CIS – SECURITY - ITM ASSOCIATE INTERN, COGNIZANT, GURUGRAM, HARYANA

DATE: 29TH MARCH 2022 – PRESENT

Internship report submitted in partial fulfilment of the requirement for the degree of

Bachelor of Technology

In

Computer Science And Engineering

By: Ritwik Tripathi

181436

CSE

To

Department of Computer Science & Engineering And Information Technology

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY,
WAKNAGHAT, SOLAN,
HIMACHAL PRADESH – 173234

CERTIFICATE

This is to certify that the work which is being presented in the internship report titled **“CIS – Security - ITM Associate Intern, Cognizant, Gurugram, Haryana**” in partial fulfilment of the requirements for the award of the degree of B.Tech in Computer Science And Engineering and submitted to the Department of Computer Science And Engineering, Jaypee University of Information Technology, Waknaghat is an authentic record of work carried out by **Ritwik Tripathi** during the said period; March 2022 – till date, ensuring proper care towards the rules and regulations as specified by the Non-Disclosure Agreement signed between Ritwik Tripathi and Cognizant Technology Solutions dated 30.01.2022 under the supervision of **Dr. Kapil Sharma**, Assistant Professor (S.G.), Jaypee University of Information Technology, Waknaghat, Solan, H.P

Ritwik Tripathi
181436
Jaypee University of Information Technology
Waknaghat, Solan, H.P.

The above statement made is correct to the best of our knowledge.

Dr. Kapil Sharma
Assistant Professor (S.G.)
Jaypee University of Information Technology
Waknaghat, Solan, H.P.

ACKNOWLEDGEMENT

This is a matter of pleasure for me to acknowledge my deep sense of gratitude to Jaypee University and my college, Jaypee University of Information Technology for giving me an opportunity to explore my abilities via this internship program. I would like to express my sincere gratitude to our Training and Placement officer, Mr. Pankaj Kumar and our faculty Coordinator, Dr. Nafis U Khan for this opportunity. I also wish to express my gratitude to my internship supervisors, for their valuable guidance and advice towards my internship.

I would like to record my sincere appreciation and gratitude towards all the officials, coaches, trainers, mentors and employees of Cognizant Technology Solutions, without whose kind assistance, my internship program would not have been proceeding in a swift direction. The facts and other vital information provided by them have contributed towards making this report as comprehensive as possible. I am indeed thankful to them.

Last but not the least, I would like to express my sincere thanks to all my family members, friends and well-wishers for their immense support and best wishes throughout the internship duration and the preparation of this report and I wish they would continue to contribute towards my well-being.

I believe that this report will be a valuable asset not only for academic institution, but will also be useful for all those who are interested to learn about internship experiences in auditing and consulting firm.

Ritwik Tripathi
181436
Jaypee University of Information Technology,
Waknaghat, Solan, H.P.

CANDIDATE'S DECLARATION

I, the undersigned solemnly declare that the internship report is based on my own work carried out during the course of my work under as CIS – Security – ITM Associate Intern at Cognizant Technology Solutions.

I assert the statements made and conclusions drawn are an outcome of my own analysis and work.

I further certify that:

1. The work contained in this report is original and has been done by me.
2. The work has not been submitted by any other Institution for any other degree/diploma/certificate in this university or any other University of India or abroad.
3. I have followed the guidelines provided by the university in writing the report.
4. Whenever I have used materials (data, theoretical analysis, and text) from other sources, I have given due credits to them in the text of the report and giving their details in the references.

Ritwik Tripathi
181436
Jaypee University of Information Technology,
Waknaghat, Solan, H.P.

INTERNSHIP REPORT UNDERTAKING

I, Ritwik Tripathi, Roll No. 181436, Branch - Computer Science and Engineering currently pursuing my internship with Cognizant from 29-03-22 to 18-08-2022.

As per procedure I have to submit my internship report to the university related to my work that I have done during this internship.

I have compiled my internship report, but due to COVID-19 situation and Work from Home procedure being followed, my mentor in the company is not able to sign this report and no digital signatures are allowed as part of the company's confidentiality policy.

So, I hereby declare that the internship report is fully designed/developed by me and no part of the work is borrowed or purchased from any agency. And I'll produce a certificate/document of my internship completion with the company to Training and Placement Cell whenever COVID-19 situation gets normal.

Ritwik Tripathi
181436
Jaypee University of Information Technology,
Waknaghat, Solan, H.P.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

S No.	Abbreviation	Meaning
1.	BU	Business Unit
2.	BH	Behavioral
3.	CIS	Cloud, Infrastructure and Security
4.	ITM	Integrated Threat Management
5.	CoE	Centre of Excellence
6.	LP	Learning Path
7.	IPS	Intrusion Prevention System
8.	IDS	Intrusion Detection System
9.	SOC	Security Operations Centre
10.	HR	Human Resources
11.	JDBC	Java Database Connectivity
14.	EDR	Endpoint Detection and Response
15.	MDR	Managed Detection and Response
16.	XDR	Extended Detection and Response
17.	SQL	Structured Query Language
18.	MySQL	My Structured Query Language
19	API	Application Programming Interface
20.	BLOB	Binary Large Object
21.	CLOB	Character Large Object
22.	AAA	Authentication, Authorization and Accounting
23.	SPOF	Single Point of Failure
24.	PKI	Public Key Infrastructure
25.	ICT	Integrated Capability Test
26.	OSI	Open System Interconnection
27.	TCP / IP	Transmission Control Protocol / Internet Protocol
28.	HTTP/HTTPS	Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure
29.	FTP	File Transfer Protocol
30.	UDP	User Datagram Protocol
31	SMTP	Simple Mail Transfer Protocol
32.	DHCP	Dynamic Host Configuration Protocol
33.	CompTIA	Computing Technology Industry Association

34.	IPv4	Internet Protocol version 4
35.	DNS	Domain Name System
36.	VLAN	Virtual Local Area Network
37.	LAN	Local Area Network
38.	RIP	Routing Information Protocol
39.	PC	Personal Computer
40.	CBROPS	Cybersecurity Operations
41.	CSSP	Cyber Security Service Provider
42.	CCSP	Certified Cloud Security Professional
43.	DLP	Data Loss Prevention
44.	SIEM	Security Information and Event Management
45.	AV	Antivirus
46.	HIPAA	Health Insurance Portability and Accountability Act
47.	PCI-DSS	Payment Card Industry Data Security Standard.
48.	GDPR	General Data Protection Regulation
49.	SSL	Secure Socket Layer
50.	SOHO	Small Office/ Home Office

LIST OF FIGURES

x	

ABSTRACT

At Gen C Next program in Cognizant, each selected intern is allotted a certain domain with each domain having specific amount of training period varying from 12 weeks to 19 weeks. Internship includes various events such as educational workshops, webinars, Udemy courses, Integrated Capability Test and group work assignments.

A large IT company based in the United States and India, Cognizant employees a large number of Indians, to be exactly about 3.4 lac employees. Cognizant Corporation having set foot in more than 40 countries and also recruits and hires international workers from all around the globe.

Cognizant provides various services to a large number of clients in the IT industry. They also have ties with one of the fastest growing companies like Cisco, Amazon Web Services, Microsoft, McAfee, etc. Work culture in Cognizant is just as professional as expected and it values ethical notes towards the progress of its employees and raises concern regarding physical and mental issues faced by its' employees.

Being placed under the domain of CIS-Security, further ITM Sub Domain. ITM deals with identifying and minimizing threats associated with any network. This includes Firewall operations, IDS / IPS, Network Filtering, Cloud Infrastructure Threat Management, SOC, etc.

Apart from full BU Training, Cognizant also ensures that Associates exhibit an optimal level of business skills while on work. For this, BH Sessions are conducted across 12 sessions (24 hours) for each Associate. The total training for BU is assigned for 16 weeks.

This report will cover all the trainings undertaken till date at Cognizant. The internship starts with breaking the ice between associates and introduction to corporate world. This involved many sessions of interactions with top tier associates of Cognizant. Courses followed in the next week regarding meditation and zero waste management and coach was assigned. Corporate training of Java was bought in with courses from Udemy for corporate level coding experience. After this mentor connect took place which led to domain assignment for BU. The Gen C Learn portal was enabled and LP was established in it. The LP provides a guided map for the 16 weeks of BU training.

CHAPTER 1
ORGANIZATION

1.1 Background

After the end of 6th semester, various company visited to the college for the placement of students. One such company was Cognizant Technology Solutions, which selected me for Gen-C Next profile. Having offered an internship program by Cognizant before the full-time role and completing the internship being necessary for the full-time role with the company, the internship is bound to be around 19 weeks containing various sessions, webinar, online Udemy courses, assessments and a project.

Cognizant is among one of the top IT companies in India, and a major IT giant in US. Cognizant employees are around 3 Lac people and recruit around 20k freshers every year from India. Cognizant also hires from different countries across the globe.

Cognizant offers various role in the company like developer, designer, tester and manager in the company, but, before becoming the associate every person should complete the intern period and after the intern period there is one year of probation period in the company for the associate to join the company.

Cognizant also provides stipend during the internship period which is around 12 thousand per month to the interns pursing internship. But the total amount in hand is 10800 only because 1200 is deducted for the purpose related to the tax i.e., 10% which is further given back to the associates after successful completion of internship. This time around, Cognizant has processed intern stipend based on milestone completion.

The internship period varies and depends on the roles which the intern gets, like for a developer profile, internship period is of around 4-5 months and for the quality insurance, it may vary from 5-6 month.

The domain allocation is random in Cognizant for the interns, but sometime it depends on the assimilation test also. The person who got higher marks in assimilation test, will have higher chances to get better profile or domain and it also depends on the first come first serve basis. Gen C Next candidates are offered their preferred domains and being one of them, the ITM domain in CIS-Security assigned to me.

1.2 Mission, Vision, Values and Objectives

1.2.1 Mission

Cognizant's mission is to train every fresher who got selected. For this, it provides internship to every selected candidate who is hired as a fresher.

Every year, Cognizant trains college freshers in bulk number before giving them the associate role. This recruit happens from all college over India.

Cognizant spends much time, effort and money in training the intern before giving them the actual work and before them to work in the real environment.

1.2.2 Vision

Cognizant's vision is to train every fresher recruited form the college no matter from which college the persons come from.

1.2.3 Values

The values of the organization are as follows:

1.2.3.1 Valuing People

Cognizant believes that its' success depends first and foremost on people. By respecting people in everything they do, they will develop and maintain high quality, mutually beneficial relationships with their clients, professional colleagues, referral sources, vendors, community members and with each other.

1.2.3.2 Building Client Relationships

Cognizant seeks to earn long-term client loyalty by developing a deep understanding of each client's business and personal goals, by demonstrating unwavering reliability and integrity in their work and by acting as an independent and objective advisor to their clients.

1.2.3.3 Upholding Quality and Integrity

We will maintain an environment where a commitment to quality, honesty, respect, fairness and professional ethics governs the actions and decisions of everyone within our firm.

1.2.3.4 Keys to Success

- Complete the work with full honesty.
- Complete the work on time.
- Complete the assessment.
- Complete the project within schedule time.
- Try to learn as much as possible from the SME, Trainer, mentor.
- Open to learn anything taught.

1.2.4 Objectives

The objectives of Cognizant are:

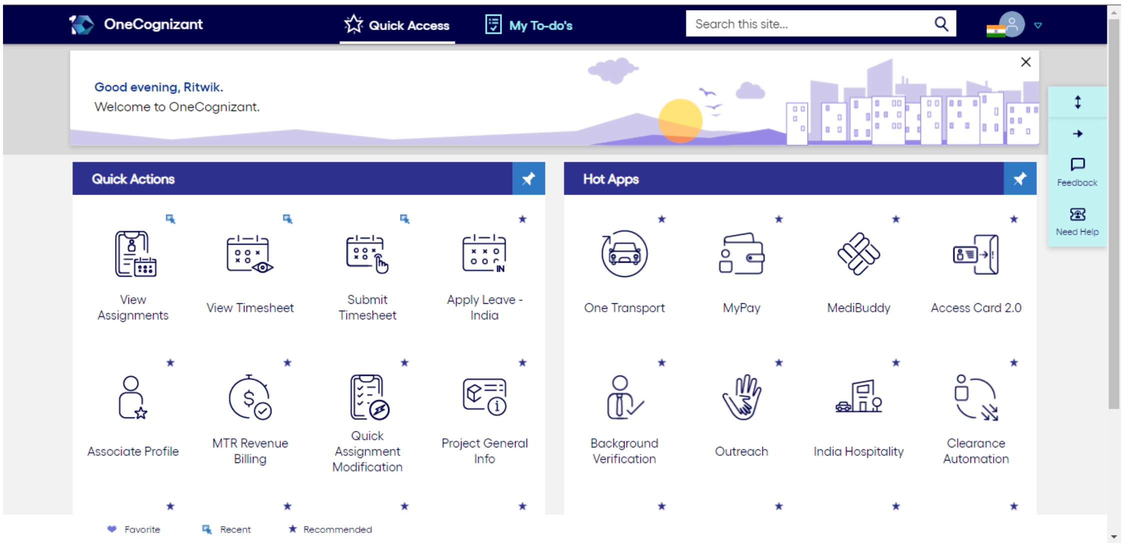
- The overall objective is to focus the activities towards its specialized services and to become a leader in this niche in the country.

- Growth - To expand the business at a rate that is both challenging and manageable, serving the market with innovation and adaptability.

1.3 Work from Home Procedures

Due to the COVID-19 pandemic, the whole internship is scheduled to be in the form of work from home mode. To make this a success, Cognizant has signed ties with Microsoft Office to progress its business in online mode. Apart from this, Cognizant provides laptops with its employees with proper EDR, MDR and XDR policies which makes it prone to even zero-day attacks.

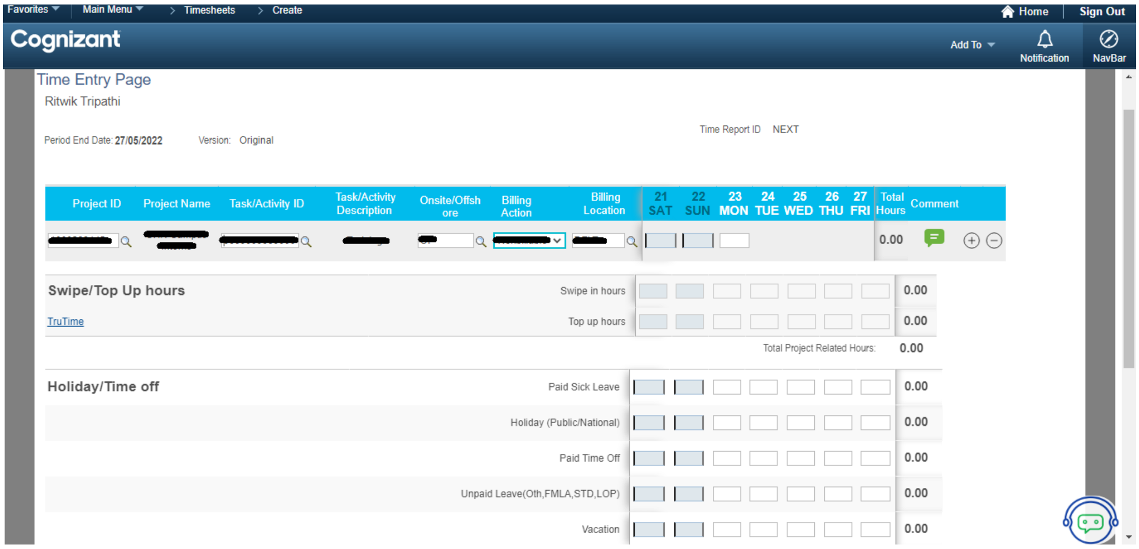
Cognizant has proposed the usage of personal laptops for interns during the train and learn period of the internship. Cognizant has developed a special portal which help the employees to download application plug-ins and access new applications monitor worktime schedule of the employees along with various supporting applications like tech support, HR support, project details, assignment details, leave approvals, etc.



Good evening, Ritwik.
Welcome to OneCognizant.

Figure 1. A look into the 1C portal

In this portal, trutime and timesheets are two applications which helps in monitoring access time to the day work. A working day comprises of 10 hours with 1 hour of lunch break. The main difference between trutime and timesheet is that trutime accounts for daily hours while logged into the system, just like an access swipe card used inside the campus premises, whereas timesheet accounts for the daily working hours only. Both the timesheets and trutime are monitored by project manager. Timesheets are approved on a weekly basis whereas trutime is approved on a daily basis. Project details can be viewed from the View Assignment App.



Time Entry Page

Ritwik Tripathi

Period End Date: 27/05/2022 Version: Original

Time Report ID NEXT

Project ID	Project Name	Task/Activity ID	Task/Activity Description	Onsite/Offshore	Billing Action	Billing Location	21 SAT	22 SUN	23 MON	24 TUE	25 WED	26 THU	27 FRI	Total Hours	Comment
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]								0.00	

Swipe/Top Up hours

TruTime

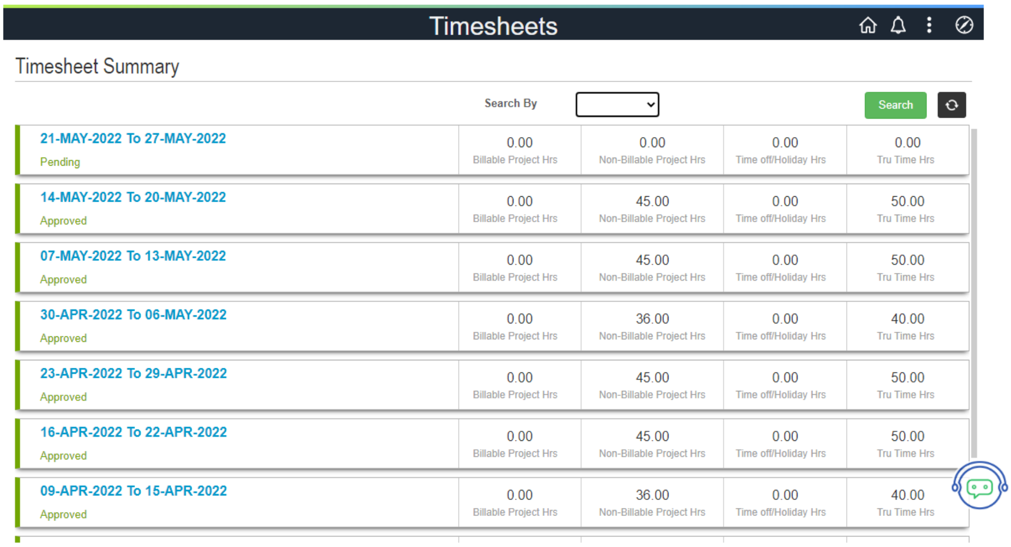
Swipe in hours								0.00
Top up hours								0.00

Total Project Related Hours: 0.00

Holiday/Time off

Paid Sick Leave								0.00
Holiday (Public/National)								0.00
Paid Time Off								0.00
Unpaid Leave(Oth,FMLA,STD,LOP)								0.00
Vacation								0.00

Figure 2. Timesheet Landing Page

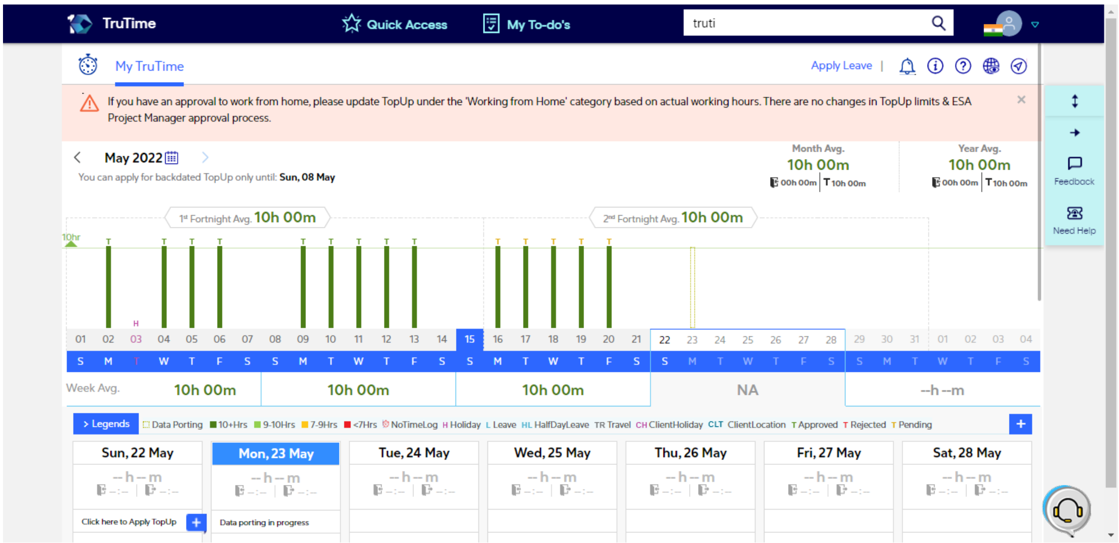


Timesheet Summary

Search By

Period	Billable Project Hrs	Non-Billable Project Hrs	Time off/Holiday Hrs	Tru Time Hrs
21-MAY-2022 To 27-MAY-2022 Pending	0.00	0.00	0.00	0.00
14-MAY-2022 To 20-MAY-2022 Approved	0.00	45.00	0.00	50.00
07-MAY-2022 To 13-MAY-2022 Approved	0.00	45.00	0.00	50.00
30-APR-2022 To 06-MAY-2022 Approved	0.00	36.00	0.00	40.00
23-APR-2022 To 29-APR-2022 Approved	0.00	45.00	0.00	50.00
16-APR-2022 To 22-APR-2022 Approved	0.00	45.00	0.00	50.00
09-APR-2022 To 15-APR-2022 Approved	0.00	36.00	0.00	40.00

Figure 3. Timesheet Summary



If you have an approval to work from home, please update TopUp under the 'Working from Home' category based on actual working hours. There are no changes in TopUp limits & ESA Project Manager approval process.

