

SABIN KHATRI 1017

ASHIM PRADHAN 10176184

ALISHA ADHIKARI 10176139

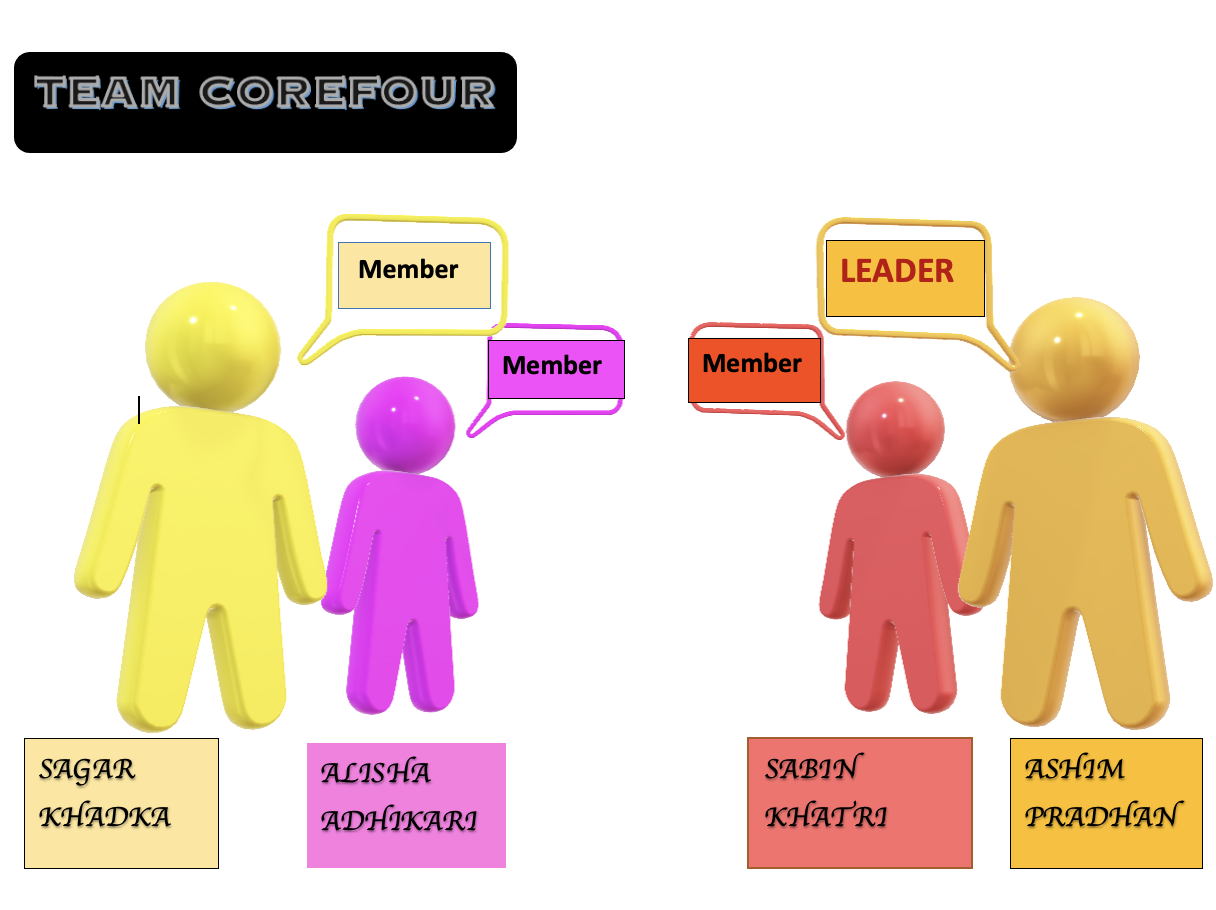
SAGAR KHADKA 1017

SUBMITTED BY

SUBMITTED TO:

