CISCO - Cyber Security Virtual Internship Program 2021

An Internship report submitted by

MASINENI KRISHNA SAI – URK18CS238

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE AND ENGINEERING

under the supervision of

Dr. V. KARUNAKARAN,M.E, (Ph.D.)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

KARUNYA INSTITUTE OF TECHNOLOGY AND SCIENCES

(Declared as Deemed to be University under Sec-3 of the UGC Act, 1956)
Karunya Nagar, Coimbatore - 641 114. INDIA

August 2021

Karunya INSTITUTE OF TECHNOLOGY AND SCIENCES
(Declared as Deemed to be University under Sec.3 of the UGC Act, 1956)
A CHRISTIAN MINORITY RESIDENTIAL INSTITUTION
AICTE Approved & NAAC Accredited

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that the report entitled, "Cyber Security Virtual Internship Program" is a bonafide record of Internship work done at CISCO Networking Academy during the academic year 2021-2022 by

MASINENI KRISHNA SAI(Reg. No: URK18CS238)

in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Computer Science and Engineering of Karunya Institute of Technology and Sciences.

Guide Signature

Dr. V. KARUNAKARAN,M.E, (Ph.D.)

ASSISTANT PROFESSOR

ACKNOWLEDGEMENT

First and foremost, I praise and thank ALMIGTHY GOD whose blessings have bestowed in me the will power and confidence to carry out my Internship.

I am grateful to our beloved founders **Late. Dr. D.G.S. Dhinakaran, C.A.I.I.B, Ph.D** and **Dr. Paul Dhinakaran, M.B.A, Ph.D**, for their love and always remembering us in their prayers.

I extend my thanks to our Vice Chancellor **Dr. P. Mannar Jawahar, Ph.D** and our Registrar **Dr. Elijah Blessing, M.E., Ph.D,** for giving me this opportunity to do the internship.

I would like to thank **Dr. Prince Arulraj, M.E., Ph.D.,** Dean, School of Engineering and Technology for his direction and invaluable support to complete the same.

I would like to place my heart-felt thanks and gratitude to **Dr. J. Immanuel John Raja, M.E., Ph.D.,** Head of the Department, Computer Science and Engineering for his encouragement and guidance.

I feel it a pleasure to be indebted to, **Mr. J. Andrew, M.E, (Ph.D.),** Assistant Professor, Department of Computer Sciences Technology and **Dr. V. KARUNAKARAN,M.E, (Ph.D.)**

for their invaluable support, advice and encouragement.

I also thank all the staff members of the Department for extending their helping hands to make this in Internship a successful one.

I would also like to thank all my friends and my parents who have prayed and helped me during the Internship.

Networking Academy

futureskills prime
A MeitY - NASSCOM Digital Skilling Initiative

Cyber Security Virtual Internship Program 2021

Enabling skillsets of the future

Cisco Networking Academy grants this recognition to

MASINENI KRISHNA SAI

Karunya Institute Of Technology and Sciences

for successfully completing cyber security virtual internship program

Marcella O' Shea
Regional Manager APJ,
Corporate Affairs, Cisco

Prof. Anil D. Sahasrabudhe
Chairman,
AICTE

Kirti Sethi
Head,
NASSCOM FutureSkills

Program Partners

AMRITA VISHWA VIDYAPEETHAM · AMITY UNIVERSITY · EduSkills · ICTACADEMY · NTTF · NIIT FOUNDATION · TASK

Student ID- STU60463e1db3efd1615216157

Corporate Social Responsibility

Cisco Networking Academy

Certificate of Course Completion

Introduction to Cybersecurity

For completing the Cisco Networking Academy® Introduction to Cybersecurity course, and demonstrating the ability to explain the following:

- Global implications of cyber threats
- Ways in which networks are vulnerable to attack
- Impact of cyber-attacks on industries
- Cisco’s approach to threat detection and defense
- Why cybersecurity is a growing profession
- Opportunities available for pursuing network security certifications

MASINENI KRISHNA SAI

Student

Karunya Institute of Technology and Sciences

Academy Name

India

Location

12 May 2021

Date

Laura Quintana
VP & General Manager, Cisco Networking Academy

Corporate Social Responsibility

Cisco Networking Academy

Certificate of Course Completion

Cybersecurity Essentials

For completing the Cisco Networking Academy® Cybersecurity Essentials course, and demonstrating the following abilities:

- Describe the tactics, techniques and procedures used by cyber criminals.
- Describe the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures.
- Describe technologies, products and procedures used to protect confidentiality, ensure integrity and provide high availability.
- Explain how cybersecurity professionals use technologies, processes and procedures to defend all components of the network.
- Explain the purpose of laws related to cybersecurity.