May 2022

You can apply for backdated TopUp only until: **Sun, 08 May**

Month Avg. 10h 00m (00h 00m | T 10h 00m)

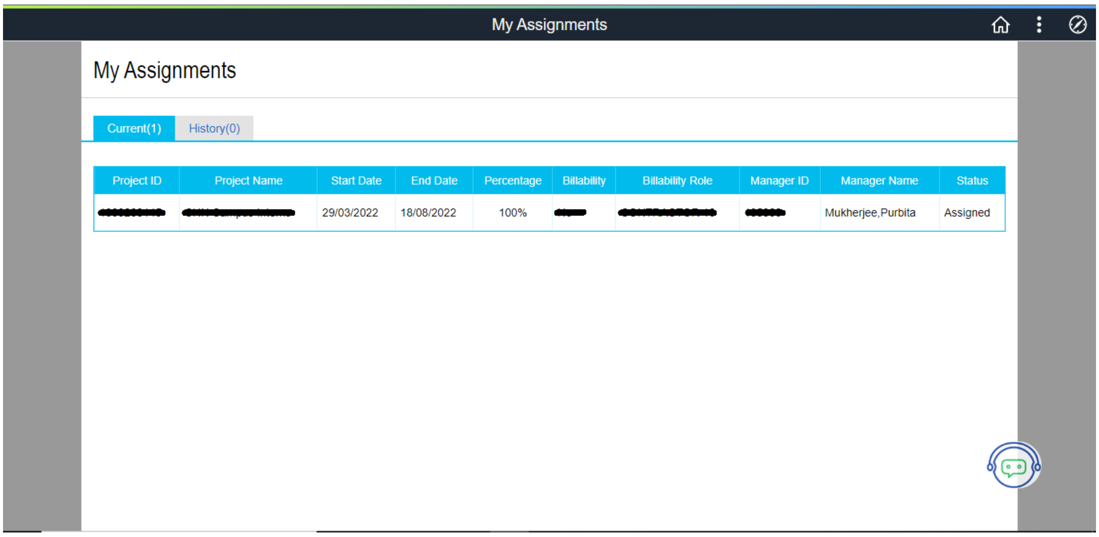
Year Avg. 10h 00m (00h 00m | T 10h 00m)

Week Avg.	10h 00m	10h 00m	10h 00m	NA	--h --m

> Legends ⬚ Data Porting 🟩 10+Hrs 🟩 9-10Hrs 🟨 7-9Hrs 🟥 <7Hrs NoTimeLog H Holiday L Leave HL HalfDayLeave TR Travel CH ClientHoliday CLT ClientLocation T Approved T Rejected T Pending

Sun, 22 May	Mon, 23 May	Tue, 24 May	Wed, 25 May	Thu, 26 May	Fri, 27 May	Sat, 28 May
--h--m --:-- | --:--	--h--m --:-- | --:--	--h--m --:-- | --:--	--h--m --:-- | --:--	--h--m --:-- | --:--	--h--m --:-- | --:--	--h--m --:-- | --:--
Click here to Apply TopUp	Data porting in progress					

Figure 4. TruTime



My Assignments

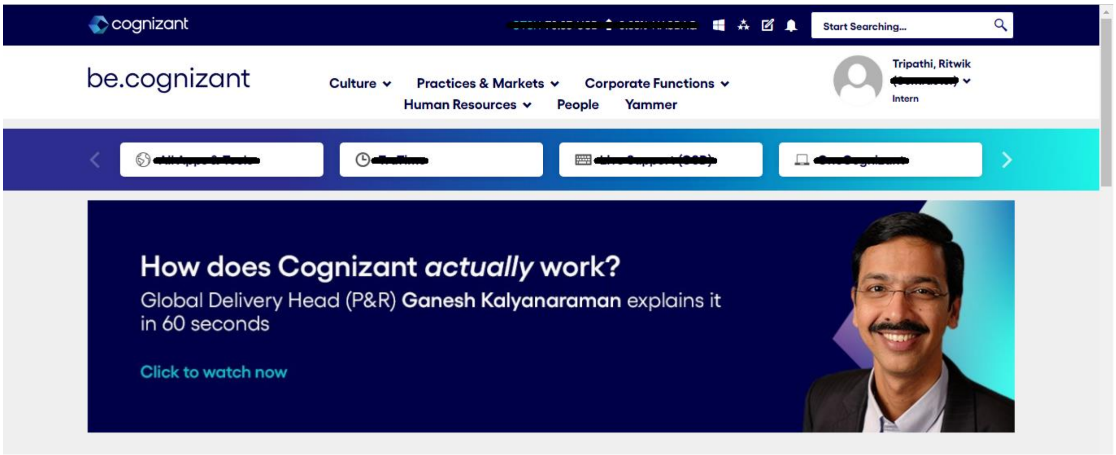
My Assignments

Current(1) History(0)

Project ID	Project Name	Start Date	End Date	Percentage	Billability	Billability Role	Manager ID	Manager Name	Status
[redacted]	[redacted]	29/03/2022	18/08/2022	100%	[redacted]	[redacted]	[redacted]	Mukherjee,Purbita	Assigned

Figure 5. My Assignments app reflect projects assigned to me with further details.

Cognizant has developed another portal which revolves regarding the highlights of the happenings inside the organisation. All the important decisions and directions regarding the company’s future, employee well-being and clientele perspectives are listed in here.

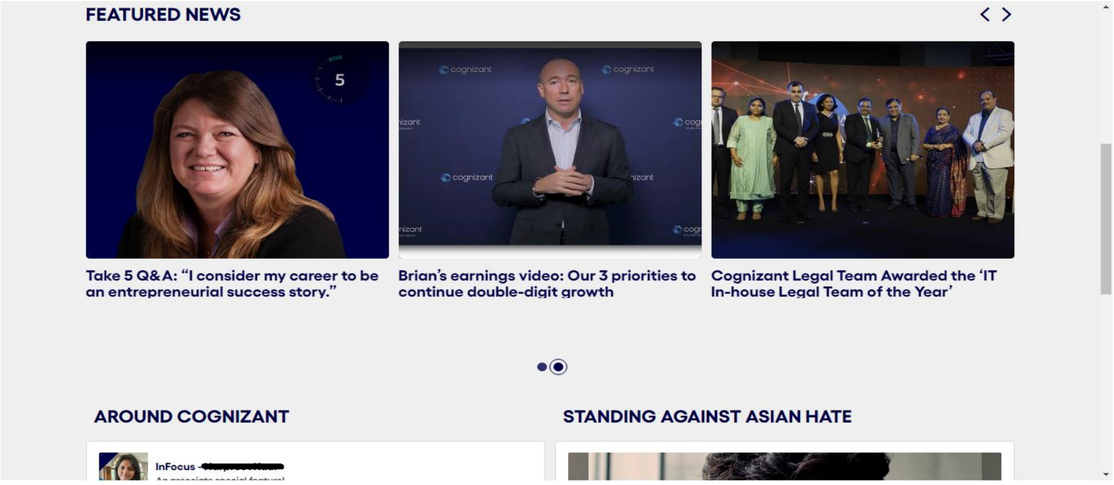


How does Cognizant *actually* work?

Global Delivery Head (P&R) **Ganesh Kalyanaraman** explains it in 60 seconds

Click to watch now

Figure 6. A look into the Be Cognizant portal



FEATURED NEWS

Take 5 Q&A: “I consider my career to be an entrepreneurial success story.”

Brian’s earnings video: Our 3 priorities to continue double-digit growth

Cognizant Legal Team Awarded the ‘IT In-house Legal Team of the Year’

AROUND COGNIZANT

STANDING AGAINST ASIAN HATE

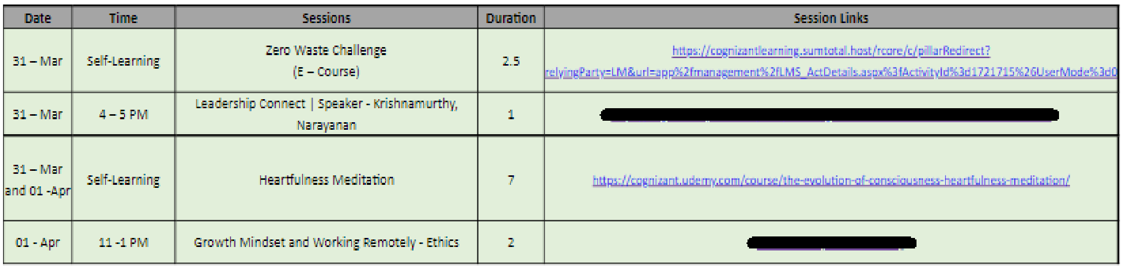
Figure 7. Be Cognizant provides latest updates on news happening around the Organization

CHAPTER – 2

INTERNSHIP PROGRAM SEQUENCE

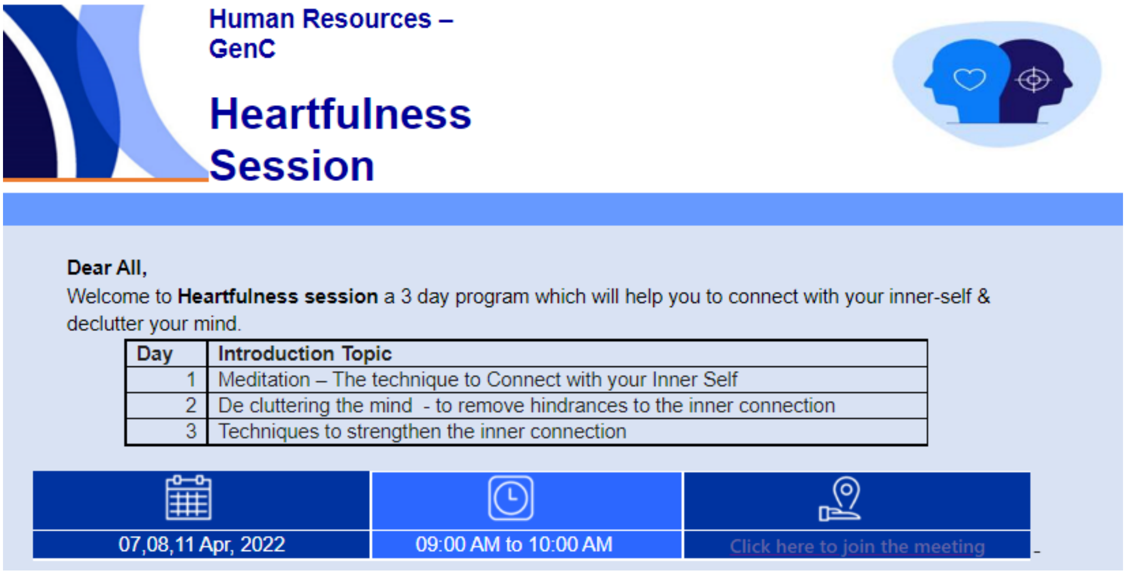
2.1 Pre-Domain Assignment

The pre-domain assignment refers to the period before the actual BU training started and it lasted from 30th March 2022 to 15th April 2022. During this period, corporate induction took place, along with ice breaking session between the new interns. Along with this, academic courses related to JDBC and Java were assigned for corporate training. Heartfulness sessions were conducted to keep mind and body agile with the corporate pressure which builds with time. Leaders connect and Ethical policy connects were conducted from the HR team.



Date	Time	Sessions	Duration	Session Links
31 – Mar	Self-Learning	Zero Waste Challenge (E – Course)	2.5	https://cognizantlearning.sumtotal.host/rcore/c/pillarRedirect?relyingParty=LM&url=app%2fmanagement%2fLMS_ActDetails.aspx%3fActivityId%3d1721715%26UserMode%3d0
31 – Mar	4 – 5 PM	Leadership Connect | Speaker - Krishnamurthy, Narayanan	1	[redacted]
31 – Mar and 01 -Apr	Self-Learning	Heartfulness Meditation	7	https://cognizant.udemy.com/course/the-evolution-of-consciousness-heartfulness-meditation/
01 - Apr	11 -1 PM	Growth Mindset and Working Remotely - Ethics	2	[redacted]

Figure 8. HR Connect Sessions and Self Learning.



Human Resources – GenC

Heartfulness Session

Dear All,
Welcome to **Heartfulness session** a 3 day program which will help you to connect with your inner-self & declutter your mind.

Day	Introduction Topic
1	Meditation – The technique to Connect with your Inner Self
2	De cluttering the mind - to remove hindrances to the inner connection
3	Techniques to strengthen the inner connection

07,08,11 Apr, 2022

09:00 AM to 10:00 AM

Click here to join the meeting

Figure 9. Heartfulness Session Invite

Cognizant takes corporate security very seriously. Cognizant's Ethics & Compliance program enables global business success by promoting an ethical culture, protecting the company from harm, ensuring customer confidence, reducing uncertainty in business decisions and guarding the company's reputation. Cognizant's Code of Ethics outlines expectations of all its associates to act with integrity and uphold an ethical company culture. Cognizant's Global Policies and Procedures provide further, specific guidance regarding how to protect associate's own privacy, and their usage of company assets in a responsible way, avoid conflicts of interest, and more.

2.1.1 Workplace and Ethical Courses

2.1.1.1 Zero Waste in 30

This course talks about the journey for each one of us to start transitioning to a zero-waste lifestyle. It provides realistic and feasible zero waste changes that can be made at a personal level to help the communities around us transition to a healthier one. The course, through the many forms of learning like articles, real-life examples, video tutorials, experts' opinion, etc. allows to make informed choices, set realistic goals and make tangible differences on a broader global scale as well. The estimated course duration is about 2 hours 30 minutes.

2.1.1.2 Meditation and the Evolution of Consciousness

Heartfulness meditation brings a simple and effective way to integrate meditation into day-to-day lifestyle. Across the globe millions of people have experienced the benefits of Heartfulness Meditation. The four basic techniques taught in this practice are:

- Relaxation
- Meditation
- Cleaning
- Prayer

These techniques will help to relax, focus, rejuvenate, reduce stress and change through meditation. This course is designed to be a practical and experiential session. This course on meditation starts with a simple and easy relaxation technique. There are guided meditation sessions to experience yogic transmission. The course will also talk about Cleaning which is a most vital element of the practice. Through Cleaning, one can get rid of all the complexities and impurities gathered in the system. The estimated duration of the course is approximate 7 hours.

2.1.1.3 Java Database Connection: JDBC and MySQL

In this course, connection to a MySQL database using Java JDBC was explained. The course starts with an overview of the JDBC API, then the setup of the development environment with the appropriate MySQL database drivers takes place. Next the course shows how to submit a SQL query and process the result set along with SQL insert, updates and deletes queries which are revised. The course moves on to further advanced topics such as Prepared Statements to handle SQL parameters. Calling out stored procedures using various parameter types (IN, INOUT, OUT and ResultSet) along with processing large data types such as BLOBs and CLOBs. Finally, the course wraps up with a section on reading database connection information from a configuration file. The estimated time for completion of this course if 1 hours 30 minutes.

2.1.1.4 Data Security

Associates at Cognizant live up to their responsibilities. Their commitment to doing business ethically includes respecting privacy, protecting information, and safeguarding assets. The volume of information that the business at Cognizant receives, creates, and stores is significant and increasing. With the increase in ransomware attacks, phishing attempts, and data protection regulations, Cognizant has been refreshing and strengthening its approach to security. A key component to that is better data privacy and management across the company. Using better passwords for accounts, transferring confidential documents through one drive, not clicking on unrecognizable emails, reporting unrecognizable mails if it is suspicious. Recognizing potential malware emails, documents, messages.

2.1.1.5 Code of Ethics and Acceptable Use

This course familiarizes with Cognizant's updated Code of Ethics and key global corporate policies (such as Acceptable Use Policy, Anti-Corruption Policy, Conflicts of Interest Policy, Global Privacy Policy, and Record Retention Policy) and procedures, and considers the responsibilities of each associate have to act in ways that promote an ethical culture of mutual trust and respect, recognize and address risks to the company, and advance the business goals the right way. Acceptable Use Policy means that each associate has to bear with the privileges given to them only. Conflicts of Interest Policies limit each Associate to act as a double agent within the company or at client site. Global Privacy Policy establishes the sense of trust between the company and associates or between associates and clients all over the globe with private information.

2.1.1.6 Prevention of Sexual Harassment at Workplace (India)

This course familiarizes associates in India with forms of sexual harassment, protections, and redress procedures under the Prevention, Prohibition and Redressal Act (POSH Act).

2.2 Domain Specific Training

The week after the pre domain training i.e., from 18th April 2022 to 22nd April 2022, was a buffer week with tower mapping (sub domain allocation) and introduction to the mentors. Mentors are assigned BU specialist who are responsible to guide the mentees into the particular BU based on the LP. Being assigned the ITM tower sub domain, learning path was enabled form 25th of April 2022 and week 1 starts from 25th April 2022 as well. The first mentor connect was to established a healthy working relationship between the mentors and mentees. Accordingly, the LP access was enabled following the mentor connect. The ITM LP follows with milestones in week 7 and week 11 as explained in the figure with a Business Aligned Project.

