LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

FC7W03NI Work Related Learning

Assessment Weightage & Type 100%

Individual Coursework

Year and Semester 2021-22

Autumn

Student Name: Himanshu Pandey

London Met ID: 19031311

College ID: NP01NTA190131

Assignment Due Date: 26th January 2022

Assignment Submission Date: 26th January 2022

Academic Supervisor: Ravi Chandra Gurung

Word Count: 3700

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Background to the placement company

Figure 1 logo of vairav technology

The company which gave me a wonderful internship opportunity was “Vairav Technology” located at Balwatar, Kathmandu. Vairav Technology, a cyber defender from the land of Gurkha, is recognized by the renowned cyber security company in Nepal via an increasing foreign consumers. It was established since the year 2019. Vairav Technology's core objective is to support various kinds of companies avoid cyber-crime, secure results, and identify cyber threats. Thus, it offers different kinds of cyber security services, such as SOC mostly as product, security monitoring, IS audit, and advice on cyber security. The solutions given therefore pursue advantages for business institutions, from big company entities to micro to businesses of all sizes in Nepal as well (vairav, 2022).

Vairav technology was titled as MSSP Alert's Top 250 security Monitoring Company, serves as a state-of-the-art data center for commercial cyber security infrastructure which fulfill the rising need for cyber security services throughout Nepal. Both developers and staff at Vairav Technology have a very good previous expertise for starting up a significant data center for operating quest facilities in Nepal for multinational companies. (technology, 2021).

1.2 Structure and Role of the company

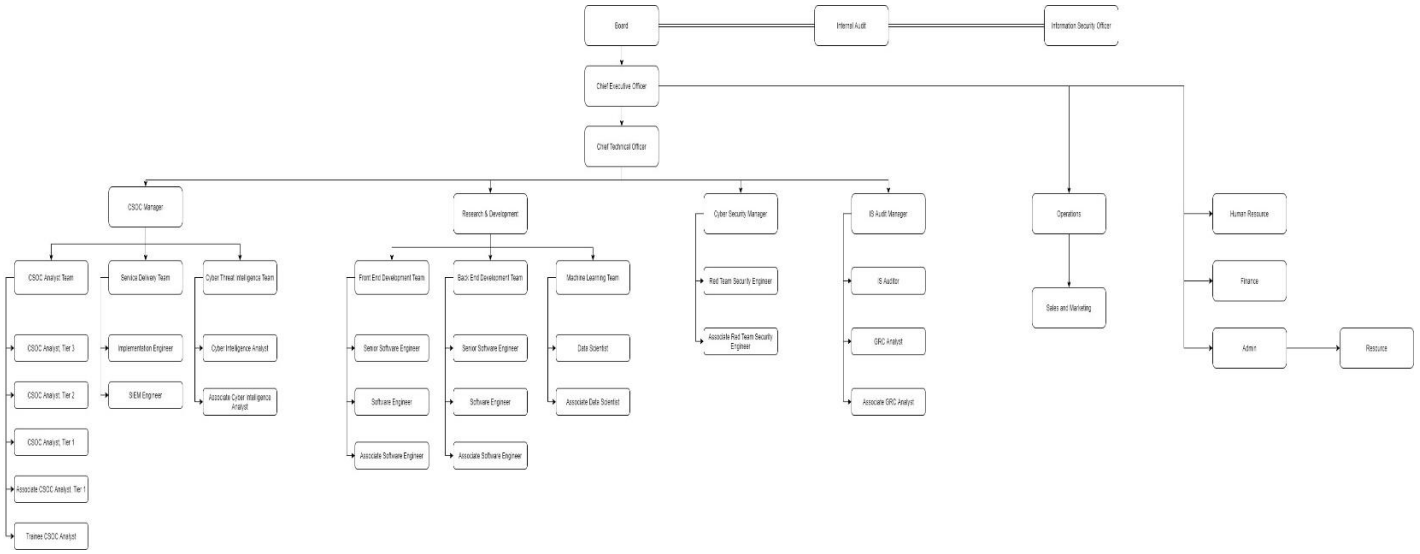


Figure 2 Structure 1 and role of Vairav technology

(I have attached another figure of structure and role of the vairav Technology in the next page as the above figure is blurry.)

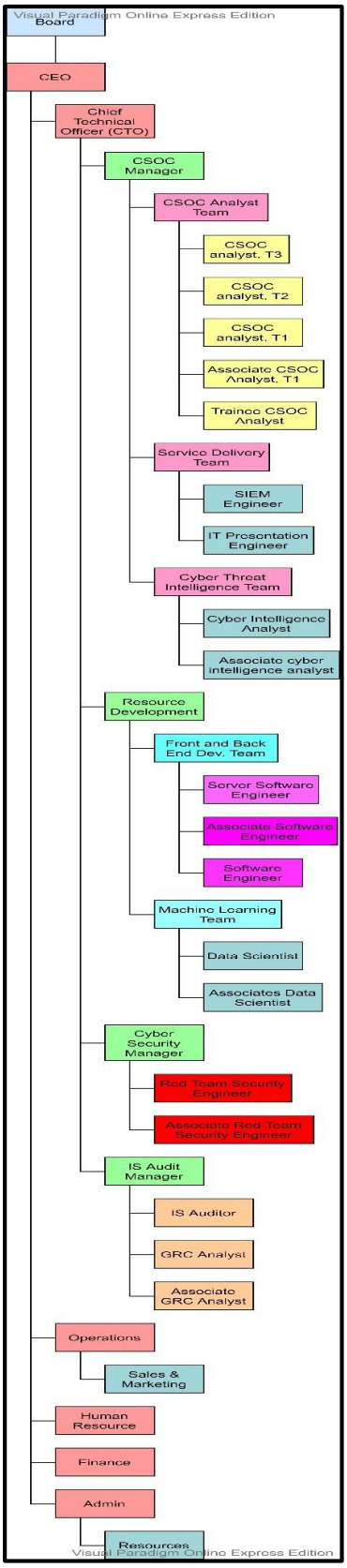

Visual Paradigm Online Express Edition
Board
CEO
Chief Technical Officer (CTO)
CSOC Manager
CSOC Analyst Team
CSOC analyst, T3
CSOC analyst, T2
CSOC analyst, T1
Associate CSOC Analyst, T1
Trainee CSOC Analyst
Service Delivery Team
SIEM Engineer
IT Presentation Engineer
Cyber Threat Intelligence Team
Cyber Intelligence Analyst
Associate cyber intelligence analyst
Resource Development
Front and Back End Dev. Team
Server Software Engineer
Associate Software Engineer
Software Engineer
Machine Learning Team
Data Scientist
Associates Data Scientist
Cyber Security Manager
Red Team Security Engineer
Associate Red Team Security Engineer
IS Audit Manager
IS Auditor
GRC Analyst
Associate GRC Analyst
Operations
Sales & Marketing
Human Resource
Finance
Admin
Resources
Visual Paradigm Online Express Edition

Figure 3 structure and role of Vairav Technology (2)

The "Vairav Technology" company is currently being handled by two highly competent Chief Executive Officers (CEO) and Chief Technical Officers (CTO) under the direction of the board that oversees the department where the internship placement was organized. The CSOC, Coordinator, Resource Management, Cyber Security Officer, and IS Audit Manager are four highly skilled professionals that operate all of the company's technical elements with reference to all of the customer's specific needs, while the CEO manages all of the company's business aspects. The Chief Executive Officer is in charge of all initiatives, marketing and sales, accounting, capital, and so on (CEO).

1.3 Details of the department worked in

During the period of internship, I worked at three different department such as Vulnerability assessment and penetration and testing (VAPT), Governance, Risk Management and Compliance management (GRC) and Security operation center (SOC).

Miss Anima, one of the company's auditors, served as my supervisor in the GRC department. During the period when the GRC department existed, she used to lead our team. She taught us how to conduct research on various topics such as GRC, IS Audit, Data Center, Business Continuity, Compliance, the importance of GRC, ISO 27001 and its data security association, human asset security, executive resources, access control, cryptography, physical and natural security, activities security, and so on, as well as internationally recognized compliance standards/polices and their cyber security.

In the SOC department I worked under Mr. Rishitosh Gatani's supervision. He used to assign research tasks on a weekly basis. Terminologies, which include asset, personal assets, business assets, current assets, fixed assets, Threat, Treat sources, Vulnerability and its types, Risk, attack and types of cyber-attack, CIA, attack methodology, OSINT and its tools and techniques, as well as their advantages and disadvantages, and CSIRT and its importance. We also learnt how to set up a virtual environment, install Nagios, Cacti, Snort, and point victim, attacker, and virtual

machines, install Wireshark and glass wire, and test and run Recon created in Nagios in this department.

The last department I worked in was the VAPT department, where I worked under Mr. Prem Basnet's supervision and he taught us how to use 'Wireshark,' one of the best host monitoring tools. Using Nmap was presented, and topics like Vulnerability Exploitation and Metasploit were briefly discussed during this phase of learning department VAPT.

2. Review of Activities

2.1 WRL Form Table

Learning Outcome ID	Learning outcomes	Activities and tasks	Evidence
LO1	Governance, Risk Management and Compliance Management (GRC)	By consume the inside review, consistence, and administration.	It could be verified through different screenshot, viva, documentation, and report.
LO2	Security operation Centre (SOC)	By getting the knowledge from the supervisor to perform the security operation.	It could be verified through different screenshot, viva, documentation, and report.
LO3	Vulnerability Assessment and	By consume the inside review,	It could be verified through different

	penetration Testing (VAPT)	consistence, and administration. I will learn the essential information through the given exercise by the supervisor of the company.	screenshot, viva, documentation, and report.
LO4	Teamwork	By working with the team member weekly and sharing the information with the team	It could be verified through information sharing sessions which will conducted weekly and by, group member.
LO5	Report writing skill	By writing the report of the task related and its test done.	It could be verified through logbooks, documentation and the assigned report at the organization through the portfolio of the company.
LO6	Develop knowledge about cyber security and defensive skills	I will conduct research on cybersecurity and for defensive skills	I will provide documents and research papers.
LO7	Appropriate communication	By developing the skills to communicate with	It can be verified through my supervisor, log

	skills required for security testing	the group member, supervisor, and the clients.	books, group member, and the proof of training session at the organization

Table 1 WRL Form Table

2.2 LO1 Governance, Risk Management and Compliance Management (GRC)

This is the first learning outcome of my work-related learning. In this learning outcome, I improved my research skills in the problem domain and solved the problems I encountered. Supervisor has assigned us the task of investigating specific topics, such as the similarities and differences between GRC, ISO 27001, GDPR and CCPA. I researched on the GRC and IS audit through different books, websites etc. also researched NIST, which is one of the standard structures of cybersecurity companies and presented the results to the meeting. I studied various attacks as well as categories of APTs and how the meaning of Defense in Detail would improve reduce certain incidents. We discovered a variety of other topics. We investigated more about the Event Viewer, the Group Policy Editor. Every day, I encouraged them to send daily activities based on the results of these studies. I used to search various websites, articles, books and magazines. In addition, my supervisor gave me ideas and tips for easy and efficient research. In addition, I was investigating problems that occurred according to my supervisor instructions.

The evidence of these remarks is given in the **LO1: Evidence** section

2.3 LO2 Security operation Centre (SOC)

This is the second thing I learned during my internship at Vairav Technology. I'm moving forward to the Security Operations Center (SOC) section to increase my SOC skills. As a result of this learning outcome, I have expanded my understanding of SOC, where we explored many topics and discussed their significance with our supervisor.

2.3 LO3 Vulnerability and Penetration Testing (VAPT)

This is the first thing I learned during my internship at Vairav Technology. I advance to the VAPT department in order to develop my VAPT skills. Because of this learning result, I learnt more about VAPT. Vulnerability Exploitation and Metasploit, as well as how to use the Metasploit tools, were briefly discussed during this period. I also used Metasploit to try to amplify vulnerabilities. Members of the group were taught concepts like vulnerability exploitation, as well as full descriptions of each Metasploit vulnerability exploitation accessibility, throughout this time.

2.5 LO4 Teamwork

This is the fourth learning outcome, and it has really aided me in improving my teamwork abilities and managing my time in meetings to complete various tasks on schedule. Our supervisor at Vairav Technology wanted that we work individually rather than as a team throughout my internship. However, once we have completed our study on a particular topic, we must present it at the next meeting and discuss our thoughts on the subject, and if we encounter any difficulties, my collagenous and supervisor will assist us in resolving the issue. As a result, it enables me to operate as part of a team with confidence, comfort, and a good attitude with professionals.

2.6 LO5 Report writing skills

This is the fifth learning consequence from my vairav technology internship. It has tremendously aided me in improving my report writing skills with the help of these learning outcomes. Every group member in the GRC and SOC departments must submit a report.

As a result, we must report on the matter on a daily and weekly basis. I enhanced my report writing skills as a result of these learning outcomes.

2.7 LO6 Develop knowledge about cyber security and defensive skills

This is the sixth learning outcome from my Vairav Technology internship. I increased my understanding and expertise about cybersecurity with the help of these learning outcomes. I built python code and received results from Elasticsearch with the help of my supervisor and research, using techniques like Requests, JSON, and Datetime. This provided me with the opportunity to learn how to automate security using the API. Supervisors also conducted a thorough investigation on CVE, CVSS, and scope protection, recommending that users detect suspicious IP addresses using VirusTotal and Malware Bazar.

2.8 LO7 Appropriate communication skills

This is the seventh and last learning consequence from my vairav technology internship. I collaborated with a group member on this learning outcome. Our supervisor used to assign us tasks requiring us to conduct research on various topics and then respond to the supervisor's question at the next meeting. That is, we debate the matter with the other members of the group and devise a plan to carry out the task in a timely manner. This intern assists me in improving my communication skills with a variety of clients, whether via email, phone calls, or in person. Through viber group chats and hangouts, I was quite good at communicating with the supervisor.

3 Academic Context

There is the module called Work Related Learning (WRL) in Islington college which required graduate students to participate in an internship program in order to get experience in the professional work environment of various sorts of businesses. Approximately 60 days. During this time, each student will have the opportunity to observe the business, play a key role, and obtain valuable work experience that will be useful after graduation. Basically, he knows that Islington

College provides students with certain types of modules, which they will need when they are ready to enter the profession. Make certain of it. Among them, several modules have benefited me considerably and provided me with the information and expertise I needed to assist me solve the challenges I faced throughout my internship.

Modules like Professional Ethics have helped me improve my personality and general skills in work efficiency. Time was also invaluable and helped during the internship, when deadlines and reports were my daily job. The IT Security and Risk Crisis module also helped the intern by teaching us real-time surveillance systems, information security, intrusion testing and risk management. Similarly, modules such as CCNA (Routing and Switching) have assisted us in learning the fundamentals of network ideas and how to construct and maintain routing protocols. Also, how the switch is configured for VLAN, VTP, and STP. During my internship, I was significantly involved in detecting and protecting against cyberattacks, as well as detecting, evaluating, and responding to incidents and threats, as well as instructing people to avoid them. The “Digital Crime Investigation” module helped us understand and gain a basic understanding of the concepts of crime and threat, crimes and threats, and how your response to their occurrence is implemented and sustained.

So, without the knowledge gained through studying, I would have played very badly during the internship. By gaining this basic knowledge with the elements described, I was able to understand the context more easily and learn more in a short amount of period during my internship.

4 Abilities Evaluation

4.1 LO1 Vulnerability Assessment and penetration Testing (VAPT)

This learning outcome has definitely aided my VAPT abilities improvement. During my internship, I worked in all three departments and learnt a variety of tools and techniques

that have helped me improve my understanding of vulnerability and penetration testing (VAPT). With Metasploit, I also learn about amplification of vulnerabilities. I will be able to implement VAPT on my network in real-time working with this expertise.

4.2 LO2 Security operation Centre (SOC)

This learning outcome has significantly improved my SOC abilities. I worked in each of the three departments during my internship. We researched many topics in this Security operation Centre and had the opportunity to learn about the topic Security operation Centre (SOC) and its importance. I will be able to apply SOC to real-time work with this understanding.

4.3 LO3 Governance, Risk Management and Compliance Management (GRC)

This learning outcome has greatly helped me improve my GRC skills. During my internship, I worked in all three departments. We researched in the different topic and get chance know about the topic Governance, Risk Management and Compliance Management and its importance. With this knowledge, I will be able to implement SOC on real-time work.

4.4 LO4 Teamwork and develop research skills

This set of learning outcomes has really aided me in honing my teamwork abilities. During the internship, we worked in groups and completed tasks with the assistance of team members. As a result, it enables me to operate as part of a team with confidence, comfort, and a good attitude with professionals. Through a research during the internship, we produced a series of well-documented reports. This learning outcome will also be very useful for conducting excellent research on all relevant topics and for producing well-researched reports on the future workplace, which gave me many ideas about research technology. In addition, my research ability to overcome all the problems of my career gradually increased to the professional level. The evidence are also given below.

