LOIC Tool	3
1.2.4 LAN	3
2. IMPLEMENTATION	4
2.1 Dictionary Attack	4
2.2 Malware Attack	6
2.3 DoS Attack	7
3.RESULT	8
3.1 Dictionary Attack	8
3.2 Malware Attack	9
4. CONCLUSION	10
5. REFERENCES	11

LIST OF FIGURES:

Figure 1.2.1 Kali linux logo	6
Figure 2.1.1 Monitor Mode	9
Figure 2.1.2. BSSID	9
Figure 2.1.3 De authenticating	10
Figure 2.1.4 Handshake Captured	10
Figure 2.2.1 Payload	11
Figure 2.2.2 Metasploit Console	11
Figure 2.3 LOIC Tool	12
Figure 3.1 Key Found	12
Figure 3.2.1 Apps list	13
Figure 3.2.2 Snapshot	13
Figure 4.1 Types of Hackers	14

1.INTRODUCTION:

1.1Objective:

Ethical hacking can prevent cyber-terrorism and terrorist attacks, ensuring the safety of the nation. Hackers can identify potential entry points from an attackers' perspective, allowing you the chance to fix them before an attack. Despite the rapidly evolving nature of cybercriminal activities, *ethical hackers* have a number of tools available at their disposal to create a solid line of defense.

1.1.1DoS attack

DOS is an *attack* used to deny legitimate users access to a resource such as accessing a website, network, emails, etc. or making it extremely slow. ... This type of *attack* is usually implemented by hitting the target resource such as a web server with too many requests at the same time.

The goal of this attacks is to exhaust the target's resources to create a denial-of-service.

1.1.2Dictionary attack

A *dictionary attack* is a method that consists of breaking into a password-protected computer or server (in this case a *Wi-Fi* network) by systematically entering every word in a *dictionary* as a password. *Dictionary attack* is a form of brute force attack technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying thousands or millions of likely possibilities, such as words in a *dictionary*.

Dictionary attacks often succeed because many people have a tendency to choose short passwords that are ordinary words or common passwords; or variants obtained, for example, by appending a digit or punctuation character.

1.1.3Malware Attack

The *purpose of malware* is to intrude on a machine for a variety of reasons. *Malware* or malicious software is certainly *dangerous*, and in some cases, it can be incredibly *dangerous*, and threaten to compromise your online banking, or lock away all your data so you can't reach it forever. It always pays to think before you click on any link or download any file, and to use a good antivirus app.

Ethical Hacking is an authorized practice of bypassing system security to identify potential data breaches and threats in a network. The company that owns the system or network allows Cyber Security engineers to perform such activities in order to test the system's defenses. Thus, unlike malicious hacking, this process is planned, approved, and more importantly, legal

Ethical hackers aim to investigate the system or network for weak points that malicious *hackers* can exploit or destroy. They collect and analyze the information to figure out ways to strengthen the security of the system/network/applications.

1.2System Requirements

System requirements listed for a hardware device may include:

1.2.1Kali Linux OS Kali Linux is mainly used for advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. All tools like msfvenom and aircrack-ng are already installed in this operating system



Fig 1.2.1

1.2.2Wireless Adapter Capable of Packet Injection

Atheros AR9271: The Alfa AWUS036NHA is long-range network adapter and the standard other long-range adapters these chipsets are known to support monitor mode and packet injection and there are many other adapters which are capable but this one is recommended.

1.2.3LOIC TOOL

Low Orbit Ion Cannon(LOIC) designed by Praetex Technologies (open source) is required.LOIC is an [open-source](#) network [stress testing](#) and [denial-of-service attack](#) application, written in [C#](#).

