GAYATRI VIDYA PARISHAD COLLEGE OF ENGINEERING FOR WOMEN
Kommadi, Madhurawada, Visakhapatnam 530 048
(Approved by AICTE, New Delhi, Affiliated to Andhra University, Visakhapatnam)
(Accredited by National Board of Acciditation [NBA] for B.Tech CSE, ECE and IT - valid from 2019-22 and 2022-25)
(Accredited by National Assesment and Accreditation Council [NAAC] with A Grade - valid from 2022-2027)
Phone: +91-891-2739144, 2739124, 2719125, 2719127 Email id: gvpcew@gmail.com, info@gvpcew.ac.in
EAPCET Councelling Code GVPW
Department of Information Technology

Internship Report on

Cyber Security

THIS REPORT IS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF

BACHELOR OF TECHNOLOGY

IN

INFORMATION TECHNOLOGY

Student Name: M L Kruthi

Student Roll Number: 20JG1A1237

GAYATRI VIDYA PARISHAD COLLEGE OF ENGINEERING FOR WOMEN
Kommadi, Madhurawada, Visakhapatnam 530 048
(Approved by AICTE, New Delhi, Affiliated to Andhra University, Visakhapatnam)
(Accredited by National Board of Accreditation [NBA] for B.Tech CSE, ECE and IT - valid from 2019-22 and 2022-25)
(Accredited by National Assesment and Accreditation Council [NAAC] with A Grade - valid from 2022-2027)
Phone: +91-891-2739144, 2739124, 2719125, 2719127 Email id: gvpcew@gmail.com, info@gvpcew.ac.in
EAPCET Councelling Code GVPW
Department of Information Technology

CERTIFICATE

This is to certify that the technical report entitled "**Cyber Security**" is a bona fide work of the following III – I B. Tech. student bearing roll number **20JG1A1237** in the Department of Information Technology of Gayatri Vidya Parishad College of Engineering for Women, affiliated to Jawaharlal Nehru Technological University, Kakinada during the academic year 2022 in partial fulfilment of the requirement for the award of the Degree of Bachelor of Technology of this university.