4.5 LO5 Report writing skills and Task tracking skill.

This is the sixth learning result that has considerably aided me in expanding my knowledge of report writing skills. During the intern period, we are required to conduct research on a variety of topics in several departments, which aids my professional development. This learning outcome has really aided my task tracking abilities. We planned activities and established deadlines for each task to track task progress and assure execution to manage meeting attendance and finish tasks on time.. Documents have been completed and presented on Google Drive with my superiors for everything else of the investigation and operate completed. Schedule and enhance with task tracking skills

Evidence of this remarks is given below on evidence section.

4.6 LO6 Develop knowledge about cyber security and defensive skills

This is the sixth learning result that has substantially aided me in improving my knowledge of cyber security law and defensive skills. During my internship, I worked in many departments and learned about the importance of cybersecurity around the world. It was simple to develop a feel for dealing with the numerous tools and techniques in Linux by practicing the command. We can simply tackle the problem by conducting study.

4.7 LO7 Appropriate communication skills

This learning outcome has significantly aided me in improving my communication skills in meetings with team members and supervisors. It was critical to maintain good contact with my supervisor and coworkers in order to complete the duties assigned throughout the internship. I was first nervous, but I was able to speak and work without difficulty. This learning outcome is quite beneficial to me.

5 Challenges

Challenges were supposed to be a learner of the job. I had theoretical knowledge of most things relevant to the job, but I had to struggle a little bit in the first week of my internship because of the lack of proper practical knowledge. I was anxious initially and was not comfortable with the professional working zone.

At the first day of the meeting, our supervisor introduced about the topic we are going through Vulnerability assessment and penetration and testing (VAPT), Governance, Risk Management and Compliance management (GRC) and Security operation center (SOC) topic which includes their working mechanism and advantages in different sectors. The meeting's major goal was to do research and gain a better understanding of the fundamental ideas of IS audit and GRC. As directed, I conducted research on the GRC and IS audit using various books, websites, and other resources. And I had to provide a brief overview of the issue; however, I had made a few attempts at giving a presentation at college, but they were not great, and I was unable to do so, and I felt ashamed; however, my colleagues and supervisors were supportive and encouraged me to speak without hesitation. I gradually learnt to speak about my study on a daily basis, and now I am confident in my ability to complete the task.

One of most challenging part of the internship was that if there was a problem somewhere, I wasn't sure where to start from. I had no idea what protocol had to be followed. The first step is to assess the problem, look for alternatives, correct the problem with specialized tools, and then resolve the problem as needed. I had to conduct substantial research using the Internet in order to obtain the concepts.

And with support of supervisors and colleagues, I was capable of dealing with it, despite the initial difficulties. They understood that I was just a student and technically wants to understand several issues, and they were really happy to support me and fix any problems for me.

6 Conclusion and Future Plans

6.1 Conclusion

The module on work-related learning was quite beneficial in terms of providing me with opportunities to gain professional work experience. I had a terrific time working at a firm and learning about so many new topics and concepts in order to improve myself. This session assisted me in generating ideas and determining my area of interest for a future job in cybersecurity and information technology. I was able to directly participate with the cybersecurity and IT industries, learning a number of topics that would be quite valuable in my future employment. I was able to supervise colleagues while also learning from them.

The WRL module has made me understand the value of logs and proof for learning. It has motivated me to work through setting targets and reaching a timetable to reach the goals, reminding me of the importance of time to achieve those goals. Working in a company has made me a better person than I was yesterday, even though it has only been for a few months, as I have acted decently and generously with coworkers and superiors. My communication and problem-solving skills increased as a result of the exercises I was able to complete with the help of my coworkers.

6.2 Future Plans

Since I've gained a lot of knowledge for this module, as well as previous modules on the concept of and computer security that I've been taught at college via internship, it's time to decide whether or not I want to pursue a professional career in the field of information technology. As a result, my current strategy is to obtain as much experience as possible while also expanding my knowledge and skills in my field of study.

As an intern at Vairav Technology, I have gained limited experience. But my full concentration right now is on finishing my bachelor's degree in networking and IT security. I have already determined that my future work will take place in the area

of cybersecurity and IT. And after bachelor's degree, I am ready to work for a year and then study masters in IT here at Islington College for graduation.

7 References

technology, 2021. *vairab technology.* [Online]
Available at: https://www.linkedin.com/company/vairavtechnology/
[Accessed 22 jan 2022].

vairav, 2022. *vairab technology.* [Online]
Available at: https://vairav.net/
[Accessed 25 jan 2022].

8 Appendix

8.1 WRL Form

London Metropolitan University School of Computing

FC6W51 Work Related Learning (WRL) Form

Student

Student Londonmet ID: 19031311

Student Name: Himanshu Pandey

College E-mail ID: np01nt4a190131@islingtoncollege.edu.np

Mobile No: 9865762000

Student's work/placement address: Vairav Technology security PvtLtd/Thirban sadak 148, Kathmandu Nepal

Employer

Employer Name : Saroj Lamichhane

Employer's Address including department: C.E.O

Company Supervisor's Name and Position: Anima Pokhrel (GRC Analyst Is Audit)

Company Supervisor's Tel No: 9779867586774

Company Supervisor's email address: anima@vairav.net

Work Related Learning Activity

Start Date: 21st September2021

End Date (if known): 16th January 2022

Your role at the placement (position): Cyber Security Intern

Brief description of your work at the placement:

My job with the placement is to fulfill the allocated quotas within the specified time frame before sending the report to the supervisor. I have been allocated 20 days for Governance, Risk Management and Compliance GRC placement then the next 20 days in the Security operation center developer placement SOC and finally the next 20 days in the Vulnerability Assessment and Penetration Testing VAPT placement inside the company.

Figure 4 WRL Form (1)

London Metropolitan University School of Computing

Proposed learning outcomes from the Work Related Learning Activity:
It is very important that you read the learning agreement guide before filling in this form. You need to list **at least 7 learning** outcomes, and at least **two** learning activities should be closely relevant to the course you are doing at the university.

Learning Outcome ID	**Learning outcomes** By the end of my work placement, I will be able to develop what skills or knowledge: (e. g. develop my XXX skills, enhance my knowledge of XXX)	**Activities and tasks** I will achieve this learning outcome by carrying out what tasks (e. g. participating in a Web development project, or to work in a team, or to engage in group discussion)	**Evidence** Evidence I could use to demonstrate that I have achieved this learning outcome? (e. g. feedback from the employer, artefacts I will develop, screenshots or video capture, meeting minutes)
LO1	Developed my knowledge in basic concepts of GRC (Governance Risk Compliance) it's importance, tools and various certification.	By partaking in the inside review, hazard and consistence exercise and administration	It can be verified through viva, soft copy documents and daily activities maintained during the Working meeting minutes. I have created some of the reports that were given during our work time.
LO2	Team Work	By taking an interest in week by week meeting and sharing data during authority and informal time.	Through screen capture, input from my other colleagues, season of meeting directed week after week.
LO3	Appropriate communication skills with mentors and team members.	Developed indispensable skills which were required to communicate with team members and supervisor.	Through input from my other colleagues, season of meeting directed week after week.
LO4	Cyber related views in Nepal as well as international laws.	By researching the cyber law from national government and international IT guidelines.	Research done on national and international cyber laws and screenshot.
LO5	Vulnerability Assessment and Penetration Testing(VAPT)	I will acquire vital information through exploration by showing learning exercise by the supervisor of the association.	Evidence I could use to demonstrate that I have achieved in this learning period are feedback from employer, screenshots etc.

Figure 5 WRL Form (2)

London Metropolitan University School of Computing

LO6	security operation centre (SOC)	Getting the knowledge from supervisor how to perform the security operation.	It could be verified through viva, different screenshots, notes and report.
LO7	Report writing skills	By writing reports of the related topics, proof of the test done and many more.	Through documentation.

This form is approved by WRL academic supervisor

Academic Supervisor Name: Ravi Chandra Gurung /Bibek Khanal

Academic Supervisor Signature:

Date of Signature: 24 January 2022

if you work at an external company or organization, the following "Health and Safety checklist" form must be completed before your placement can be approved.

Figure 6 WRL Form (3)

London Metropolitan University School of Computing

If you work at an external company or organization, the following "Health and Safety checklist" form must be completed before your placement can be approved.

LONDON METROPOLITAN UNIVERSITY

External Work Related Learning (PLACEMENT) PROVIDER
HEALTH AND SAFETY CHECKLIST

Name of the Placement Provider (Company name): vairav.net
Placement site Supervisor: Richa Nepal
Supervisor's Position: GRC Analyst
Address: Baluwatar, Kathmandu
Email: richa.nepal@vairav.net
Telephone: 9779867586774

		Yes	No
1	Do you have a written Health & Safety policy? no	Yes	
2	Do you have a policy regarding health and safety training for people working in your undertaking, including use of vehicles, plant and equipment, and will you provide all necessary health and safety training for the student ?		No
3	Is the organization registered with? (tick as appropriate) (a) the Health & Safety Executive or (b) the Local Authority Environmental Health Department		No No
4	**Insurance** (a) Is Employer and Public Liability Insurance which will cover the duration of the placement? (b) Employer and Public Liability Insurance policy number —————— (c) (c)Will your insurance cover any liability incurred by a placement student as a result of his/her duties as an employee?		No No No
5	**Risk Assessment** (a)Have you carried out any risk assessment of your work practices to identify possible risks whether to your own employees or to others within your undertaking? b) Are risk assessments kept under regular review? (c)Are the results of risk assessment implemented?		Yes Yes Yes
6	**Accidents and Incidents** (a)Is there a formal procedure for reporting and recording accidents and incidents in accordance with RIDDOR (Reporting of Injuries, Disease & Dangerous Occurrence Regulations)? (b)Have you procedures to be followed in the event of serious and imminent danger to people at work in your undertaking? (c)Will you report to the university all recorded accidents involving placement students? (d)Will you report to the university any sickness involving placement students which may be attributable to the work.		Yes Yes Yes Yes

The above statements are true to the best of my knowledge and belief.

Signed on behalf of the company with the company stamp:

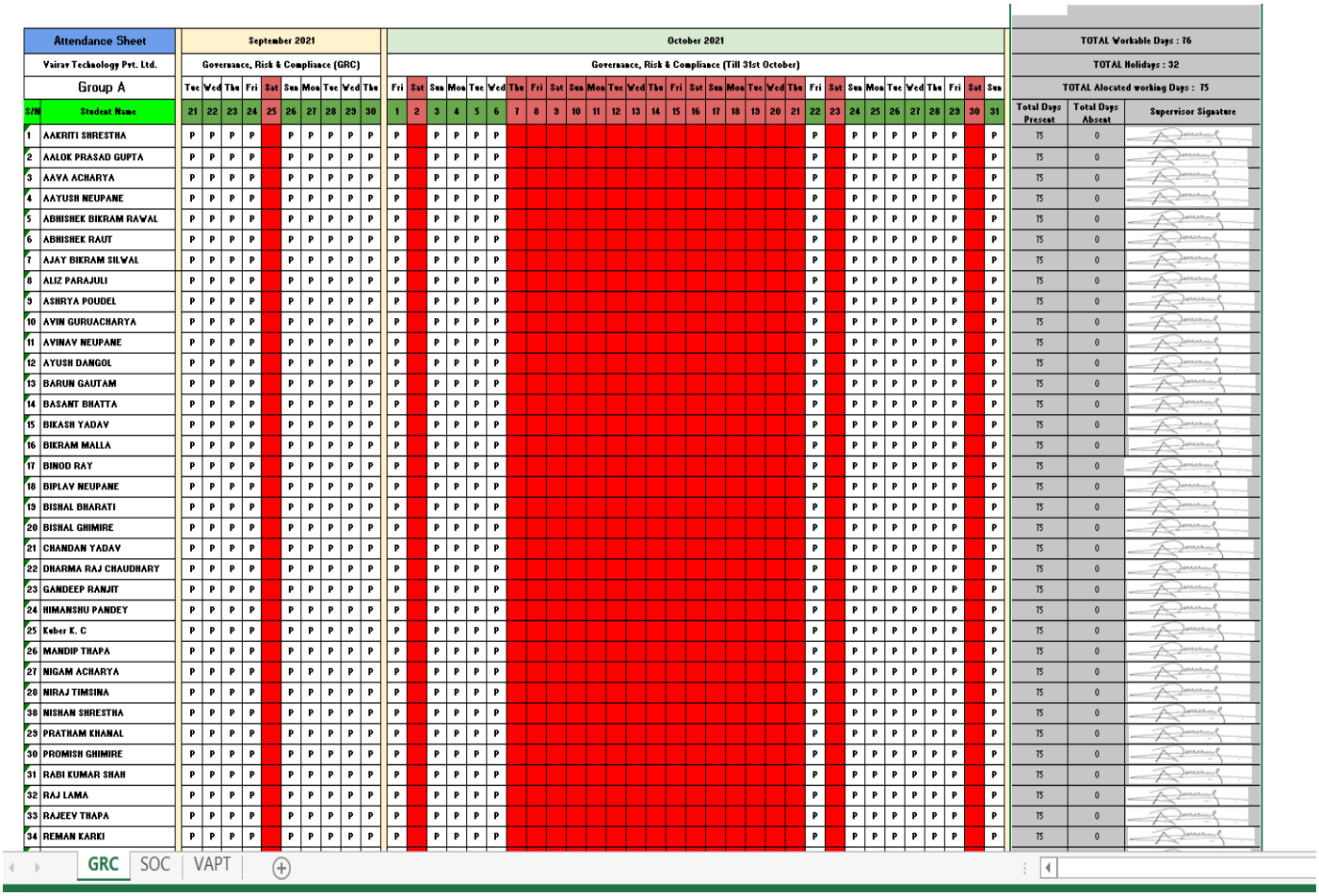
Name:

Signature:

Date:

Figure 7 WRL Form (4)