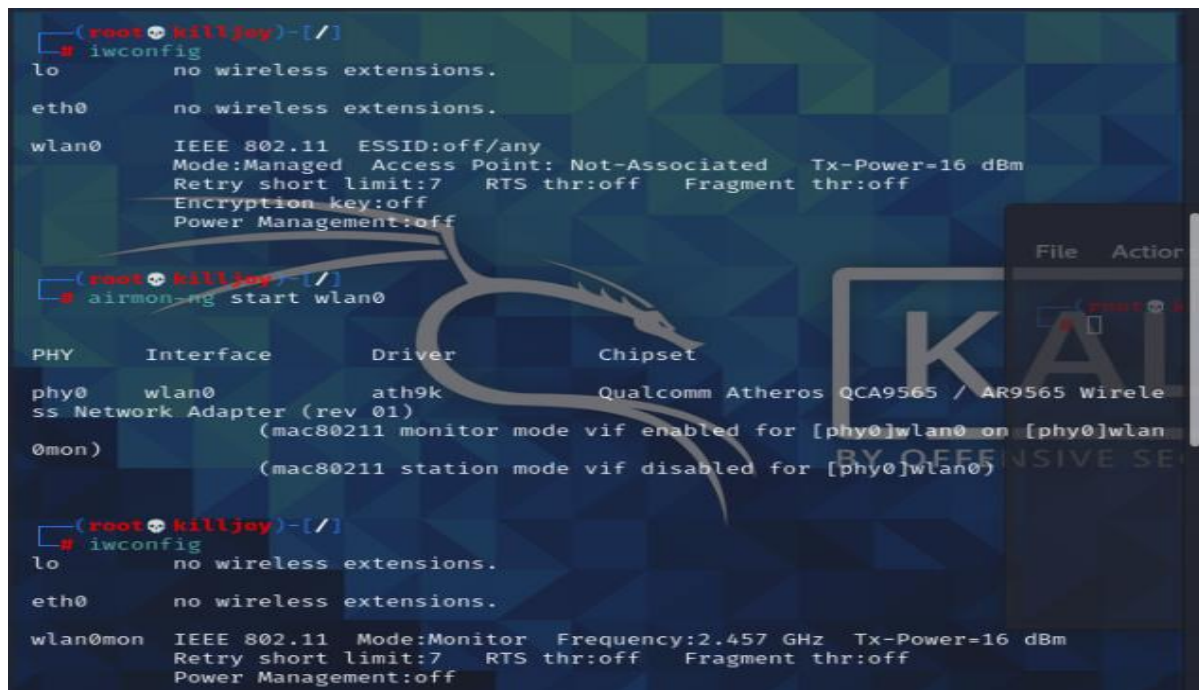
1.2.4.LAN

Small Local Area Network(LAN) has to be established before starting the attacks. At least 2 devices are required to connect to this Network for successful attack.

2.IMPLEMENTATION:

2.1.Dictionary attack

Step1: Start the wireless interface in monitor mode



```
(root@killjoy)-[/]
# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated  Tx-Power=16 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

(root@killjoy)-[/]
# airmon-ng start wlan0

PHY      Interface  Driver      Chipset
-----
phy0     wlan0         ath9k       Qualcomm Atheros QCA9565 / AR9565 Wireless Network Adapter (rev 01)
0mon)    (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

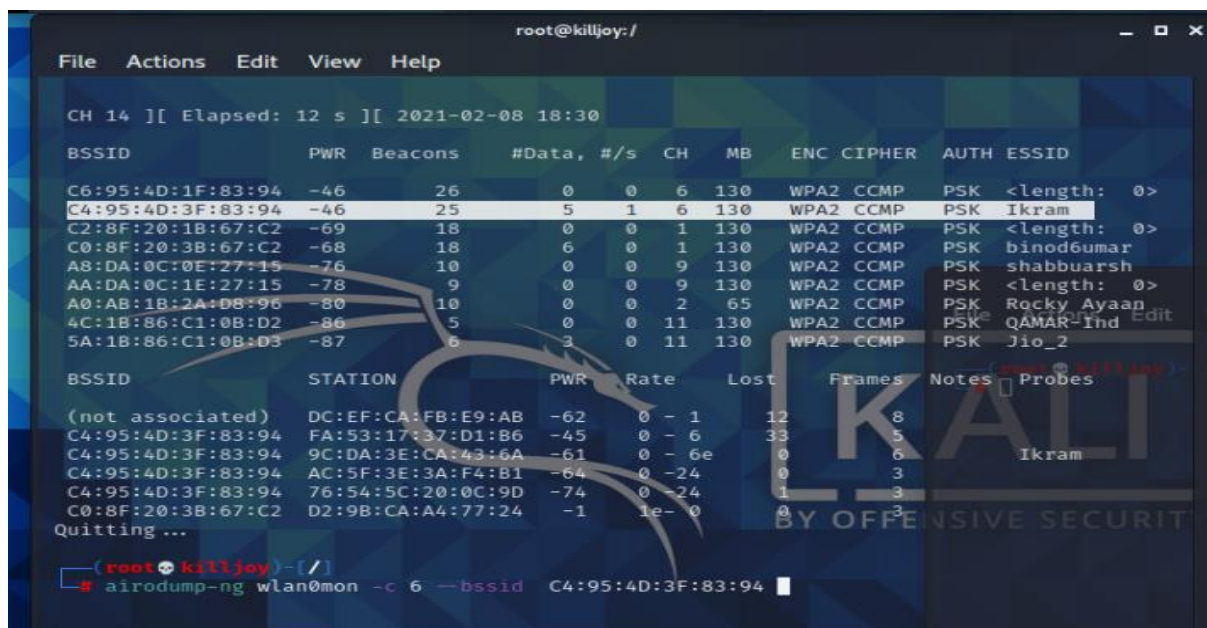
(root@killjoy)-[/]
# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=16 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Fig 2.1.1

Step2: Select the target victim and copy the BSSID