MASINENI KRISHNA SAI

Student

Karunya Institute of Technology and Sciences

Academy Name

India

Location

11 May 2021

Date

Laura Quintana
VP & General Manager, Cisco Networking Academy

Corporate Social Responsibility

Cisco Networking Academy

Certificate of Course Completion

Introduction to Packet Tracer

For completing the Cisco Networking Academy® Introduction to Packet Tracer course.

MASINENI KRISHNA SAI

Student

Karunya Institute of Technology and Sciences

Academy Name

India

Location

1 Jun 2021

Date

Laura Quintana
VP & General Manager, Cisco Networking Academy

Design a secure network of Campus Area Network

Done By,

Masineni Krishna Sai

URK18CS238

Karunya Institute of Technology and Sciences

Introduction

Network design involves evaluating, understanding and scopingthenetworktobeimplemented.Quantity,typeand location of network devices (router, switches, servers) IP addressing structure. Network security architecture and overall network security processes.

Existing network infrastructure and its features

Network infrastructure comprises hardware and software, systems and devices, and it enables computing and communication between users, services, applications and processes. Anything involved in the network, from servers to wireless routers, comes together to make up a system's network infrastructure.

Features

- Communication speed.
- File sharing.
- Backup and Rollback is easy.
- Software and Hardware sharing.
- Security.
- Scalability.
- Reliability.

Devices Used

- Switches.
- Routers.
- Access Point.
- Multilayer Switches.
- Servers.
- IOT Devices.
- Firewalls.
- Cloud.
- Controllers.
- End Devices

Security Threats

- Computer Viruses and Computer Worms.
- Trojan horse.
- SQL Injection attack.
- DOS and DDOS attack.
- Rootkit.
- Rogue Security Software.
- Phishing.
- Adware and Spyware.
- Man-in-the-middle attacks.

Mitigation Measures to improve the security

Organizations are constantly attacked by hackers,the attackers may be inside or outside.More organizations than ever before are dealing with insider security threats. Here are some of the steps that all organizations should take to mitigate these threats and protect important company data:

1. Always encrypt your data

If you want to minimize the impact of an insider threat, always encrypt data. Not all employees need access to all data and encryption adds another layer of protection.

2. Use monitoring solutions

There are monitoring solutions that you can use, such as application, identity and device data, which can be an invaluable resource for tracking down the source of any insider attack.

3. Use Access Control

Access controls may help to deter both malicious and negligent threats. This also makes it more difficult to access data. Access control is an important part of security. Weak access control leaves your data and systems susceptible to unauthorized access. Boost access control measures by using a strong password system. You should have a mix of uppercase and lowercase letters, numbers, and special characters. Also, always reset all default passwords.

4. Keep All Software Updated

As pesky as those update alerts can be, they are vital to your network's health. From anti-virus software to computer operating systems, ensure your software is updated. When a new version of software is released, the version usually includes fixes for security vulnerabilities. Manual software updates can be time-consuming. Use automatic software updates for as many programs as possible.

5. Standardize Software

Keep your systems protecting by standardizing software. Ensure that users cannot install software onto the system without approval. Not knowing what software is on your network is a huge security vulnerability. Make sure that all computers use the same:

- Operating system
- Browser
- Media player
- Plugins

Standardization also makes system updates less of a hassle.

6. Use Network Protection Measures

Protecting your network is crucial. To keep your network and its traffic secured:

- Install a firewall
- Ensure proper access controls
- Use IDS/IPS to track potential packet floods
- Use network segmentation
- Use a virtual private network (VPN)
- Conduct proper maintenance

7. Install Network Monitoring Software

Network monitoring software provides early warning at the slightest instance of detecting a threat. It does this by keeping track of the entire IT infrastructure, establishing contact with all devices, and the system.

- Monitors the entire security systems.
- Measures bandwidth bottlenecks.
- Inspects environmental parameters.

8.Monitoring

Monitoring the health of your application is often a huge step toward monitoring the security of your application.