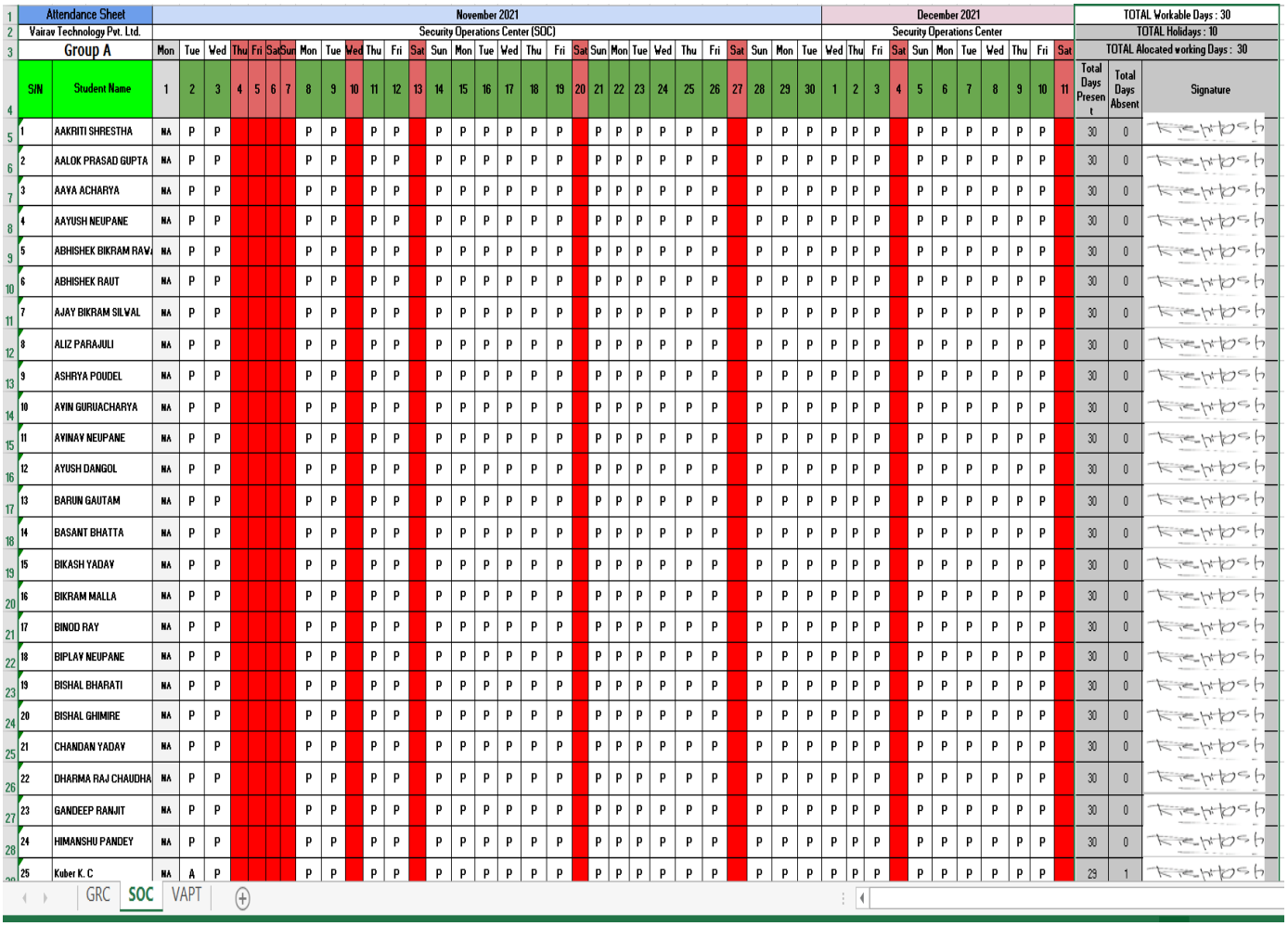
8.2 Attendance Sheet



Attendance Sheet		September 2021										October 2021																													TOTAL Workable Days : 76		
Vairav Technology Pvt. Ltd.		Governance, Risk & Compliance (GRC)										Governance, Risk & Compliance (Till 31st October)																													TOTAL Holidays : 32		
Group A		Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun						TOTAL Alocated working Days : 75		
S/N	Student Name	21	22	23	24	25	26	27	28	29	30	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	Total Days Present	Total Days Absent	Supervisor Signature
1	AAKRITI SHRESTHA	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
2	AALOK PRASAD GUPTA	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
3	AAVA ACHARYA	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
4	AAYUSH NEUPANE	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
5	ABHISHEK BIKRAM RAWAL	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
6	ABHISHEK RAUT	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
7	AJAY BIKRAM SILWAL	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
8	ALIZ PARAJULI	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
9	ASHRYA POUDEL	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
10	AVIN GURUACHARYA	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
11	AVINAV NEUPANE	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
12	AYUSH DANGOL	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
13	BARUN GAUTAM	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
14	BASANT BHATTA	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
15	BIKASH YADAV	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
16	BIKRAM MALLA	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
17	BINOD RAY	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
18	BIPLAV NEUPANE	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
19	BISHAL BHARATI	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
20	BISHAL GHIMIRE	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
21	CHANDAN YADAV	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
22	DHARMA RAJ CHAUDHARY	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
23	GANDEEP RANJIT	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
24	HIMANSHU PANDEY	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
25	Kober K. C	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
26	MANDIP THAPA	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
27	NIGAM ACHARYA	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
28	NIRAJ TIMSINA	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
38	NISHAN SHRESTHA	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
29	PRATHAM KHANAL	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
30	PROMISH GHIMIRE	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
31	RABI KUMAR SHAH	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
32	RAJ LAMA	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
33	RAJEEV THAPA	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	
34	REMAN KARKI	P	P	P	P		P	P	P	P	P	P		P	P	P	P																P		P	P	P	P	P		P	75	0	

GRC SOC VAPT

Figure 8 Attendance of GRC department



Attendance Sheet		November 2021																																December 2021										TOTAL Workable Days : 30		
Vairav Technology Pvt. Ltd.		Security Operations Center (SOC)																																Security Operations Center										TOTAL Holidays : 10		
Group A		Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	TOTAL Allocated working Days : 30		
S/N	Student Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	1	2	3	4	5	6	7	8	9	10	11	Total Days Present	Total Days Absent	Signature
1	AAKRITI SHRESTHA	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
2	AALOK PRASAD GUPTA	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
3	AAYA ACHARYA	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
4	AAYUSH NEUPANE	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
5	ABHISHEK BIKRAM RAV	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
6	ABHISHEK RAUT	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
7	AJAY BIKRAM SILWAL	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
8	ALIZ PARAJULI	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
9	ASHRYA POUDEL	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
10	AYIN GURUACHARYA	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
11	AYINAY NEUPANE	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
12	AYUSH DANGOL	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
13	BARUN GAUTAM	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
14	BASANT BHATTA	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
15	BIKASH YADAV	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
16	BIKRAM MALLA	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
17	BINOD RAY	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
18	BIPLAV NEUPANE	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
19	BISHAL BHARATI	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
20	BISHAL GHIMIRE	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
21	CHANDAN YADAV	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
22	DHARMA RAJ CHAUDHA	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
23	GANDEEP RANJIT	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
24	HIMANSHU PANDEY	NA	P	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		30	0	
25	Kuber K. C	NA	A	P					P	P		P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		29	1	

GRC SOC VAPT

Figure 9 Attendance of SOC department

		Dec-21														Jan-22													TOTAL Workable Days : 24		
		Vulnerability assessment and penetration testing (VAPT)																											TOTAL Holidays : 3		
	Group A	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	TOTAL Alocated working Days : 24		
S/N	Student Name	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6	7	Total Days Present	Total Days Absent	Signature
1	AAKRITI SHRESTHA	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
2	AALOK PRASAD GUPTA	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
3	AAVA ACHARYA	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
4	AAYUSH NEUPANE	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
5	ABHISHEK BIKRAM RAWAL	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
6	ABHISHEK RAUT	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
7	AJAY BIKRAM SILWAL	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
8	ALIZ PARAJULI	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
9	ASHRYA POUDEL	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
10	AVIN GURUACHARYA	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
11	AVINAV NEUPANE	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
12	AYUSH DANGOL	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
13	BARUN GAUTAM	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
14	BASANT BHATTA	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
15	BIKASH YADAV	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
16	BIKRAM MALLA	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
17	BINOD RAY	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
18	BIPLAV NEUPANE	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
19	BISHAL BHARATI	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
20	BISHAL GHIMIRE	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
21	CHANDAN YADAV	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
22	DHARMA RAJ CHAUDHARY	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
23	GANDEEP RANJIT	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
24	HIMANSHU PANDEY	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	
25	Kaber K. C	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	1	
26	MANDIP THAPA	P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P		P	P	P	P	P	P	24	0	

GRC | SOC | VAPT

Figure 10 Attendance of VAPT department

8.3 Internship Completion Letter

VAIRAV
TECHNOLOGY SECURITY PVT. LTD

Date: 20th January, 2022

EXPERIENCE CERTIFICATE

This is to certify that **Mr. Himanshu Pandey**, worked as an **Intern** in Vairav Technology Security from **21st September, 2021** to **7th January, 2022.**

During his tenure he was found committed and dedicated towards his responsibilities concerned with his job roles.

We wish him all the best for his future endeavors.

Thank You.

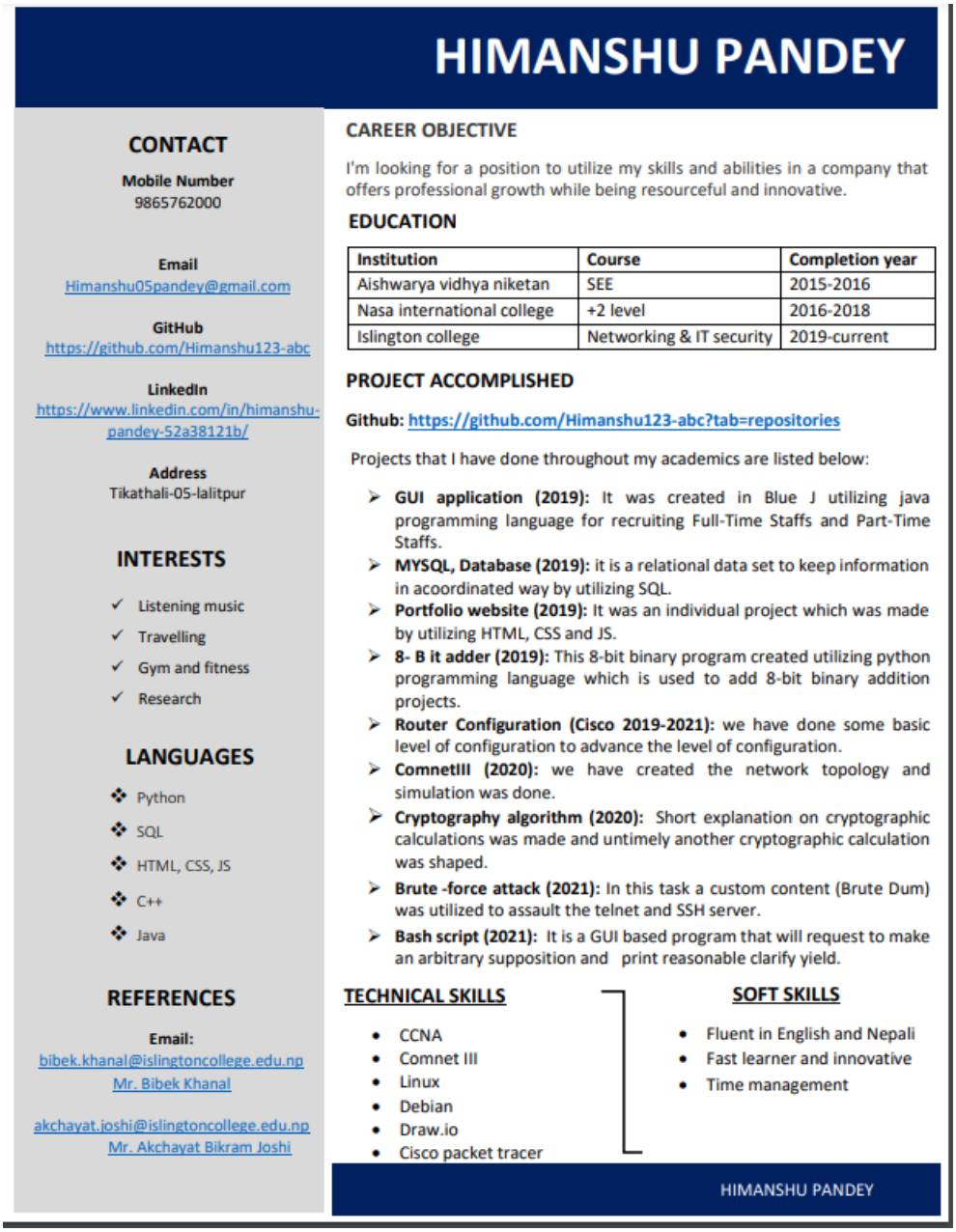
With Regards,

Subita Kapali
Group Head - Human Resource

CYBER DEFENDER FROM THE LAND OF GURKHA

Figure 11 Experience Certificate given by the company

8.4 CV



HIMANSHU PANDEY

CONTACT

Mobile Number
9865762000

Email
Himanshu05pandey@gmail.com

GitHub
https://github.com/Himanshu123-abc

LinkedIn
https://www.linkedin.com/in/himanshu-pandey-52a38121b/

Address
Tikathali-05-lalitpur

INTERESTS

- ✓ Listening music
- ✓ Travelling
- ✓ Gym and fitness
- ✓ Research

LANGUAGES

- ❖ Python
- ❖ SQL
- ❖ HTML, CSS, JS
- ❖ C++
- ❖ Java

REFERENCES

Email:
bibek.khanal@islingtoncollege.edu.np
Mr. Bibek Khanal

akchayat.joshi@islingtoncollege.edu.np
Mr. Akchayat Bikram Joshi

CAREER OBJECTIVE

I'm looking for a position to utilize my skills and abilities in a company that offers professional growth while being resourceful and innovative.

EDUCATION

Institution	Course	Completion year
Aishwarya vidhya niketan	SEE	2015-2016
Nasa international college	+2 level	2016-2018
Islington college	Networking & IT security	2019-current

PROJECT ACCOMPLISHED

Github: https://github.com/Himanshu123-abc?tab=repositories

Projects that I have done throughout my academics are listed below:

- **GUI application (2019):** It was created in Blue J utilizing java programming language for recruiting Full-Time Staffs and Part-Time Staffs.
- **MYSQL, Database (2019):** it is a relational data set to keep information in acoordinated way by utilizing SQL.
- **Portfolio website (2019):** It was an individual project which was made by utilizing HTML, CSS and JS.
- **8- B it adder (2019):** This 8-bit binary program created utilizing python programming language which is used to add 8-bit binary addition projects.
- **Router Configuration (Cisco 2019-2021):** we have done some basic level of configuration to advance the level of configuration.
- **ComnetIII (2020):** we have created the network topology and simulation was done.
- **Cryptography algorithm (2020):** Short explanation on cryptographic calculations was made and untimely another cryptographic calculation was shaped.
- **Brute -force attack (2021):** In this task a custom content (Brute Dum) was utilized to assault the telnet and SSH server.
- **Bash script (2021):** It is a GUI based program that will request to make an arbitrary supposition and print reasonable clarify yield.

TECHNICAL SKILLS

- CCNA
- Comnet III
- Linux
- Debian
- Draw.io
- Cisco packet tracer

SOFT SKILLS

- Fluent in English and Nepali
- Fast learner and innovative
- Time management

HIMANSHU PANDEY

Figure 12 CV (Updated)

8.5 Evidence

8.5.1 LO1: Evidence

Home > IT Leadership > Compliance

ANALYSIS

What is GRC and why do you need it?

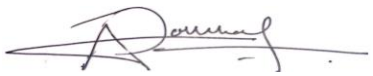
GRC can help you align IT activities to business goals, manage risk effectively and stay on

By Kim Lindros

CIO | JUL 11, 2017 2:20 AM PDT

Governance, risk and compliance (GRC) refers to a strategy for managing an organization's overall governance, enterprise risk management and compliance with regulations. Think of GRC as a structured approach to aligning IT with business objectives, while effectively managing risk and meeting compliance requirements.

Figure 13 Research page on GRC



Supervisor Signature

Network protection is the state or cycle of ensuring and recuperating organizations, gadgets and projects from a cyberattack network safety alludes to the act of guaranteeing the respectability, secrecy, and accessibility (ICA) of data. Network safety alludes to a bunch of devices, hazard the board methods, innovation, preparing, and best practices that are continually developing to secure organizations, gadgets, projects, and information from assaults or unapproved access.

Common kinds of cyber security

Organization Security ensures network traffic by controlling approaching and active associations with keep dangers from entering or spreading on the organization.

Information Misfortune Avoidance (DLP) ensures information by zeroing in on the area, order and checking of data very still, being used and moving.

Cloud Security gives insurance to information utilized in cloud-based administrations and applications.

Interruption Identification Frameworks (IDS) or Interruption Anticipation Frameworks (IPS) work to recognize possibly antagonistic digital movement.

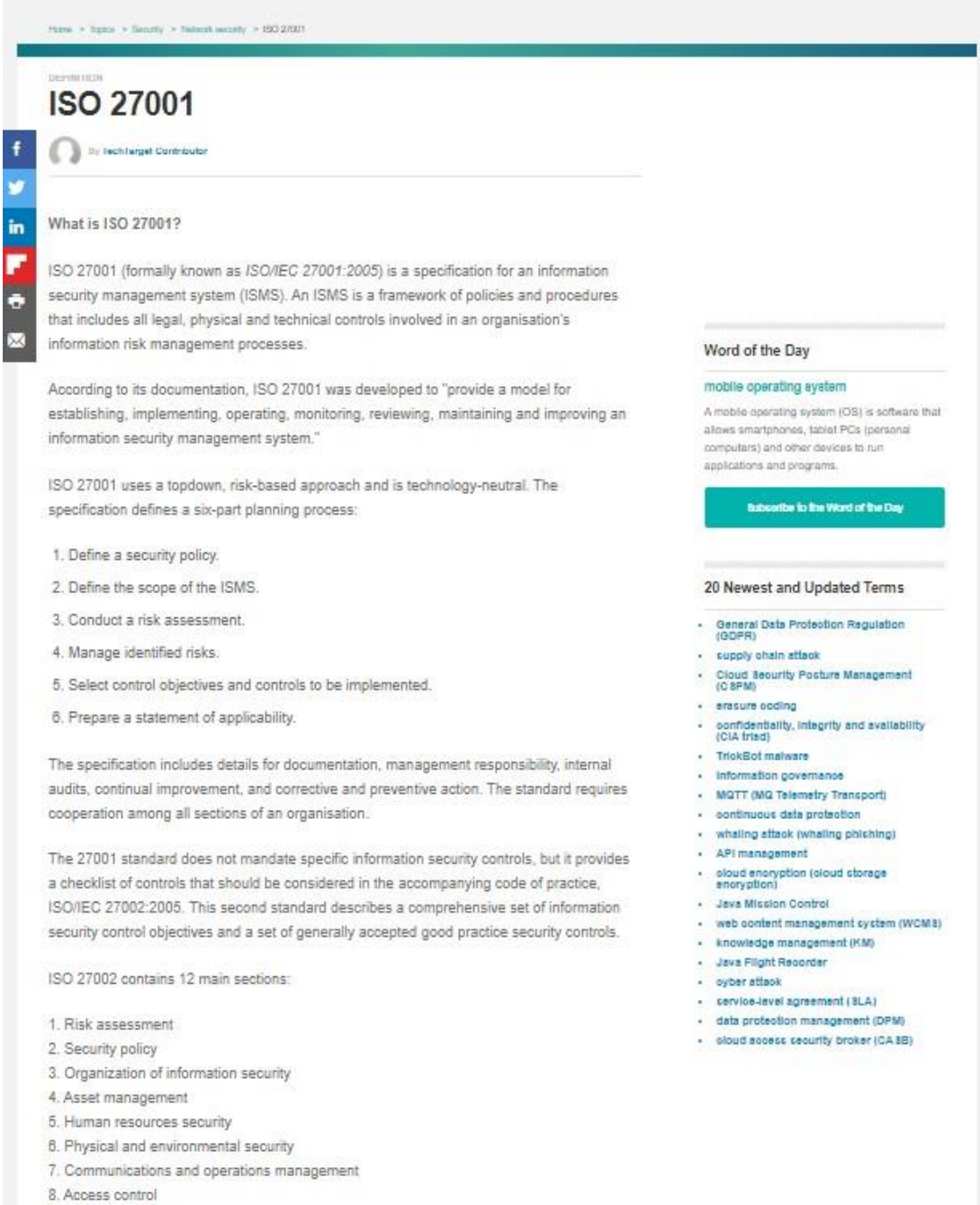
Personality and Access The executives (IAM) use validation administrations to restrict and follow representative admittance to shield inward frameworks from noxious elements.