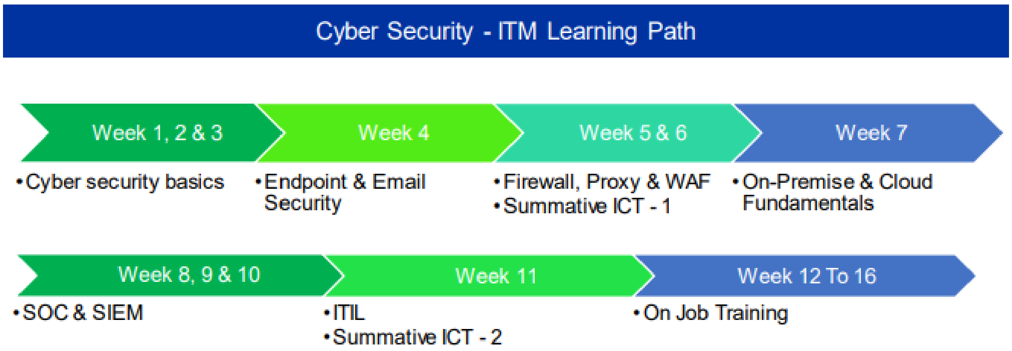


Figure 10. ITM Learning Path (LP) flowchart.

Cognizant has collaborated with Udemy to provide world class learning videos for the evolving future of work. These Udemy programs are woven in the learning path, empowering the interns to plan and learn at their pace and style. The program also connects the interns with Subject Matter Experts to get the professional guidance on their queries in the learning journey. The program continuously evaluates if interns are able to apply those self-learnt skills to solve a business problem through ICTs, Assessments, Hands on Challenges, etc. The LP platform gives a clearer picture about the performance of the interns. The LP guides through various weeks of training.

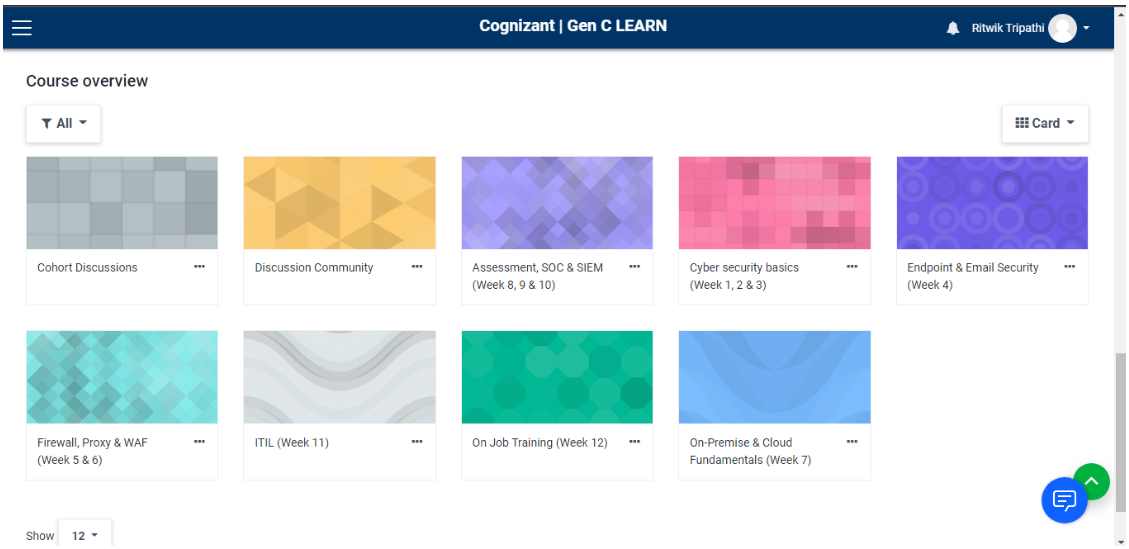

Cognizant | Gen C LEARN
Ritwik Tripathi
Course overview
All
Card
Cohort Discussions
Discussion Community
Assessment, SOC & SIEM (Week 8, 9 & 10)
Cyber security basics (Week 1, 2 & 3)
Endpoint & Email Security (Week 4)
Firewall, Proxy & WAF (Week 5 & 6)
ITIL (Week 11)
On Job Training (Week 12)
On-Premise & Cloud Fundamentals (Week 7)
Show
12

Figure 11. The LP overview

Week 1 to Week 3 consisted of three self-paced learning courses. Weeks from Week 4 to Week 11 have a guided curriculum consisting of mentor sessions and mentor suggested courses. The courses are spread across two platforms, namely, Udemy and Cybrary. Cognizant provides unlimited enterprise access to both these course platforms on a specific condition. The specific condition for Udemy is to complete at least one course per month and for Cybrary is to complete at least 10 hours of learning per month. If any associate fails to do so, privileges to both the course portals will be revoked. These courses provide the general ideology of what the associates will be working with in the future. As the internship is in offline mode, hands on each of the tools was not possible as software legitimate rights for usage of official data on personal computers is prohibited by Cognizant due to its Data Protection Policy. Practice activities related to most of the work is carried out on Cisco Packet Tracer. To this date, the internship progresses in Week 6. So, all the work carried out till Week 5 is briefly mentioned into this report.

2.2.1 Cybersecurity Basics (Week 1, Week 2 and Week 3)

Week 1, 2 and 3 consisted of three self-paced learning courses, one of them mostly theoretical teaching the basis of cybersecurity. The other two courses provided hands on experience on some of the essential topics.

2.2.1.1 CompTIA Security Plus (SY0-601) Course

CompTIA Security+ is an essential certification for beginners. It covers up the basis of cybersecurity fundamentals including the following

- Attacks, Vulnerabilities, Threats
- Security Architecture and Security Design Principles
- Security Implementation Techniques
- Security Operations and Incident Response Methodology
- Governance, Risk and Compliance

The course is the complete guide for taking up the CompTIA Security+ Certification exam. It starts with the basic CIA triad in security methodology and adds up Authentication, Authorization and Non-Repudiation with this methodology as well. All six together make up the basic building blocks of cybersecurity. The contents of this course include

- Identity Management
- End User Management
- Access Control Models and their comparison of different models.
- Network Technologies and their Security principles
- Types of Attacks (Network, Password, Code, Web Servers, Social Engineering)
- Understanding Vulnerabilities of different devices
- Data and Database Security
- AAA
- SPOF
- Cryptography and PKI
- Email, Web and Webserver Security

- Risk Mitigation Techniques

The course accumulated of a total of 18 hours.

2.2.1.2 Introduction to Computer Networks for Non-Techies

A role as a cybersecurity engineer will only be beneficial if what needs to be protected is known. Network security is an important element in cybersecurity. This course is a step-by-step guide towards understanding the rudiments of Computer Networks. Computer network is the interconnection between two or more computers communicating each other to either send or receive resources or both. A network is composed of two main aspects; Physical and Logical. The interconnection of computers on any network is bounded by some set of rules known as protocols, HTTPS, FTP, SMTP, TCP, IP, UDP, DHCP to name some. The contents of this course include

- Network Topologies and Networking Devices
- OSI Model and TCP/IP Model
- VLAN
- IPv4 Addressing / Subnetting
- Classful and Classless Addressing
- DNS Fundamentals
- Hands on activities on Cisco Packet Tracer

The course accumulated of a total of 18 hours. Seven hands-on activities were included into the course namely creating a simple home LAN, Static IP configuration, Subnetting two LANs, Dynamic IP configuration using DHCP server, DNS and Web Server Configuration, VLAN configuration and Router configuration using RIP. Hands-on activities are mentioned into this report.

- **Creating a Simple Home LAN**

  This activity was based on connect a bunch of different devices together into a basic home local area network. This LAN consists of a PC, a Laptop, a File Server, a Network Printer, a Tablet and a Smartphone. All these devices are connected to the LAN with different connecting mediums. For example, the tablet and smartphone are connected to the wireless router.

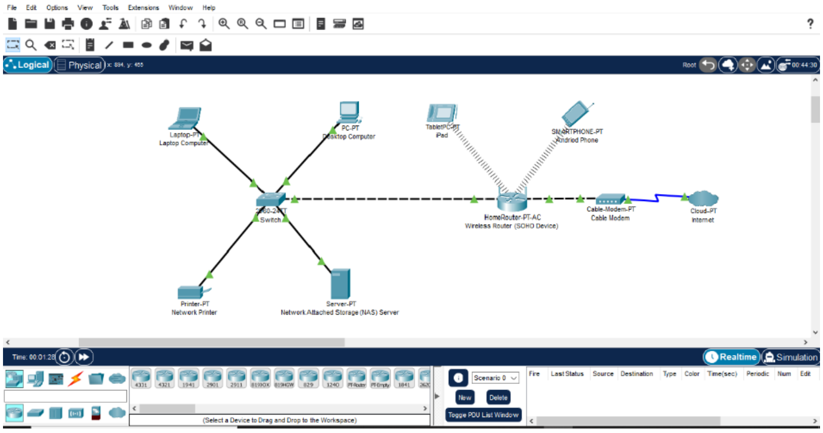
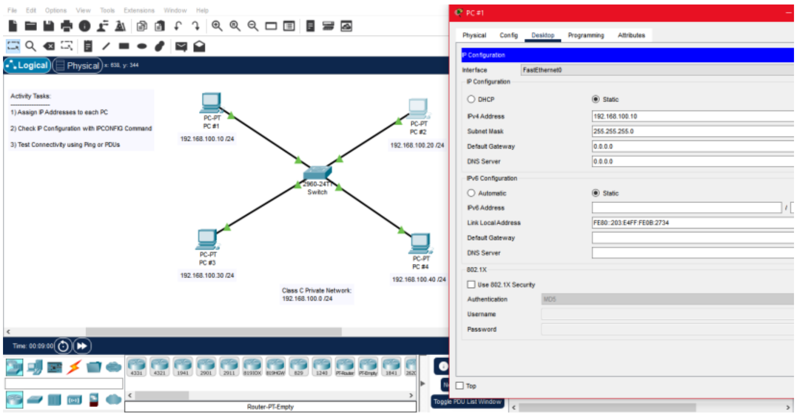


Figure 12. Creating a Simple Home LAN

- **Static IP Configuration**

  This activity was to configure a LAN with static IP address to all the PCs in it for a given public IP address. Further, checking each PC IP with the ipconfig command and at last check the connection either using ping command or by PDU packets.


Activity Tasks:

1) Assign IP Addresses to each PC

2) Check IP Configuration with IPCONFIG Command

3) Test Connectivity using Ping or PDUs

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.100.10

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address:

Link Local Address: FE80::203:E4FF:FE0B:2734

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

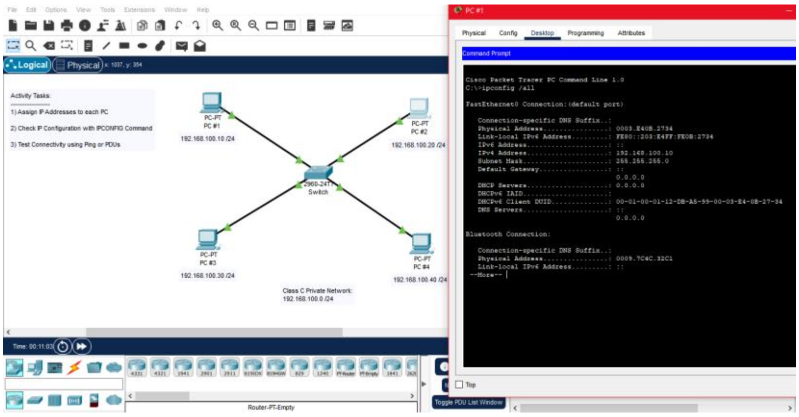
Authentication: MD5

Username:

Password:

□ Top

Figure 13. Static IP Configuration for PC#1

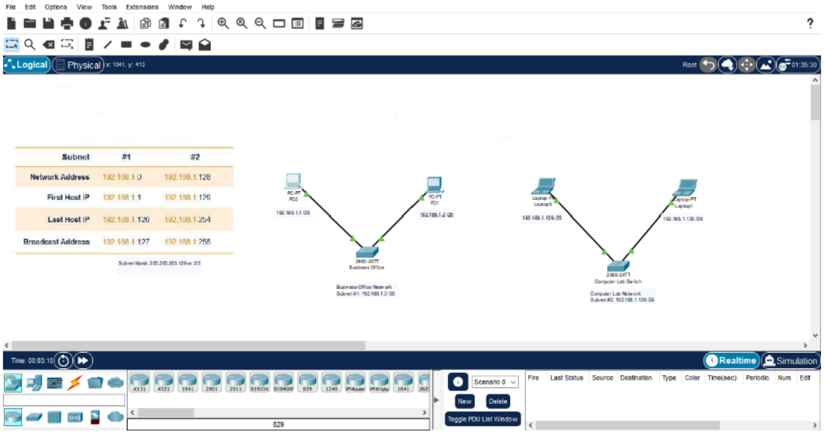


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0003.E40B.2734
   Link-local IPv6 Address.........: FE80::203:E4FF:FE0B:2734
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.100.10
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-12-DB-A5-55-00-03-E4-0B-27-34
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0009.7C4C.32C1
   Link-local IPv6 Address.........: ::
 --More--
```

Figure 14. ipconfig /all command to check IP configuration for PC#1

- **Subnetting two LANs**

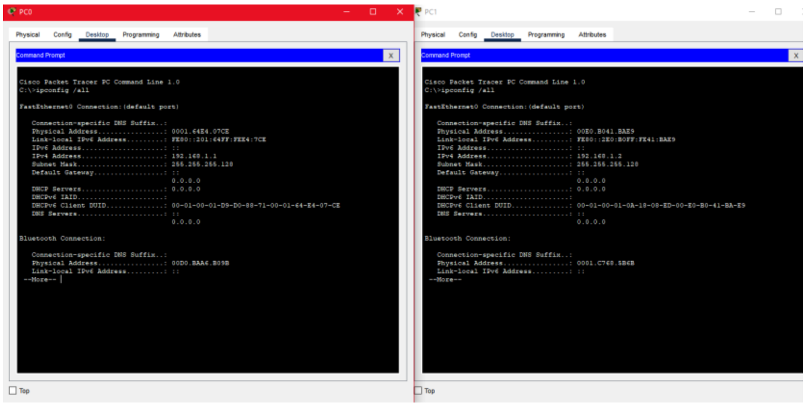
  In this activity, subnetting of a network address into two separate LANs. A network address was given which was needed to form two subnets. Since, the number of host bits needed to form 2 subnets is 1, therefore number of host IP addresses available are $2^7 - 2 = 126$ (two subtracted, one each for network address and broadcast address). The IP configuration was static.



Subnet	#1	#2
Network Address	192.168.1.0	192.168.1.128
First Host IP	192.168.1.1	192.168.1.129
Last Host IP	192.168.1.126	192.168.1.254
Broadcast Address	192.168.1.127	192.168.1.255

Subnet Mask: 255.255.255.128 or /25

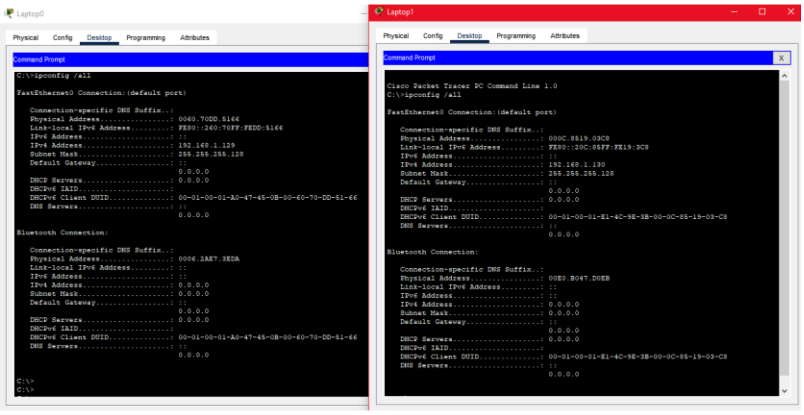
Figure 15. Subnetting two LANs



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0001.64E4.07CE
   Link-local IPv6 Address.........: FE80::201:64FF:FEE4:7CE
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.1
   Subnet Mask.....................: 255.255.255.128
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-D9-D0-88-71-00-01-64-E4-07-CE
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 00D0.BAA6.B09B
   Link-local IPv6 Address.........: ::
 --More--
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 00E0.B041.BAE9
   Link-local IPv6 Address.........: FE80::2E0:B0FF:FE41:BAE9
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.2
   Subnet Mask.....................: 255.255.255.128
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-0A-18-08-ED-00-E0-B0-41-BA-E9
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0001.C768.5B6B
   Link-local IPv6 Address.........: ::
 --More--
```

Figure 16. Subnetting the two PCs in Business Office Network



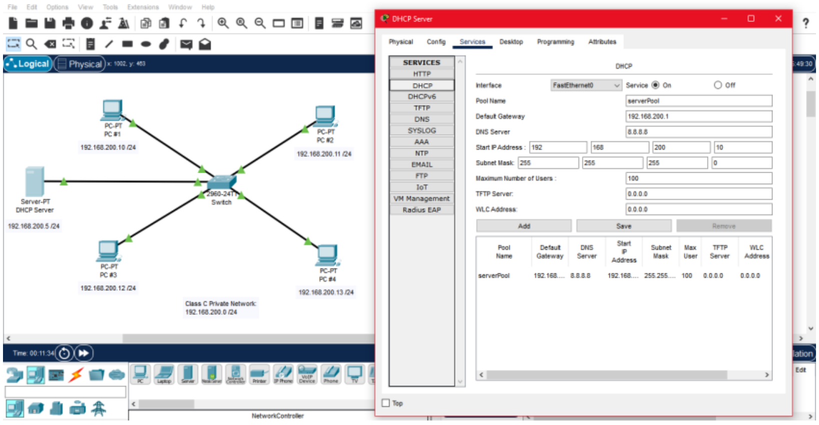
```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0060.70DD.5166
   Link-local IPv6 Address.........: FE80::260:70FF:FEDD:5166
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.129
   Subnet Mask.....................: 255.255.255.128
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-A0-47-45-0B-00-60-70-DD-51-66
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0006.2AE7.3EDA
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-A0-47-45-0B-00-60-70-DD-51-66
   DNS Servers.....................: ::
                                     0.0.0.0


C:\>
C:\>
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 000C.8519.03C8
   Link-local IPv6 Address.........: FE80::20C:85FF:FE19:3C8
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.130
   Subnet Mask.....................: 255.255.255.128
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-E1-4C-9E-3B-00-0C-85-19-03-C8
   DNS Servers.....................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 00E0.B047.D0EB
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-E1-4C-9E-3B-00-0C-85-19-03-C8
   DNS Servers.....................: ::
                                     0.0.0.0
```

Figure 17. Subnetting the two Laptops in Computer Lab Network

- **Dynamic IP configuration using DHCP server**

  In this activity, a server is used to configure IP for the LAN devices dynamically. A network consisting of four PCs connected to a switch is constructed and a server is connected to the switch completing the LAN and a network address is provided. The server is assigned a default gateway address along with DNS Server address. DHCP service is started for assigning IP addresses dynamically for up to 100 devices in the network.



DHCP Server

DHCP

Interface: FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 192.168.200.1

DNS Server: 8.8.8.8

Start IP Address: 192 168 200 10

Subnet Mask: 255 255 255 0

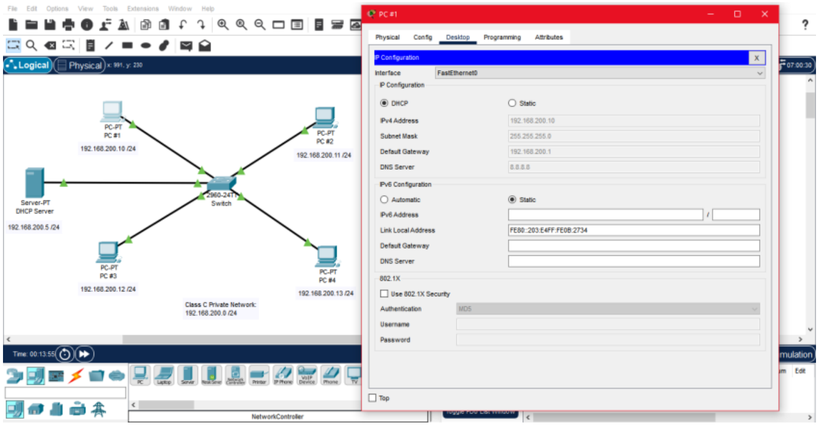
Maximum Number of Users: 100

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168....	8.8.8.8	192.168....	255.255....	100	0.0.0.0	0.0.0.0

Figure 18. Dynamic IP configuration using DHCP server.