There are three main parts to good monitoring:

- Aggregating the data,
- Alerting on abnormalities,
- Responding

9. Attack Surface Analysis

To reduce your attack surface and hacking risk, you must understand your network's security environment. An attack surface analysis will help you identify immediate risks and potential future risks.

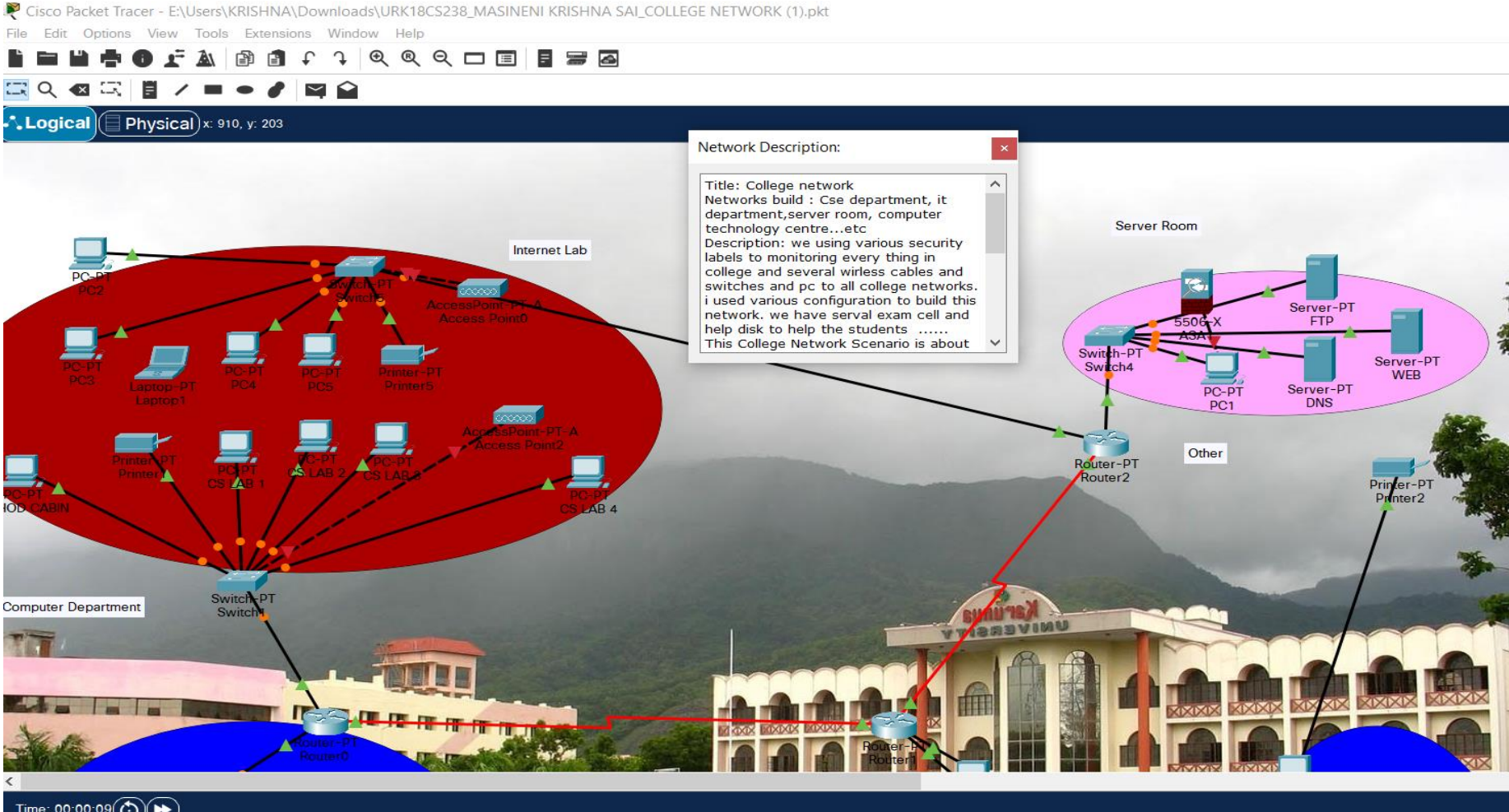
- Identify Vulnerabilities.
- Pinpoint User Types.
- Perform a risk assessment.
- Secure your reporting.
- Create Strong User Access Protocols.
- Protect your Backups.