```
root@killjoy:/
File Actions Edit View Help

CH 14 ][ Elapsed: 12 s ][ 2021-02-08 18:30

BSSID          PWR Beacons #Data, #/s CH  MB  ENC CIPHER AUTH ESSID
C6:95:4D:1F:83:94 -46    26      0  0  6  130 WPA2 CCMP PSK <length: 0>
C4:95:4D:3F:83:94 -46    25      5  1  6  130 WPA2 CCMP PSK Ikram
C2:8F:20:18:67:C2 -69    18      0  0  1  130 WPA2 CCMP PSK <length: 0>
C0:8F:20:3B:67:C2 -68    18      6  0  1  130 WPA2 CCMP PSK binod6umar
A8:DA:0C:0E:27:15 -76    10      0  0  9  130 WPA2 CCMP PSK shabbuarsh
AA:DA:0C:1E:27:15 -78     9      0  0  9  130 WPA2 CCMP PSK <length: 0>
A0:AB:1B:2A:08:96 -80    10      0  0  2  65  WPA2 CCMP PSK Rocky Ayaan
4C:1B:86:C1:0B:D2 -86     5      0  0  11 130 WPA2 CCMP PSK QAMAR-Ind
5A:1B:86:C1:0B:D3 -87     6      3  0  11 130 WPA2 CCMP PSK Jio_2

BSSID          STATION  PWR  Rate  Lost  Frames  Notes  Probes
(not associated) DC:EF:CA:FB:E9:AB -62  0 - 1  12  8
C4:95:4D:3F:83:94 FA:53:17:37:D1:B6 -45  0 - 6  33  5
C4:95:4D:3F:83:94 9C:DA:3E:CA:43:6A -61  0 - 6e 0  6
C4:95:4D:3F:83:94 AC:5F:3E:3A:F4:B1 -64  0 - 24 0  3
C4:95:4D:3F:83:94 76:54:5C:20:0C:9D -74  0 - 24 1  3
C0:8F:20:3B:67:C2 D2:9B:CA:A4:77:24 -1  1e-0 0  3

Quitting ...

