CISCO – NASSCOM – AICTE
Virtual Internship Program

CISCO PACKET TRACER

INTERNSHIP PROJECT

TOPIC: DESIGN A NETWORK FOR YOUR INSTITUTIO

AMRITA VISHWA VIDYAPEETHAM

Introduction

About the project and the Cisco Packet Tracer

01

Equipment used in CPT

The devices which were used in the project

02

Physical Layout

How the project looks in a physical view

03

Security

The protection given to the devices in the network

04

Possible Attacks

What are the attacks that can affect our network

05

Future Developments

What are the improvements which will be made

06

Introduction

CISCO

PACKET TRACKER

Our Institution consists of 7 buildings and, a simple and secure network between these building is designed using the logical and physical views in the Cisco Packet Tracer.

The connections are established basically using the Access Points(wireless connections), Switches, Routers and some Packet sniffers. Some IoT devices were also placed for physical security purposes and decorations.

Devices List

- Switches
- Routers
- Access Points
- Packet Sniffers
- Server
- Street Lights
- Lawn Sprinklers
- Home Gateways
- Motion Sensor
- Webcam

- Personal Computers
- Laptops
- Smartphones
- Printer

Physical Layout

- To get a better understanding of our Institution, a precise physical layout is also designed.
- The background in the intercity window is the map our college and the buildings in it are represented by the building containers.
- Some generic containers were also used in it, so as to represent the lane accessories and decorations designed for our institution which mostly contain the IoT devices.
- Inside each building, the rooms which contain the equipment for forming the network connections are represented as wiring closets.
- In each of these wiring closets, we can see the physical view of the connection between the devices.

Security Provisions

Some of the main security provision followed in the network are:

- Each Access Point in the campus is given a strong WPA-2 password for any device to connect.
- All the unused ports in the Switches are shutdown and a secret password (which is displayed in an encrypted form while showing running processes) is set to enable the privileged execution mode in the CLI.
- Similarly, all the unused ports in the router are shutdown and a secret password is set to enable the privileged execution mode in the CLI.
- Firewall setting in the mail server is configured so as to only allow the mails from trusted devices in the network.
- The Home Gateway has a strong WPA-2 password for other devices to connect to it.
- A webcam and a motion sensor have been set up in the admin room so as to ensure the physical security for the servers in it.
- They have been configured so that if the motion sensor is triggered, the webcam turns on and gives telecast in the smartphone connected to the Home Gateway.

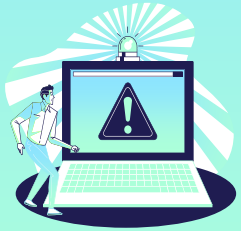
Possible Attacks

Password Cracking

The WPA-2 password set for the APs can be cracked using brute force attacks

Phishing

Attackers send fraudulent mails to trick users into clicking malicious links



Social Engineering

Attackers can psychologically manipulate the users into leaking confidential information

Malware attack

Attackers can inject malicious viruses, spywares, etc.., without user's knowledge.

DoS/DDoS attacks

Attacker can make the server unresponsive by spamming mails from various devices

MitM attack

The attacker might eavesdrop or interrupt the data transfer in the network.

Future Developments

- An SSH encryption can be set up to access routers and switches so as to secure them more effeciently.
- An ASA firewall can be set up and configuredto the server so as to prevent the network to suffer with DoS/DDoS attacks.
- A smoke detector can be put in the server room to enhance the physical security in the admin room.
- Additional servers to be added to ensure that there are backup servers available, if the existing one goes down or gets flooded.
- Set up an authorized only access to the admin room.
- Install anti-virus softwares in all the end devices.

THANKS!

Any Questions?
Contact me via
Email:
ch.en.u4cse19119@ch.students.amrita.edu