Internship Coordinator

Mr. CHVVD Prasad

Assistant Professor

Department of IT, GVPCEW

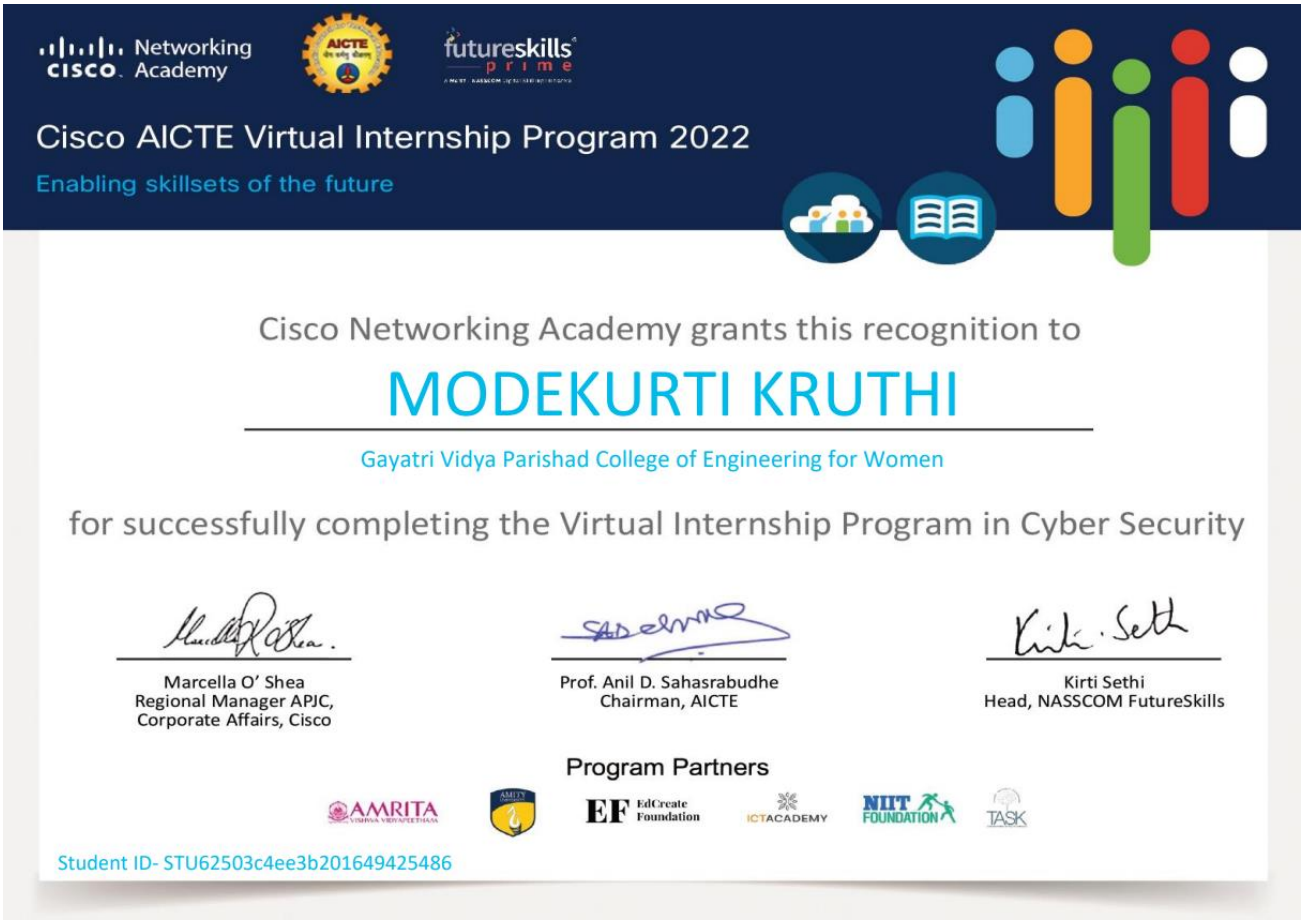
Head of the Department

Dr. Dwiti Krishna Bebarta

Associate Professor

Department of IT, GVPCEW

External Examiner


Networking Academy
futureskills prime
Cisco AICTE Virtual Internship Program 2022
Enabling skillsets of the future
Cisco Networking Academy grants this recognition to
MODEKURTI KRUTHI
Gayatri Vidya Parishad College of Engineering for Women
for successfully completing the Virtual Internship Program in Cyber Security
Marcella O' Shea
Regional Manager APJC,
Corporate Affairs, Cisco
Prof. Anil D. Sahasrabudhe
Chairman, AICTE
Kirti Sethi
Head, NASSCOM FutureSkills
Program Partners
AMRITA
EF EdCreate Foundation
ICTACADEMY
NIIT FOUNDATION
TASK
Student ID- STU62503c4ee3b201649425486

ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of people who made it possible and whose constant guidance and encouragement crown all the efforts with success.

We feel elated to extend our sincere gratitude to,Mr. CHVVD Prasad Assistant Professor for encouragement all the way during analysis of the project. Her annotations, insinuations and criticisms are the key behind the successful completion of the thesis and for providing us all the required facilities.

We express our deep sense of gratitude and thanks to Dr. D Krishna Bebarta, Professor and Head of the Department of Information Technology for his guidance and for expressing valuable and grateful opinions in the project for its development and for providing lab sessions and extra hours to complete the project.

We would like to take this opportunity to express our profound sense of gratitude to Vice Principal, Dr. G. Sudheer for allowing us to utilize the college resources thereby facilitating the successful completion of our thesis.

We would like to take the opportunity to express our profound sense of gratitude to the revered Principal, Dr. R. K. Goswami for allowing us to utilize the college resources thereby facilitating the successful completion of our thesis.

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

The internship report shall have only a one-page executive summary. It shall include five or more Learning Objectives and Outcomes achieved, a brief description of the sector of business and intern organization and summary of all the activities done by the intern during the period.

Learning Objectives:

1. To know about experts and criminals who access data of users illegally.
2. To learn about Cybersecurity cubes.
3. To know about cybersecurity threats, vulnerability and attacks.
4. To learn the art of protecting secrets.
5. To study about ensuring integrity.
6. To study about five nines concepts.