Encryption is the method involved with encoding information to deliver it garbled, and is regularly utilized during information move to forestall burglary on the way.

Antivirus/against malware arrangements filter PC frameworks for known dangers. Current arrangements are even ready to recognize already obscure dangers dependent on their conduct.

Common types of cyber threats

Figure 14 research report on GRC



DEFINITION

ISO 27001

By TechTarget Contributor

What is ISO 27001?

ISO 27001 (formally known as *ISO/IEC 27001:2005*) is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

According to its documentation, ISO 27001 was developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system."

ISO 27001 uses a topdown, risk-based approach and is technology-neutral. The specification defines a six-part planning process:

1. Define a security policy.
2. Define the scope of the ISMS.
3. Conduct a risk assessment.
4. Manage identified risks.
5. Select control objectives and controls to be implemented.
6. Prepare a statement of applicability.

The specification includes details for documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action. The standard requires cooperation among all sections of an organisation.

The 27001 standard does not mandate specific information security controls, but it provides a checklist of controls that should be considered in the accompanying code of practice, ISO/IEC 27002:2005. This second standard describes a comprehensive set of information security control objectives and a set of generally accepted good practice security controls.

ISO 27002 contains 12 main sections:

1. Risk assessment
2. Security policy
3. Organization of information security
4. Asset management
5. Human resources security
6. Physical and environmental security
7. Communications and operations management
8. Access control

Word of the Day

mobile operating system

A mobile operating system (OS) is software that allows smartphones, tablet PCs (personal computers) and other devices to run applications and programs.

Subscribe to the Word of the Day

20 Newest and Updated Terms

- General Data Protection Regulation (GDPR)
- supply chain attack
- Cloud Security Posture Management (CSPM)
- erasure coding
- confidentiality, integrity and availability (CIA triad)
- TrickBot malware
- information governance
- MQTT (MQ Telemetry Transport)
- continuous data protection
- whaling attack (whaling phishing)
- API management
- cloud encryption (cloud storage encryption)
- Java Mission Control
- web content management system (WCMS)
- knowledge management (KM)
- Java Flight Recorder
- cyber attack
- service-level agreement (SLA)
- data protection management (DPM)
- cloud access security broker (CASB)

Figure 15 Research on ISO 27001

Supervisor Signature

Network protection is the state or cycle of ensuring and recuperating organizations, gadgets and projects from a cyberattack network safety alludes to the act of guaranteeing the respectability, secrecy, and accessibility (ICA) of data. Network safety alludes to a bunch of devices, hazard the board methods, innovation, preparing, and best practices that are continually developing to secure organizations, gadgets, projects, and information from assaults or unapproved access.

Common kinds of cyber security

Organization Security ensures network traffic by controlling approaching and active associations with keep dangers from entering or spreading on the organization.

Information Misfortune Avoidance (DLP) ensures information by zeroing in on the area, order and checking of data very still, being used and moving.

Cloud Security gives insurance to information utilized in cloud-based administrations and applications.

Interruption Identification Frameworks (IDS) or Interruption Anticipation Frameworks (IPS) work to recognize possibly antagonistic digital movement.

Personality and Access The executives (IAM) use validation administrations to restrict and follow representative admittance to shield inward frameworks from noxious elements.

Encryption is the method involved with encoding information to deliver it garbled, and is regularly utilized during information move to forestall burglary on the way.

Antivirus/against malware arrangements filter PC frameworks for known dangers. Current arrangements are even ready to recognize already obscure dangers dependent on their conduct.

Common types of cyber threats

Figure 16 task 1 report

Supervisor Signature

ISO 27001

ISO 27001 is the global standard centered in data security which was created to help associations of any industry or association to ensure their data in an orderly and practical manner through the reception of a data security the board framework.

ISO system is a bunch of arrangements and techniques that organizations can utilize. ISO 27001 gives a structure to ventures of any size or industry to utilize a Data Security The executives Framework to ensure their data in a deliberate and practical way (ISMS). It not just gives organizations the vital consistence for data yet additionally demonstrate its costumer that it shields their information.

The fundamental objective of ISO 27001 is to secure three parts of data.

Privacy: To give admittance to the data to just individuals which are approved for it.

Trustworthiness: Just the approved individual can change the data.

Accessibility: The data ought to be gotten to by individual just when it is required.

ISO 27001 controls list

Add-on A.5 - Data security

This addendum is planned to guarantee that approaches are set up and changed as per the association's general data security procedure.

Add-on A.6 - Association of Data Security

The task of obligations for specific errands is canvassed in this addition. It is isolated into two segments, with Addition A.6.1 checking that the association has constructed a design fit for executing and keeping up with data security methodology successfully.

Add-on A.6.2, then again, manages cell phones and remote working. It's planned to guarantee that everybody telecommuting or out and about, regardless of whether low maintenance or full-time, follows legitimate methods.

Add-on A.7 - Human asset security

Figure 17 task 2 report

Supervisor Signature

Domain 1: Business Continuity

This domain of cyber security focuses on restoring business operations after a catastrophic event, such as a natural disaster. This includes disaster recovery and business continuity plans and procedures. Of course, we should also make sure we're periodically reviewing these plans as well as testing them. The business continuity domain revolves around understanding which functions of the organization are vital to the survival of that organization. Once we've identified these critical functions and associated systems, we should put in place procedures to ensure they are operable as soon as possible, with as little data loss as possible, in the event of catastrophic failures.

Domain 2: Compliance

As you can probably imagine, the compliance domain centers on making sure the organization has the appropriate security controls in place necessary to meet compliance with the legislation and regulations applicable to the organization. This domain usually includes understanding those regulations to the point that we then can implement the appropriate security controls, and then regularly auditing those controls. Whether those audits are performed in-house or outsourced to a third-party audit agency is usually outlined in the regulations themselves, but regardless of who is performing the audit, it will be part of the compliance domain. Now, it's important that the compliance domain has a hand in driving our security management domain

Figure 18 task 3 report

Supervisor Signature

GRC

GRC is the incorporated assortment of capacities that empower an association to dependably accomplish goals, address vulnerability and act with respectability.

GRC is made of three sections – we should separate these:

Governance: the foundation of approaches, while proceeding to screen their appropriate execution.

Risk: a likelihood or danger of harm and injury.

Compliance: affirmation that activities are meeting necessities.

Key Roles:

For instance, a business client who needs to react to a verification or hazard evaluation, or who needs to remediate an issue might require this job. Clients with this job are given restricted admittance to information and to data applicable to their alloted assignments.

- perform and endorse hazard appraisals
- remediate assignments
- respond to/determine issues
- perform pointer errands
- mitigate hazard errands
- create an issue emergency
- work on proof solicitation errands

Figure 19 task 4 report

Supervisor Signature

DATA CENTER

A server farm is an office made out of arranged PCs, stockpiling frameworks and figuring foundation (the board and backing for end-client PCs, servers, stockpiling frameworks, working frameworks, data sets, middleware) that organizations and different associations use to coordinate, cycle, store and spread a lot of information

How it functions

A server farm office empowers an association to gather its assets and framework for information handling, stockpiling and interchanges, which include:

• frameworks for putting away, sharing, getting to and handling information across the association;

• actual foundation to help information handling and information interchanges; and

• utilities like cooling, power, network access and uninterruptible power supplies (UPS).

The Job of the Server farm

A server farm is an office made out of arranged PCs, stockpiling frameworks and registering infrastructure(management and backing for end-client PCs, servers, stockpiling frameworks, working frameworks, data sets, middleware) that organizations and different associations use to put together, interaction, store and spread a lot of information

How it functions

A server farm office empowers an association to gather its assets and framework for information handling, stockpiling and correspondences, which include:

• frameworks for putting away, sharing, getting to and handling information across the association;

• actual foundation to help information handling and information correspondences; and

• utilities like cooling, power, network access and uninterruptible power supplies (UPS).

Significance of Server farm

Figure 20 task 5 report

Supervisor Signature

Governance, Risk and Compliance (GRC): GRC is an administration for an association by and large administration, endeavor hazard the executives, and administrative consistence. GRC assists with adjusting IT to business objectives while viably overseeing hazard and accomplishing administrative necessities.

IS Audit: An IS Audit is the strategy and methods to assess the data framework adequacy. An IS review assists with deciding if data frameworks are securing organization resources, safeguarding the uprightness of put away and passed on information, successfully supporting corporate objectives, and running productively.

Figure 21 task 6 report

Supervisor Signature

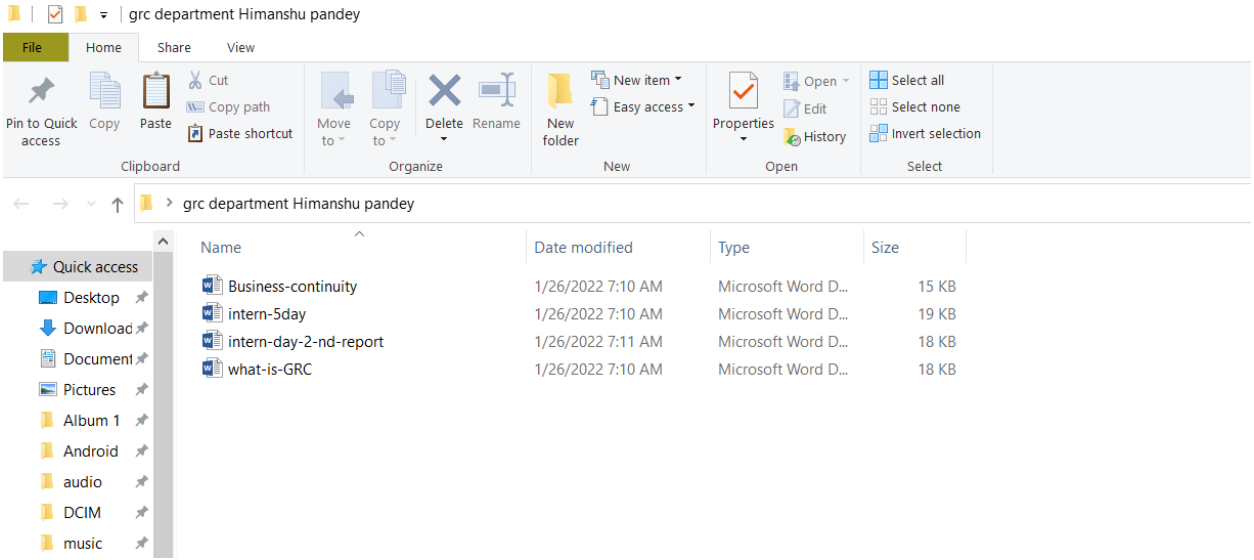


Figure 22 GRC department task files

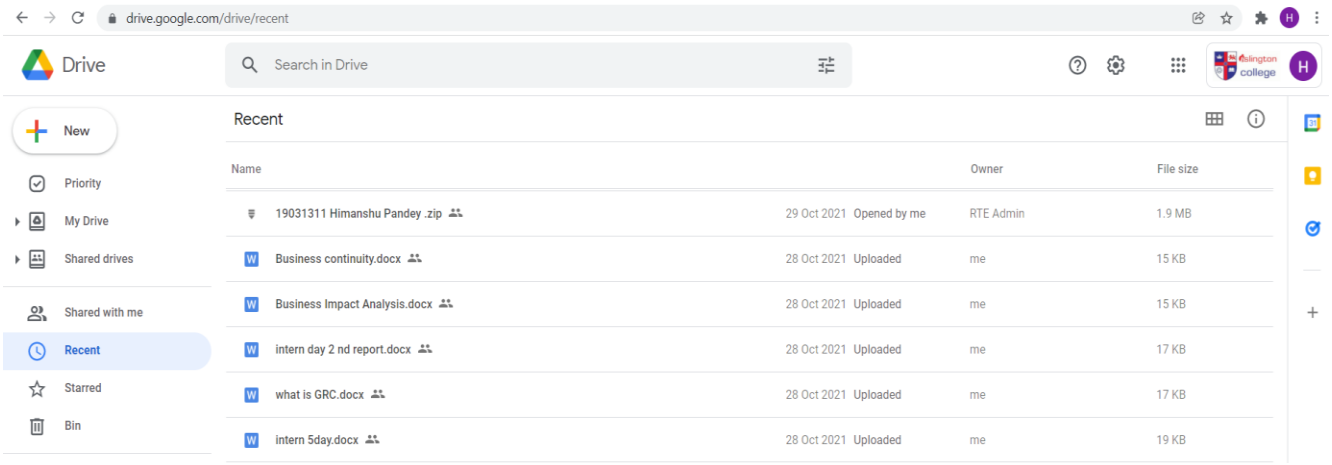
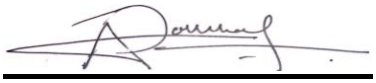