10. Prioritize Analytics

The final measure to reduce the attack surface is analysis.

- Security configuration assessments
- Traffic flow analysis
- Quantitative risk scores

Thank You!


Cisco Packet Tracer - E:\Users\KRISHNA\Downloads\URK18CS238_MASINENI KRISHNA SAI_COLLEGE NETWORK (1).pkt
File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 910, y: 203
Network Description:
Title: College network
Networks build : Cse department, it department,server room, computer technology centre...etc
Description: we using various security labels to monitoring every thing in college and several wirless cables and switches and pc to all college networks. i used various configuration to build this network. we have serval exam cell and help disk to help the students .....
This College Network Scenario is about
Internet Lab
Server Room
Other
Computer Department
PC-PT PC2
Switch-PT Switch3
AccessPoint-PT-A Access Point0
PC-PT PC3
Laptop-PT Laptop1
PC-PT PC4
PC-PT PC5
Printer-PT Printer5
AccessPoint-PT-A Access Point2
Printer-PT Printer4
PC-PT CS LAB 1
PC-PT CS LAB 2
PC-PT CS LAB 3
PC-PT CS LAB 4
Switch-PT Switch4
5506-X ASA
Server-PT FTP
Server-PT WEB
Server-PT DNS
PC-PT PC1
Router-PT Router2
Printer-PT Printer2
Switch-PT Switch1
Router-PT Router0
Router-PT Router1
Time: 00:00:09

Cisco Packet Tracer - E:\Users\KRISHNA\Downloads\URK18CS238_masineni krishna sai (1).pka

File Edit Options View Tools Extensions Window Help

Logical Physical x: 806, y: 326 [Root]

PT Activity: 00:55:01

Packet Tracer – Skills Integration Challenge

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ_Router	G0/0	10.44.1.1	255.255.255.0	N/A
	G0/1	209.165.201.2	255.255.255.248	N/A
VPN server	NIC	209.165.201.19	255.255.255.248	N/A
HQ_Wireless	LAN	10.44.0.254	255.255.255.0	10.44.1.1
FTP/Web server	NIC	10.44.1.252	255.255.255.0	10.44.1.1
BackupFiles server	NIC	10.44.2.10	255.255.255.0	10.44.2.1

This culminating activity includes many of the skills that you have acquired during this course. You will configure a wireless router, upload and download files using FTP, connect securely to a remote site using a VPN, and secure a Cisco IOS router.

Implementation

Note: You only have access to the Metropolis HQ site. You can access all the servers and PCs within this

Time Elapsed: 00:55:01 Completion: 100/100

Top Dock Check Results Reset Activity < 1/1 >

Time: 00:01:11 Realtime

4331 4321 1941 2901 2911 819IOX 819HGW 829 1240 PT-Router PT-Empty 1841 2620XM

Scenario 0 New Delete

Fire | Last Status | Source | Destination | Type | Color | Time(sec) | Periodic | Num | Edit | Delete

RSA Encryptor/Decryptor/Key Generator/Cracker

Directions are at the bottom.

Public Modulus (hexadecimal):

```
d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e
3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d7925
2f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24b
eb9c825b73ebf549
```

Public Exponent (hexadecimal):

10001

Private Exponent (hexadecimal):

```
47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e
09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da
038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352
df58848adad11a1
```

Text:

```
0xc8 0x93 0xa9 0x0d 0x8f 0x4e 0xc5 0xc3 0x64 0xec 0x86 0x9d 0x2b 0x2e 0xc9 0x21
0xe3 0x8b 0xab 0x23 0x4a 0x4f 0x45 0xe8 0x96 0x9b 0x98 0xbe 0x25 0x41 0x15 0x9e
0xab 0x6a 0xfb 0x75 0x9a 0x13 0xb6 0x26 0x04 0xc0 0x60 0x72 0x28 0x1a 0x73 0x45
0x71 0x83 0x42 0xd4 0x7f 0x57 0xd1 0xac 0x91 0x8c 0xae 0x2f 0x3b 0xd2 0x99 0x30
0x3e 0xe8 0xa8 0x3a 0xb3 0x5d 0xfb 0x4a 0xc9 0x18 0x19 0xfd 0x3f 0x0c 0x0a 0x1f
0x3d 0xa4 0xa4 0xfe 0x02 0x9d 0x96 0x2f 0x50 0x34 0xd3 0x95 0x55 0xe0 0xb7 0x2a
0x46 0xa4 0x9e 0xae 0x80 0xc9 0x77 0x43 0x16 0xc0 0xab 0xfd 0xdc 0x88 0x95 0x05
0x56 0xdf 0xc4 0xfc 0x13 0xa6 0x48 0xa3 0x3c 0xe2 0x87 0x52 0xc5 0x3f 0x0c 0x0d
```