Outcome Achieved:

1. Learnt about ways to protect cybersecurity domain.
2. Learnt about cybersecurity specialist.
3. Learnt about Packet Tracer.
4. Learnt about User Interface.
5. Learnt about Packet Tracer Usage.
6. Learnt about Simulation View.
7. Learnt about IoT Components in Packet Tracer.
8. Learnt about creating and programming objects in Packet Tracer.

Sector of business of CISCO:

Cisco Systems, Inc. designs, manufactures, and sells Internet Protocol based networking and other products related to the **communications and information technology industry** in the Americas, Europe, the Middle East, Africa, the Asia Pacific, Japan, and China.

Intern Organization:

I really enjoyed the freedom mentors gave us in finding workable solutions that we could build and present. I never once felt like I couldn't ask them a question, and they guided us into finding the best solutions. To know that, even as an intern, I made a true impact was the best thing I could wish for and that put to bed some of the initial angst I felt coming into Cisco.

Summary of all activities done:

Cisco internship was a self-paced internship where we had to submit our allocated course assignments before deadline. And, at the end on internship we were asked to do a project.

I divided my work by completing a single module of the internship for two days.

Total modules given to us were 16 and we took nearly 30 days to complete our tasks before deadline.

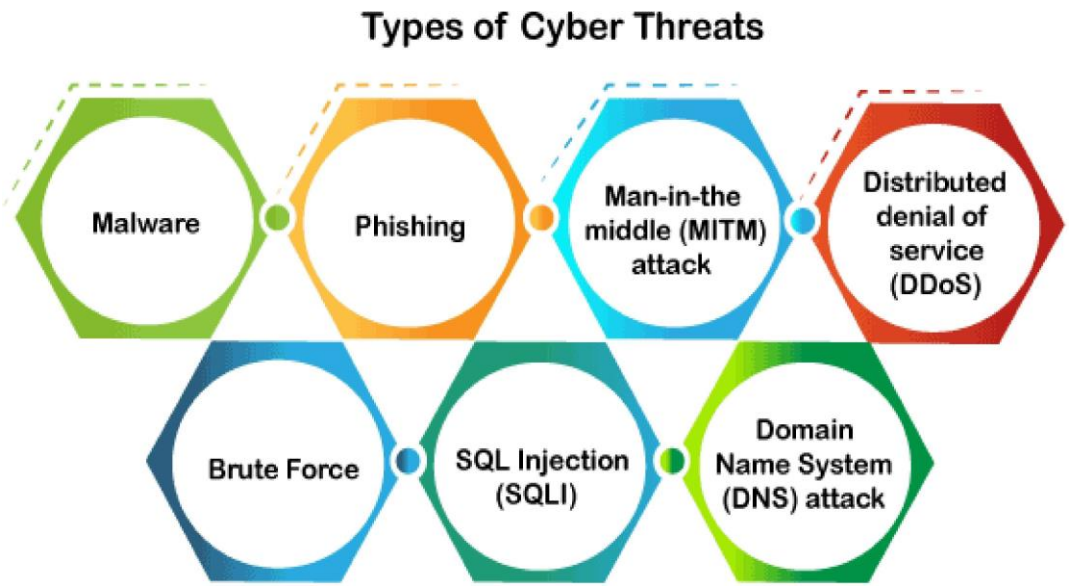
Concepts which were covered were:

1. Experts and Criminals.
2. Cybersecurity Cube
3. Cybersecurity threats, vulnerabilities and attacks
4. Art of protecting secrets
5. Art of ensuring integrity
6. Five nine concepts
7. Methods to protect cybersecurity domain
8. Cybersecurity specialist
9. Basics of Packet Tracer
10. User Interface
11. Simulation View
12. Packet Tracer Usage
13. IoT Components in PT
14. Creating and controlling a smart home network
15. PT environment controls
16. Creating and programming objects in PT

2. INTRODUCTION

INTROUCTION TO CYBER SECURITY

- The technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks is known as cybersecurity. We can divide cybersecurity into two parts one is cyber, and the other is security.
- Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called **electronic information security** or **information technology security**.



Some other definitions of cybersecurity are:

- "Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access."
- "Cyber Security is the set of principles and practices designed to protect our computing resources and online information against threats."