ACHYUT TIMSINA

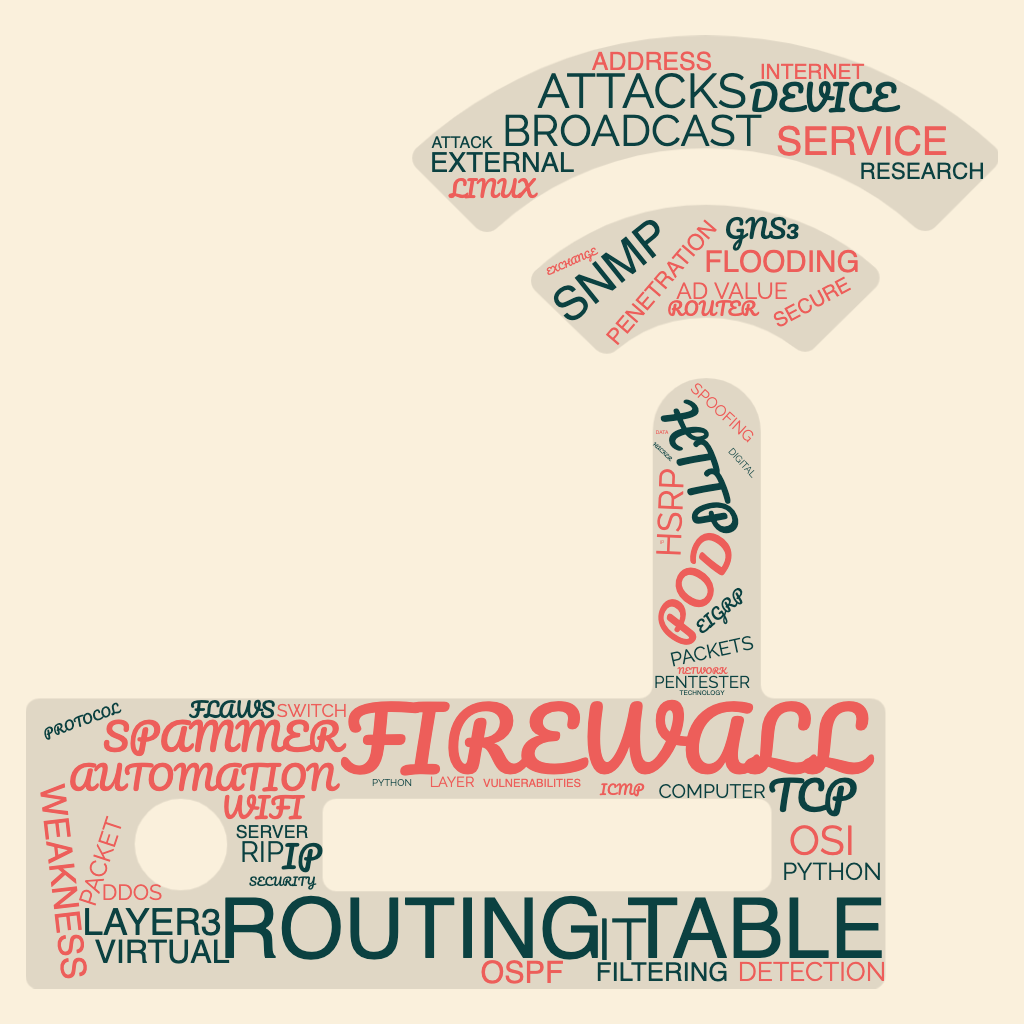
**LAYER 3 (NETWORK LAYER] INCRUSION**

****

**ABSTRACT**

In this era of technology, everyone is connected to one another by exchanging data through network worldwide. The more use of the technology the more chances for network to be vulnerable. As the most vulnerable layer within the network, the layer 3 or network layers attacks are most commonly addressed with huge security issues. If a layer 3 attack is successfully established, the whole network is possibly compromised. In this project, an advanced code written in Python Programming Language is virtually tested with an aim to find different conceivable Layer 3 network vulnerabilities generated by lack of network layers security as IP spoofing, DoS attack, Routing attacks within routing protocol as RIP, EIGRP and OSPF & also ICMP flooding. The project moreover encourages real time detection using the GNS3 tool and VirtualBox mounted with Kali Linux. The security issues detected or performed in this project are mostly caused by insufficient security. Research on the security issues caused previously by unethical hackers gave us insight to build our project.