- ○ Hexadecimal
- ○ Character String

Encrypt Sign

RSA Encryptor/Decryptor/Key Generator/Cracker

Directions are at the bottom.

Public Modulus (hexadecimal):

```
d94d889e88853dd89769a18015a0a2e6bf82bf356fe14f251fb4f5e2df0d9f9a94a68a30c428b39e
3362fb3779a497eceaea37100f264d7fb9fb1a97fbf621133de55fdcb9b1ad0d7a31b379216d7925
2f5c527b9bc63d83d4ecf4d1d45cbf843e8474babc655e9bb6799cba77a47eafa838296474afc24b
eb9c825b73ebf549
```

Public Exponent (hexadecimal):

```
10001
```

Private Exponent (hexadecimal):

```
47b9cfde843176b88741d68cf096952e950813151058ce46f2b048791a26e507a1095793c12bae1e
09d82213ad9326928cf7c2350acb19c98f19d32d577d666cd7bb8b2b5ba629d25ccf72a5ceb8a8da
038906c84dcdb1fe677dffb2c029fd8926318eede1b58272af22bda5c5232be066839398e42f5352
df58848adad11a1
```

Text:

```
Alice
```

RSA Encryptor/Decryptor/Key Generator/Cracker

Directions are at the bottom.

Public Modulus (hexadecimal):

```
f47e3c01a6a7daa1629e81bb82425880dcaeaa61a11ecd8242e138b2d65aab67e8cb81e2e546b9d8
29ab8d67006e24c3fd6539fe3f38c28ed6d0c343ef659f2830ddfe4e0d35ea2a2a9dc8198124e691
422651d29f405d0789d646501406b9baf307d1111fb026561fde9cbdcb7be54523fc0340702919d6
f50db6594971cb65
```

Public Exponent (hexadecimal):

```
10001
```

Private Exponent (hexadecimal):

```
8ab34e617565061fc5edbc155ee93a82282fa292ee2fa6507e967c6ee031e1c97a04717401b3e4dc
5f8f661187e9f44b876634c72aa08da730f08fc5eb7ad01585fdf071ad6a35128583c5e497505674
3c327534a4a58153fc30ff3168247d7ab28a4ebda7ba4feaac01f6b522d03d2be4516a7c292ff8e6
efe92fb716ada5c1
```

Text:

```
0x95 0x4e 0x44 0x8f 0x9e 0x6c 0xcc 0x43 0xb4 0x60 0x82 0x6a 0x80 0x55 0xd7 0x10
0x22 0xd7 0x65 0x1e 0x38 0x9b 0x80 0x4e 0x5e 0x8e 0x1e 0xea 0x19 0xb2 0xfc 0x81
0xcb 0x3f 0x30 0xe4 0xe6 0xde 0xe4 0x1e 0x5d 0x89 0xab 0x5a 0x60 0x75 0x2d 0x22
0x91 0x9b 0xd6 0x5e 0x73 0x60 0xe9 0xf5 0xf8 0x98 0xb5 0xa7 0xb0 0xd1 0x40 0x34
0x87 0x93 0xcb 0xbc 0x5d 0x4f 0x9e 0xcc 0x4e 0xb4 0x87 0x57 0x62 0xd2 0xa8 0x53
0xce 0x38 0x0c 0x47 0xf0 0xfb 0x3e 0x65 0x56 0x7d 0xfd 0xf4 0x57 0x9b 0xc7 0x14
0xe2 0xad 0xb9 0x17 0xc3 0x25 0x73 0x2e 0xce 0x2f 0x21 0xc1 0x9f 0x98 0xa8 0x09
0x3c 0x30 0xe4 0xac 0x93 0xae 0xb6 0x24 0xd0 0xb9 0x8b 0x8e 0x7a 0xa9 0x2a 0xf9
```