ATTACKS, CONCEPTS AND TECHNIQUES

ATTACKS

The cyber-attacks are general terminology that covers a large number of topics, but some of the popular are:

- Tampering systems and data stored within
- Exploitation of resources
- Unauthorized access to the targeted system and accessing sensitive information
- Disrupting the normal functioning of the business and its processes
- Using ransomware attacks to encrypt data and extort money from victims

To understand the need for Cyber Security measures and their practices, let's have a quick look at the types of threats and attacks.

Ransomware

It is a file encryption software program that uses a unique, robust encryption algorithm to encrypt the files on the target system.

Botnets Attacks

Botnets were initially designed to carry out specific tasks within a group.

Some of the botnet attacks include:

- Distributed Denial of Service (DDoS) attacks
- Spreading spam emails
- Stealing of confidential data
-

Social Engineering Attacks

Social Engineering attacks is now a common tactic used by cybercriminals to gather user's sensitive information.

Cryptocurrency Hijacking

Cryptocurrency hijacking is the new addition to this cyber world.

Cryptocurrency hijacking is also known as "Cryptojacking". It is a program designed to inject mining codes silently into the system. Thus, the hacker silently uses the CPU, GPU, and power resources of the attacked system to mine for the cryptocurrency.

Phishing

Phishing is a fraudulent action of sending spam emails by imitating to be from any legitimate source.

CONCEPTS

Cyber Security is a very broad term but is based on three fundamental concepts known as "**The CIA Triad** ".

It consists of Confidentiality, Integrity, and Availability. This model is designed to guide the organization with the policies of Cyber Security in the realm of Information security.

TECHNIQUES

- Authentication
- Encryption
- Digital Signatures
- Anti-virus
- Firewall
- Steganography

PROTECTING YOUR DATA AND PRIVACY

Some Tips to protect your Data and privacy are as follows:

1. Know your rights
2. Read privacy policies and collection notices
3. Always ask why, how and who
4. Check your credit report
5. Protect yourself online
6. Be aware of your mobile security
7. Use security software
8. Be careful what you share on social media
9. Don't leave your personal information lying around
10. Beware of scams

Some rules for protecting your organisation from cyber attacks

1.Create strong passwords

2.Don't Reuse or share your passwords

3.Backup important files

4.Watch out for Fishing attacks

5.Apply patches

6.Protect your Physical assets

7.Conduct regular staff training courses

3. OVERVIEW OF THE ORGANIZATION

Cisco Systems, Inc., commonly known as **Cisco**, is an American-based multinational digital communications technology conglomerate corporation headquartered in San Jose, California. Cisco develops, manufactures, and sells networking hardware, software, telecommunications equipment and other high-technology services and products. Cisco specializes in specific tech markets, such as the Internet of Things (IoT), domain security, videoconferencing, and energymanagement with leadingproducts including Webex, OpenDNS, Jabber, Duo Security, and Jasper. Cisco is one of the largest technology companies in the world ranking 74 on the Fortune 100 with over $51 billion in revenue and nearly 80,000 employees.

Cisco Systems was founded in December 1984 by Leonard Bosack and Sandy Lerner, two Stanford University computer scientists who had been instrumental in connecting computers at Stanford. They pioneered the concept of a local area network (LAN) being used to connect distant computers over a multiprotocol router system. By the time the company went public in 1990, Cisco had a market capitalization of $224 million; by the end of the dot-com bubble in the year 2000, this had increased to $500 billion, surpassing Microsoft as the world's most valuable company. As of December 2021, Cisco had a market capitalization of around $267 billion.

Cisco stock (CSCO) was added to the Dow Jones Industrial Average on June 8, 2009, and is also included in the S&P 500 Index, the Russell 1000 Index, NASDAQ-100 Index and the Russell 1000 Growth Stock Index.

In 2021, *Fortune* ranked Cisco number one for the second year on their annual list of the 100 Best Companies to Work For based on employee satisfaction surveying.

Cisco Systems also sponsors a line of IT professional certifications for Cisco products. There are four or five (path to network designers) levels of certification: Entry (CCENT), Associate (CCNA/CCDA), Professional (CCNP/CCDP), Expert (CCIE/CCDE) and recently Architect (CCAr: CCDE previous), as well as nine different paths, Routing & Switching, Design, Industrial Network, Network Security, Service Provider, Service Provider Operations, Storage Networking, Voice, Data centre and Wireless.