PC #1

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.200.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.200.1

DNS Server: 8.8.8.8

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::203:E4FF:FE0B:2734

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

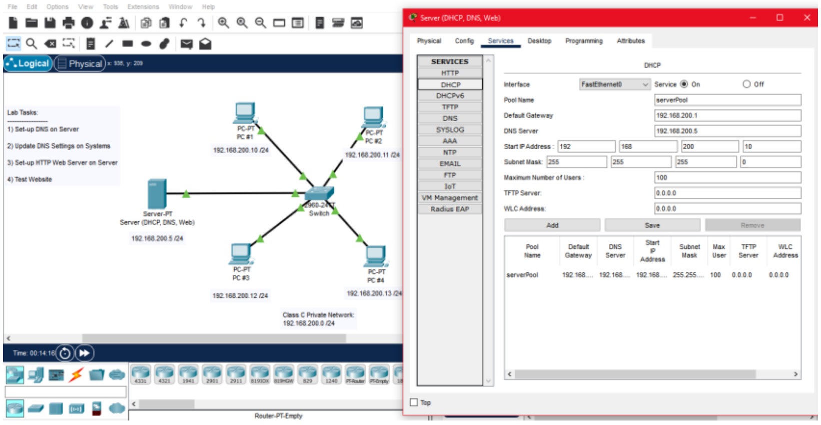
Username:

Password:

Figure 19. DHCP IP configuration on PC#1. Similarly for all other PCs.

- **DNS and Web Server Configuration**

  In this activity, the previous LAN setup is updated and the DHCP server acts as DHCP, DNS and Web server. While setting up the DNS server, the DNS server address is changed and subsequently, IP configuration on all the PCs is renewed by using the ipconfig /renew in command prompt. After this configure the DNS service by entering the website name as a record and assigning it the IP address of the DHCP / DNS / Web server. Start the DNS service and turn off the HTTPS option in the HTTP services.


Logical
Physical
Lab Tasks:
1) Set-up DNS on Server
2) Update DNS Settings on Systems
3) Set-up HTTP Web Server on Server
4) Test Website
PC-PT PC #1 192.168.200.10 /24
PC-PT PC #2 192.168.200.11 /24
Server-PT Server (DHCP, DNS, Web) 192.168.200.5 /24
2960-24TT Switch
PC-PT PC #3 192.168.200.12 /24
PC-PT PC #4 192.168.200.13 /24
Class C Private Network: 192.168.200.0 /24
Server (DHCP, DNS, Web)
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
Add
Save
Remove

DHCP

Interface FastEthernet0 Service ● On ○ Off

Pool Name: serverPool

Default Gateway: 192.168.200.1

DNS Server: 192.168.200.5

Start IP Address: 192 168 200 10

Subnet Mask: 255 255 255 0

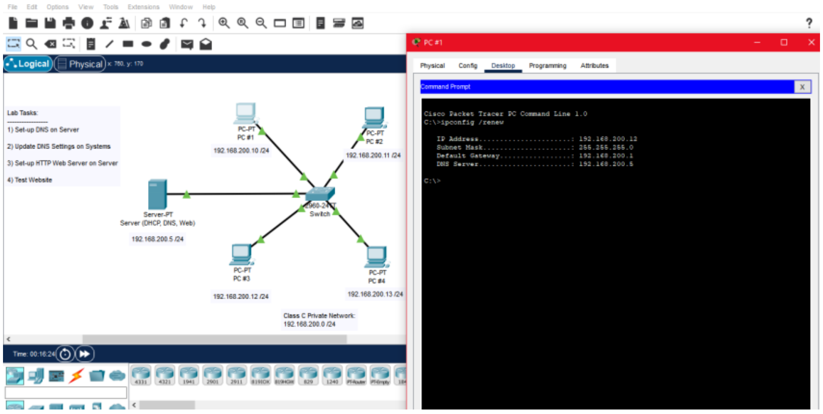
Maximum Number of Users: 100

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

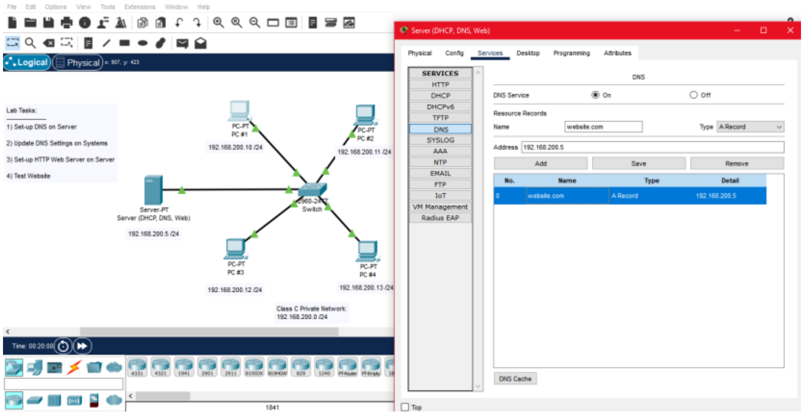
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168....	192.168....	192.168....	255.255....	100	0.0.0.0	0.0.0.0

Figure 20. Assigning the DNS Server


Logical
Physical
Lab Tasks:
1) Set-up DNS on Server
2) Update DNS Settings on Systems
3) Set-up HTTP Web Server on Server
4) Test Website
PC-PT PC #1 192.168.200.10 /24
PC-PT PC #2 192.168.200.11 /24
Server-PT Server (DHCP, DNS, Web) 192.168.200.5 /24
2960-24TT Switch
PC-PT PC #3 192.168.200.12 /24
PC-PT PC #4 192.168.200.13 /24
Class C Private Network: 192.168.200.0 /24
PC #1
Physical
Config
Desktop
Programming
Attributes
Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /renew

   IP Address......................: 192.168.200.12
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.200.1
   DNS Server......................: 192.168.200.5

C:\>
```

Figure 21. ipconfig /renew command to refresh the DNS server on PC#1.


Logical
Physical
Lab Tasks:
1) Set-up DNS on Server
2) Update DNS Settings on Systems
3) Set-up HTTP Web Server on Server
4) Test Website
PC-PT PC #1 192.168.200.10 /24
PC-PT PC #2 192.168.200.11 /24
Server-PT Server (DHCP, DNS, Web) 192.168.200.5 /24
2960-24TT Switch
PC-PT PC #3 192.168.200.12 /24
PC-PT PC #4 192.168.200.13 /24
Class C Private Network: 192.168.200.0 /24
Server (DHCP, DNS, Web)
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
Add
Save
Remove
DNS Cache

DNS

DNS Service ● On ○ Off

Resource Records

Name: website.com Type: A Record

Address: 192.168.200.5

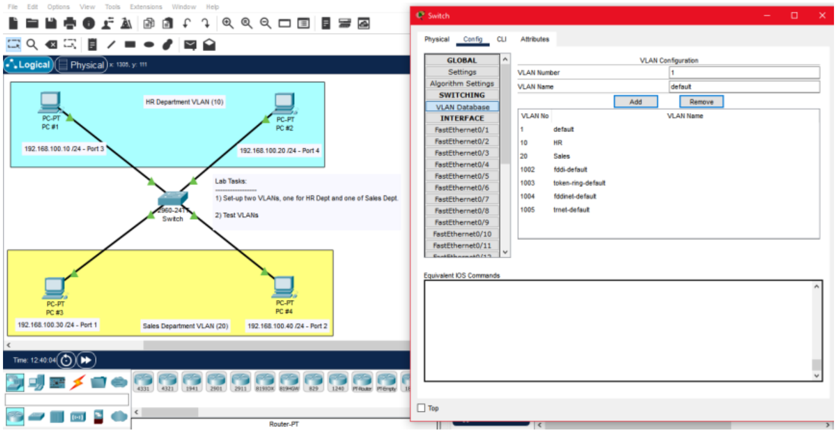
No.	Name	Type	Detail
0	website.com	A Record	192.168.200.5

Figure 22. Assigning the website address in the DNS service.

- **VLAN configuration**

  VLAN stands for Virtual LAN. VLAN is a LAN within a LAN. It is used to break up a large physical LAN into smaller logical

LANs. For example, for a university with different departments (CSE, IT, ECE, Mechanical, ECE, Accounts, Academics, etc.), purchasing different LANs for each department will be very costly and will further increase the managing cost as well. Managed switches can be used to create VLANs. It is possible by assigning specific switch interfaces to specific VLANs. VLANs are separated from each other. No flow of information can be done from one VLAN to another VLAN. In this activity, two VLANs are set up to segregate the HR department and Sales department. Addresses are assigned to the PCs connected to a managed switch. Managed switches contain a VLAN database in which VLAN numbers are assigned. Further each port connected to the switch from the PC is identified and VLAN a number is assigned to them. With this, the interconnection between VLANs is not possible but within a VLAN is possible.



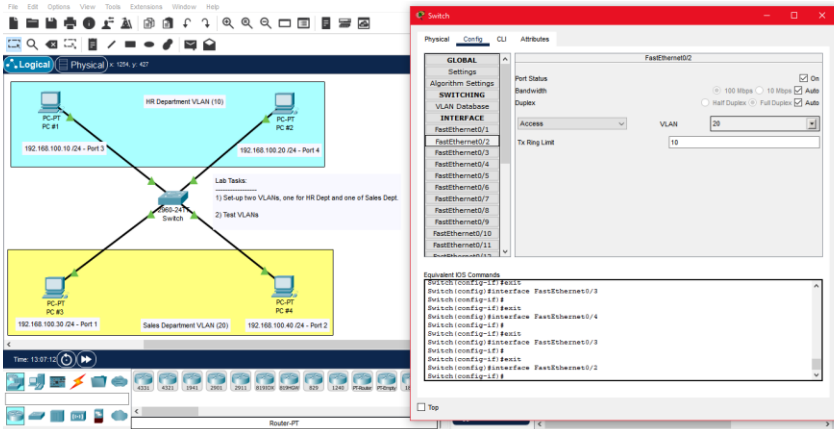
VLAN Configuration

VLAN Number: 1

VLAN Name: default

VLAN No	VLAN Name
1	default
10	HR
20	Sales
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default

Figure 23. Assigning VLAN numbers in the VLAN database of the switch.



FastEthernet0/2

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

Access VLAN 20

Tx Ring Limit 10

Equivalent IOS Commands

```
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/4
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/3
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#
```

Figure 24. Assigning the ports with appropriate VLAN numbers.

- **Router configuration using RIP**

  Routers form up the interconnection between two different networks. The configuration of routers is done to make sure that these devices know how to communicate with each other. RIP is a method used to configure routers. In this method, each router is provided with the addresses of the other routers with whom they need to connect. There can be various ways through which information is transferred from one router to another. It can be done either directly or through a number of routers, in each case being guided by a set of protocols e.g., Link-State Routing Protocol, Routing Information Protocol, etc.

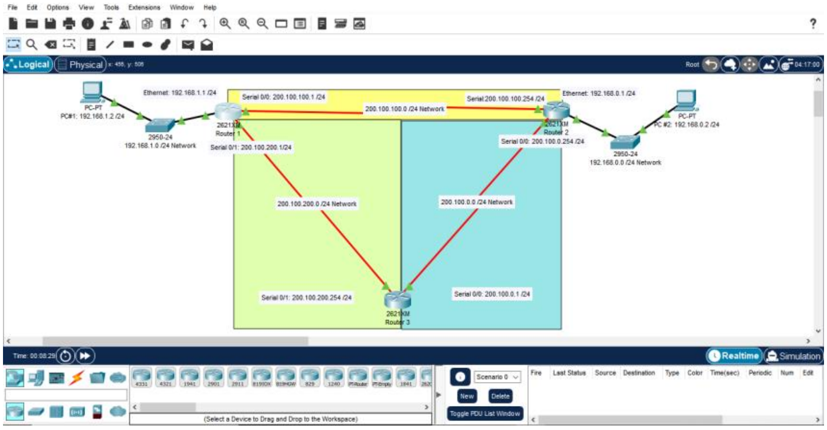
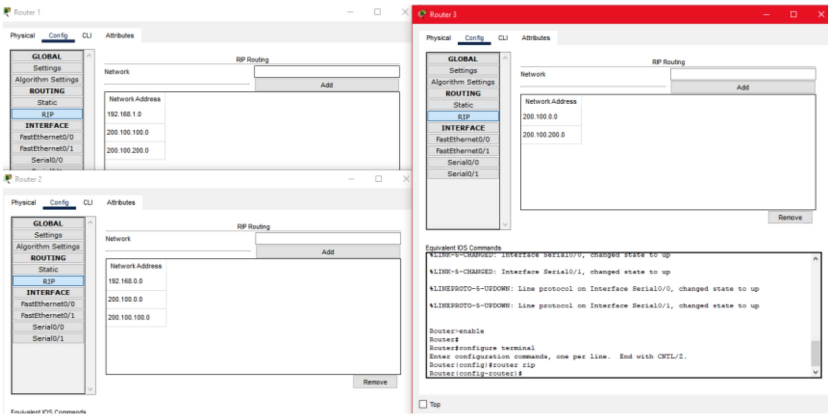

File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 456, y: 506
Root
04:17:00
PC-PT
PC#1: 192.168.1.2 /24
2950-24
192.168.1.0 /24 Network
Ethernet: 192.168.1.1 /24
2621XM
Router 1
Serial 0/0: 200.100.100.1 /24
Serial 0/1: 200.100.200.1/24
200.100.100.0 /24 Network
Serial 200.100.100.254 /24
Ethernet: 192.168.0.1 /24
2621XM
Router 2
Serial 0/0: 200.100.0.254 /24
PC-PT
PC #2: 192.168.0.2 /24
2950-24
192.168.0.0 /24 Network
200.100.200.0 /24 Network
200.100.0.0 /24 Network
Serial 0/1: 200.100.200.254 /24
Serial 0/0: 200.100.0.1 /24
2621XM
Router 3
Time: 00:08:29
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit
(Select a Device to Drag and Drop to the Workspace)

Figure 25. A simple network connection consisting of three routers



Router 1 — RIP Routing

Network

Network Address
192.168.1.0
200.100.100.0
200.100.200.0

Router 2 — RIP Routing

Network

Network Address
192.168.0.0
200.100.0.0
200.100.100.0

Router 3 — RIP Routing

Network

Network Address
200.100.0.0
200.100.200.0

Equivalent IOS Commands

```
%LINK-5-CHANGED: Interface Serial0/0, changed state to up

%LINK-5-CHANGED: Interface Serial0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to up


Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
```

Equivalent IOS Commands

Figure 26. RIP configuration on the three routers

2.2.1.3 Cisco CyberOps Associate CBROPS 200-201: Part 1

Cisco is one of the leading companies when it comes to network operations and security. Cisco has not only limited its research to form a safer network environment for its users but is also known to provide the upcoming generations with logistics such as Cisco Packet Tracer, Cisco Network Academy, etc. The CBROPS 200-201 is a certification examination launched by Cisco which has received the United States Department of Defence (DoD) approval for the DoD 8570.01-M for the CSSP Analyst and CCSP Incident Responder categories. This course focuses on four aspects of network security namely, basic network concepts, security concepts, security monitoring and host-based analysis. Basic network concepts in this course included the following:

- Network Fundamentals
- Network Protocols
- Network Devices
- IPS and AMP

Security included the following concepts in this course:

- CIA triad
- Defense in Depth
- Vulnerabilities
- Exploit
- AAA
- Zero Trust
- Access Control Methods
- 5-tuple rule

Security monitoring included the following concepts in this course:

- Network Attacks
- Web Application Attacks
- Endpoint Attacks
- Social Engineering
- Evasion methods
- Packet Captures
- Monitoring Challenges
- Basics of Encryption and Hashing
- PKI

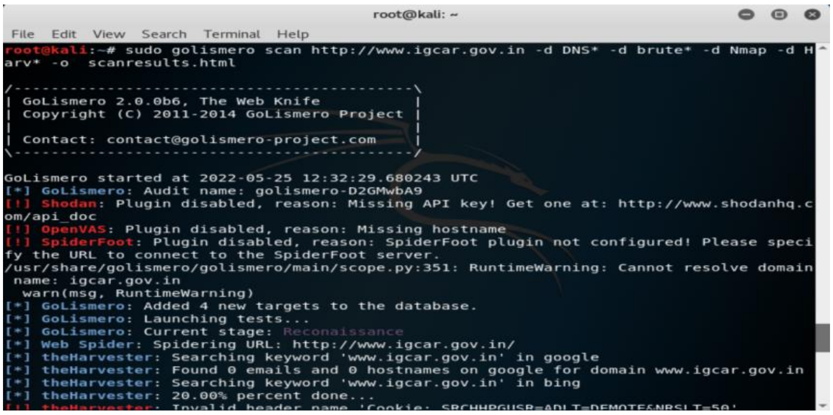
Host-based analysis included the following concepts in this course:

- Basic Windows and Linux commands
- Endpoint Protection
- Whitelisting and Blacklisting
- Systems-Based Sandboxing
- System Logs
- Evidence and Attribution.

Apart from the learnings in this course there were two hands on activities based on Kali Linux tools to better understand some of these concepts.

- **Golismero**

  Golismero is a vulnerability analysis tool which scans websites for vulnerabilities. Golismero has many keywords, scan, -d, -o, Harv*, DNS*, Nmap*, to name a few. It is a carving script which carves the data like host IP, host name, port number, email associated, etc. which can be used to find out any weak points or vulnerabilities into the system. A simple Golismero command is initiated into the terminal by using the keyword scan with the website name. The example command in the figure below is; sudo golismero scan http://www.igcar.gov.in -d DNS* -d brute* -d Nmap -d Harv* -o scanresults.html. In the above example command -d means deduct, DNS* means all DNS servers, brute* means all brute force attacks, Harv* means all Harvesting attacks. -o is for generating an output file.

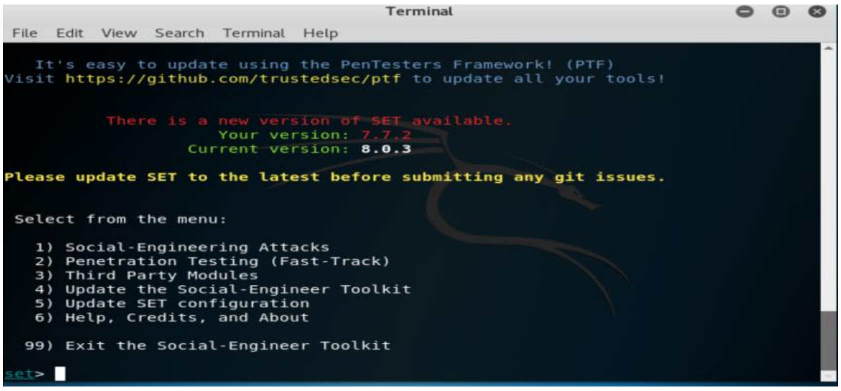


```
root@kali:~# sudo golismero scan http://www.igcar.gov.in -d DNS* -d brute* -d Nmap -d H
arv* -o  scanresults.html

/-------------------------------------------\
| GoLismero 2.0.0b6, The Web Knife          |
| Copyright (C) 2011-2014 GoLismero Project |
|                                           |
| Contact: contact@golismero-project.com    |
\-------------------------------------------/