Figure 23 Tracking Task of GRC department



Supervisor Signature

8.5.2 LO2 Evidence

Signature

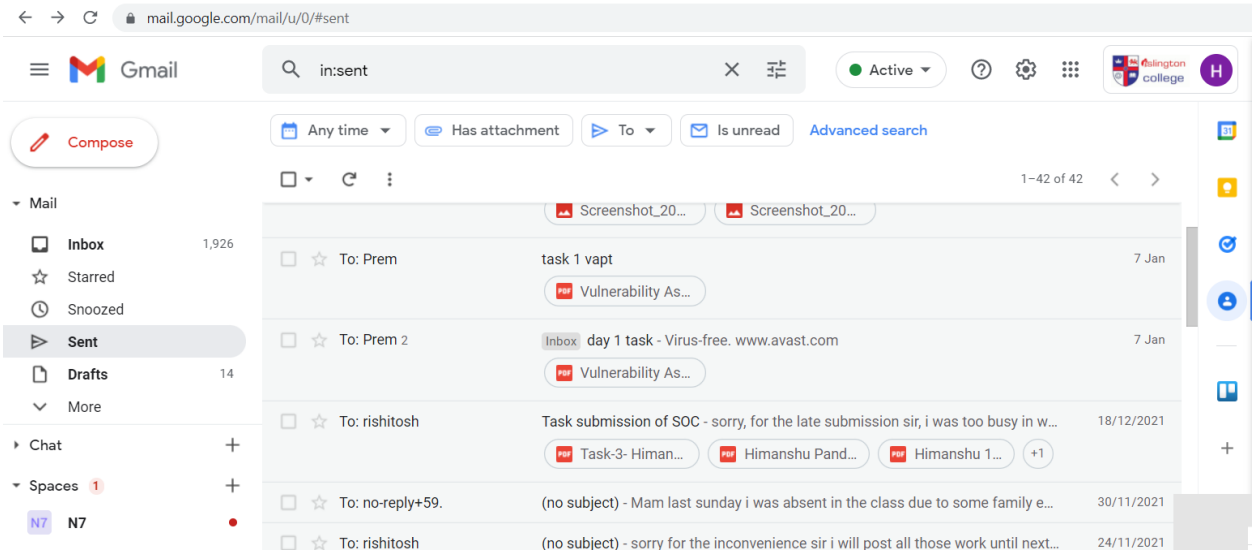


Figure 24 sending SOC task through gmail

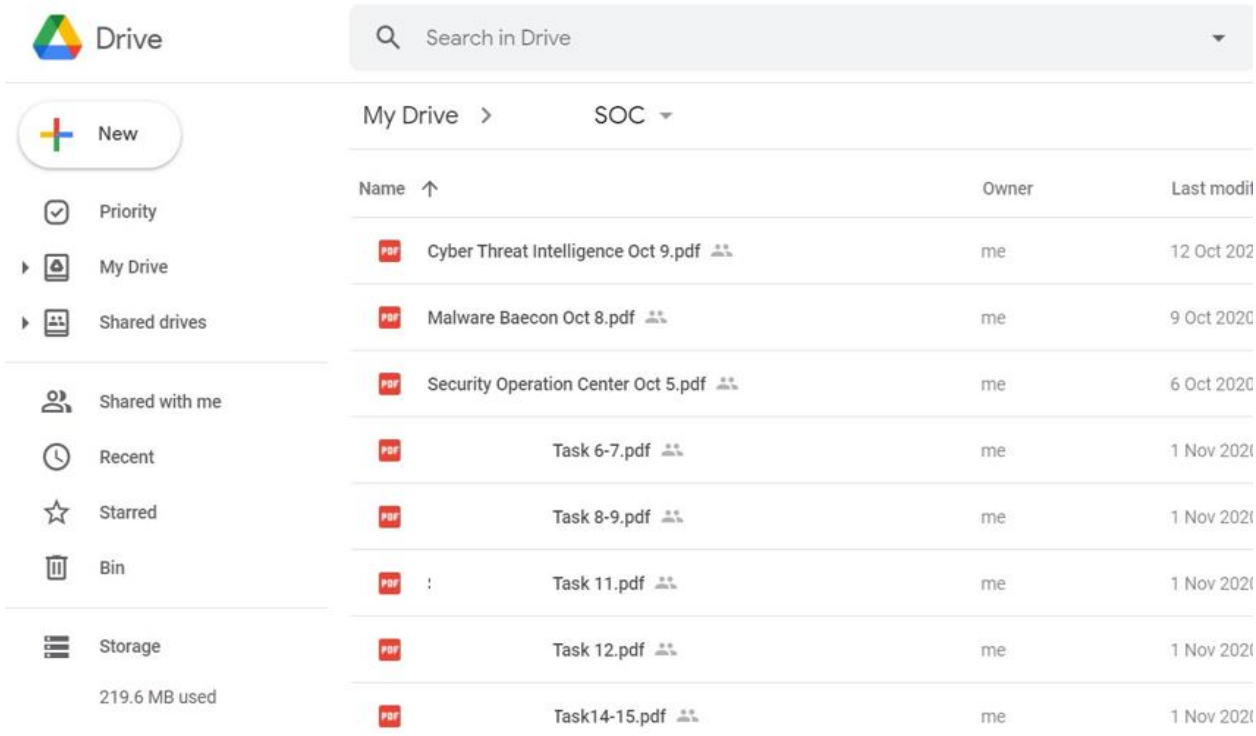


Figure 25 Tracking Task of SOC department

Signature

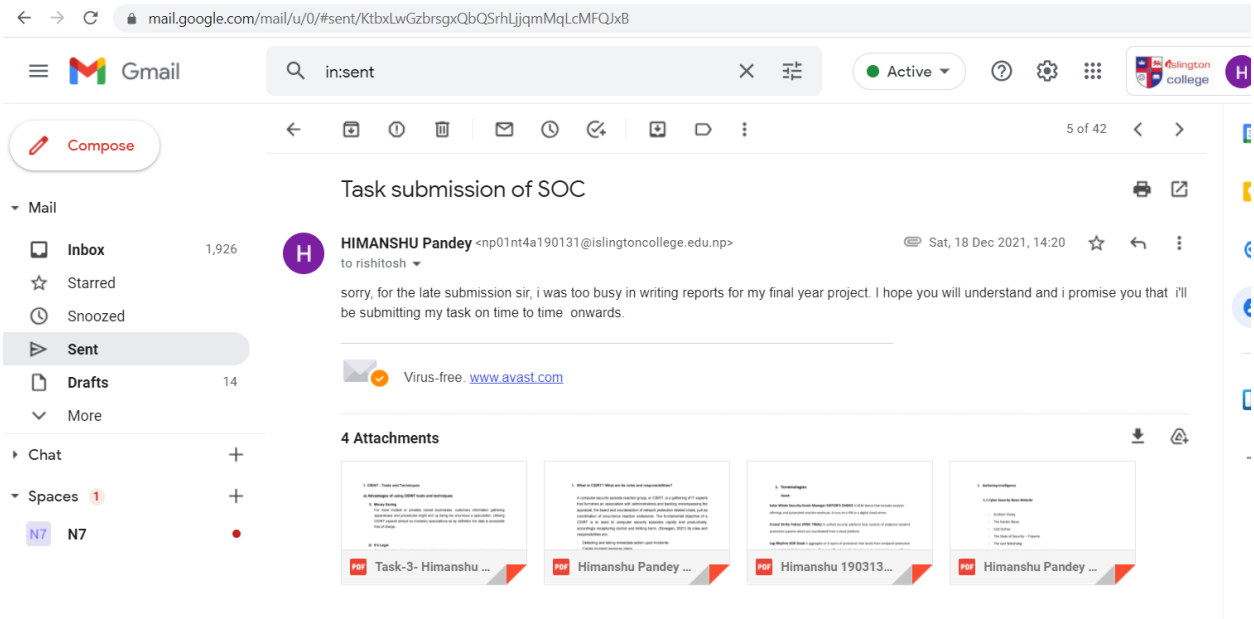


Figure 26 SOC task submission

1. Terminologies

- Asset

An asset is anything of value or a resource of value that can be converted into cash. Individuals, companies, and governments own assets. For a company, an asset might generate revenue, or a company might benefit in some way from owning or using the asset. Types of Assets:

A. Personal Assets

Personal assets are things of present or future value owned by an individual or household. Common examples of personal assets include:

- Cash and cash equivalents, certificates of deposit, checking, and savings accounts, money market accounts, physical cash, Treasury bills
- Property or land and any structure that is permanently attached to it
- Personal property—boats, collectibles, household furnishings, jewelry, vehicles

Investments—annuities, bonds, the cash value of life insurance policies, mutual funds, pensions, retirement plans, (IRA, 401(k), 403(b), etc.) stocks Your net worth is calculated by subtracting your liabilities from your assets. Essentially, your assets are everything you *own*, and your liabilities are everything you *owe*. A positive net worth indicates that your assets are greater in value than your liabilities; a negative net worth signifies that your liabilities exceed your assets (in other words, you are in debt).

B. Business Assets

For companies, assets are things of value that sustain production and growth. For a

Figure 27 task 1 SOC

Signature

1 Creating a virtual environment

1.1 Linux

1.1.1 Install Nagios

1.1.1.1 Downloading steps: -

Step 1: - Visiting side of Nagios

To download the Nagios package,

https://www.nagios.org/downloads/nagios-core/

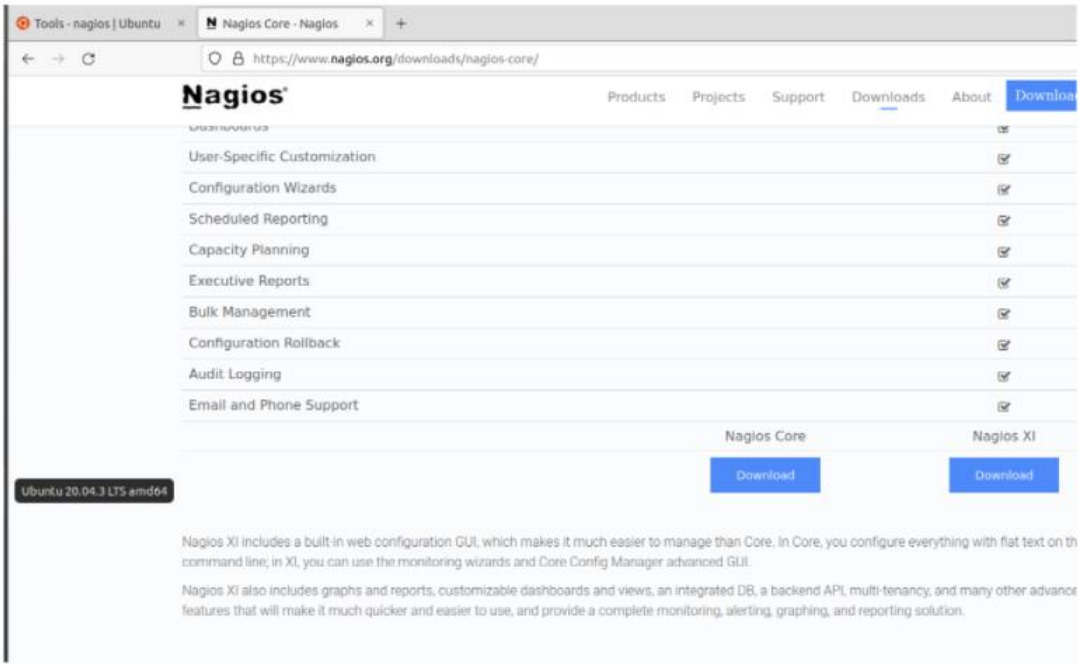


Figure 1: negios website visit

Page 3 / 62

Figure 28 task 2 SOC

Signature

1. OSINT - Tools and Techniques (provide references of your research as well)

a. List 3-4 advantages of using the OSINT tools and techniques.

Ans: Advantages of using the OSINT tools and techniques are as follows:

- **Money-Saving**
  For smaller or private companies, regular data collecting tools and techniques may prove to be too big an investment. Using OSINT requires little to no financial investments as by definition the information is available for free.
- **It'sLegal**
  Since the information gathered has not been defined as classified and has been publicly revealed with the consent of the original source, it is entirely legal to gather any data you may find.
- **RegularlyUpdated**
  Due to the public nature of the resources used in OSINT, users are likely to add and update their information regularly.
- **NationalSecurity**
  OSINT has proven to be an extremely useful tool in dealing with national security matters.
- **BigPictureView**
  Business owners and other corporate decision-makers can gain a broader view of their investigations using OSINT information, allowing them to create long-term strategic plans to achieve a range of business goals. (technologies, 2021)

Page 1 / 10

Figure 29 task 3 SOC

Rishtosh

Signature

1. What is CSIRT? What are its roles and responsibilities?

A computer security incident response team or CSIRT is responsible for exposing and averting cyber attacks that target an enterprise. It focuses on responding to security incidents.

The computer security incident response team members analyze all data about cyber incidents to develop prevention methods. If necessary, they share their insights and solutions with the rest of the company, making them part of the response process before, during, and after a cybersecurity incident occurs.

There tasks are:

- Remediating security incidents.
- Detecting and taking immediate action when an incident occurs.
- Providing a 360-degree view and in-depth analyses of all past incidents to come up with and implement preventive measures to avoid recurrences.
- Training staff members so they can respond appropriately to new threats.
- Managing security audits. (what is CSIRT, 2020)

2. List out the Incident Response Framework developed by NIST.

NIST stands for National Institute of Standards and Technology. They're a government agency proudly proclaiming themselves as "one of the nation's oldest physical science laboratories". They work in all-things-technology, including cybersecurity, where they've become one of the two industry standard go-tos for incident response with their incident response steps.

The incident response framework develop by NIST are given:

Figure 30 Task 4 SOC

Signature

8.5.3 LO3 Evidence

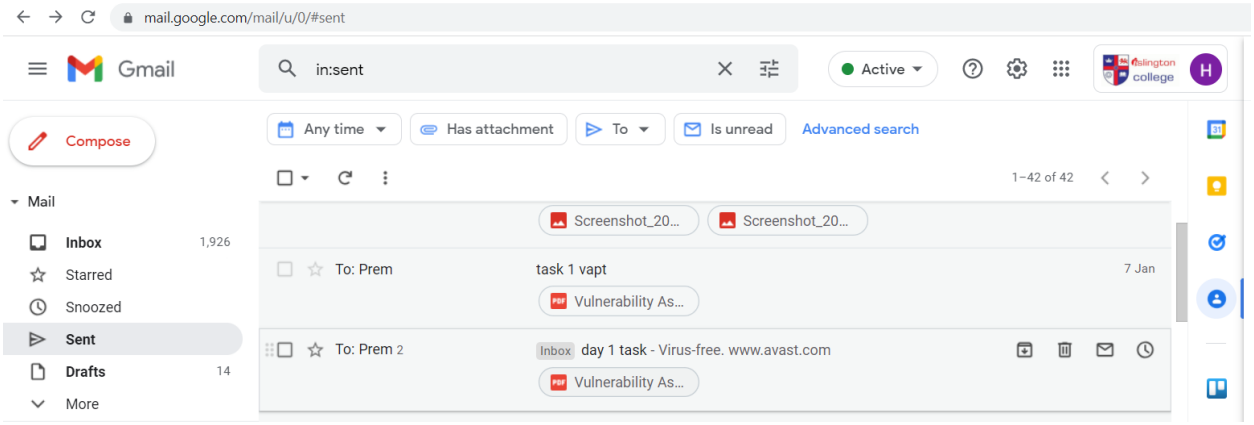


Figure 31 Task 4 SOC task submission

Supervisor signature

Vulnerability Assessment and Penetration Testing (VAPT) is a testing process to find security bugs within a software program (web/mobile) or a computer network. VAPT is often misunderstood as two different types of testing techniques. The objective of Vulnerability Assessment is entire to search and find bugs. Penetration Testing is performed to see whether the vulnerability exists by exploring and exploiting the system. Every day, we hear about cyber-attacks into computer systems and servers, stealing everything from passwords to financial information and data. No matter how strong we build the security team to combat the security breaches, the attacker is always one step ahead. So, in order to secure its environment from hackers one should know its own security weakness and vulnerabilities. Organization can know its information security IS weakness and vulnerabilities by doing Vulnerability Assessment and Penetration Testing (VAPT) audit.

The word Vulnerability Assessment and Penetration Testing (VAPT) audit are two different types of vulnerability testing methodologies in information security IS. Therefore, these testing methodologies have different strengths which are combined to achieve a complete vulnerability analysis. Vulnerability assessment is the process of identifying and measuring security vulnerability in an environment which finds out the weaknesses and reduce the risk associated with them. Vulnerability assessment cannot differentiate between exploitable and non-exploitable vulnerabilities. Whereas, Penetration Testing relies upon Vulnerability Assessment.

Types of Penetration Testing

Penetration Testing attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible. So, Penetration testing helps find exploitable weakness and measure the severity of each. A Penetration testing includes network penetration testing and application security testing as well as controls and processes around the networks and applications which should occur from both inside (internal testing) and outside (external testing) of the network. A penetration testing shows how damaging a flaw could be in a real attack rather than find every flaw in a system.

There are three types of Penetration Testing:

1. Black Box Testing;
2. White Box Testing;
3. Grey Box Testing.

Figure 32 VAPT task 1

Supervisor signature

- Confidentiality Agreement.

Phase 2: Testing Phase

In this phase the actual testing is done. The operations divided into two parts, vulnerability assessment and the other penetration testing. Whereas,In Vulnerability Assessment the pen tester aims to find and analyze the existing set of vulnerabilities in the target system.

As this process is compose of many sub-processes which are:

Target Discovery

The pen tester collects the information of the target system which would help to generate an image of the target's security infrastructure environment.

Scanning

After discovering the target the pen tester performs a scan on target system to identify the list of existing vulnerabilities, which intend to impose a threat to the security of the target system.

Result Analysis

In this phase it inherits the output of the scanning phase and analyzes the set of vulnerabilities identified after scanning. However, The pen tester prioritizes the identified vulnerabilities based on their severity and impact which can be critical, high, medium or low. The vulnerabilities later address and resolve in the same order.

Reporting

After the successful accomplishment of initial phases, the pen tester documents the various operations performed and results obtained in the entire process.

In Penetration Testing the pen tester exploits the identified set of vulnerabilities. By exploiting the vulnerabilities it checks the difficulty level of exploiting the vulnerabilities. This process also provides a Proof-of-Concept to support the test finding during later stage.

Supervisor signature

Figure 33 VAPT task 2

3. Grey Box Testing.

Black Box Testing:

In a real scenario, cyber-attacks happen when the hacker does all types of attacks and brute force against the IT infrastructure environment of an organization, in hopes of trying to find vulnerabilities or weakness in the system as the hacker does not know the ins and outs of an IT infrastructure environment. In other words, this type of pen testing is called dynamic analysis security testing (DAST) where the tester has no relevant information about the target machine or the system, except the basic information of an organization

for general understanding. Black box testing identifies the vulnerabilities, including input and output validation problems, server configuration errors and application specific problems testing from an external network with no prior knowledge of the internal networks and systems.

White Box Testing:

White box testing, also known as static analysis security testing (SAST), is a critical tool for finding and fixing security vulnerabilities and flaws in applications. As the black box testing seeks to find vulnerabilities from outside the application the way a hacker would, white box testing analyzes the source code or the compiled binaries to catch semantic coding errors and flaws in the application or its infrastructure. Similarly, In this type of pen testing the pen-tester gets some information about the implemented security structure of

Supervisor signature

Gray Box Testing:

Grey Box Testing is a combination of black box and white box testing method where it has a partial knowledge of internal working structure. It is based on UML diagrams, architectural view, database diagrams and functional specification. Moreover, Grey box testing is best fit for web based application specific errors as it is a best approach for functional or domain testing. Also, Testing can be done from internal or external network, with knowledge of internal networks and systems.

VAPT Audit and information security IS Methodology

A complete process of Vulnerability Assessment and Penetration Testing (VAPT) is compose of many sub processes. The VAPT testers uses many open source and licensed tools in each of these sub-processes to analyze the security arrangements of the entire infrastructure and system.