4. INTERNSHIP PART

Activities done as an Intern:

As an Intern, I did courses on: Experts and Criminals, Cybersecurity Cube, Cybersecurity threats, vulnerabilities and attacks, Art of protecting secrets, Art of ensuring integrity, five nine concepts, Methods to protect cybersecurity domain, Cybersecurity specialist, Basics of Packet Tracer, User Interface, Simulation View, Packet Tracer Usage, IoT Components in PT, Creating and controlling a smart home network, PT environment controls, Creating and programming objects in PT.

Working Condition:

This internship was self-paced which taught us about basics of cybersecurity and importance of cybersecurity in real life. It was a virtual internship with deadline of one week to complete given course. These courses were really helpful during projects as they improved our way of thinking regarding cybersecurity.

Equipment Used:

In order to complete this internship, interns just used their laptops and used IP addresses and few commands in order to do network penetration and also to try packet tracing.

Skills Acquired:

Through our allocated courses, interns learnt about: Experts and Criminals, Cybersecurity Cube, Cybersecurity threats, vulnerabilities and attacks, Art of protecting secrets, Art of ensuring integrity, five nine concepts, Methods to protect cybersecurity domain, Cybersecurity specialist, Basics of Packet Tracer, User Interface, Simulation View, Packet Tracer Usage, IoT Components in PT, Creating and controlling a smart home network, PT environment controls, Creating and programming objects in PT.

5. ACTIVITY LOG AND WEEKLY DESCRIPTION

ACTIVITY LOG FOR THE FIRST WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day – 1	Did a course on experts and criminals.	Learnt about experts and criminals, and difference between them.	
Day - 2	Did a course on experts and criminals.	Learnt about experts and criminals, and difference between them.	
Day – 3	Did a course on 'Cybersecurity Cube'	Learnt about cybersecurity cube	
Day – 4	Did a course on 'Cybersecurity Cube'	Learnt about cybersecurity cube	
Day – 5	Did a course on cybersecurity threats, vulnerabilities and attacks	Learnt about cybersecurity threats, vulnerabilities and attacks.	
Day –6	Did a course on cybersecurity threats, vulnerabilities and attacks	Learnt about cybersecurity threats, vulnerabilities and attacks.	

WEEKLY REPORT

WEEK – 1 (From Dt 1-07-2022 to Dt 7-07-2022)

Objective of the Activity Done:

To know the basics of experts and criminals, cybersecurity cubes, cybersecurity threats, vulnerabilities and attacks.

Detailed Report:

I first created an account in Cisco Net Academy Portal and then started doing my course in it. I completed a single course in two days and tried to submit assignments before deadline.

Many of the world's original hackers were computer hobbyists, programmers and students during the 60's. Originally, the term hacker described individuals with advanced

programming skills. Hackers used these programming skills to test the limits and capabilities of early systems. These early hackers were also involved in the development of early computer games. Many of these games included wizards and wizardry. As the hacking culture evolved, it incorporated the lexicon of these games into the culture itself. Even the outside world began to project the image of powerful wizards upon this misunderstood hacking culture. Books such as where Wizards Stay up Late: The Origins of The Internet published in 1996 added to the mystique of the hacking culture. The image and lexicon stuck.

Cybersecurity cube is a **tool developed to help manage the protection of networks, domains, and the Internet**. The first dimension of the Cybersecurity Cube is the three principles of information security. The second dimension identifies the three states of information or data.

A cybersecurity threat is a **malicious** and **deliberate attack** by an individual or organization to gain unauthorized access to another individual's or organization's network to damage, disrupt, or steal IT assets, computer networks, intellectual property, or any other form of sensitive data.

ACTIVITY LOG FOR THE SECOND WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day – 1	Studied about art of protecting secrets.	Learnt about protecting secrets	
Day - 2	Studied about art of protecting secrets.	Learnt about protecting secrets	
Day – 3	Studied about art of ensuring integrity.	Learnt about methods to ensure integrity.	
Day – 4	Studied about art of ensuring integrity.	Learnt about methods to ensure integrity.	
Day – 5	Studied about five nines concepts.	Learnt about five nines concepts.	
Day –6	Studied about five nines concepts.	Learnt about five nines concepts.	