GoLismero started at 2022-05-25 12:32:29.680243 UTC
[*] GoLismero: Audit name: golismero-D2GMwbA9
[!] Shodan: Plugin disabled, reason: Missing API key! Get one at: http://www.shodanhq.c
om/api_doc
[!] OpenVAS: Plugin disabled, reason: Missing hostname
[!] SpiderFoot: Plugin disabled, reason: SpiderFoot plugin not configured! Please speci
fy the URL to connect to the SpiderFoot server.
/usr/share/golismero/golismero/main/scope.py:351: RuntimeWarning: Cannot resolve domain
 name: igcar.gov.in
  warn(msg, RuntimeWarning)
[*] GoLismero: Added 4 new targets to the database.
[*] GoLismero: Launching tests...
[*] GoLismero: Current stage: Reconaissance
[*] Web Spider: Spidering URL: http://www.igcar.gov.in/
[*] theHarvester: Searching keyword 'www.igcar.gov.in' in google
[*] theHarvester: Found 0 emails and 0 hostnames on google for domain www.igcar.gov.in
[*] theHarvester: Searching keyword 'www.igcar.gov.in' in bing
[*] theHarvester: 20.00% percent done...
[!] theHarvester: Invalid header name 'Cookie: SRCHHPGUSR=ADLT=DEMOTE&NRSLT=50'
```

Figure 27. Golismero running in the command prompt

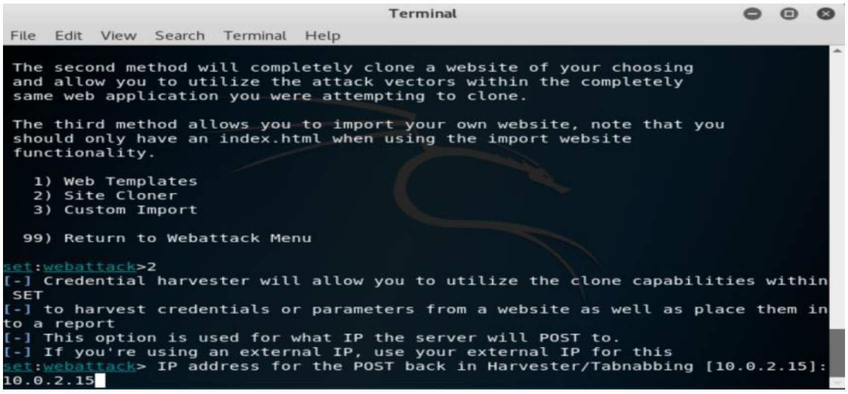
- **Social Engineering Toolkit**

  The social engineering toolkit, SET, is a command interface for visualizing social engineering attacks. A basic social engineering attack is the credential harvesting attack. It can be done by either cloning the website or by using a web template. A credential harvesting attack is only feasible when the target website is an authentication page. Once the website address is written, the SET clones the website.



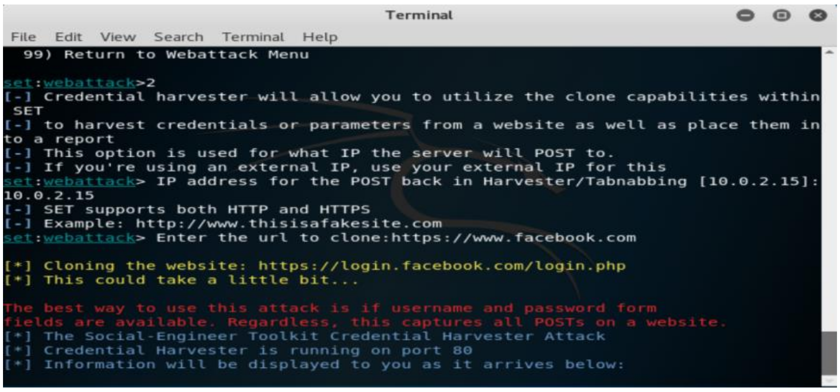
```
   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


          There is a new version of SET available.
                     Your version: 7.7.2
                  Current version: 8.0.3

Please update SET to the latest before submitting any git issues.


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

Figure 28. SET command line



```
 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
 SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
10.0.2.15
```