Phases of VAPT for information security

A complete process of VAPT is conduct in following three phases:

Phase 1: Test Preparation Phase

In this phase the organization needs to decide the Scope of Work, Objectives, Time and Duration of the VAPT. All the documents related to the scope of work are organized and finalized. Therefore, Issues like confidentiality, information leakage and downtime is resolve and put into legal agreement document. Some of the documents required to conduct Vulnerability Assessment and Penetration Testing as follows:

- Memorandum of Understanding.
- Non-Disclosure Agreement.

Supervisor signature

Phase 4:Attack Phase

The pen tester tries to compromise the target system in real, by using different tools and techniques to exploit the logical and physical vulnerabilities exposed during the pre-attack phase. Also, Some of the techniques which perform in attack phase are perimeter penetration, target acquisition and privilege escalation.

Phase 5:Post Attack Phase

The pen tester aims at returning the modified system to the pretest state. The pen tester performs the reversal of each change made to the system to restore to its pre attack state. The activities performed during post attack phase includes removal of any files, tools, exploits, or other test created objects uploaded to the system during testing.

Phase 6:Reporting Phase

In this phase a thorough investigation and validation of all the findings. Similarly, the final report is hand over to the concern authorities along with the mitigation plan. Which holds recommendations for remediation of the identified vulnerabilities and exploits.

Tools to conduct VAPT that have been used by the professional these days are:

- Nessus
- Nmap
- Wireshark
- Metasploit
- Hydra
- W3af
- Zenmap
- John the Ripper

Vulnerability Assessment and Penetration Testing (VAPT) is a process of securing computer systems from attackers by evaluating them to find loopholes and security vulnerabilities.

Some VAPT tools assess a complete IT system or network, while some carry out an assessment for a specific niche. There are VAPT tools for wi-fi network security testing as well as web application testing. Tools that execute this process are called VAPT tools.

Figure 34 full report of VAPT task 1

Supervisor signature

8.5.4 LO4 Evidence

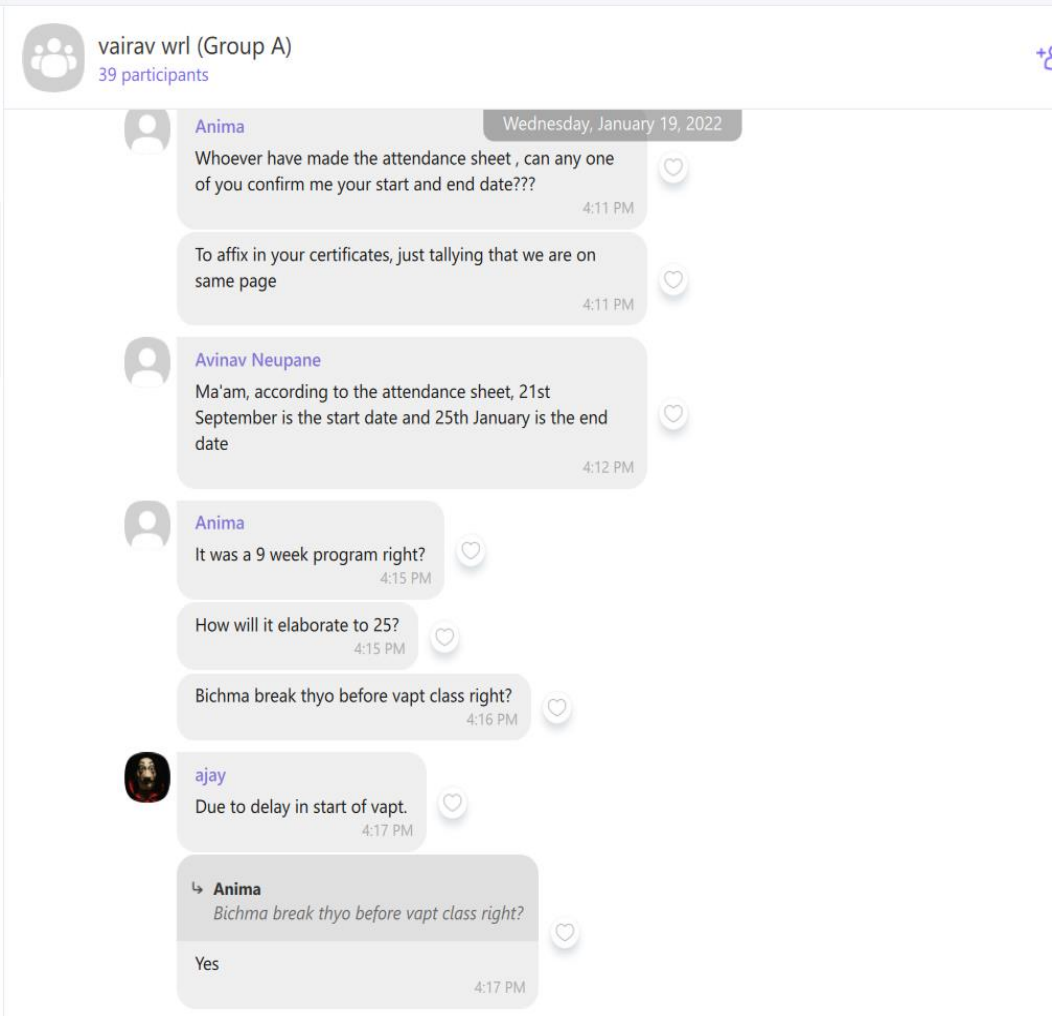


Figure 35 working with the group member and supervisor

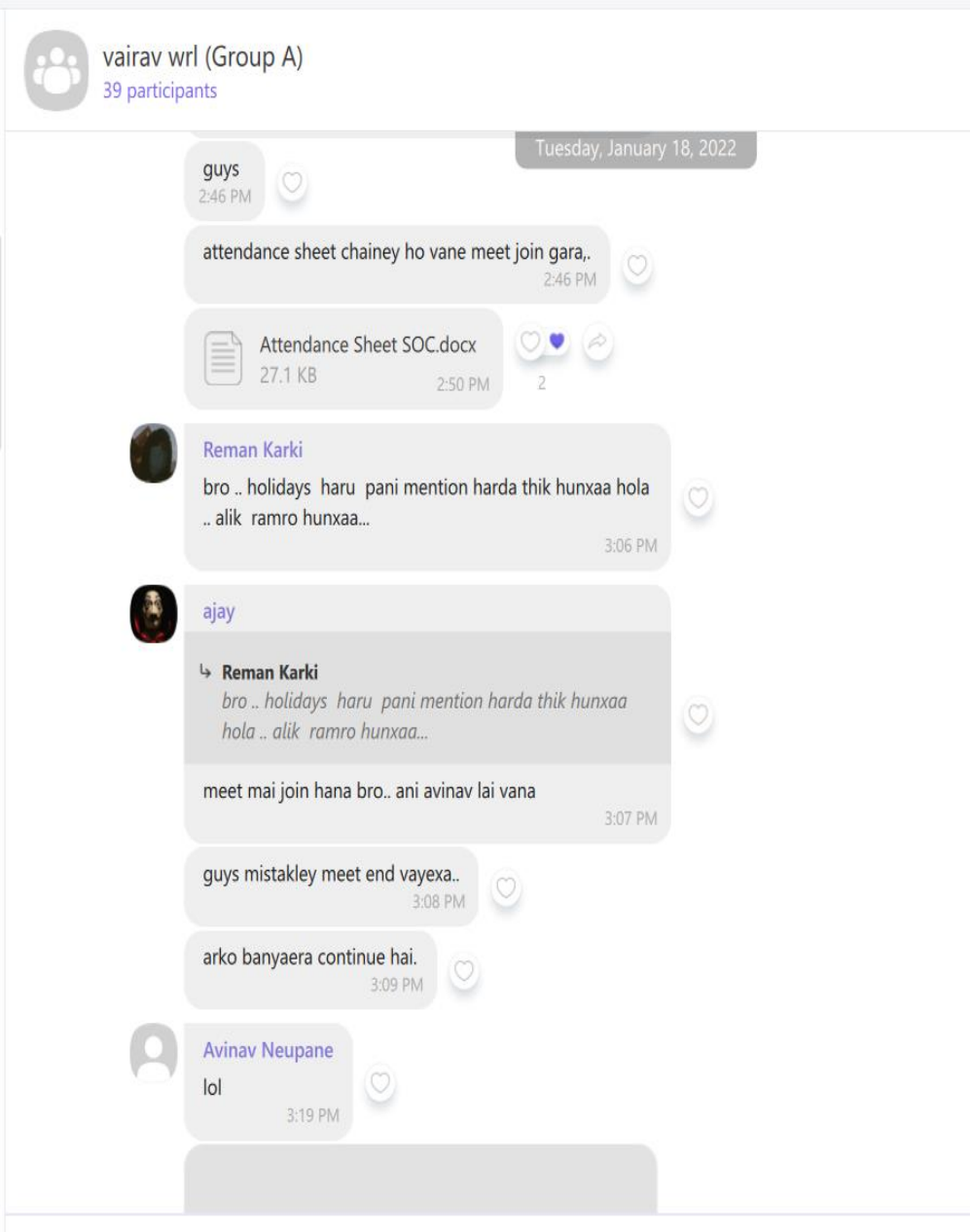


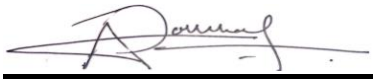
Figure 36 working with the group member'

Supervisor Signature

8.5.5 LO5 Evidence

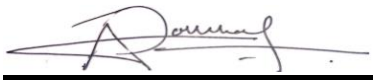
Table of Contents

Figure 37 report writing 1



Supervisor Signature

Figure 38 report writing 2



Supervisor

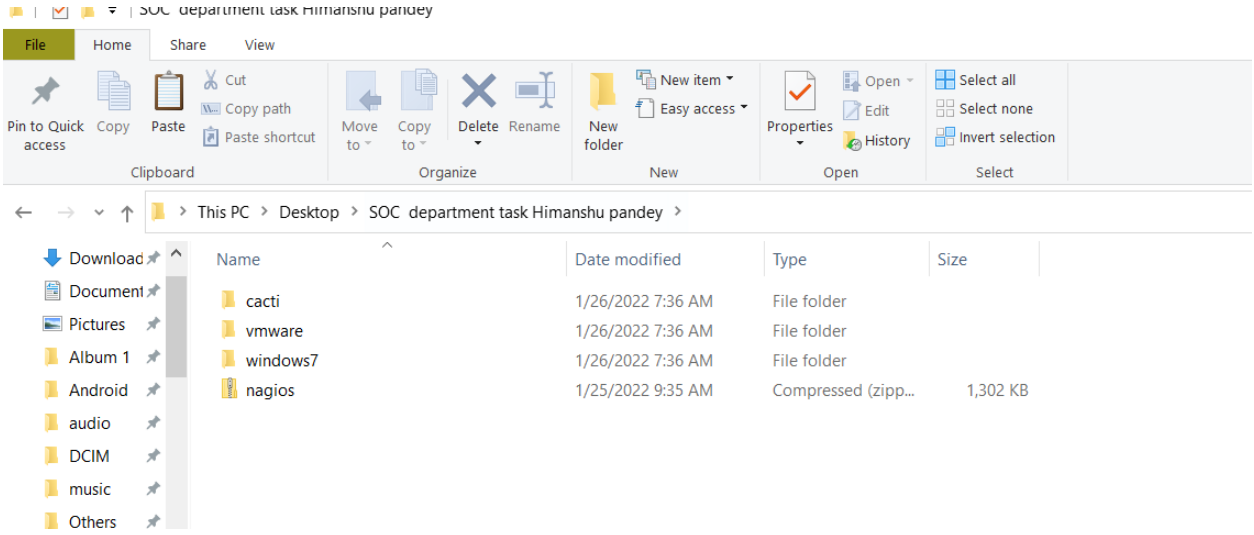
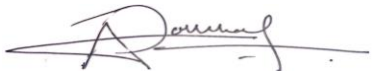