**KEYWORDS**

****

**Figure 1: Word Cloud.**

Table of Contents

[LIST OF FIGURES 6](#_Toc95210935)

[INTRODUCTION 6](#_Toc95210936)

[MISSION, VISION AND GOALS 8](#_Toc95210937)

[Objective 9](#_Toc95210938)

[Mind map 10](#_Toc95210939)

[Justification. 11](#_Toc95210940)

[ISSUES 12](#_Toc95210941)

### 

### **LIST OF FIGURES**

Figure 1: Word Cloud.

### **INTRODUCTION**

Security has been one of the most highlighted topics in every part and mainly when it comes to network it is considered as the vital aspect to secure data from any kind of damage, theft and sabotage. As the world now has been fully involved in digitalized world for every aspect which means every work is done through working over the internet. Maintaining the network security has been very challenging. As many users are getting involved into technology, equally the cyberpunks seek chances to get into the system in order to exploit and gain access to the devices to acquire sensitive data.

Despite having multiple high level security devices, network breaches are addressed around the globe. However, securing data is a crucial part in computer network. The knowledge and infrastructure to secure the network are limited as technology is escalating on daily basis. It is very important to protect the network equipment’s as routers, switches and servers. Layer 3 devices are basically the foundation of the network as it provides a gateway to the attackers to gain sensitive data about the internal as well as external network and servers. It has been commonly addressed to be attacked despite having security features as packet filtering. Therefore, network protocols as ICMP, IP, RIP, EIGRP, OSPF, HSRP are involved and tested to demonstrate the security flaws in real time.





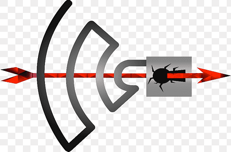


FIGURE 2:

### MISSION, VISION AND GOALS

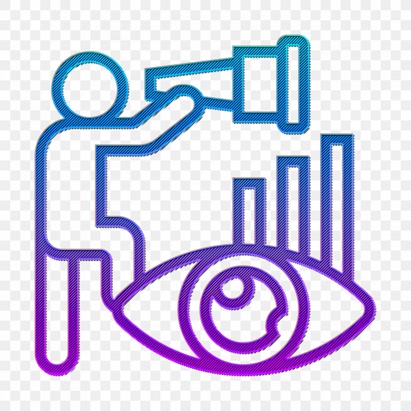


FIGURE:

**Vision**

* Core Four’s vision is to Successfully implement possible attack on layer 3 device.

**Mission.**

* To secure the layer3 devices from every possible attack.
* To provide a pentester’s tools which can simulate an automation attack on layer 3.

**AIM**

* Our project will feature command line tool as well as graphical user interface (GUI) with high-level programming language to execute the possible attack in the router. The main objective of the project is to provide an eyesight to the security expert where the layer3 device weakness is occurred and how the weakness is compromised to execute an attack into the device and get into the system connected to it.

### 

### Objective

* To maintain the CIA Triad security.
* Explore the different types of vulnerabilities.
* Research about the protocols used in Network layer.
* Identify the layer 3 device flaws.
* risk factors analysis.
* Developing the high-level program required to execute an attack.
* Implementing the developed program in real time detection tool.

### Mind map

STAGES

STAGE1 STAGE 2

* Vision - Executing
* Planning - GUI/ CLI
* Coding -Documentation.

RISKS

* Insufficient Knowledge
* Lack of Experience
* Lack of infrastructure
* Possibility of
* Technical Difficulties



MOTIVE

* To provide a brief disclaimer on Network Layer 3 attacks and effects.