(root@killjoy)-[/]
# airodump-ng wlan0mon -c 6 -bssid C4:95:4D:3F:83:94
```

Fig.2.1.2

Step3: Start airodump-ng to collect authentication handshake

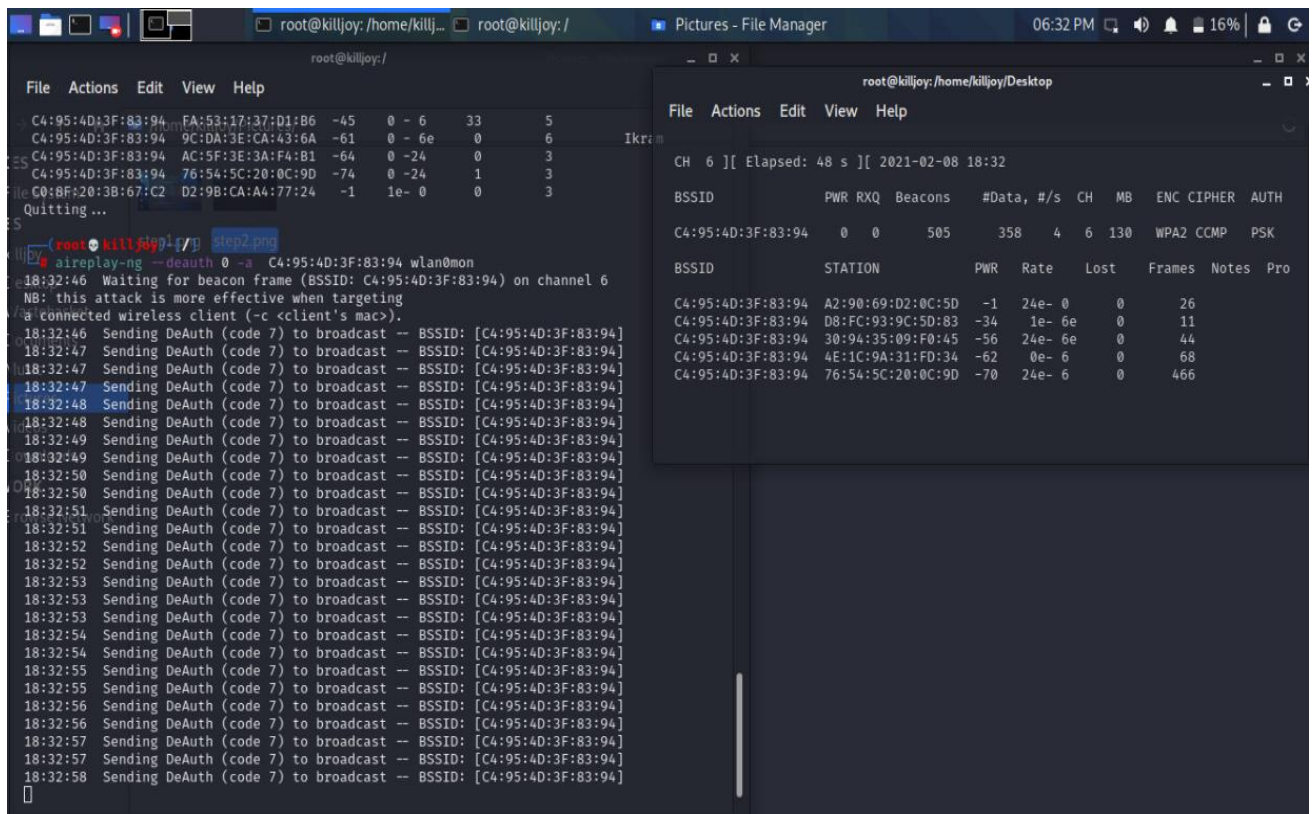


Fig 2.1.3

Step4: Use aireplay-ng to deauthenticate the wireless client

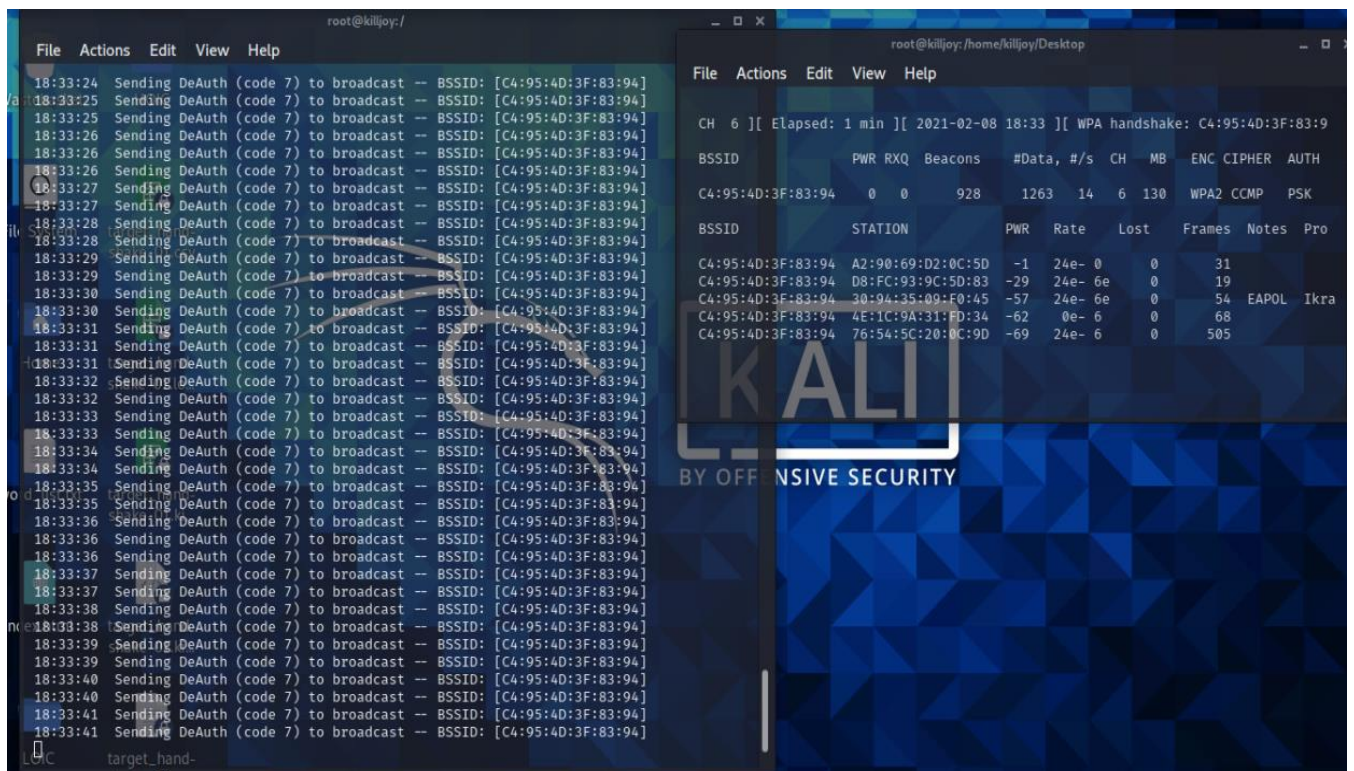


Fig 2.1.4

2.2 Malware Attack

Step1: Create a payload

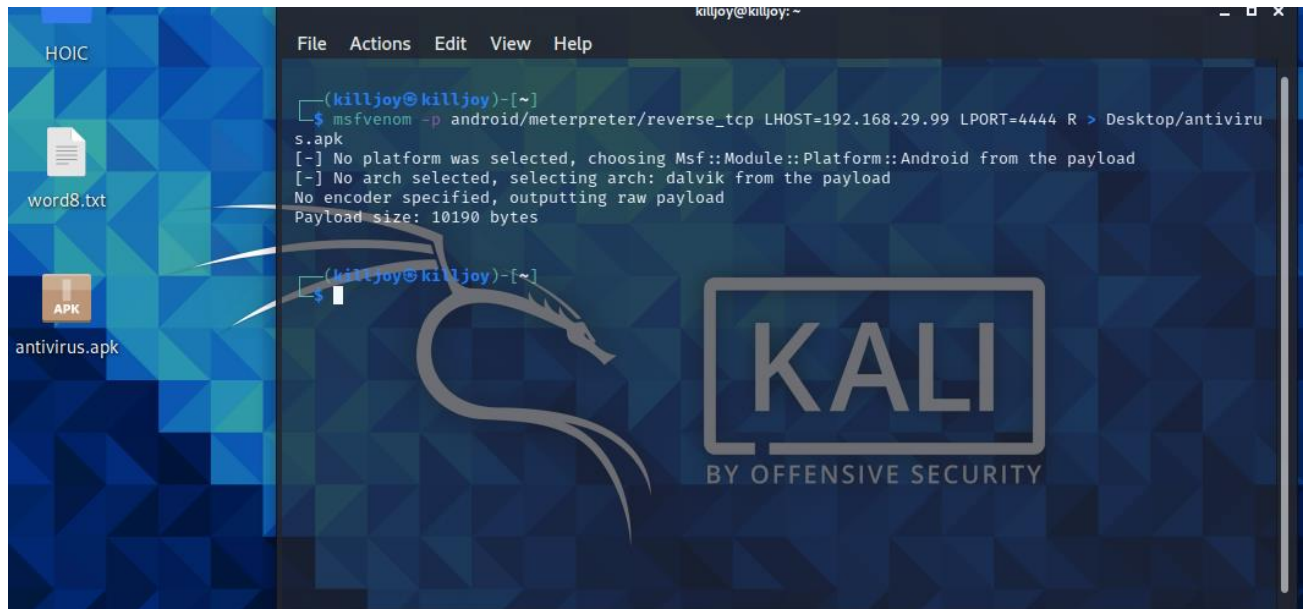


Fig 2.2.1

Step2: After installing the payload to target device ,setting up exploit

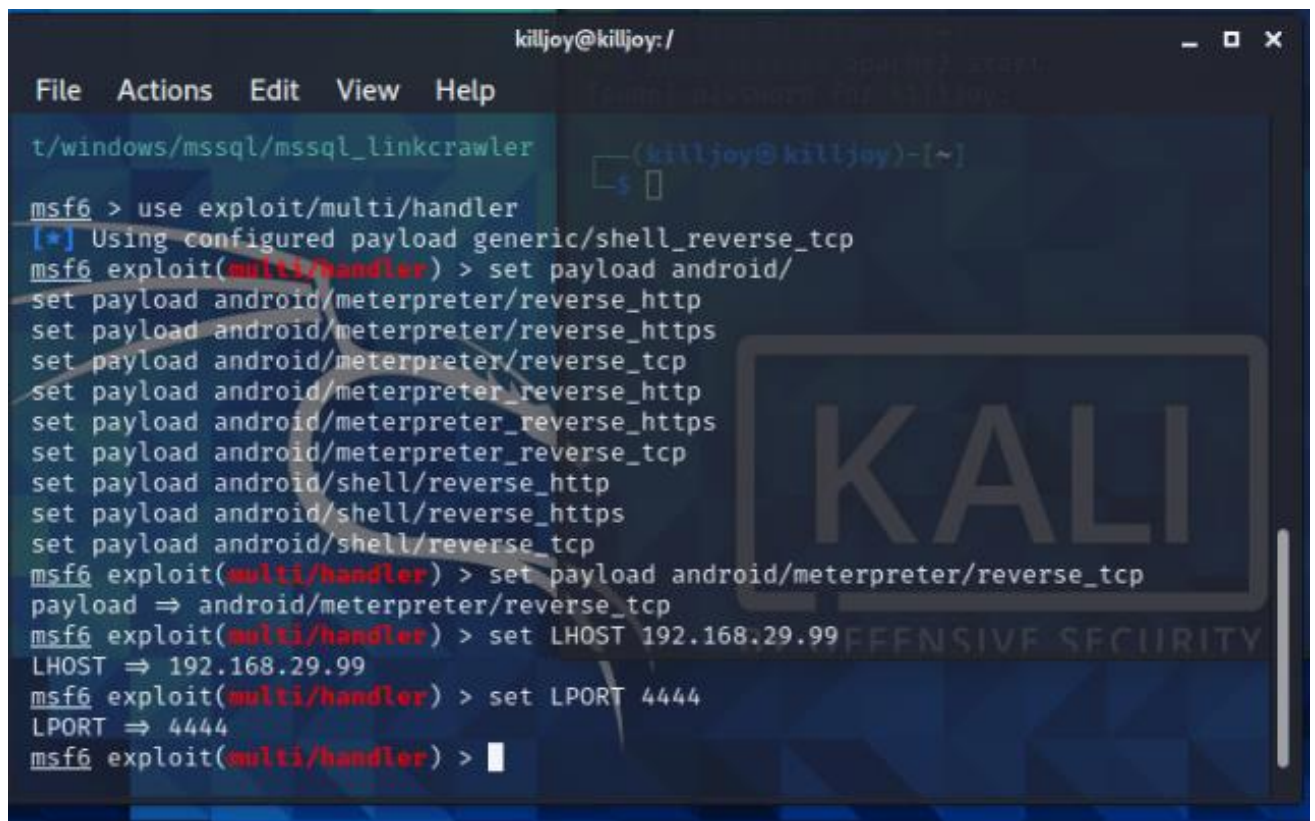


Fig 2.2.2

2.3 DoS attack

Flooding a private server (192.168.29.240) with HTTP requests . The server becomes slow then later crashes .

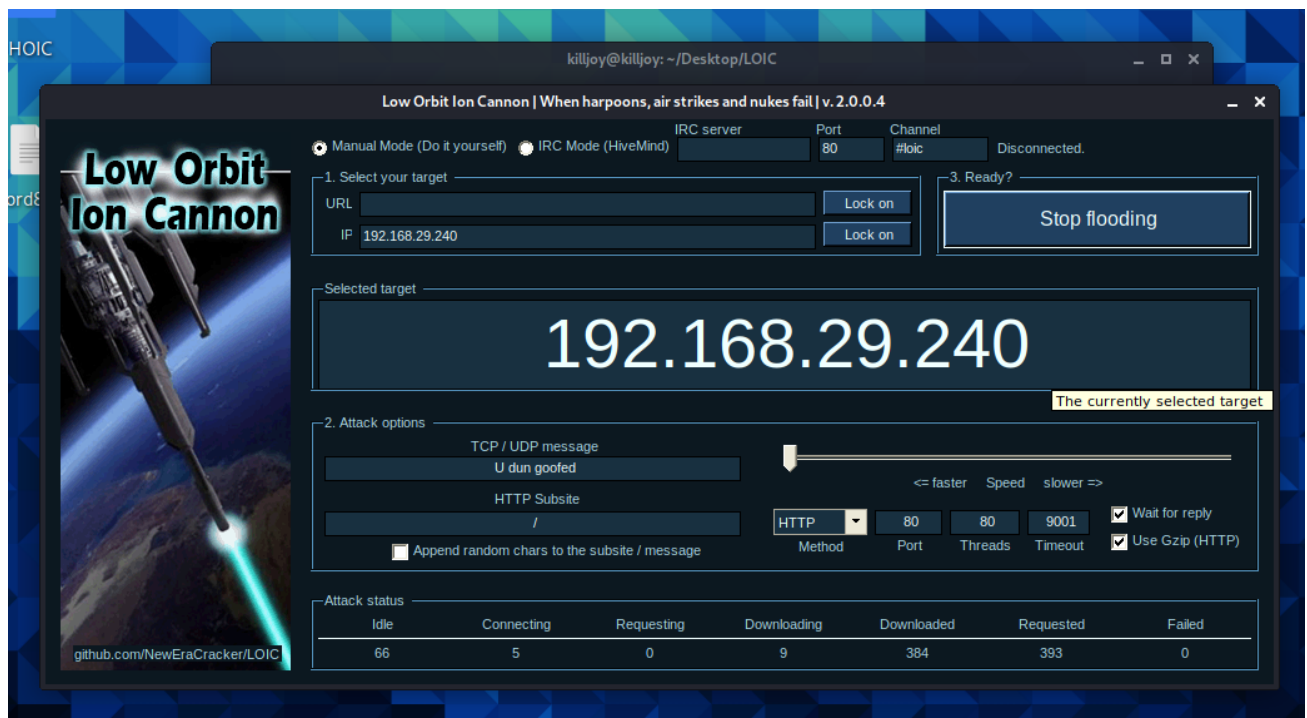


Fig 2.3

3.RESULT:

3.1 Dictionary attack: Run aircrack-ng to crack the pre-shared key.

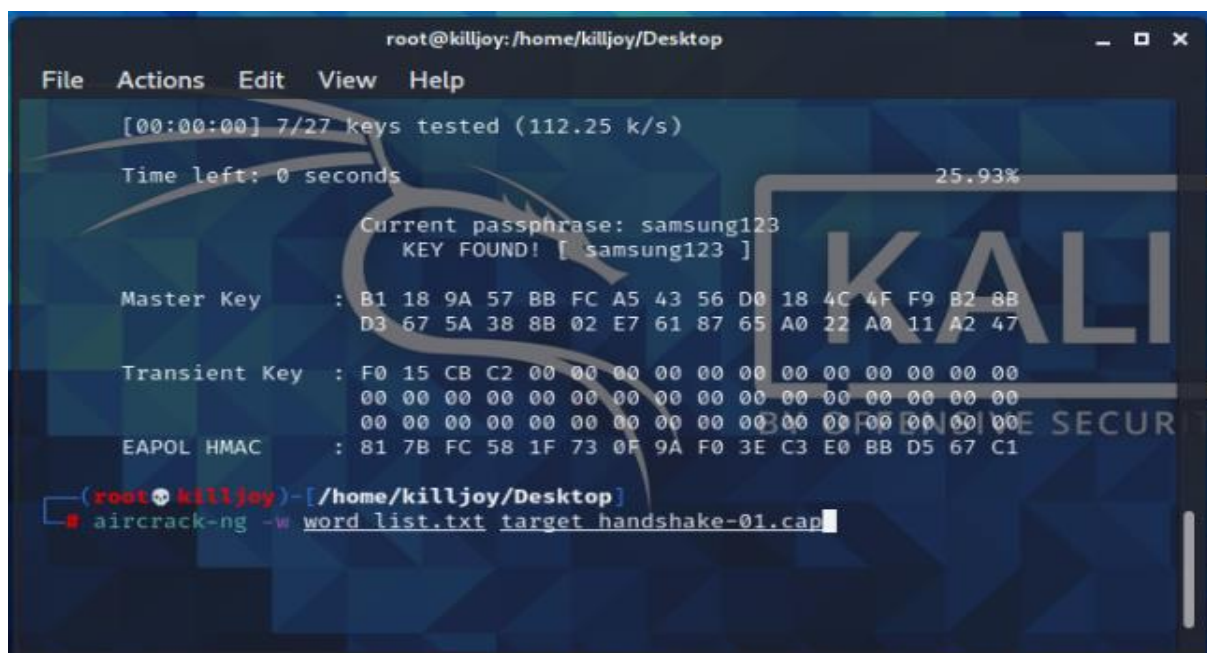


Fig 3.1

3.2 Malware Attack

Exploiting the victim device

Listing installed apps in target device