Figure 39 Tasking Tracking in saved file



Supervisor Signature

1 Creating a virtual environment

1.1 Linux

1.1.1 Install Nagios

1.1.1.1 Downloading steps: -

Step 1: - Visiting side of Nagios

To download the Nagios package,

https://www.nagios.org/downloads/nagios-core/

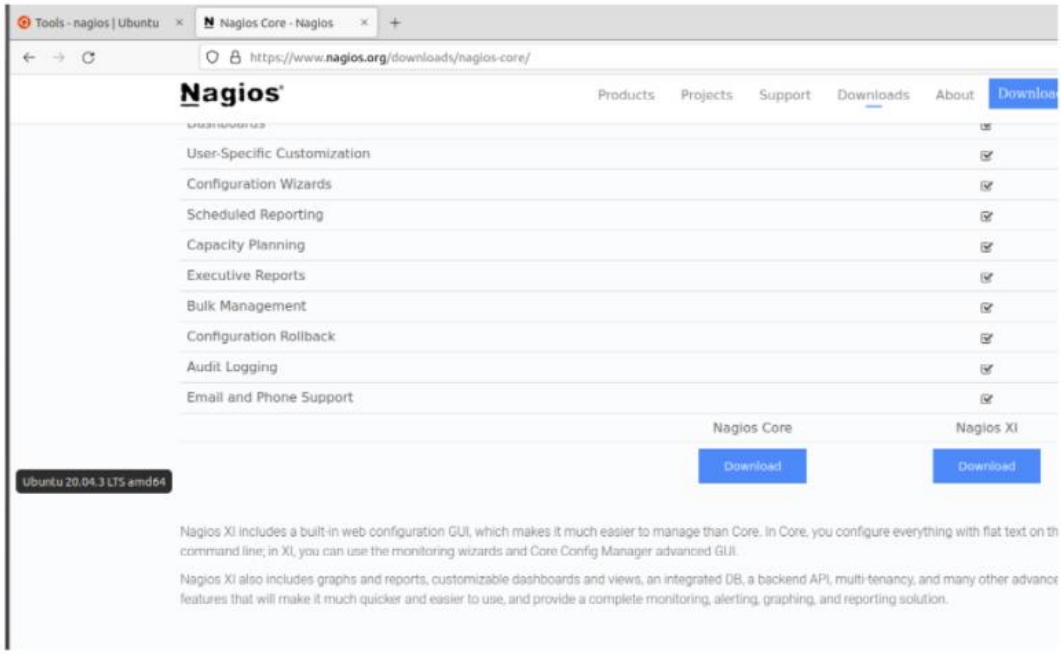


Figure 1: negios website visit

Figure 40 Report writing 3

Signature

Step 2:- Choosing options as operating system

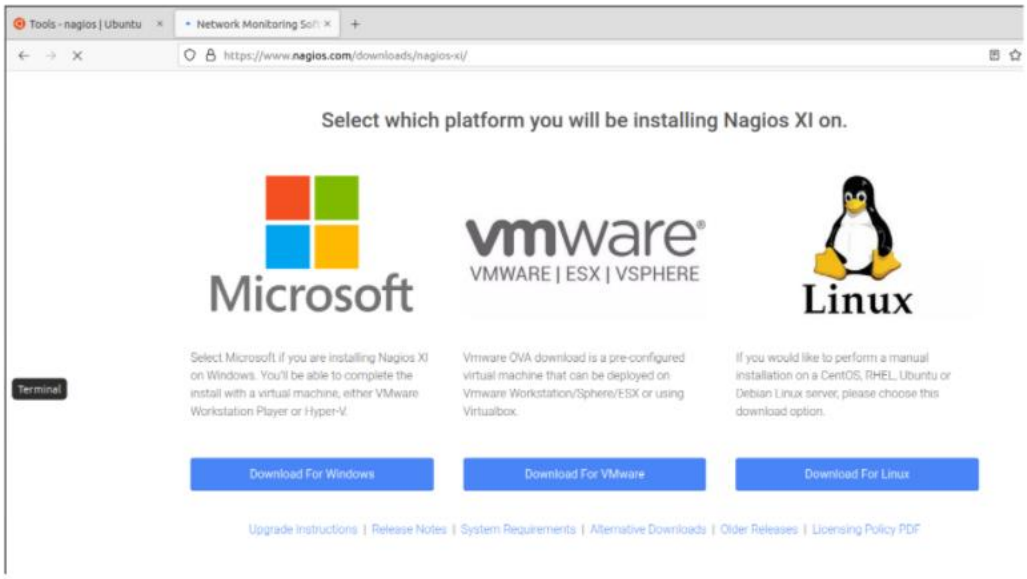


Figure 2: package for operation system chosen

Step 3:- Click on Download now option

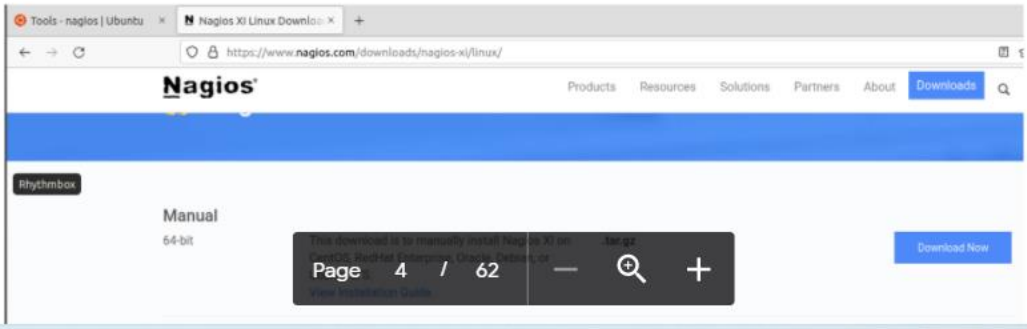


Figure 41 Report writing 4

Signature

8.5.6 LO6 Evidence

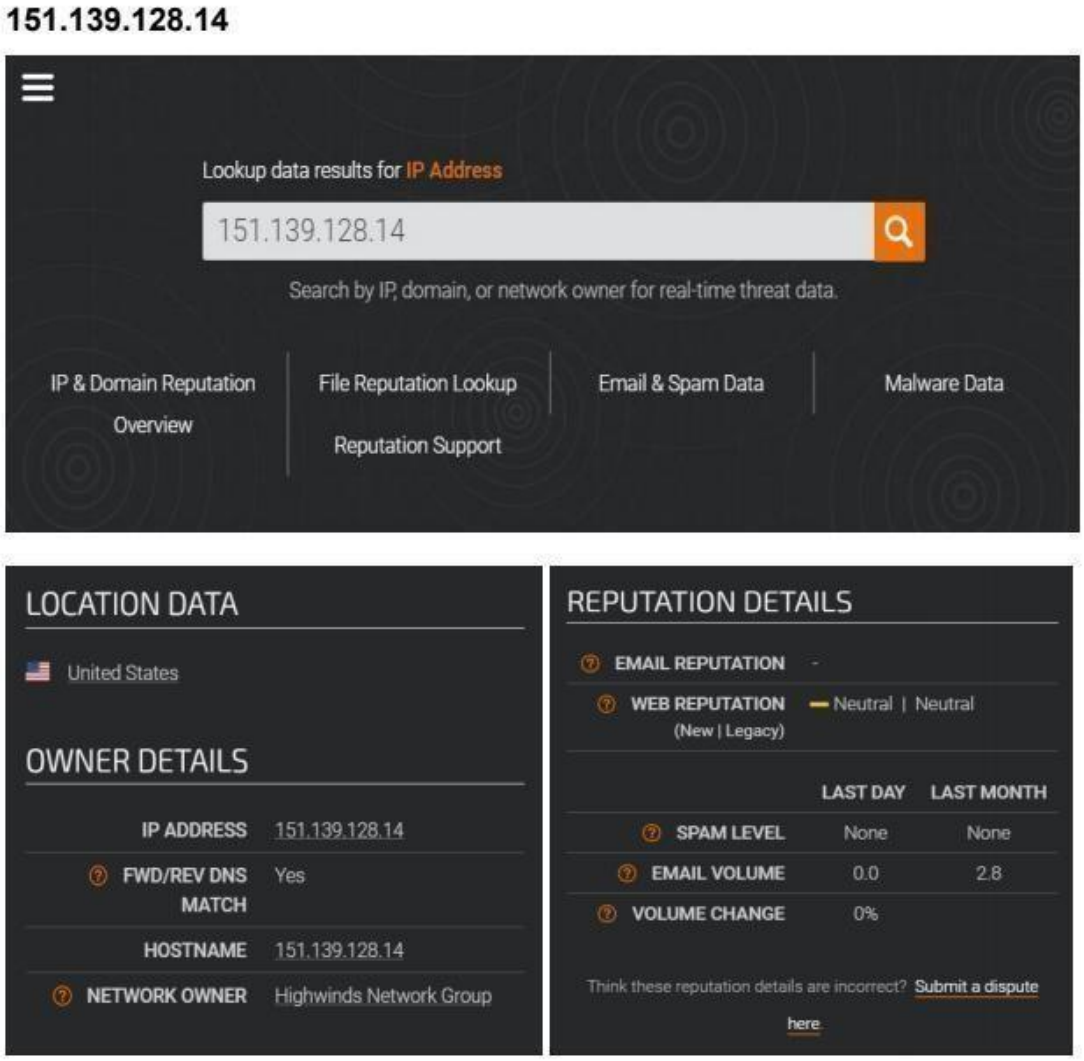
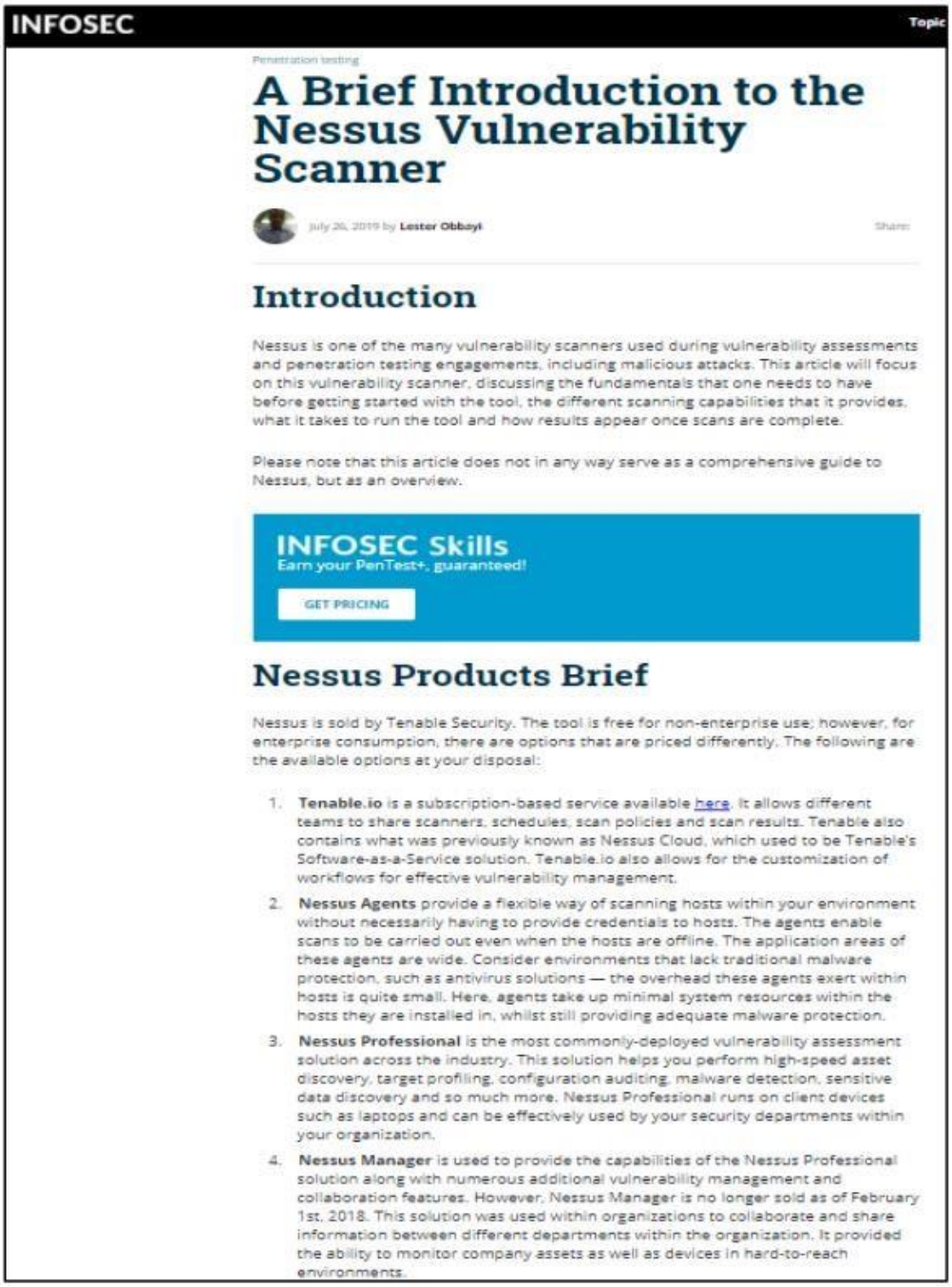


Figure 42 Scanning IP address

Signature

8.5.7 LO7 Evidence



INFOSEC Topic

Penetration testing

A Brief Introduction to the Nessus Vulnerability Scanner

July 26, 2019 by **Lester Obbayi** Share:

Introduction

Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. This article will focus on this vulnerability scanner, discussing the fundamentals that one needs to have before getting started with the tool, the different scanning capabilities that it provides, what it takes to run the tool and how results appear once scans are complete.

Please note that this article does not in any way serve as a comprehensive guide to Nessus, but as an overview.

INFOSEC Skills
Earn your PenTest+, guaranteed!
GET PRICING

Nessus Products Brief

Nessus is sold by Tenable Security. The tool is free for non-enterprise use; however, for enterprise consumption, there are options that are priced differently. The following are the available options at your disposal:

1. **Tenable.io** is a subscription-based service available here. It allows different teams to share scanners, schedules, scan policies and scan results. Tenable also contains what was previously known as Nessus Cloud, which used to be Tenable's Software-as-a-Service solution. Tenable.io also allows for the customization of workflows for effective vulnerability management.
2. **Nessus Agents** provide a flexible way of scanning hosts within your environment without necessarily having to provide credentials to hosts. The agents enable scans to be carried out even when the hosts are offline. The application areas of these agents are wide. Consider environments that lack traditional malware protection, such as antivirus solutions — the overhead these agents exert within hosts is quite small. Here, agents take up minimal system resources within the hosts they are installed in, whilst still providing adequate malware protection.
3. **Nessus Professional** is the most commonly-deployed vulnerability assessment solution across the industry. This solution helps you perform high-speed asset discovery, target profiling, configuration auditing, malware detection, sensitive data discovery and so much more. Nessus Professional runs on client devices such as laptops and can be effectively used by your security departments within your organization.
4. **Nessus Manager** is used to provide the capabilities of the Nessus Professional solution along with numerous additional vulnerability management and collaboration features. However, Nessus Manager is no longer sold as of February 1st, 2018. This solution was used within organizations to collaborate and share information between different departments within the organization. It provided the ability to monitor company assets as well as devices in hard-to-reach environments.

Figure 43 Installation process of Nessus

Supervisor Signature

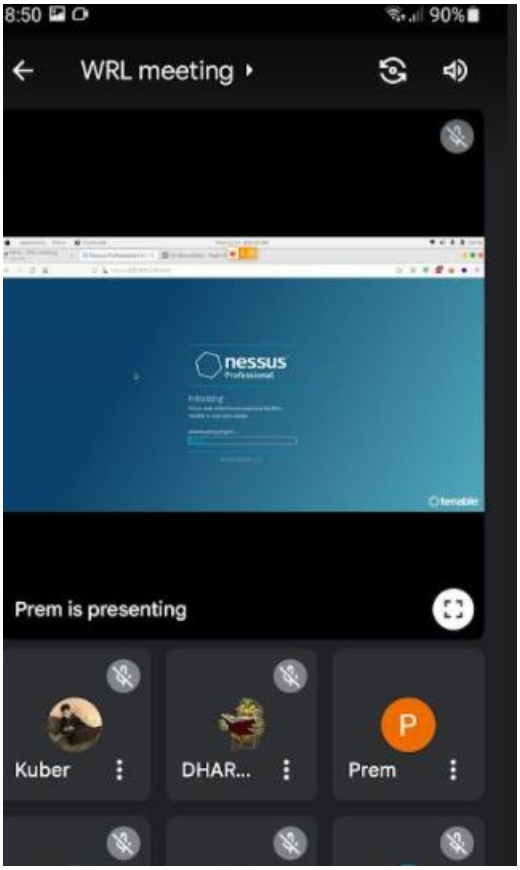


Figure 44 using of Nessus

Supervisor signature

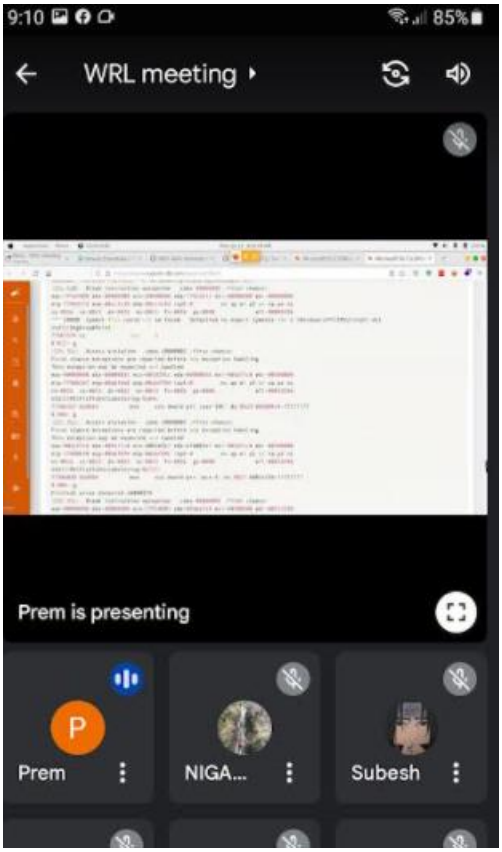


Figure 45 scanning

Supervisor signature

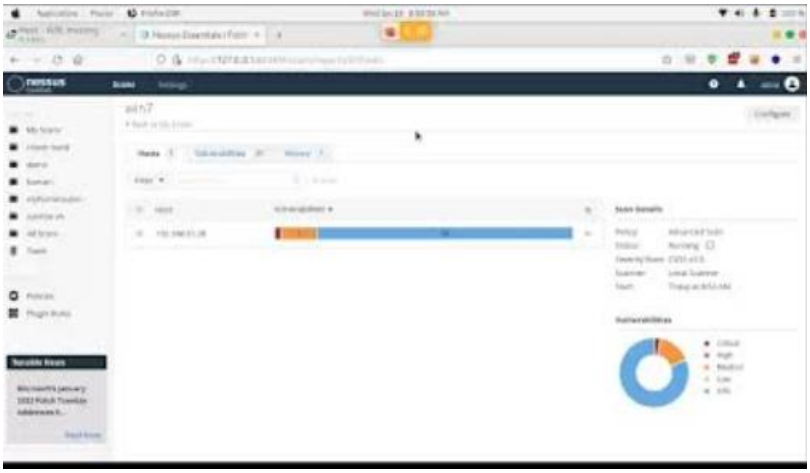


Figure 46 using Nessus

Supervisor signature

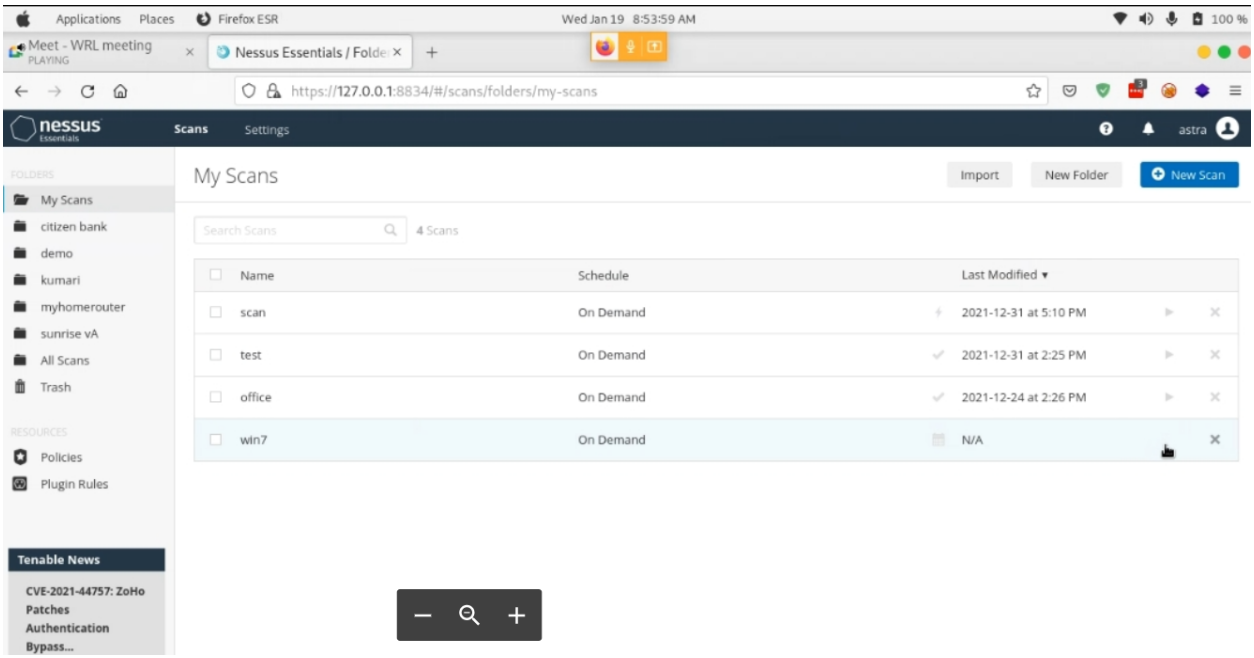


Figure 47 scanned in Nessus

Supervisor signature

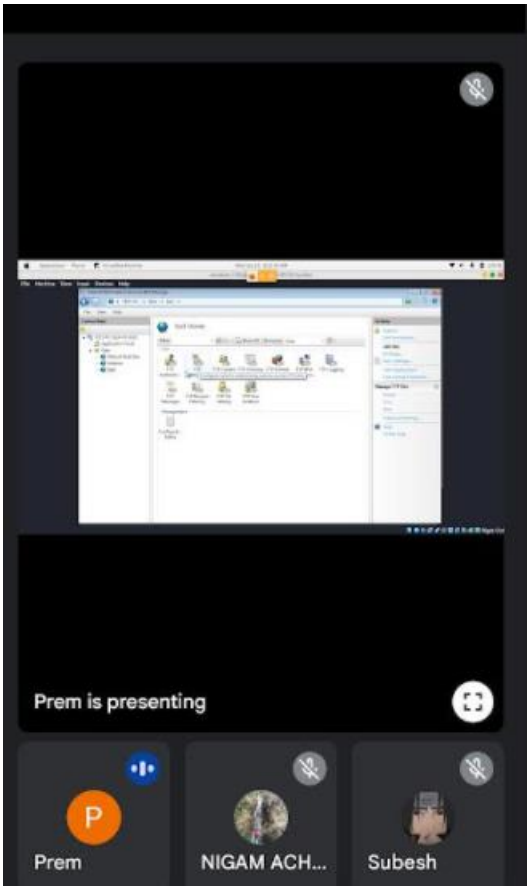
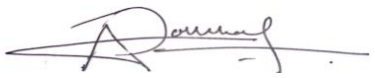