Figure 29. Entering domain IP address



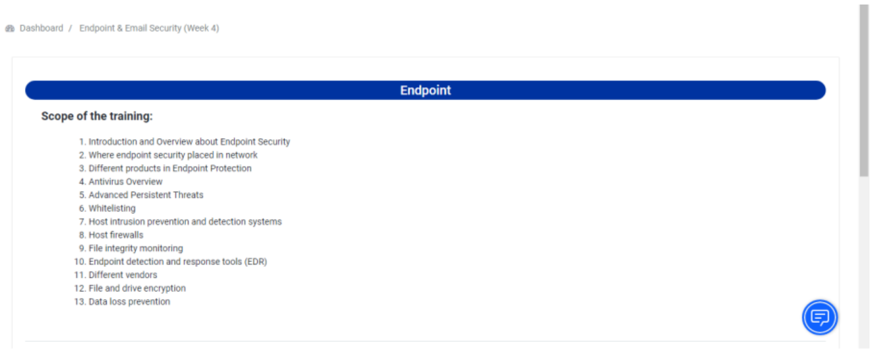
```
  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
 SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
10.0.2.15
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Figure 30. Using https://www.facebook.com as cloned site

2.2.2 Endpoint and Email Security (Week 4)

2.2.2.1 Endpoint Security

Endpoint security, or endpoint protection, is the cybersecurity approach to defending endpoints such as desktops, laptops, and mobile devices from malicious activity. No course was suggested on this topic. Five sessions of one hour each per day were conducted to cover up the topics in the LP.



Endpoint

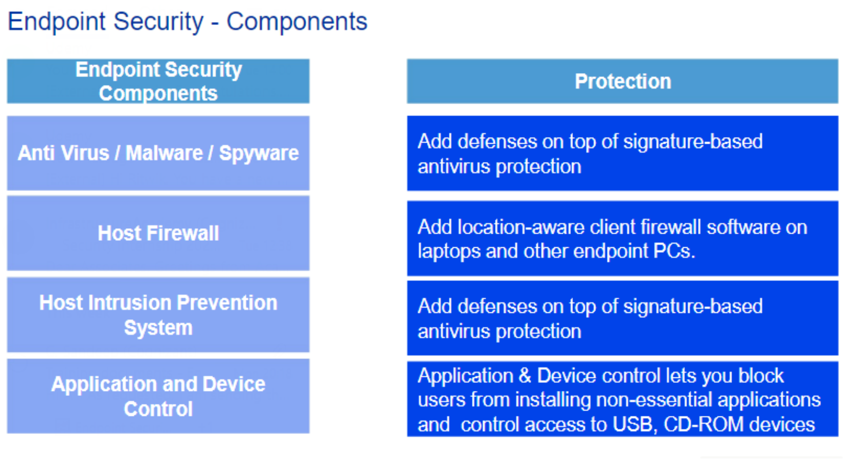
Scope of the training:

1. Introduction and Overview about Endpoint Security
2. Where endpoint security placed in network
3. Different products in Endpoint Protection
4. Antivirus Overview
5. Advanced Persistent Threats
6. Whitelisting
7. Host intrusion prevention and detection systems
8. Host firewalls
9. File integrity monitoring
10. Endpoint detection and response tools (EDR)
11. Different vendors
12. File and drive encryption
13. Data loss prevention

Figure 31. Endpoint Security topics

Traditional endpoint security is reactive and detects potential security threats by matching known signatures and attack patterns. For performance reasons, antivirus vendors try to keep the signature database as small as possible. That’s why many traditional AV vendors’ databases only contain the updates of the latest malware threats. Coping both with the performance and threat detection aspect is challenging using a signature-based detection method. Threat actors can easily adapt the malware code or their techniques to circumvent the malware signatures developed for traditional AV solutions. Some of the traditional AV vendors are Symantec, McAfee, Sophos, etc.

Endpoint security solutions are a combination of four components, Antivirus / Malware / Spyware, Host Firewall, Host IPS, Application and Device Control. Endpoint software are more advanced than traditional AV software. The basic difference between these two is that while traditional AV software filters files based of signature patterns, Endpoint security software filters file based on their behaviour with the use of artificial intelligence. Some of the common endpoint security vendors are Crowdstrike, Microsoft Defender, Kaspersky, Sentinel One, Cisco AMP, etc.

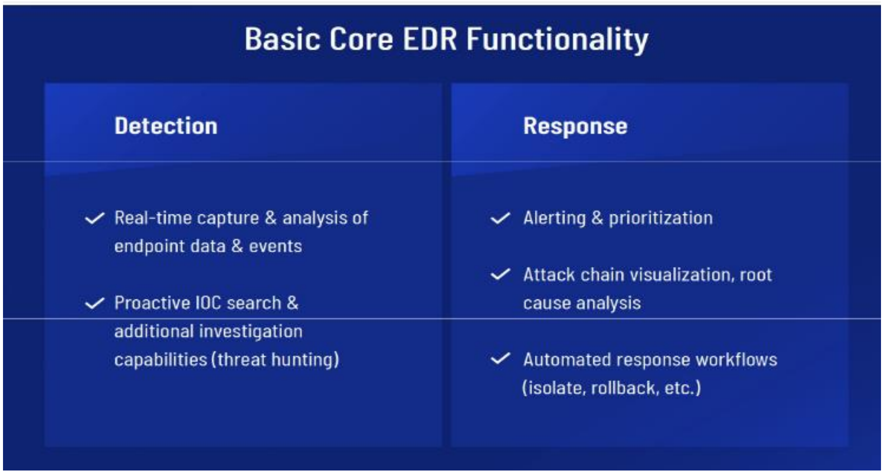


Endpoint Security - Components

Endpoint Security Components	Protection
Anti Virus / Malware / Spyware	Add defenses on top of signature-based antivirus protection
Host Firewall	Add location-aware client firewall software on laptops and other endpoint PCs.
Host Intrusion Prevention System	Add defenses on top of signature-based antivirus protection
Application and Device Control	Application & Device control lets you block users from installing non-essential applications and control access to USB, CD-ROM devices

Figure 32. Components of Endpoint Security

The Endpoint Detection and Response solutions are designed to provide state of the art protection for endpoints. These solutions provide multi-layer, fully integrated endpoint protection. Real-time continuous monitoring is combined with data analytics to detect threats, and automated, rule-driven response enables rapid mitigation of detected threats. The initial goal of an EDR solution is to provide deep visibility into a particular endpoint. This visibility is leveraged by EDR's automated response capabilities for threat mitigation, enables prevention of attacks, and can support proactive threat hunting activities. This transition from traditional, responsive security to proactive threat management is EDR's primary objective. There are five key capabilities of EDR, comprehensive visibility, data collection, behavioural protection, real-time responses, whitelisting and blacklisting. Comprehensive visibility finds the roots of the malware detected in the endpoint and reports back. Data collection refers to the collection of malware data from endpoints. Behavioural protection refers to the detection and termination of any malware process or file not on the basis of signatures but on the basis of behaviour. With EDR, real-time responses are generated based on the detection and further mitigation of the detected intrusion or malware. EDRs are capable of whitelisting and blacklisting host firewall to make internet browsing safer. The basic core EDR functionality is to detect and respond to any intrusion made onto the endpoint.



Basic Core EDR Functionality

Detection

- ✓ Real-time capture & analysis of endpoint data & events
- ✓ Proactive IOC search & additional investigation capabilities (threat hunting)

Response

- ✓ Alerting & prioritization
- ✓ Attack chain visualization, root cause analysis
- ✓ Automated response workflows (isolate, rollback, etc.)

Figure 33. Basic Code EDR Functionality

Some of the top EDR vendors are Crowdstrike, Sentinel One, Carbon Black, Cisco, FireEye, etc. The EDR works with a six-step process. Step one is to install an EDR agent onto the endpoint. Next, the EDR performs behavioural analysis to collect information about the endpoint and categorises them based on the level of criticality. It further detects and reports any malicious activities. Through algorithms, it identifies the breach points into the endpoint. Each of the data points are categorised narrowly. The reported data is analysed by agent analyst and review alerts and information regarding any threats against the end point is generated and reverted back.

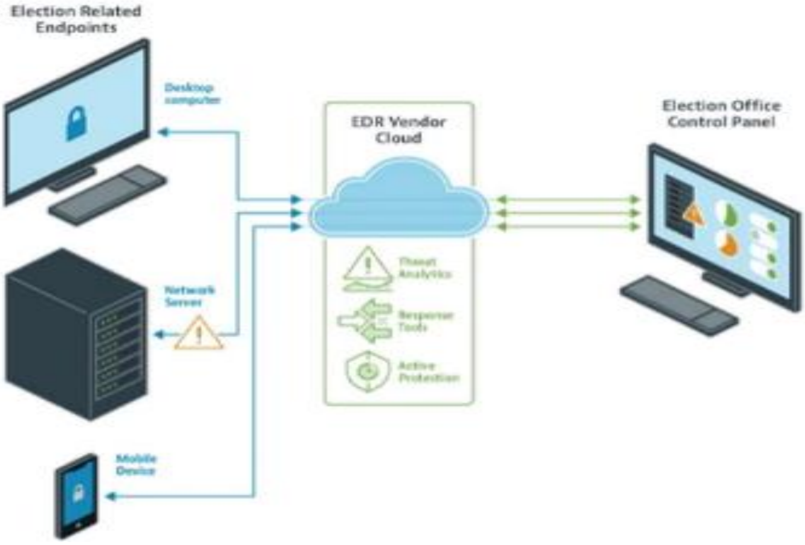


Figure 34. Most of the EDR vendors monitor endpoint data through cloud.

MDR stands for managed detection and response. MDR is a service that continuously monitors, prioritizes, and responds to cybersecurity threats with humans behind the wheel. MDR is augmented with EDR solutions by empowering analysts with data and abilities to act on the endpoint. These actions can range from gathering data to better prioritize threats, like getting running services, applications, users logged in, local files, etc., to containment actions like quarantines, shutting down services, etc. Cognizant's Cyber Threat Defence with MDR (Cisco Secure Endpoint) services helps bridge the gap by delivering advanced detection and response as a service, thereby removing the complexity and cost of building an in-house next generation security operation.

XDR is a more evolved, holistic, cross-platform approach to endpoint detection and response. While EDR collects and correlates activities across multiple endpoints, XDR broadens the scope of detection beyond endpoints and analyses data across endpoints, networks, servers, cloud workloads, SIEM and much more. This provides a unified, single pane of glass view across multiple tools and attack vectors. XDR solutions can also respond automatically to identified threats. This includes taking both preventative measures to block malicious content from reaching a system and working to mitigate an in-progress attack on a compromised endpoint.

Data loss prevention (DLP) is a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. It is a strategy to detect and prevent confidential data leaks e.g., Email addresses, credit card information, source code files, invoices, payslips, important documents, etc. DLP provides reporting to meet compliance and auditing requirements and identify areas of weakness and anomalies for forensics and incident response. DLP software classifies regulated, confidential and business critical data and identifies violations of policies defined by organizations or within a predefined policy pack, typically driven by regulatory compliance such as HIPAA, PCI-DSS, or GDPR. Once those violations are identified, DLP enforces remediation with alerts, encryption, and other protective actions to prevent end users from accidentally or maliciously sharing data that could put the organization at risk. DLP technology is used for three main purposes namely Securing Information, Maintaining Backup Operations and Ensuring Compliance. DLP has four key capabilities on which it works.

- Discover – Find data wherever it is stored. Create inventory of sensitive data. Manage data clean up.
- Monitor – Understand how data is being used. Understand content and context. Gain visibility into policy violations.
- Protect – Proactively secure data. Prevent confidential data loss. Enforce data protection policies.
- Manage – Define unified policy across enterprise. Remediate and report on incidents. Detect content accuracy.

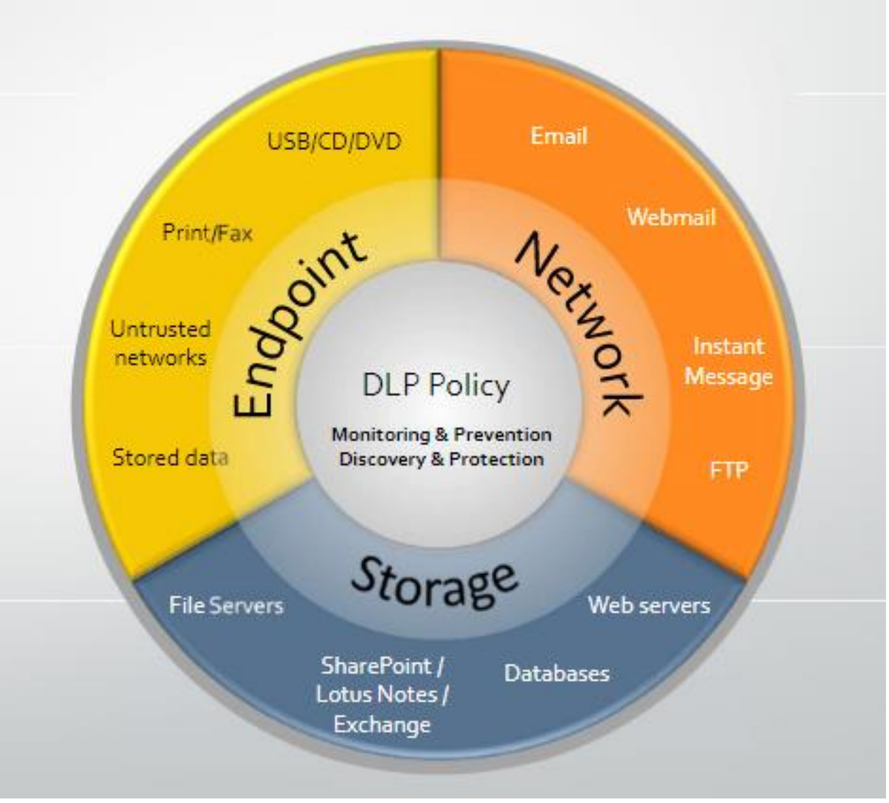


Figure 35. DLP policy covers Endpoint, Network and Storage.

DLP policy covers endpoint, network and storage metrices. It is a five-step process starting with customizing policy templates, discovering scan targets, monitoring data, network and endpoint events, protecting important files by blocking, removing and encrypting and remediating and reporting risk reductions.

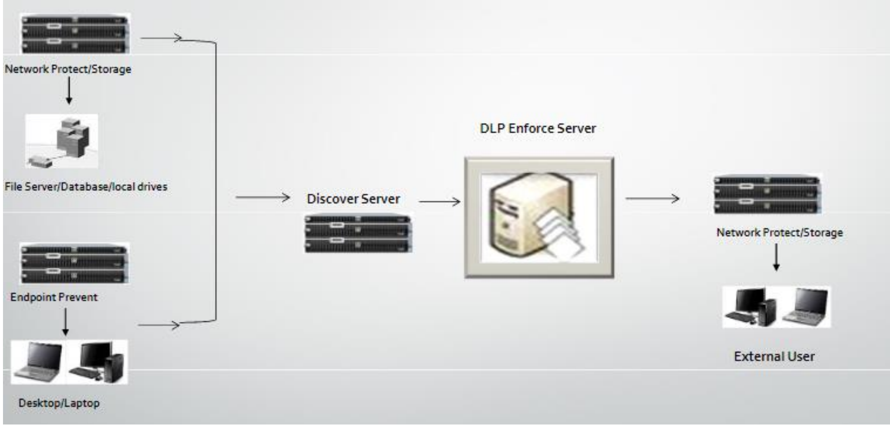
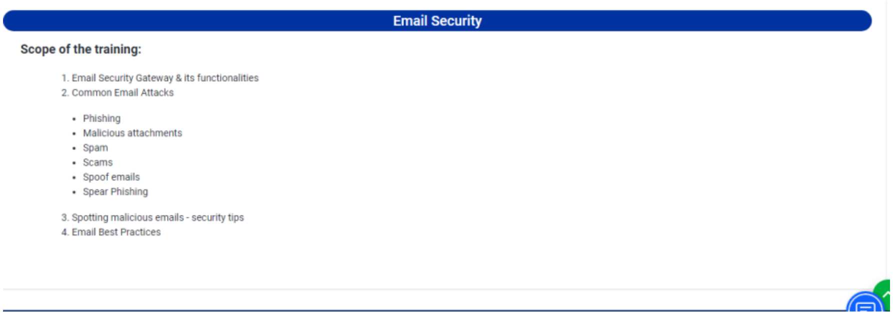


Figure 36. DLP architecture.

Some of the top vendors of DLP technology are Symantec DLP, McAfee DLP, Force Point DLP, etc.

2.2.2.2 Email Security

As network protection tools are getting stronger day by day, attackers have shifted their focus towards attacking end users as they're less protected. Email security refers to the collective measures used to secure the access and content of an email account or service. No mentor sessions were conducted for Email Security and a self-paced course was assigned to cover up the topics in LP named End User Email Security on the Cybrary platform.



Email Security

Scope of the training:

1. Email Security Gateway & its functionalities
2. Common Email Attacks
   - Phishing
   - Malicious attachments
   - Spam
   - Scams
   - Spoof emails
   - Spear Phishing
3. Spotting malicious emails - security tips
4. Email Best Practices

Figure 37. Email Security Topics

Some of the common email attacks are:

- **Phishing**

  Phishing is a fraudulent attempt to obtain sensitive information or data. Phishing is commonly done through emails, websites and phone calls in order to steal sensitive information or money. Phishing emails are used to trick the receivers into sharing sensitive information often by posing as legitimate business or trusted contacts.

- **Social Engineering**

  Social engineering is when an attacker uses fear, urgency and deception to manipulate the receiver into sharing information of taking some action. Typically, attackers always try to trick people into giving access to safer environments, sharing confidential information with them.

- **Spear Phishing**

  Spear phishing is targeting individuals based on research, impersonating either as a brand or other known entity, with the goal of acquiring confidential information or installing spyware.

- **Spam**

  Also known as junk email, is unsolicited message – i.e., harmless, advertising businesses or controversial ideas.

- **Spoof Emails**

  A technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust.

- **Malicious Attachments and Malicious Links**