RESOURCES

* + Python - -Programming
  + SCAPY

* + Networking Devices
  + GNS3 .
  + Kali Linux OS
  + CANVA
  + MS WORD
  + Documentation

DEVELOPING TOOLS

EXECUTION TOOLS

DESIGNING TOOLS

### 

### Justification.

The lower the layer, the greater the impact. If any one layer is attacked, connection is compromised without other layers noticing it. If network layer is compromised all the layer above it and also the data link layer is compromised though layer 3 is not considered to be the weakest in networking as it has some secured inbuilt security features on the device.

**PICTURE**

As all the corporates, organization has been updated with new technology and performs all works through the digital platform it is likely to be affected if any vulnerability is successfully carried out into the network layer. Most of the private as well as governmental works, data are saved and exchanged through the internet within different networks. Most of the times, the network is compromised and organizational sensitive data are fetched by performing various cyberattacks.

### ISSUES

Everything from small work office, households to large organization as well as sharing private life has been in trend and all involves working on different Networks, data, IT. The exchange or interaction between network-to-network makes the use of internet possible. (<https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/>) The more involvement with the Internet the more news and reports on spammers breaking the systems and services of multiple large industry networks. Providing basic knowledge about system security and also infrastructure, resources and strong manpower that secures the network from hackers and safeguard every data is most essential step to be implemented by every organization. A misinterpretation is implemented that the Routers or network systems are safe as it has some inbuilt security features on it. Despite the fact that layer 2 is known to be the most vulnerable to attacks. At present, most layer 3 devices are reported to be compromised. Having said that, data link layer is most commonly compromised within all the OSI module layers, researchers have created several ways to detect and prevent from attacks of layer2 as Port security, DHCP Snooping, Root guard, BPDU Guard. Therefore, the network layer has been neglected due to its some inbuilt security features. Rather than focusing on creating a proper infrastructure for an entire company, they mostly focused on ethernet network security. It is quite easy for an experienced attacker to attack network layer after getting access its IP address. As a result, most organization are facing attacks through network layers and most shared sensitive data are being compromised.

If an attack is accomplished by an insider of an organization, then it is very easy for the attacker to launch various attack as per the outsider because, the attacker doesn’t need much effort to gain connection to the network of the company. Since the insiders are provided with authorized access and broad knowledge about the organizations systems, network architecture, the protocols being used for the network establishment, systems policy and procedures then any attacks can be successfully implemented. Similarly, if an outsider has to accomplish an attack to a network, then he/she must have deep research on the target organization about all the network devices, infrastructure, possible topologies used, protection, devices implemented into the organization. If the outsider somehow gain access to the network of the targeted organization and gain information about the network architecture being used an attack might be successfully accomplished.

A network layer is basically used to deliver data in a packet across different links from source to destination. It uses routing table to store information as network IP, next hop, subnet mask and all other required information. The network links are not directly connected to end users, it uses different routing protocols for transferring data packets from one network to other. The main protocol through which the attacker gets into the network is IP (internet protocol) to inject various attack. The layer 3 attack is accomplished by attacking the routing protocol. Through the routing protocol the attackers can gain information of network traffic and use it by injecting self into the path within the source and the destination to control the flow of the network traffic. The attacker could also forward packets to non-optimal path to create delay or even froward to a no existing path then the receiver won’t receive the packets as it gets lost. Through these behaviors the services provided by an organization can be spoiled.

Various issues on network security occurs due to improper implementation of security infrastructure on layer 3 device. This project provides a brief overview on how the improper network security causes threats and an open way for attacker to accomplish vulnerable attempts on the layer 3 device such as IP Spoofing, RIP Attack, DDOs ATTACK and so on. These attacks targets on network devices and protocols used in routers like EIGRP, OSPF, RIP etc.

1. IP Spoofing.
2. RIP ATTACK
3. EIGRP ATTACK
4. ICMP FLOOD ATTACK
5. POD (PING OF DEATH)