WEEKLY REPORT

WEEK – 2 (From Dt 8-07-2022 to Dt 14-07-2022)

Objective of the Activity Done:

To know the art of protecting secrets, art of ensuring integrity and about five nines concept.

Detailed Report:

I first created an account in Cisco Net Academy Portal and then started doing my course in it. I completed a single course in two days and tried to submit assignments before deadlines.

In this week, I learnt about art of protecting secrets, art of ensuring integrity and studied about five nines concept. Five nines are the term used for describing the availability of a computer or a service at 99.999 percent of the time it is required. In other words, the system or service is only unavailable for 5.39 minutes throughout the year for planned or unplanned downtime. Five nines are recommended and required for mission-critical requirements and for certain areas such as e-commerce. However, five nines availability has always been a challenge for a service or network and is often impossible to guarantee.

ACTIVITY LOG FOR THE THIRD WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day – 1	Studied about protecting a cybersecurity domain.	Learnt about ways to protect cybersecurity domain.	
Day - 2	Studied about protecting a cybersecurity domain.	Learnt about ways to protect cybersecurity domain.	
Day – 3	Studied about cybersecurity specialist.	Learnt about cybersecurity specialist.	
Day – 4	Studied about cybersecurity specialist.	Learnt about cybersecurity specialist.	
Day – 5	Did a course on 'Introduction to Packet Tracer'	Learnt about packet tracers	
Day –6	Did a course on 'Introduction to Packet Tracer'	Learnt about packet tracers.	

WEEK – 3 (From Dt 15-07-2022 to Dt 21-07-2022)

Objective of the Activity Done:

To know the protecting cybersecurity domains, studied about cybersecurity specialists and learnt about packet tracer.

Detailed Report:

Every business nowadays needs a digital presence to remain relevant and reach more customers. What most businesses fail to grasp is that their competitors aren't the only "threat" to their venture. More hackers are now equipped with smarter tools and they are using more advanced techniques to breach your security protocols in order to steal data, scam your customers, or take over your domain. That is why companies need to take on a more strategic approach to enhance their defense systems and to implement the most relevant tactics to help prevent such security breaches.

ACTIVITY LOG FOR THE FORTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day – 1	Did a course on 'User Interface'	Learnt about User Interface	
Day - 2	Did a course on 'User Interface'	Learnt about User Interface	
Day – 3	Did a course on 'Simulation View'	Learnt about Simulation View	
Day – 4	Did a course on 'Simulation View'	Learnt about Simulation View	
Day – 5	Did a course on 'Packet Tracer Usage'	Learnt about Packet Tracer Usage.	
Day –6	Did a course on 'Packet Tracer Usage'	Learnt about Packet Tracer Usage.	

WEEKLY REPORT

WEEK – 4 (From Dt 22-07-2022 to Dt 28-07-2022)

Objective of the Activity Done: To know about user interface, simulation view and learnt about packet tracer usage.

Detailed Report:

Cybersecurity isn't what it used to be. Safeguarding the information of our companies and customers used to be the sole concern for those of us in the profession—but no longer. Now, we must consider the user experience, as well.

Digital is poised to pervade every facet of life not only because it makes living easier, but also because it's fun—by design. Likewise, to do security right, we've got to ask not just whether it works, but if it's user-friendly—simple to navigate, reliable, and pleasurable to use.

The simulation research section details the current role that simulation plays in cybersecurity, which mainly falls on representative environment building; test, evaluate, and explore; training and exercises; risk analysis and assessment; and humans in cybersecurity research.

The main purpose of Cisco Packet Tracer is to help students learn the principles of networking with hands-on experience as well as develop Cisco technology specific skills. Since the protocols are implemented in software only method, this tool cannot replace the hardware Routers or Switches. Interestingly, this tool does not only include Cisco products but also many more networking devices.