  Malware can be in attachment and links which come in an email. Attachments can carry malware in the background and can infect the endpoint. Similarly, links which come with the email may redirect the user to a certain webpage demanding some action or may download malicious software.

Some of the best email practices are:

- Always check whether the email is from a trusted source. Check the from address for any wrong spellings or unfamiliar domain names.
- Review the subject of the mail as attackers provide either too much or too less information.

- Review the content of the mail.
- If the mail is not relevant, report to the phishing team.
- If the mail refers to an action, like sharing it with 100 people for a reward or filling up a survey form, etc. which is not entitled from a trusted source.
- Be vigilant to attachments.
- Be vigilant to links.
- Don’t click on hyperlinks.

Email Security gateways are tools which promote end user email security by filtering emails, routing incoming and outgoing mails, configuring policies for email processing and monitoring email flow. Besides the above, these gateways have the listed features as well:

- Blocks a wide range of email addresses at the connection level, filters spams and viruses, and can approve and block messages based on sender address or domain, origin IP address, attachment size or file type, text content, and more.
- Spam and viruses are separated from the legitimate messages.
- Legitimate messages are delivered to recipients with minimal delay, while suspicious messages are blocked or sent to the quarantine.
- Stops malware and non-malware threats such as imposter email.
- Block malware, phishing, spear phishing and spam emails at the perimeter of your network.
- Attack blocking Connection Protection from directory harvest attacks and denial of service attacks.
- Email encryption and data loss prevention.

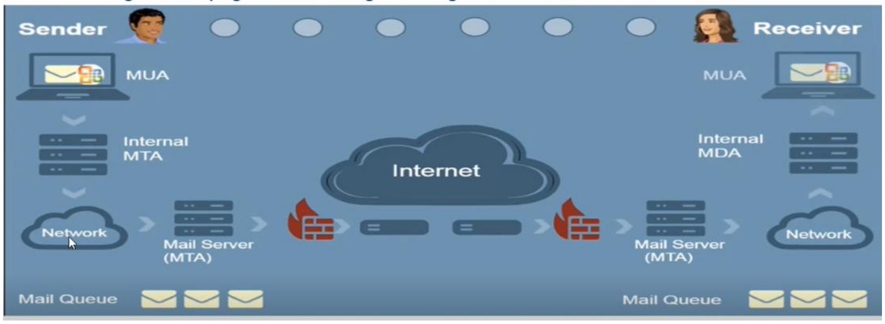
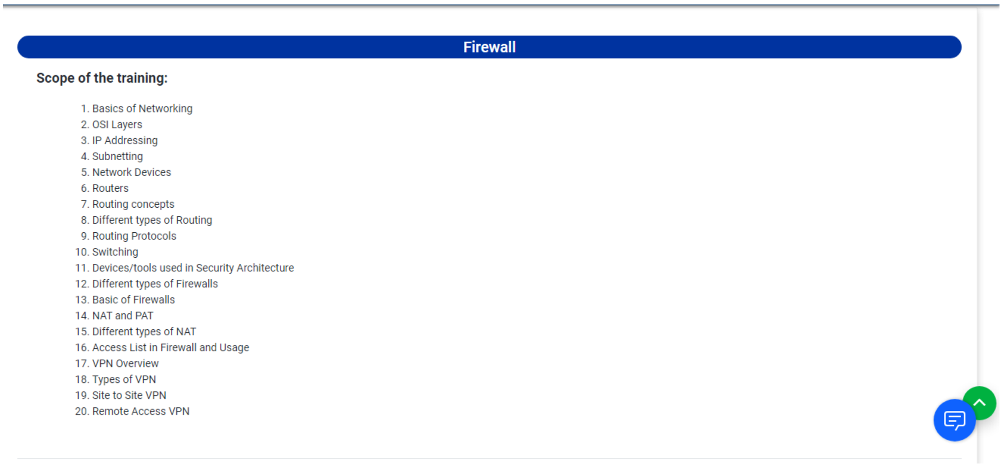


Figure 38. A typical email lifecycle with an email security gateway

Some of the common venders of email security gateway software are Proofpoint Email Protection, Cisco Cloud Email Security, Symantec Email Security, Forcepoint Email Security Gateway, etc.

2.2.3 Firewall (Week 5)

A firewall is a device or a software configuration specifically designed to control the flow of traffic into and out of the network. In general, firewalls are installed to prevent network attacks like, Web application attacks, XXS, DNS tunnelling etc. Three mentor sessions of one-hour each were conducted on Firewall. No course was assigned from the mentors on the topic.



Firewall

Scope of the training:

1. Basics of Networking
2. OSI Layers
3. IP Addressing
4. Subnetting
5. Network Devices
6. Routers
7. Routing concepts
8. Different types of Routing
9. Routing Protocols
10. Switching
11. Devices/tools used in Security Architecture
12. Different types of Firewalls
13. Basic of Firewalls
14. NAT and PAT
15. Different types of NAT
16. Access List in Firewall and Usage
17. VPN Overview
18. Types of VPN
19. Site to Site VPN
20. Remote Access VPN

Figure 39. Firewall topics

The basis of network was already covered in the first three weeks with the course Introduction to network to non-techies, so only firewall and VPN were covered in the sessions.

A firewall acts as a barrier or a shield between an endpoint and cyber space. They provide critical protection to the endpoints from unauthorised access. Firewalls are categorized into these following categories:

- **1st Generation Firewall**
  The first-generation firewall worked on packet filtering principle. Since, packets are formed in the transport layer. A rule set is defined in the TCP / IP layer which consists of some actions in order to match some criteria in the packets. There are two lists, permit list and the deny list. Filtering was based on the information obtained from the network packets like source IP, destination IP, source port, destination port and internet

protocol which is also known as the 5-tuple rule.

- **2nd Generation Firewall**

  The second-generation firewall worked on the application gateways and proxies. These firewalls work on the application layer. They evaluate network packets for valid data at the application layer before allowing a connection. Proxy servers are used for special purpose in order to manage traffic such as FTP or HTTP. Proxy services can provide increased access control, detailed checks for valid data, and they generate audit records about the traffic to identify and track traffic.

- **3rd Generation Firewall**

  The third-generation firewall is also known as stateful packet inspection firewall worked on the same packet screening technique like first generation firewalls. In addition, it investigates the packet header information from the network layer to the application layer in order to verify that the packet is part of an agreeable connection and the protocols are behaving as expected. It tightens the rules for TCP traffic by creating a directory of TCP connections.

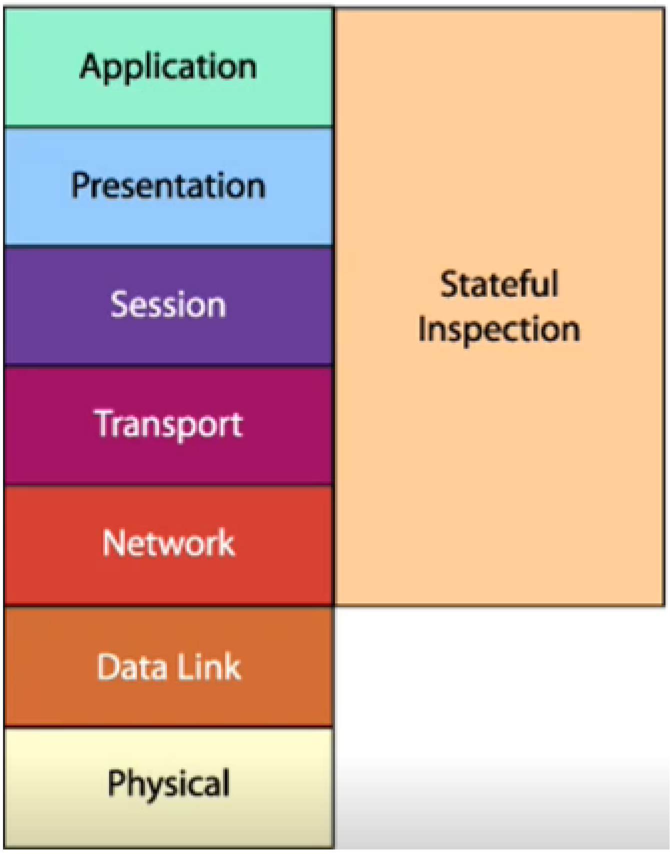
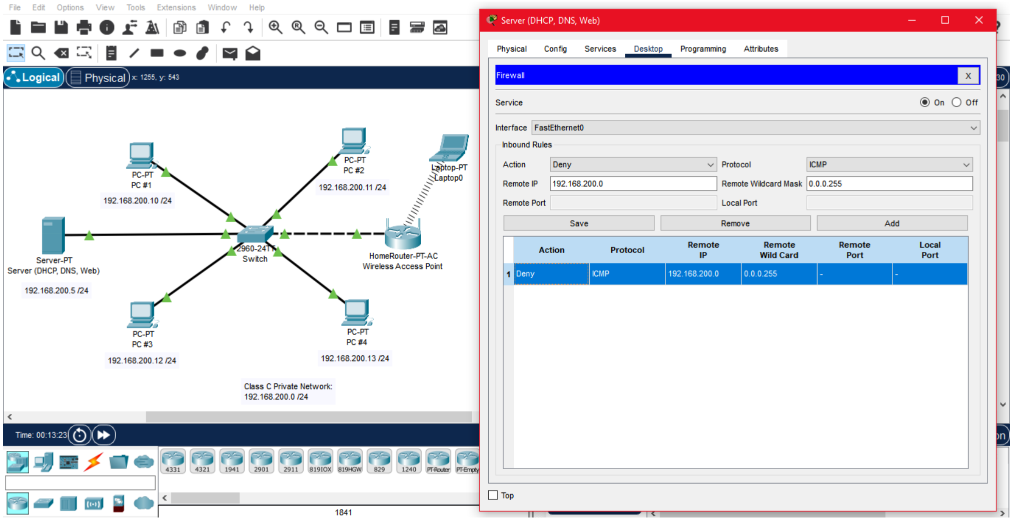


Figure 40. Stateful Inspection Layers

- **Next Generation Firewalls**

  Next generation firewalls are more capable of detecting application-specific attacks than standard firewalls and this can prevent more malicious intrusions. They do a full-packet inspection by checking the signatures and payload of packets for any anomalies or malware. Next generation firewalls provide all traditional firewall capabilities along with identification of undesired encrypted applications with the help of SSL decryption.

An activity related to firewall was performed on Cisco Packet Tracer. In this activity, a LAN connected to a Web Server through a switch and a wireless SOHO device. The aim was to block ICMP requests on endpoints.



Service ● On ○ Off

Interface: FastEthernet0

Inbound Rules

Action: Deny
Protocol: ICMP
Remote IP: 192.168.200.0
Remote Wildcard Mask: 0.0.0.255
Remote Port:
Local Port:

	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Deny	ICMP	192.168.200.0	0.0.0.255	-	-

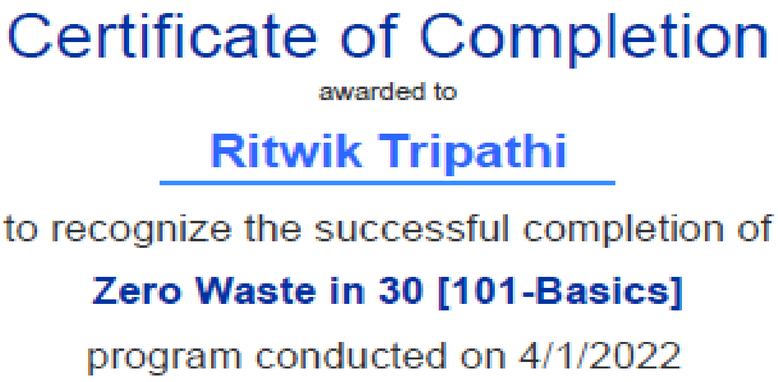
Figure 41. A firewall is setup on the Webserver which blocks ICMP requests.

CHAPTER 3

RESULTS

3.1 Pre Domain-Assignment Certification

3.1.1 Zero Waste in 30



Certificate of Completion

awarded to

Ritwik Tripathi

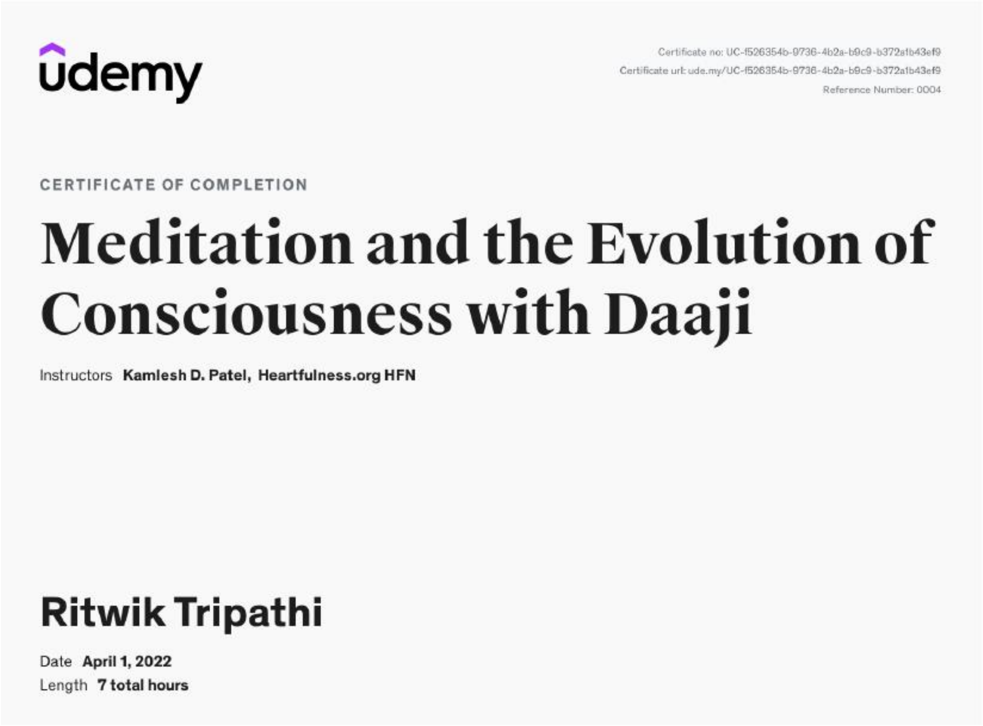
to recognize the successful completion of

Zero Waste in 30 [101-Basics]

program conducted on 4/1/2022

Figure 42. Completion Certificate of Zero Waste in 30.

3.1.2 Meditation and the Evolution of Consciousness



udemy

Certificate no: UC-f526354b-9736-4b2a-b9c9-b372a1b43ef9
Certificate url: ude.my/UC-f526354b-9736-4b2a-b9c9-b372a1b43ef9
Reference Number: 0004

CERTIFICATE OF COMPLETION

Meditation and the Evolution of Consciousness with Daaji

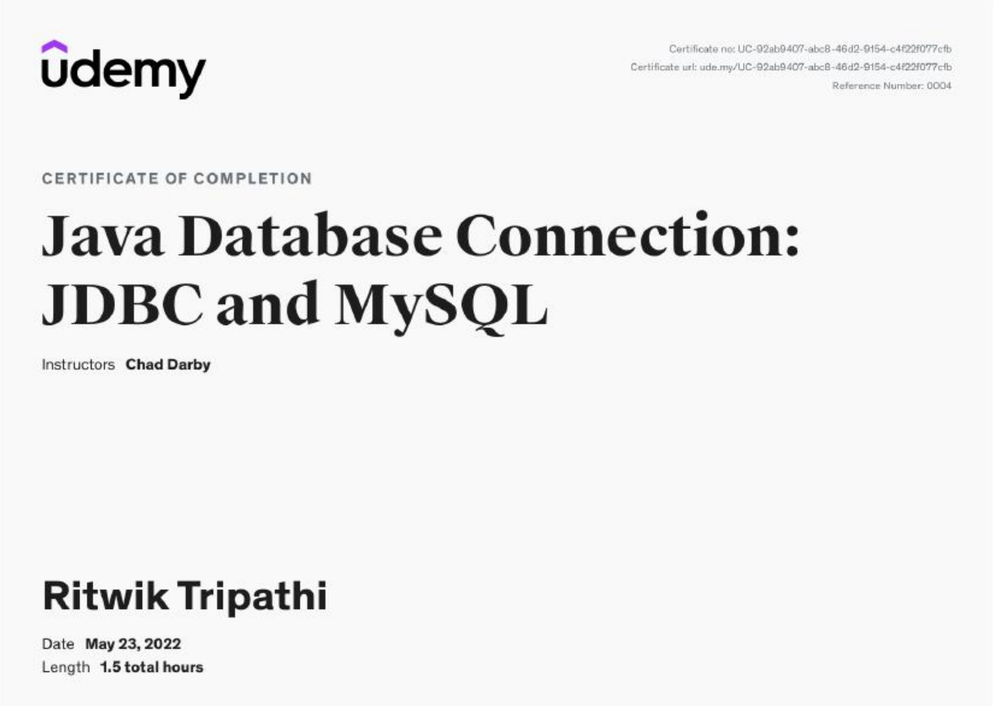
Instructors **Kamlesh D. Patel, Heartfulness.org HFN**

Ritwik Tripathi

Date **April 1, 2022**
Length **7 total hours**

Figure 43. Meditation and Evolution of Consciousness Certification.

3.1.3 Java Database Connection: JDBC and MySQL



udemy

Certificate no: UC-92ab9407-abc8-46d2-9154-c4f22f077cfb
Certificate url: ude.my/UC-92ab9407-abc8-46d2-9154-c4f22f077cfb
Reference Number: 0004

CERTIFICATE OF COMPLETION

Java Database Connection: JDBC and MySQL

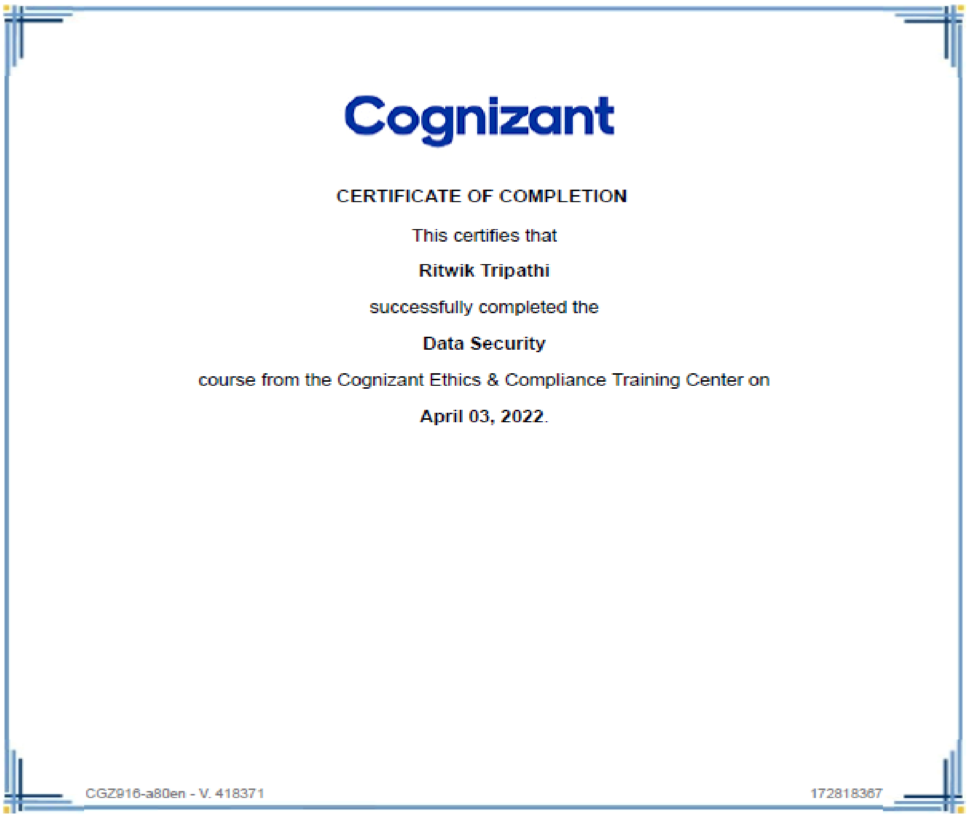
Instructors **Chad Darby**

Ritwik Tripathi

Date **May 23, 2022**
Length **1.5 total hours**

Figure 44. JDBC and MySQL certification

3.1.4 Data Security



Cognizant

CERTIFICATE OF COMPLETION

This certifies that

Ritwik Tripathi

successfully completed the

Data Security

course from the Cognizant Ethics & Compliance Training Center on

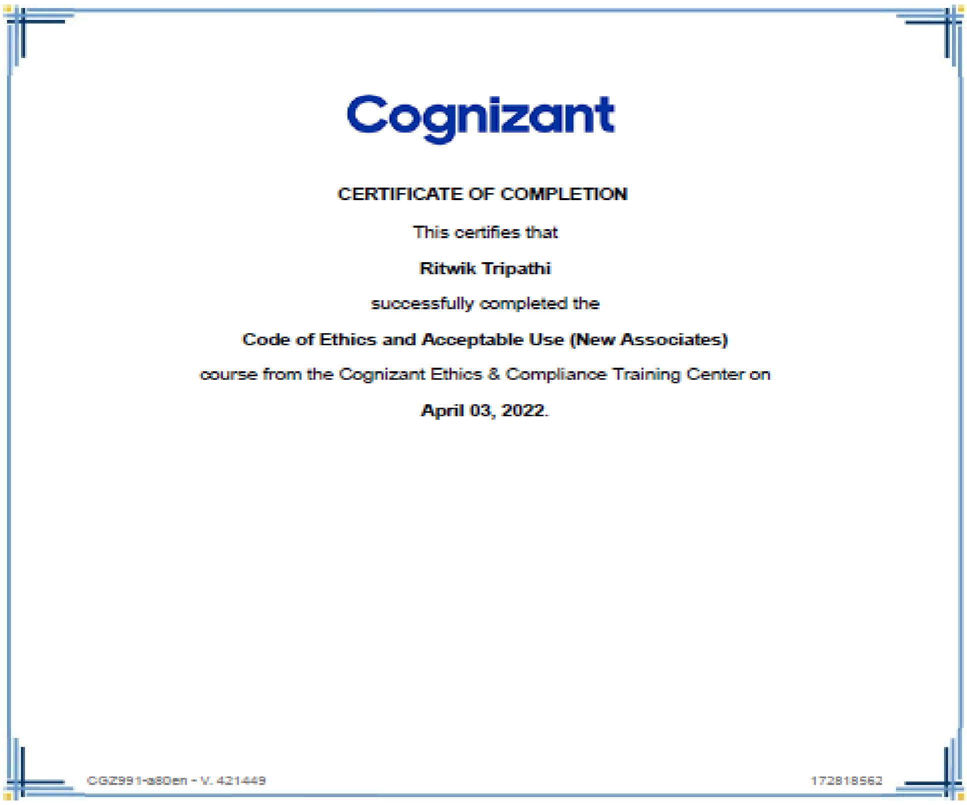
April 03, 2022.

CGZ916-a80en - V. 418371

172818367

Figure 45. Data Security Certification

3.1.5 Code of Ethics and Acceptable Use



Cognizant

CERTIFICATE OF COMPLETION

This certifies that

Ritwik Tripathi

successfully completed the

Code of Ethics and Acceptable Use (New Associates)

course from the Cognizant Ethics & Compliance Training Center on

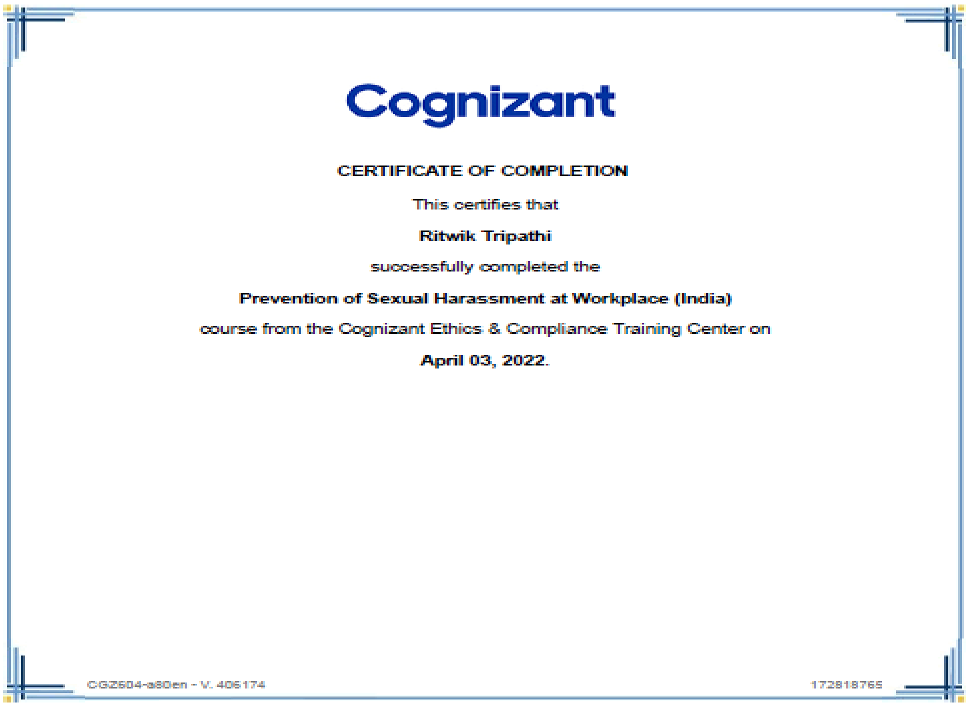
April 03, 2022.

CGZ991-a80en - V. 421449

172818562

Figure 46. Code of Ethics and Acceptable Use Certification.

3.1.6 Prevention of Sexual Harassment at Workplace (India)



Cognizant

CERTIFICATE OF COMPLETION

This certifies that

Ritwik Tripathi

successfully completed the

Prevention of Sexual Harassment at Workplace (India)

course from the Cognizant Ethics & Compliance Training Center on

April 03, 2022.

CGZ604-a80en - V. 406174

172818765

Figure 47. Prevention of Sexual Harassment in Workplace (India) Certification

3.2 Domain Specific Training Results and Certification

The Gen C Learn platform tracks the performance of the interns in the learning phase based on the learning hours and mentor session reviews. This platform records the learning progress as well as provides XP points based on course completion and mentor reviews. The platform also assigns ranks to top learners based on XP stars which are mini milestones in the LP. There are ten mini milestones in the LP for ITM. The learning progress is updated every 24 hours.

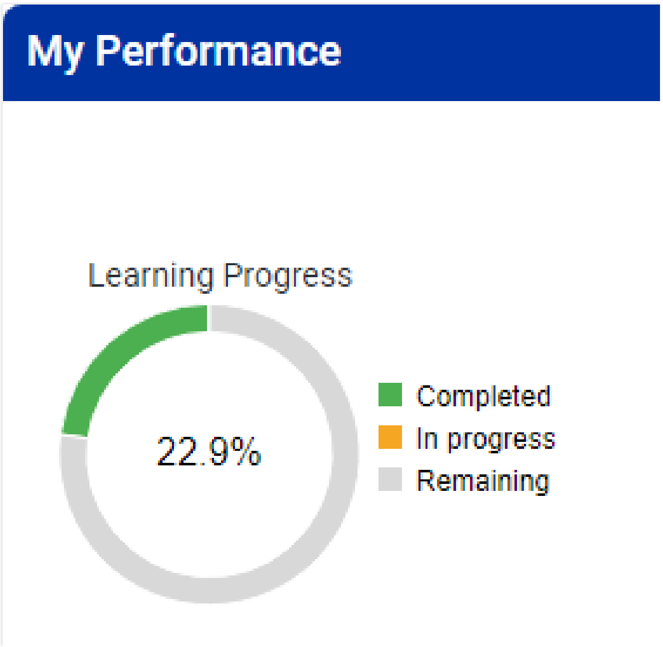
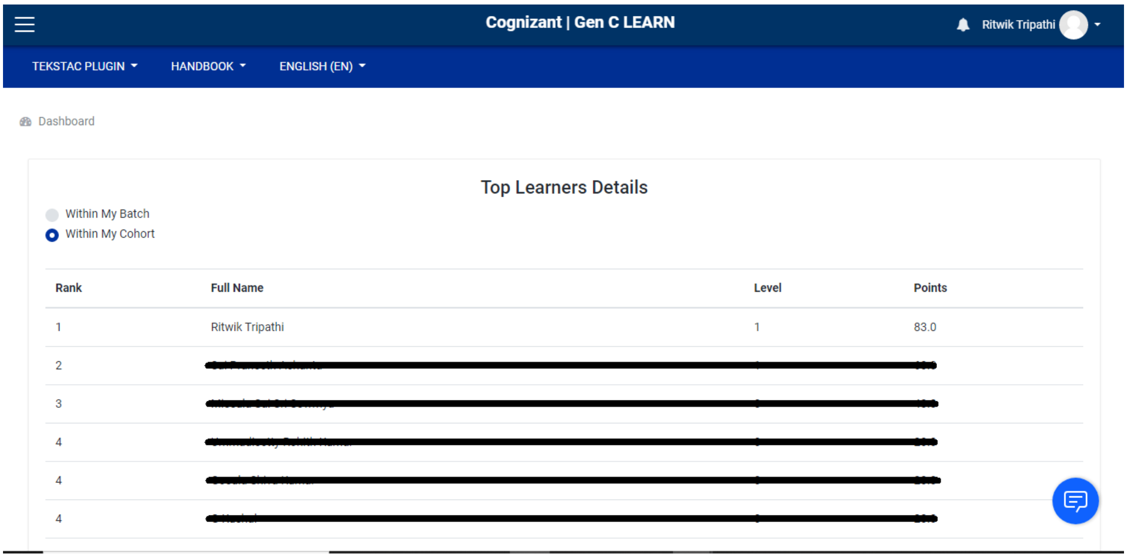


Figure 48. Learning Performance up to Week 5



Top Learners Details

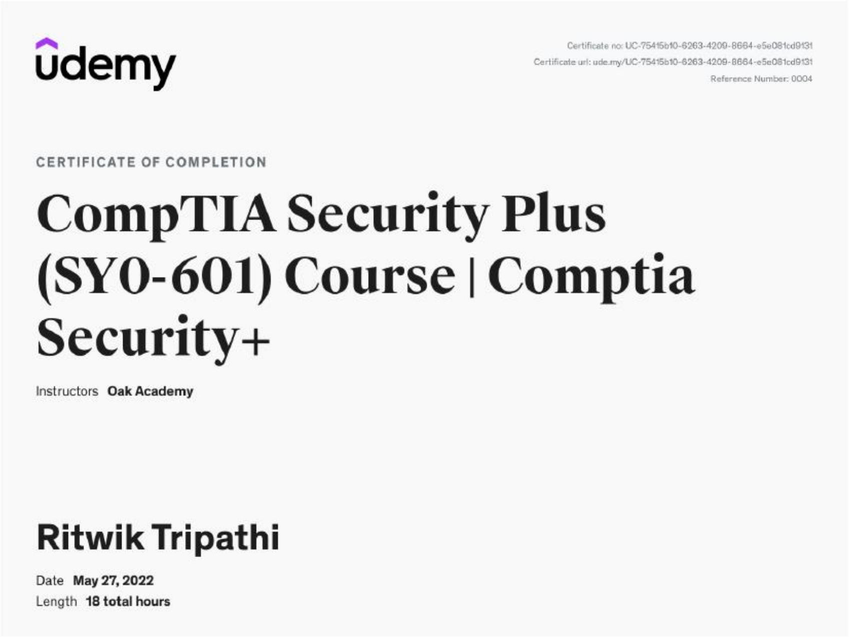
○ Within My Batch
● Within My Cohort

Rank	Full Name	Level	Points
1	Ritwik Tripathi	1	83.0
2	[redacted]	[redacted]	[redacted]
3	[redacted]	[redacted]	[redacted]
4	[redacted]	[redacted]	[redacted]
4	[redacted]	[redacted]	[redacted]
4	[redacted]	[redacted]	[redacted]

Figure 49. Top Learners Details

3.2.1 Cybersecurity Basics (Week 1, Week 2 and Week 3)

3.2.1.1 CompTIA Security Plus (SY0-601) Certification



udemy

Certificate no: UC-75415b10-6263-4209-8664-e5e081cd9131
Certificate url: ude.my/UC-75415b10-6263-4209-8664-e5e081cd9131
Reference Number: 0004

CERTIFICATE OF COMPLETION

CompTIA Security Plus (SY0-601) Course | Comptia Security+

Instructors **Oak Academy**

Ritwik Tripathi

Date **May 27, 2022**
Length **18 total hours**

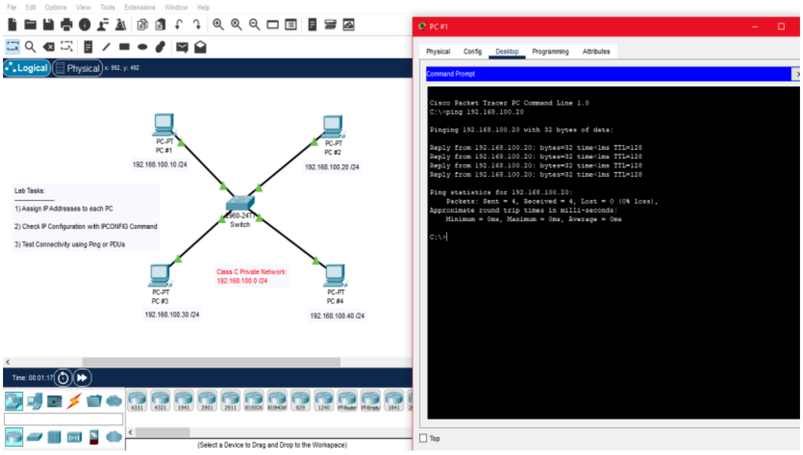
Figure 50. CompTIA Security Plus (SY0-601) Course Certification.

3.2.1.2 Introduction to Computer Networks for Non-Techies

The results for the hands-on activities apart from the first one and the third one (as they do not generate any results and are static outputs) is as follows:

- **Static IP Configuration**

  The static IP configuration can be verified by generating ICMP request from one endpoint to the other endpoints in the LAN



Lab Tasks:

1) Assign IP Addresses to each PC

2) Check IP Configuration with IPCONFIG Command

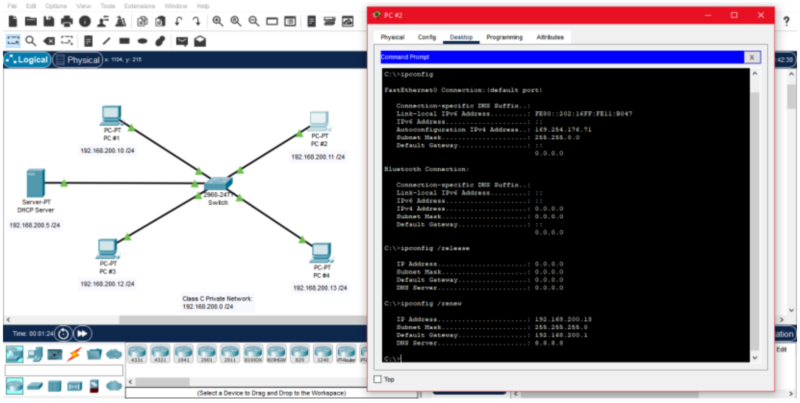
3) Test Connectivity using Ping or PDUs

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.20

Pinging 192.168.100.20 with 32 bytes of data:

Reply from 192.168.100.20: bytes=32 time<1ms TTL=128
Reply from 192.168.100.20: bytes=32 time<1ms TTL=128
Reply from 192.168.100.20: bytes=32 time<1ms TTL=128
Reply from 192.168.100.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.100.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 51. Generating ICMP requests from PC#1 to PC#2.

- **Dynamic IP configuration using DHCP Server**

  The dynamic IP configuration from a DHCP server can be checked by ipconfig /renew command on any endpoint.

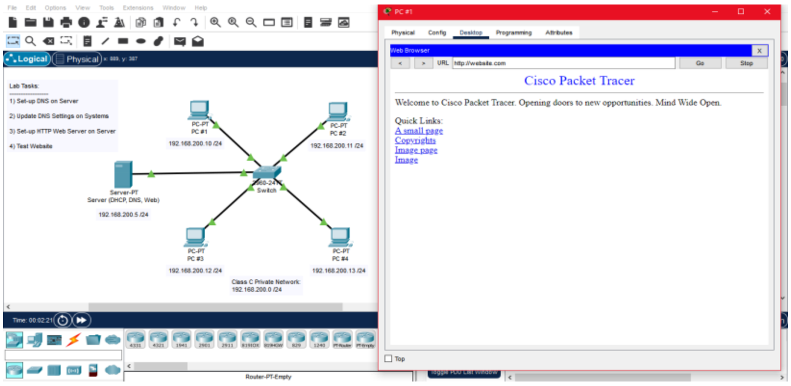


