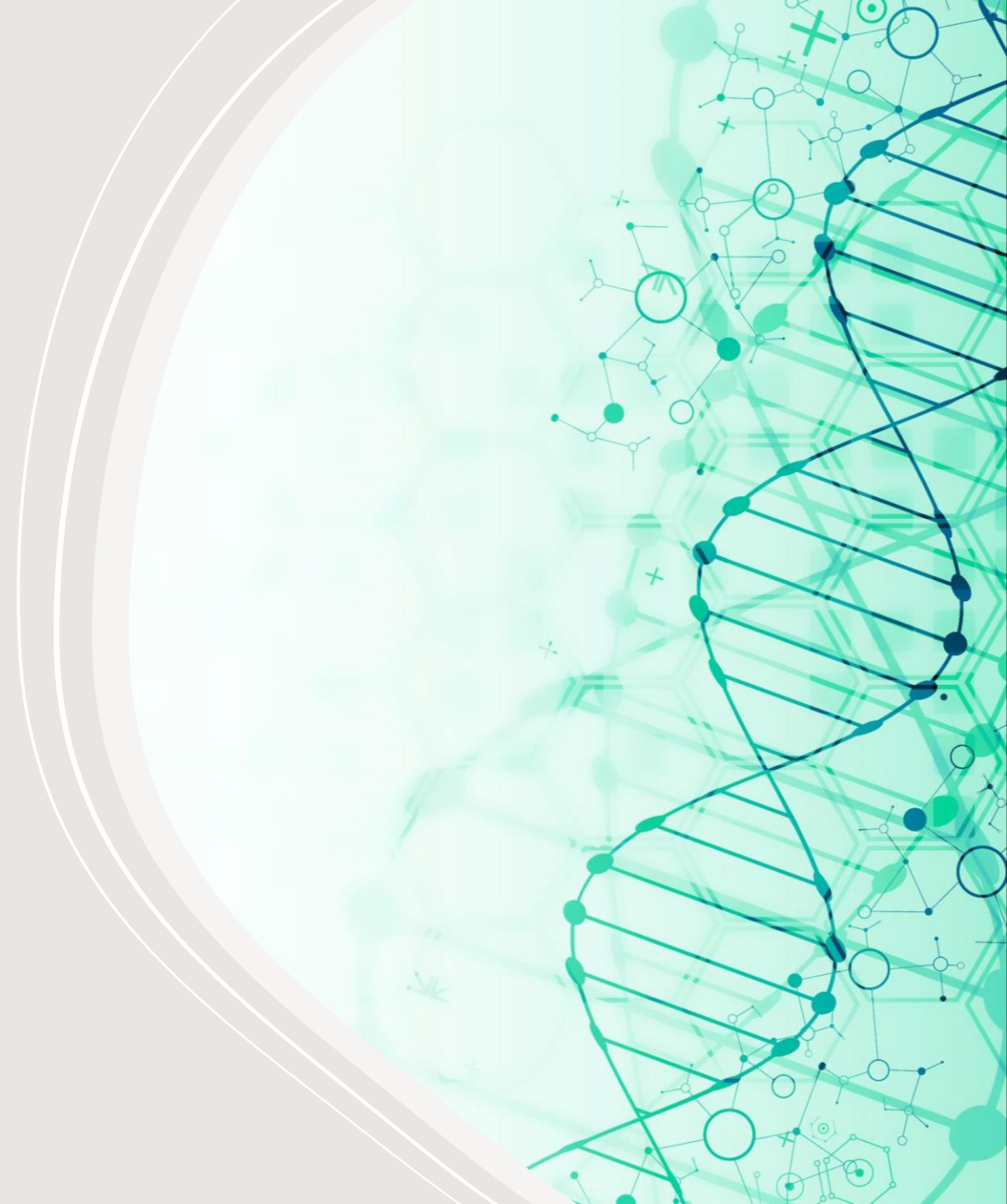



# **COLLEGE NETWORK INFRASTRUCTURE**

USING PACKET TRACER



# CONTENTS

- INTRODUCTION
  - COLLEGE INFRASTRUCTURE
  - MAJOR TYPES OF ATTACKS
  - PREVENTION METHODS
  - CONCLUSION
- 

# INTRODUCTION

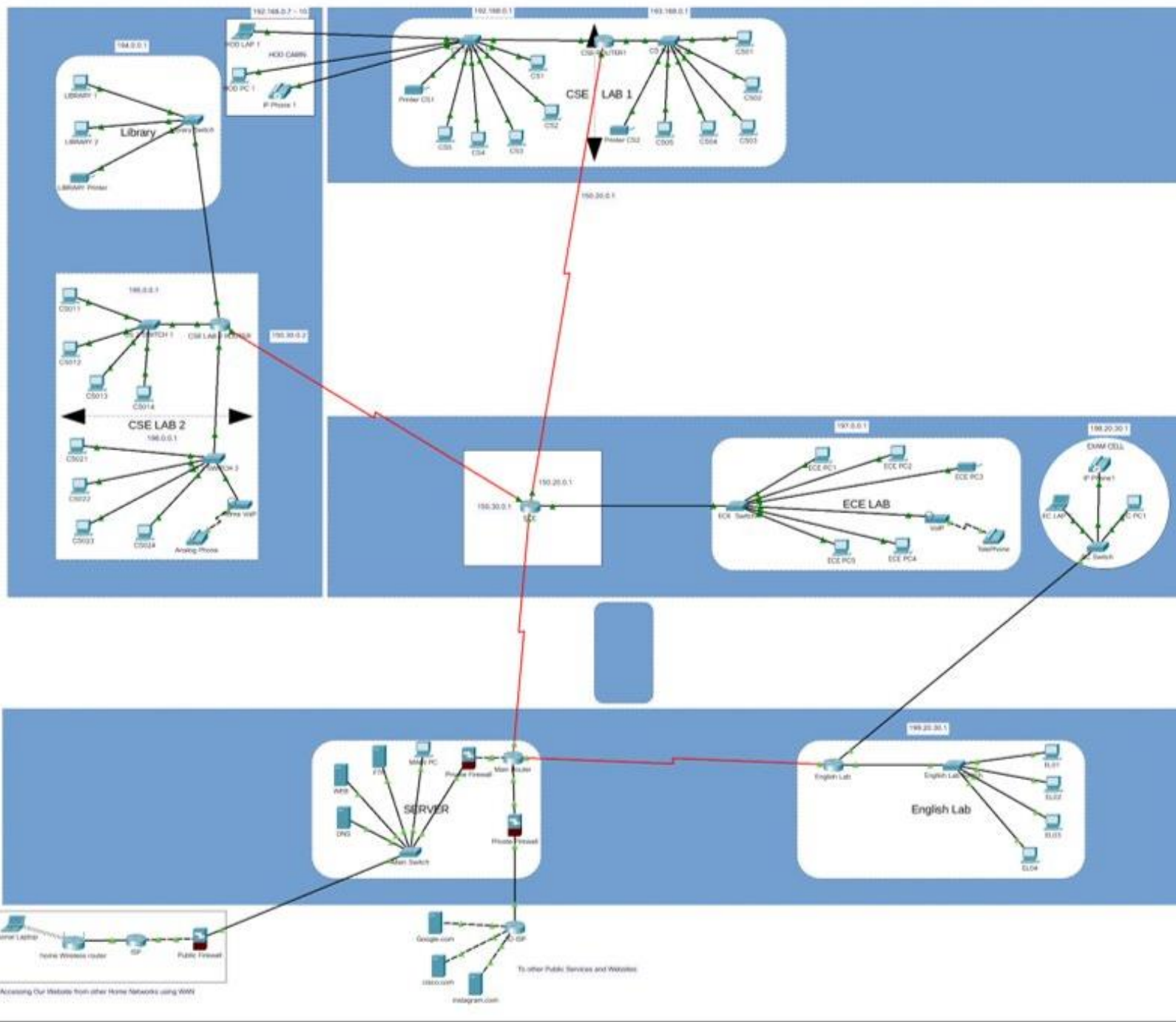
In this presentation we are going to Learn about how our college infrastructure is designed internally and externally in a secure manner to prevent from attacks to our private network and server and protect from the Loss of Data assets.

We Have designed in a efficient way to solve the problems and attacks that Occur in our Network.

# COLLEGE INFRASTRUCTURE

## FEATURES :

- Segregated Sections of Department Wise.
- Routing Protocols like RIP, OSPF.
- Firewall Enabled to Prevent Sniffing and Spoofing.
- Need Auth to Connect a new Device to the Network.
- Double DMZ Enabled Firewall  
for Prevent Network Traffic to access our Private Network.