ACTIVITY LOG FOR THE FIFTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day – 1	Did a course on 'IoT Components in Packet Tracer'	Learnt about IoT components in packet tracer.	
Day - 2	Did a course on 'IoT Components in Packet Tracer'	Learnt about IoT components in packet tracer.	
Day – 3	Read a case study of creating and controlling a smart home network.	Learnt about how smart home networks are controlled.	
Day – 4	Read a case study of creating and controlling a smart home network.	Learnt about how smart home networks are controlled.	

Day – 5	Read a case study on packet tracer environment controls.	Learnt about packet tracer environment control.	
Day –6	Read a case study on packet tracer environment controls.	Learnt about packet tracer environment control.	

WEEKLY REPORT

WEEK – 5 (From Dt 1-08-2022 **to Dt** 7-08-2022**)**

Objective of the Activity Done: To know about Iot components in packet tracer, simulation view and reading two case studies.

Detailed Report:

In Packet Tracer, depending on the scenario, typical Internet of Things (IoT) systems can be designed or configured in three ways: first, IoT smart things can be directly connected to the gateway; second, IoT components and smart things can be connected to microcontroller (MCU) for automatic working without using gateway connectivity; and third, IoT smart things can be connected either directly to the gateway or indirectly through MCU. This chapter discusses the implementation of first two scenarios. It helps students to learn the controlling of two appliances, i.e. fan and light in smart home with mobile phone through gateway connectivity. The chapter also helps students create a smart room, which consists of the following smart objects: smart light, smart fan, smart coffee maker, smart air cooler, and smart heating element.

In our smart house right now we have a smart ceiling fan, we have a thermostat, smoke detector, smart lamp, a smart appliance, which is a coffee maker, a smart door, and even a garage door. We have a battery system and a solar panel that can collect energy for us as well. Down below we have something called an MCU, which is a microcontroller, and this microcontroller allows us to program events, and when the door or the fan should be activated. We also have something called a home gateway. And the home gateway is connected to all of our smart devices. If we click on that home gateway, we can take a look at it. There's a physical tab, config, GUI, and attributes. In the physical tab of this home gateway, we can see that this device has wireless antennas. It supports wireless connections. We also have wired network ports as well. In the config tab we have settings that we can configure here regarding those wireless and wired interfaces. We even have a GUI tab, and in this GUI tab, this home gateway is running a web server. It has an index.php file, and this actually has a webpage on it that you can connect to and control your smart devices. In the attributes tab, we're able to see items such as cost and mean time between failure.

ACTIVITY LOG FOR THE SIXTH WEEK

Day & Date	Brief description of the daily activity	Learning Outcome	Person In-Charge Signature
Day – 1	Read a case study on creating and programming objects in PT.	Learnt about ways to create objects in PT.	
Day - 2	Read a case study on creating and programming objects in PT.	Learnt about ways to create objects in PT	
Day – 3	Chapter Wise quizzes on 'Cybersecurity essentials'	Completed Chapter Wise Quizzes	
Day – 4	Complete assessment on 'Cybersecurity essentials'	Completed assessment on 'Cybersecurity essentials'	
Day – 5	Chapter Wise quizzes on 'Introduction to Packet Tracer.'	Completed Chapter Wise quizzes on 'Introduction to Packet Tracer.'	
Day –6	Complete assessment on 'Introduction to Packet Tracer.'	Completed Complete assessment on 'Introduction to Packet Tracer.'	

WEEKLY REPORT

WEEK – 6 (From Dt 8-08-2022 **to Dt** 14-08-2022**)**

Objective of the Activity Done: **To know about creating and programming objects in packet tracer.**

Detailed Report:

Since Packet Tracer simulates networks and network traffic, the physical aspects of these networks also need to be simulated. This includes actually finding and deploying physical devices, customizing those devices, and cabling those devices. After the physical deployment and cabling is done, then it is time for configuration of the interfaces used to connect the devices. Finding a device to deploy requires looking in the Device-Type Selection Box. The Device-Type Selection Box works on the concept of categories and sub-categories as shown in the figure. The top row of icons represents the category list consisting of: [Networking

Devices], [End Devices], [Components], [Connections], [Miscellaneous], and [Multiuser]. Each category contains at least one sub-category group.

Creating and Programming Objects in Packet Tracer. In this chapter, we got to know about:

- How to create a new Thing.
- How to connect your new Thing to the network.
- How to use available scripts for the new Thing.
- How to access the programming environment.
- How to review and modify existing scripts.