```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::202:16FF:FE11:B047
   IPv6 Address....................: ::
   Autoconfiguration IPv4 Address..: 169.254.176.71
   Subnet Mask.....................: 255.255.0.0
   Default Gateway.................: ::
                                     0.0.0.0

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0

C:\>ipconfig /release

   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0
   DNS Server......................: 0.0.0.0

C:\>ipconfig /renew

   IP Address......................: 192.168.200.13
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.200.1
   DNS Server......................: 8.8.8.8

C:\>
```

Figure 52. Using the ipconfig /renew command on PC#2.

- **DNS and Web Server**

  The web server can be tested if the test website is loaded onto the endpoints.



Lab Tasks:

1) Set-up DNS on Server

2) Update DNS Settings on Systems

3) Set-up HTTP Web Server on Server

4) Test Website

Cisco Packet Tracer

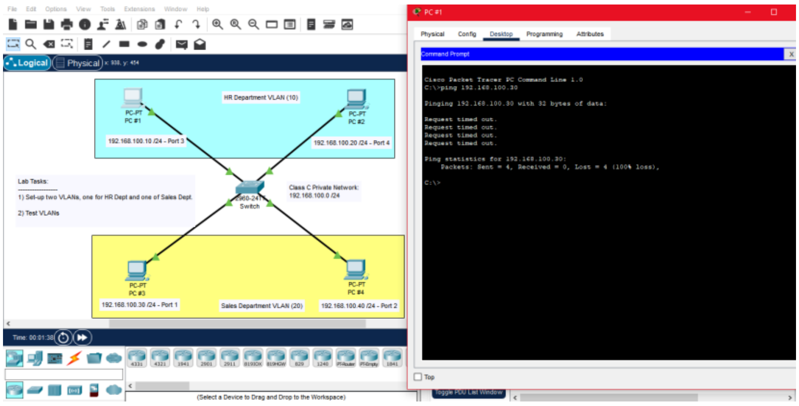
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Figure 53. Using PC#1 web browser to test the website on the web server

- **VLAN Configuration**

  The VLAN can be checked by sending ICMP requests across VLANs. If it fails, then VLANs are independent.



Lab Tasks:

1) Set-up two VLANs, one for HR Dept and one of Sales Dept.

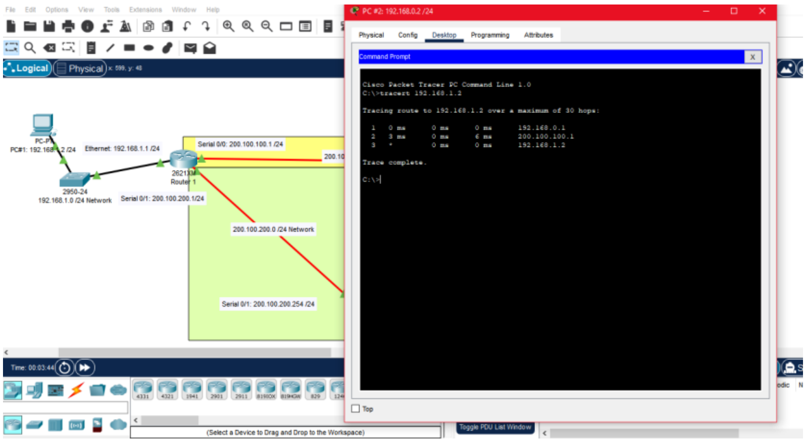
2) Test VLANs

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.100.30

Pinging 192.168.100.30 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.100.30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 54. Sending ICMP requests from PC#1 to PC#3.

- **Router Configuration using RIP**

  Router configuration can be verified by using the tracert command on any endpoint.

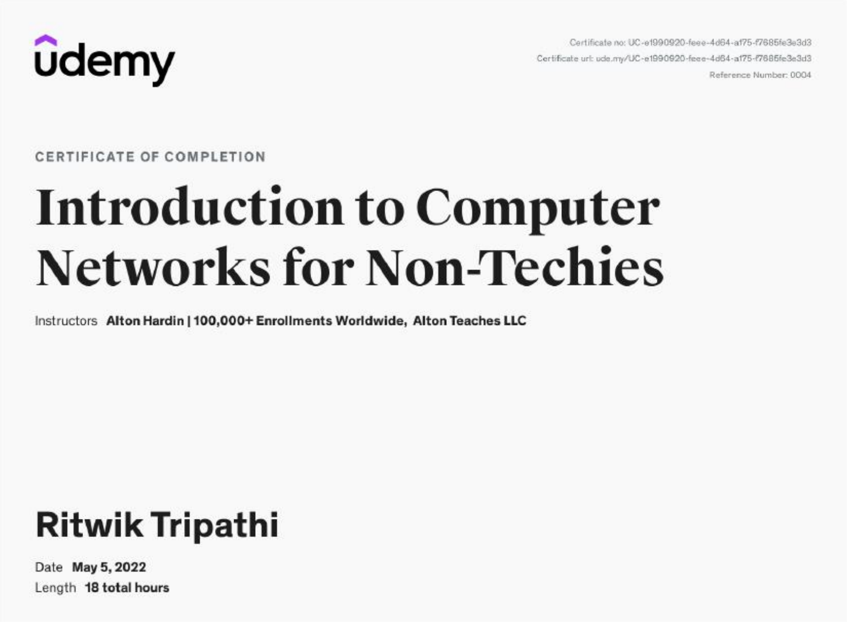


File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 599, y: 48
PC-PT
PC#1: 192.168.1.2 /24
Ethernet: 192.168.1.1 /24
2950-24
192.168.1.0 /24 Network
2621XM
Router 1
Serial 0/0: 200.100.100.1 /24
Serial 0/1: 200.100.200.1/24
200.100.200.0 /24 Network
Serial 0/1: 200.100.200.254 /24
Time: 00:03:44
4331 4321 1941 2901 2911 819IOX 819HGW 829
(Select a Device to Drag and Drop to the Workspace)
Toggle PDU List Window
PC #2: 192.168.0.2 /24
Physical Config Desktop Programming Attributes
Command Prompt
X
□ Top

```
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.0.1
  2   3 ms      0 ms      6 ms      200.100.100.1
  3   *         0 ms      0 ms      192.168.1.2

Trace complete.

C:\>
```

Figure 55. Using the tracert from PC#2 to PC#1

The course completion certificate is as below



udemy

Certificate no: UC-e1990920-feee-4d64-af75-f7685fe3e3d3
Certificate url: ude.my/UC-e1990920-feee-4d64-af75-f7685fe3e3d3
Reference Number: 0004

CERTIFICATE OF COMPLETION

Introduction to Computer Networks for Non-Techies

Instructors **Alton Hardin | 100,000+ Enrollments Worldwide, Alton Teaches LLC**

Ritwik Tripathi

Date **May 5, 2022**
Length **18 total hours**

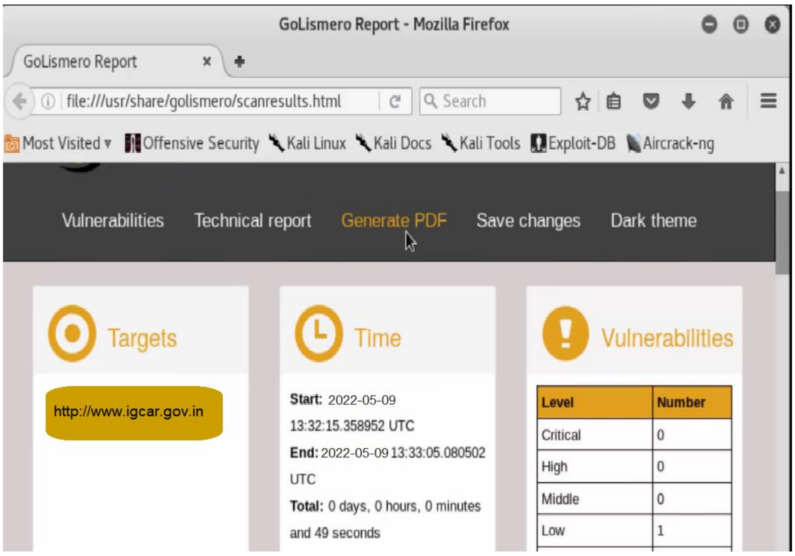
Figure 56. Introduction to Computer Networks for Non-Techies Certification

3.2.1.3 Cisco CyberOps Associate CBROPS 200-201:Part 1

Cisco CyberOps Associate CBROPS 200-201 is a cyber operation certification by Cisco. This certification covers Network Concepts, Security Concepts, Security Monitoring Concepts and Host Based Analysis. The two hands on activities were an addition to the course apart from the obvious. The results of the two hands on activities associated with the course are as follows:

- **Golismero**

With this tool, the vulnerability analysis of the website http://www.igcar.gov.in was performed which generated the following report:



http://www.igcar.gov.in

Start: 2022-05-09 13:32:15.358952 UTC
End: 2022-05-09 13:33:05.080502 UTC
Total: 0 days, 0 hours, 0 minutes and 49 seconds

Level	Number
Critical	0
High	0
Middle	0
Low	1

Figure 57. Vulnerability analysis report generated by Golismero

Only one vulnerability was detected by Golismero for the website. The website was not SSL secured, which was detected by Golismero. This is obviously understood by the fact that the port used was http and not https.

- **Social Engineering Toolkit (SET)**

The social engineering toolkit clones a website and after the credentials are submitted, it travels to the original webpage. In this hands-on activity, https://www.facebook.com was cloned. The credentials entered into this cloned website is returned into the terminal.

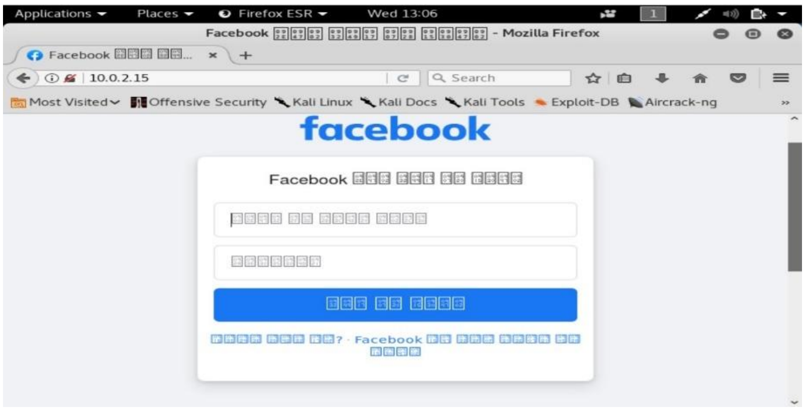
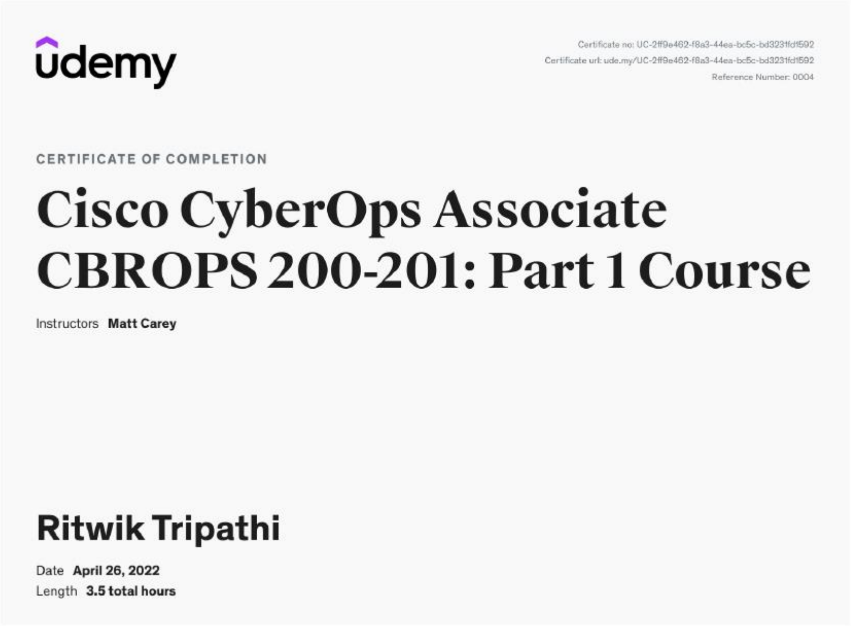


Figure 58. The cloned website for credential engineering.

The certification for this course is as below:



udemy

Certificate no: UC-2ff9e462-f8a3-44ea-bc5c-bd3231fd1592
Certificate url: ude.my/UC-2ff9e462-f8a3-44ea-bc5c-bd3231fd1592
Reference Number: 0004

CERTIFICATE OF COMPLETION

Cisco CyberOps Associate CBROPS 200-201: Part 1 Course

Instructors **Matt Carey**

Ritwik Tripathi

Date **April 26, 2022**
Length **3.5 total hours**

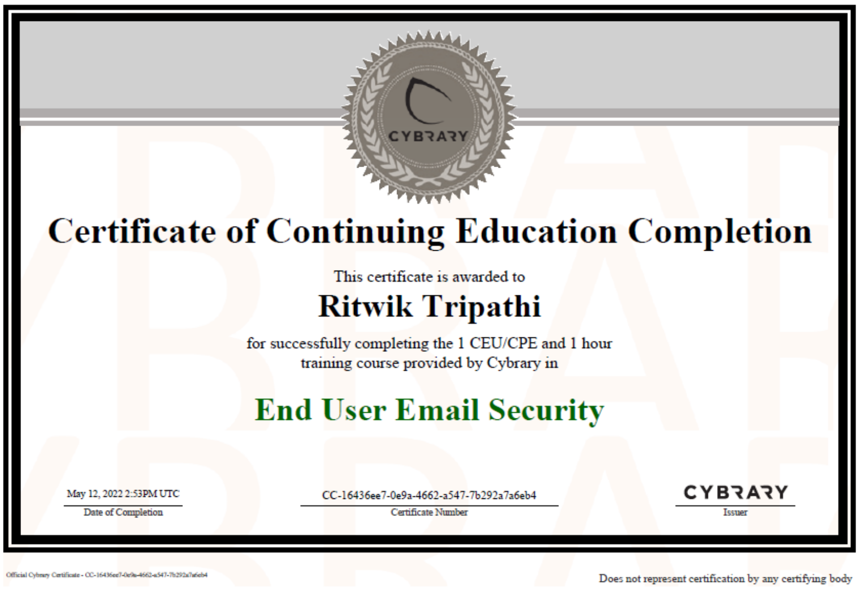
Figure 59. Cisco CyberOps Associate CBROPS 200-201: Part 1

3.2.2 Endpoint and Email Security (Week 4)

3.2.2.1 Endpoint Security

This week talked about endpoint security and how traditional antiviruses were less efficient when it came to endpoint protection. Many endpoint vendors having deployable endpoint solutions are in the market. MDR (Managed Detection and Response) and XDR (Extensive detection and Response) are extensions of EDR software. Endpoint security solutions are a combination of four components, Antivirus / Malware / Spyware, Host Firewall, Host IPS, Application and Device Control. All these components work together to secure endpoints. DLP tools enable protection of data which can be in many places. Data leakage is a major problem for the business of the companies. It can be either intentional or unintentional. Data can be at rest, in transit or in usage, e.g., data stored in an endpoint is data at rest, data being transmitted over a network and data in usage refers to the data currently in use. That is why it is said that DLP policy covers endpoint, network and storage metrices. DLP tools work on the data stored, on in usage on any endpoint along with while being in a transmitted across a network.

3.2.2.2 Email Security



CYBRARY

Certificate of Continuing Education Completion

This certificate is awarded to

Ritwik Tripathi

for successfully completing the 1 CEU/CPE and 1 hour training course provided by Cybrary in

End User Email Security

May 12, 2022 2:53PM UTC
Date of Completion

CC-16436ee7-0e9a-4662-a547-7b292a7a6eb4
Certificate Number

CYBRARY
Issuer

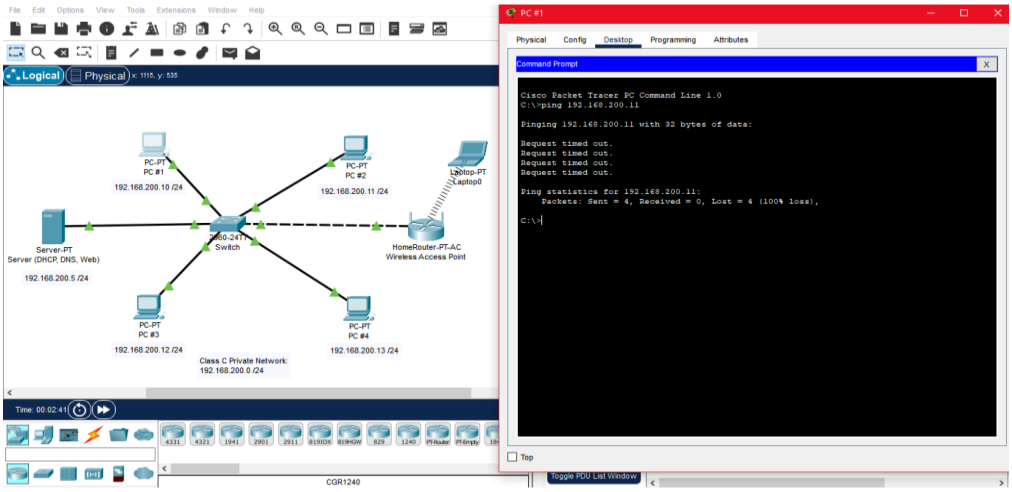
Official Cybrary Certificate - CC-16436ee7-0e9a-4662-a547-7b292a7a6eb4

Does not represent certification by any certifying body

Figure 60. Email Security Certification.

3.2.3 Firewall (Week 5)

A firewall can either be a device or a software configuration which acts as a barrier between any endpoint and the cyber space and authorised access. It protects from various malicious software that can cause harm to the endpoint. There are two types of firewalls, legacy firewalls and next generation firewalls. Legacy firewalls include packet filtration, web application / proxies and stateful inspection firewall. Next generation firewalls include IPS / IDS, AMP technologies. The hands-on activity on firewall can be checked by generating ICMP requests on any endpoint into the LAN.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.200.11

Pinging 192.168.200.11 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.200.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figure 61. Blocking ICMP requests while using the Firewall on DHCP server.

CHAPTER 4

CONCLUSION

As this internship will be concluding in the month of August, during the past few weeks it was really fun to gather knowledge in the field of cybersecurity. Having learnt so much from till now, this internship has really helped in shaping with the knowledge of these technologies.

The final internship project is still remaining with this internship which is due in 12th to 16th week of this internship.

Starting the internship with the corporate introduction while being addressed on various issues like data security, code of ethics, acceptable usage and learning how to control anxiety and stress which can build up in work from home mode, it was a warm welcome from the company. Once every general rules and policies were introduced, the BU assignment took place and further tower mapping inside the BU on a random basis was given. The BU mentors connect on a regularly basis to clarify doubts and conduct training sessions to make the interns business ready. Week 1 to week 3 was more inclined towards basic courses which helped in grasping core cybersecurity concepts along with revision of computer networks.

Mentor sessions were conducted on a regular basis from week 4 and discussions on endpoint safety and security enriched the understanding of how behavioural aspects are nowadays more prominent in detection of malware and other threats to the endpoints as compared to the traditional antivirus. DLP tools were also discussed and a difference was made clear between EDR and DLP tools. Mentor suggested course for email security covered all the points as mentioned into the learning path. Moreover, the course also discussed about the roles and responsibilities of HR department towards protection of end users.

Week 5 was all about Firewall. Firewalls are the barriers between the cyber space and the endpoint devices. There are still 11 weeks left into this internship and a lot more is there to learn. In the end, it can be concluded that the overall experience of working with Cognizant has been really nice.

REFERENCES

As per the NDA policy, references can be mentioned for data if taken from Cognizant but they cannot be sited. Also, the documents for reference are only available within the organization.

1 Cognizant LP handbook.

2 Mentor session slides.

3 Cognizant website.

4 Cognizant Gen C Internship curriculum.