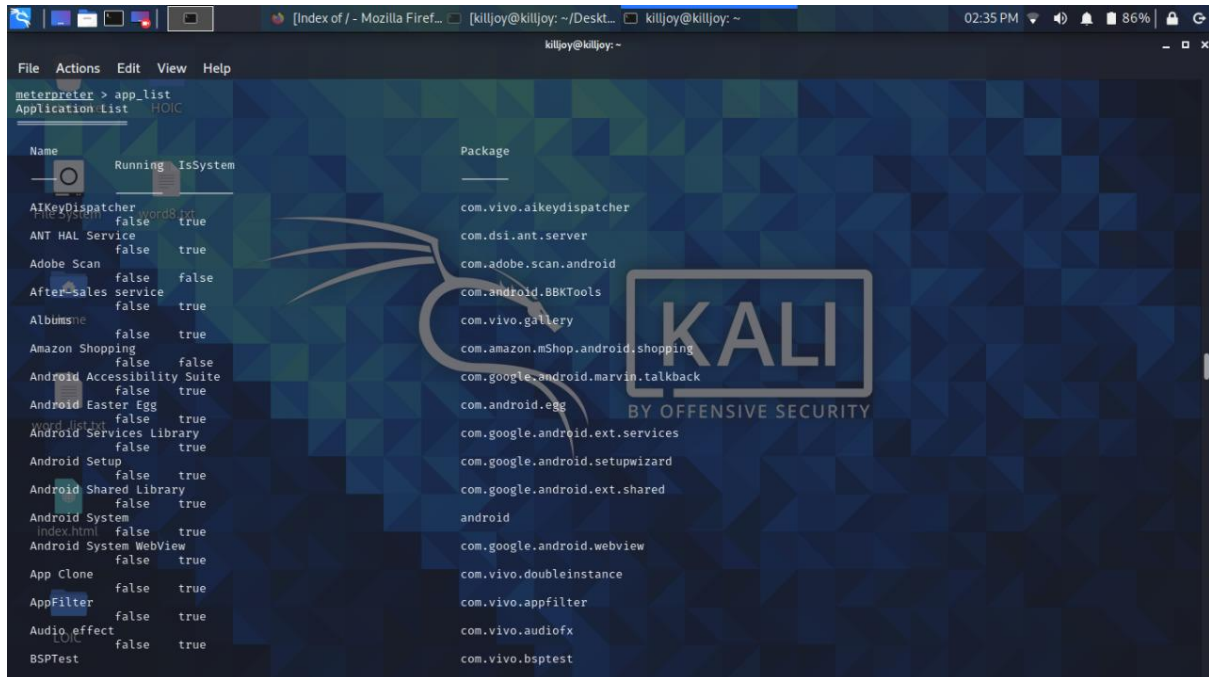


Fig 3.2.1

Taking a web-snap from target device

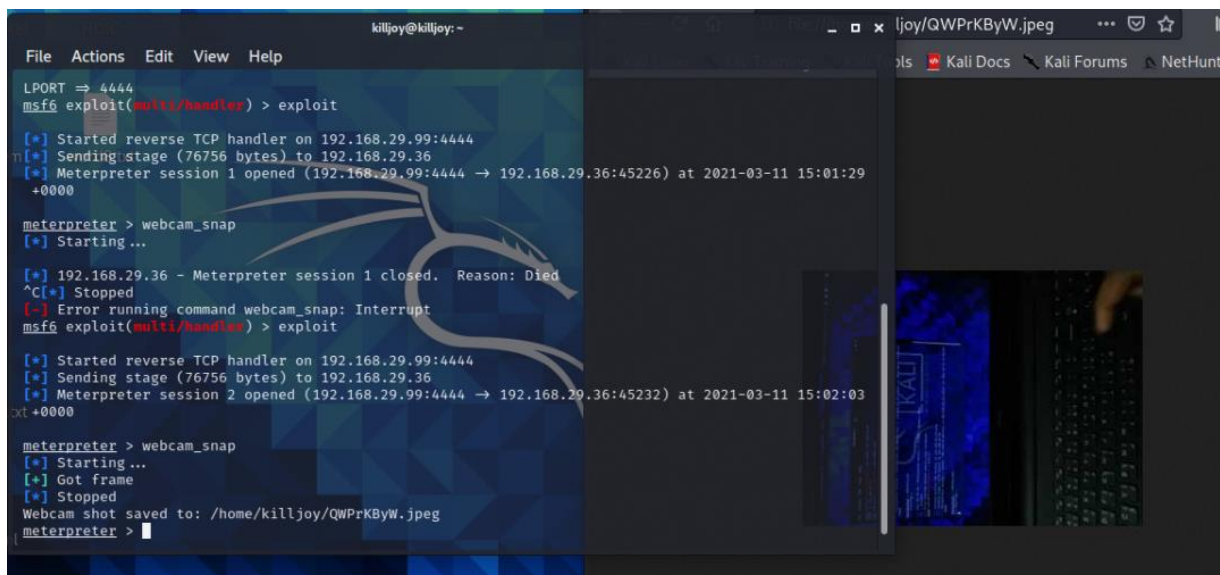


Fig 3.2.2

4.CONCLUSION:

The primary threat to any organization's security is a hacker: learning, understanding, and implementing how hackers operate can help network defenders prioritize potential risks and learn how to remediate them best

Ethical hackers are hired by organizations to look into the vulnerabilities of their systems and networks and develop solutions to prevent data breaches. Consider it a high-tech permutation of the old saying “It takes a thief to catch a thief.”

Ethical hackers are hired by organizations to look into the vulnerabilities of their systems and networks and develop solutions to prevent data breaches. Consider it a high-tech permutation of the old saying “It takes a thief to catch a thief.”

They check for key vulnerabilities include but are not limited to:

- Injection attacks