Creating and Connecting a Thing. Before attempting to create a new Thing, you need to decide what the Thing will do, how it will connect to the network, and how it will work. You need to find graphics to represent the states of your new Thing. Usually you will need two graphics, one to represent the beginning or default state and another to represent the end state. You also need to identify an existing Thing that functions in a similar manner as the new Thing. The existing script can then be modified to create the new script. Clicking on any IoT device that is in the workspace will reveal the specifications about that device. The specifications include: • Features – how the device works or what it does. Devices can generate high and low values based on a button being pushed or toggled on and off or they can detect certain environmental values (eg. Smoke or sunlight)

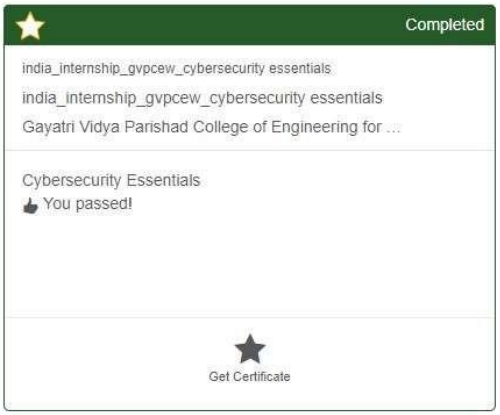
• Usage – Things may connect to other IoT devices in order to receive LOW or HIGH inputs or it may read the variable set in the Environment object

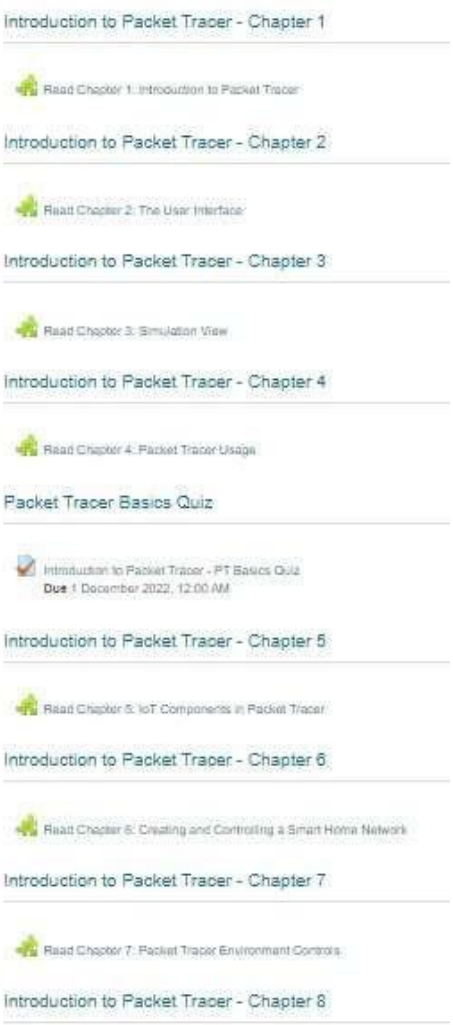
• Direct Control – shows you what keystrokes will allow you to physically interact with the Thing

• Local and Remote Control – shows how to control the Thing locally or remotely (if applicable)

• Data Specifications – how the values are produced or the port/slot used to connect to the sensor.

PHOTOS & VIDEO LINKS





6. OUTCOMES DESCRIPTION

❖ Managerial skills

The following are the managerial skills that were acquired

- Time management: Time management is the first and most important skill that every individual must have. I had a very good time management throughout my internship.
- Coaching: I learnt all the required concepts individually with the help of Google and YouTube. Alongside I helped my friends with their doubts.
- Negotiating
- Communication: I had conversations with people from different states. So, I talked to them in a way that is understandable.
- Problem solving: This is the major skill required to complete the tasks.
- Coordinating: I coordinated with the friends in LinkedIn from different colleges in case of queries. They helped me with my doubt.

References

1. Introduction to Packet Tracer: https://lms.netacad.com/course/view.php?id=1367718

2. Cybersecurity essentials: https://lms.netacad.com/course/view.php?id=1349503