# OVERVIEW:

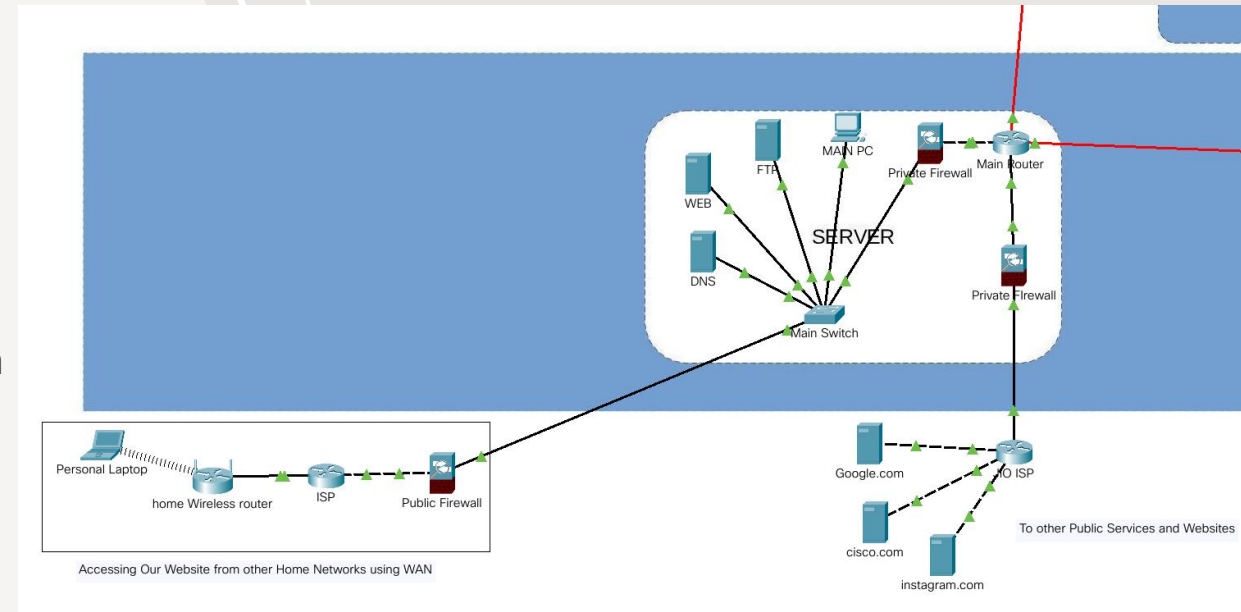
This is the Design of Overall College network infrastructure overview.

That we have Developed Securely to maintain the integrity availability confidentiality.

# Secure Architecture

We Have Assigned 3 firewalls that to prevent attacks ,

1. Private Firewall – The systems which are accessing the server would not allow the users to access private router and PC's
- 2 . College Public Firewall - The Request which are sending and receving to the outer Network Router to prevent the malware and unrequired access or malwares to college network which affects the whole system.
- 3 . This is to Prevent the DMZ Attacks where the firewall is configures before and after the server to prevent the unwanted network traffic.



# MAJOR TYPES OF ATTACKS

- DOS & DDOS
- BOTNETS
- ACCESS ATTACKS
- SPOOFING AND MALWARE ATTACKS
- WEBAPP ATTACKS
- PASSWORD CRACKING

# DOS & DDOS ATTACKS

- Denial of service & Distributed Denial of service attacks is of repeatedly sending requests to a single server continuously without time limit may cause the server that cannot able to respond to packets and hang out. This is the most common type of attacks Occurs in all the Servers .

## SOLUTION

To Prevent DOS Attacks we Configured IPS(Intrusion Prevention System and IDS(Intrusion Detection System) to reroute or block the Traffic from same IP address which is configures in our Public Firewall .



# ACCESS ATTACKS

An Attacker is able to access to the files which are accessed by the authorized user and able to modify the details is Access Attacks . This is most Dangerous attacks which can able to delete the files and make our malware presistent in the server that may affect the users who access the site.

## SOLUTION

To Prevent unauthorized Access to the Storage Devices we need to configure the files as only by Authorized peoples can Access the datas , And the Data must be encrypted to prevent the access and read the data assets.

# BOTNETS & MALWARES

Malwares and Botnets or form of virus which may annoy the user by installing residual files or deleting the main Booting files which may cause the system unboot able or installing some spyware and keyloggers to view the usage logs And statics of user.

## **SOLUTION**

- To Prevent this attack All the router , Switches and PC should be a user .
- Root access to any users is Prohibited.
- If We need to install any application needs admin authorization and not able to connect 3rd party devices to system or any unauthorized softwares.

# WEBAPP ATTACKS

- Website attacks are majorly occurs to servers like XSS,SQL,Broken Authentication , Broken Access Control , Security Misconfiguration,Oauth and many attacks occur on the websites which is not correctly tested.

## SOLUTION

To Prevent webapp attacks the application must be tested for any security bugs and all the firewall , SSL and other certificates should be updated.

This Type of may lead to loss of Business and other important Details

# PASSWORD CRACKING

- Password Cracking Attacks in the ports Like FTP , SSH and other Open ports which can able to handle the data that is in the server.Brute Forcing or Hashing Techniques are used to crack the

## SOLUTION

To Prevent we need to set the access attempt limit from each IP address and request based on account to prevent bruteforcing attacks.

# CONCLUSION

In this Network we Learned that what are the types of attacks which are possible and solutions to Prevent the attacks from Happening in the Network. But 100% Security is Just a Myth.

---

**THANK YOU**

**-VINOTH S**