- Changes in security settings
- Exposure of sensitive data
- Breach in authentication protocols
- Components used in the system or network that may be used as access



Fig 4.1

5.REFERENCES:

- Axelsson S. Intrusion detection systems: a survey and taxonomy. Technical Report, Chalmers University. Aydın M, Zaim A, Ceylan K. A hybrid intrusion detection system design for computer network security. *Computers and Electrical Engineering* 2009;35 (3):517–26.
- Barber R. Hacking techniques: the tools that hackers use and how they are evolving to become more sophisticated. *Computer Fraud and Security* 2001;2001 (3):9–12.
- Beverly R. A robust classifier for passive TCP/IP fingerprinting. *Passive and Active Network Measurement* 2004:158–67.
- Bhuyan MH, Bhattacharyya DK, Kalita JK. Surveying port scans and their detection methodologies. *The Computer Journal* 2011a;54:1565–81.
- Bhuyan MH, Bhattacharyya DK, Kalita JK. Survey on incremental approaches for network anomaly detection. *International Journal of Communication Networks and Information Security* 2011b;3(3):226–39.
- Bhuyan M, Bhattacharyya D, Kalita J. NADO: network anomaly detection using outlier approach. In: *Proceedings of the 1st international conference on communication, computing and security*. New York, NY, USA: ACM; 2011c. p. 531–6.
- N. Hoque et al. / *Journal of Network and Computer Applications* 40 (2014) 307–324
- 323 Bhuyan M, Bhattacharyya D, Kalita J. Network anomaly detection: methods, systems and tools. *IEEE Communications Surveys and Tutorials Early Access* 2013;1:1–34.
- Brahmi I, Yahia SB, Poncelet P. MAD-IDS: novel intrusion detection system using mobile agents and data mining approaches. In: *Proceedings of the Pacific Asia conference on intelligence and security informatics*. Berlin, Heidelberg: Springer-Verlag; 2010. p. 73–6.
- Chandola V, Banerjee A, Kumar V. Anomaly detection: a survey. *ACM Computing Surveys* 2009;41(3):15.
- Chen W-H, Hsu S-H, Shen H-P. Application of SVM and ANN for intrusion detection. *Computer and Operation Research* 2005;32(10):2617–34.
- Chen Y, Hwang K, Ku W-S. Collaborative detection of DDoS attacks over multiple network domains. *IEEE Transactions on Parallel Distributed Systems* 2007;18 (12):1649–62.
- Chu J, Ge Z, Huber R, Ji P, Yates J, Yu Y-C. Alert-ID: analyze logs of the network element in real time for intrusion detection. In: *Research in attacks, intrusions, and defenses*. Springer; 2012. p. 294–313.
- Conti G, Abdullah K. Passive visual fingerprinting of network attack tools. In: *Proceedings of the 2004 workshop on visualization and data mining for computer security*. Washington, DC, USA: ACM; 2004. p. 45–54.
- Corona I, Giacinto G, Roli F. Adversarial attacks against intrusion detection systems: taxonomy, solutions and open issues. *Information Sciences* 2013;239:201–25.