Figure 48 48 files



Supervisor Signature

8.5.8 LO8:LO9 Evidence

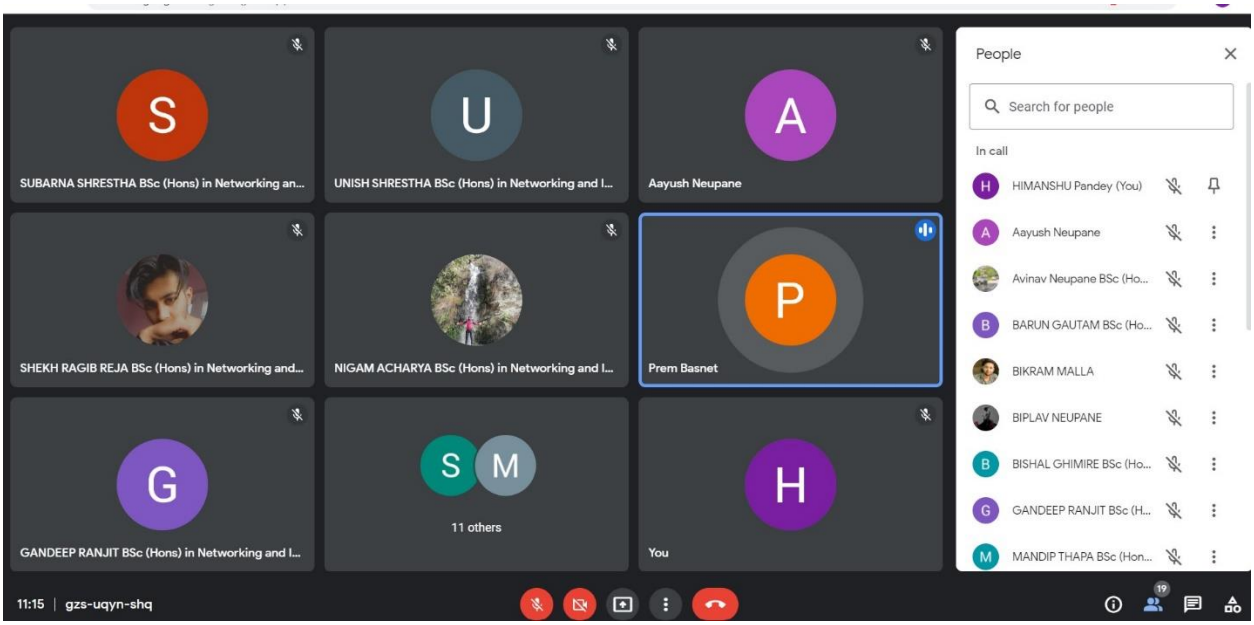
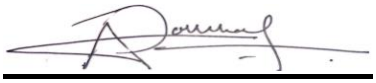


Figure 49 Google meet session of VAPT



Supervisor Signature

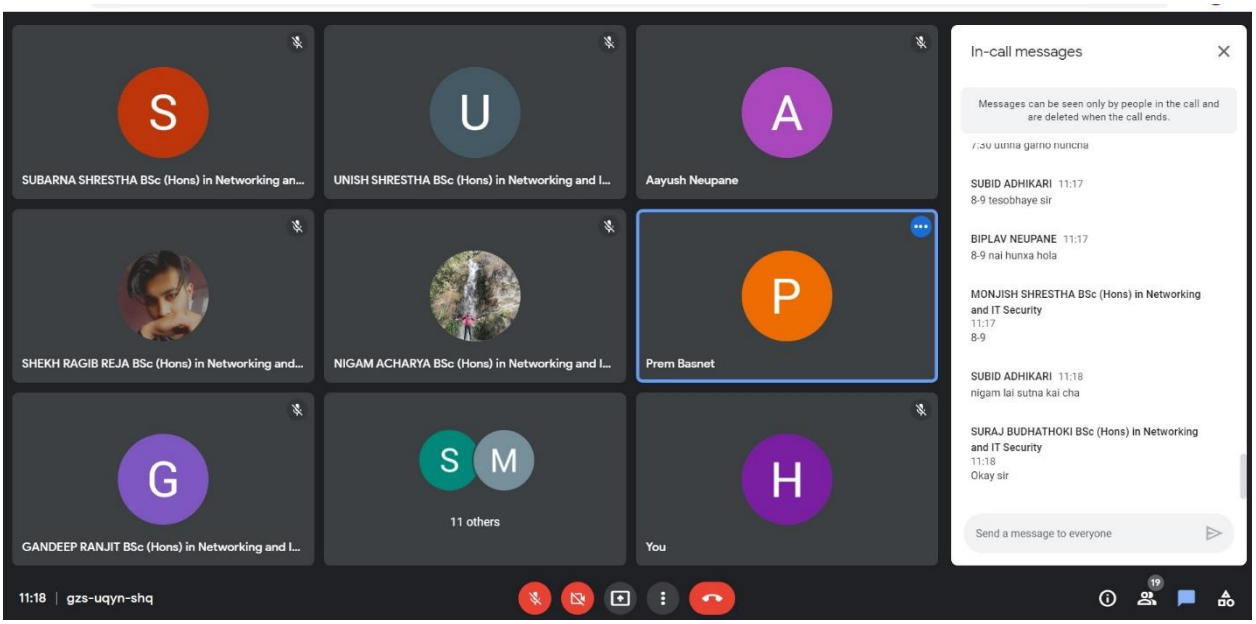


Figure 50 Google meet session VAPT 2

Supervisor Signature

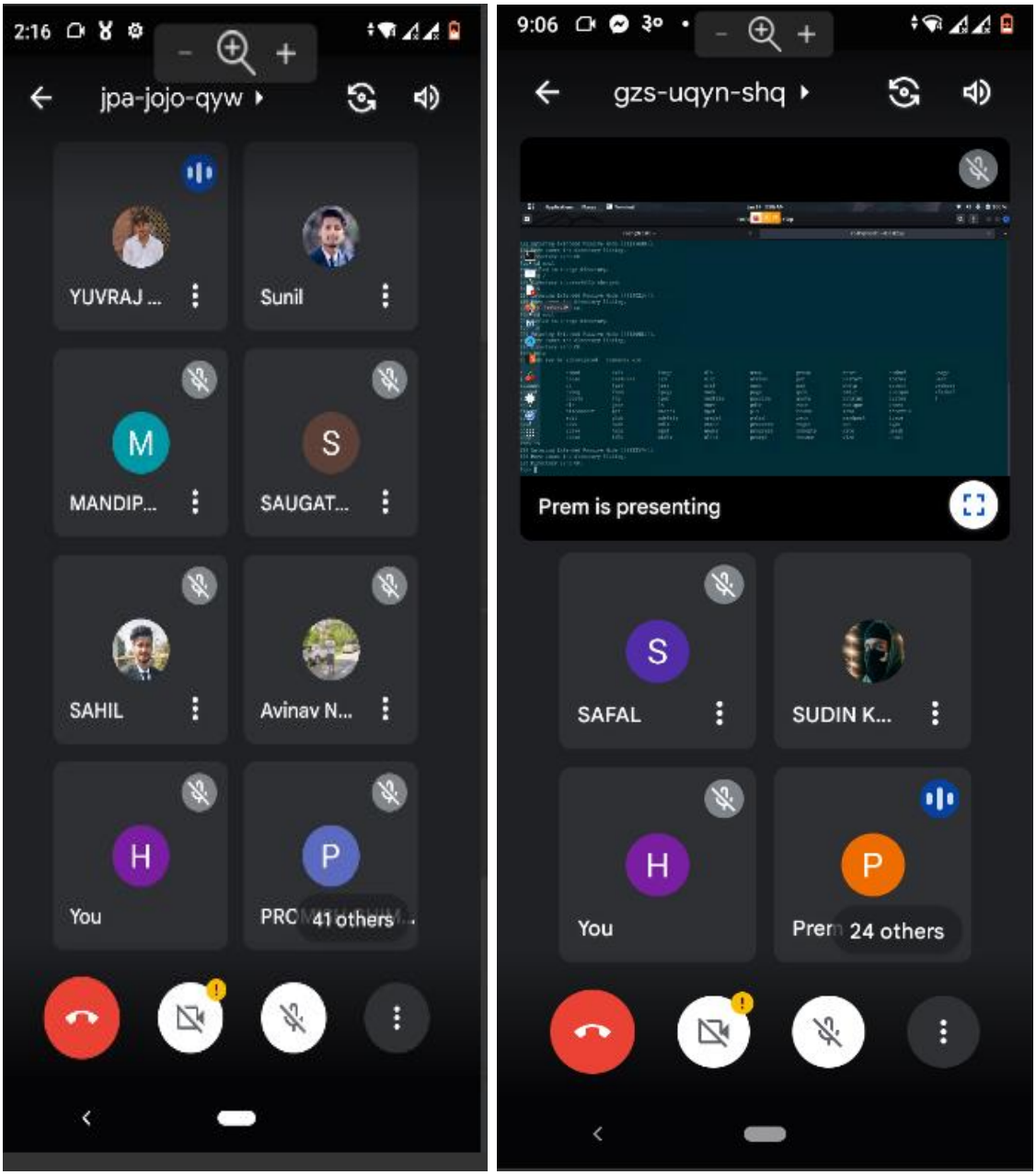


Figure 51 Google meet session VAPT 3

Supervisor Signature

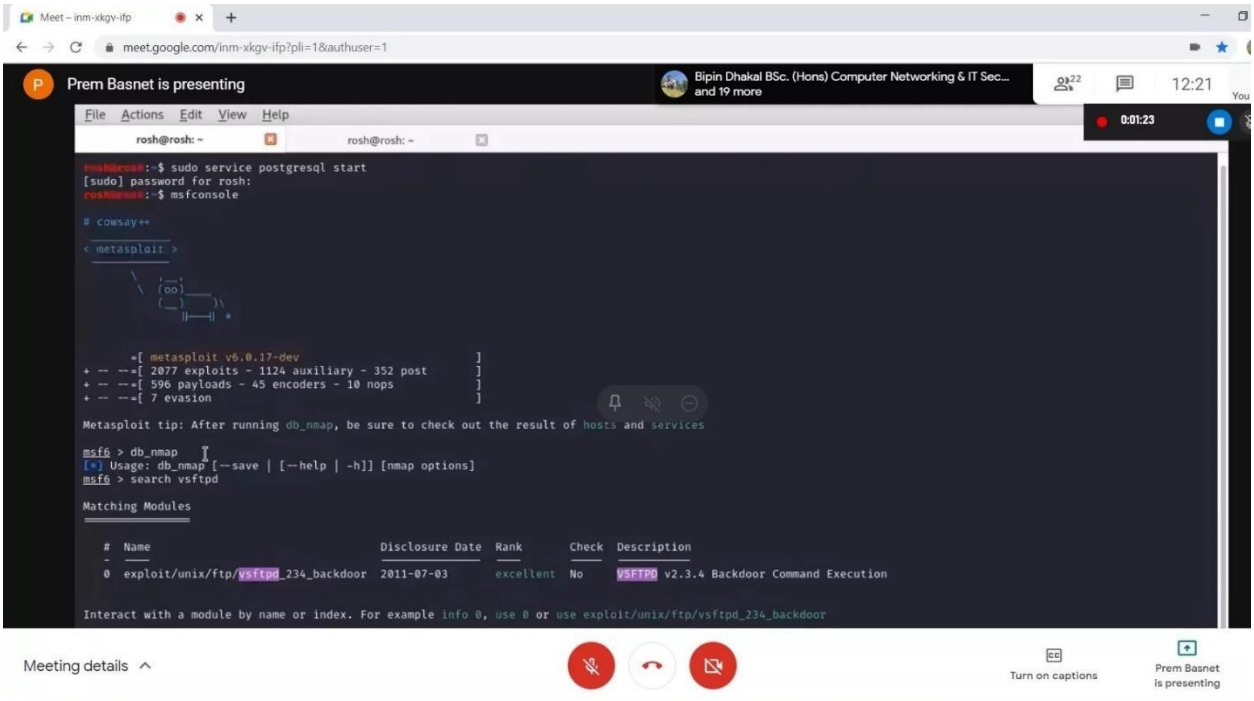
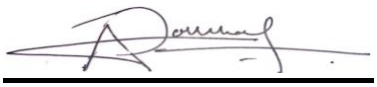
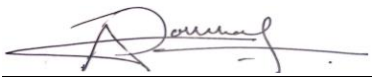


Figure 52 Teaching session by VAPT supervisor

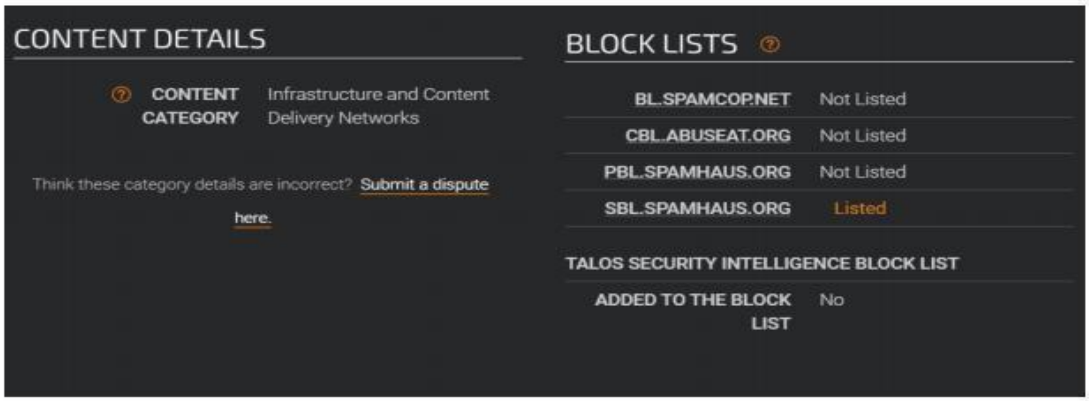


Supervisor Signature

Figure 53 Communication with teammates



Supervisor Signature



For the Ip address **"167.89.115.54"** I used **"Cisco Talos"**. According to **Cisco Talos**, the location of given Ip address was based on **Herndon, United States**. Alike, this particular address belongs to domain **sentgrid.net** and has very poor email reputation; which denotes the link of this Ip for email frauds such as email spams, spoofing, web spam and so on.

According to **AbuseIPDB**, this address is from **Denver, Colorado, USA** and belongs to domain **sendgrid.com**. In addition to that, this Ip was reported **154 times** and is used for data center, web hosting or transit.

Figure 54 report of ip scanning address

Supervisor Signature

1. Executive Summary

The purpose of this vulnerability scan is to gather data on the connection between NAT and my Wi-Fi module in 192.168.1.0/24 network. 45 vulnerabilities found by Nessus network scan.

2. Scan Results

The raw scan result is shown in figure below.

3. Our Findings

The results from the credentialed patch audit are listed below.

4. Risk Assessment

This report identifies security risks that could have significant impact on mission-critical applications used for day-to-day business operations.

Critical Severity	High Severity	Medium Severity	Low Severity	Info
0	0	3	0	42

4.1. Critical Severity Vulnerability

No Critical severity vulnerabilities were found during this scan.

4.2. High Severity Vulnerability

No High severity vulnerabilities were found during this scan.

Figure 55 Vulnerability Assessment final report

Supervisor Signature

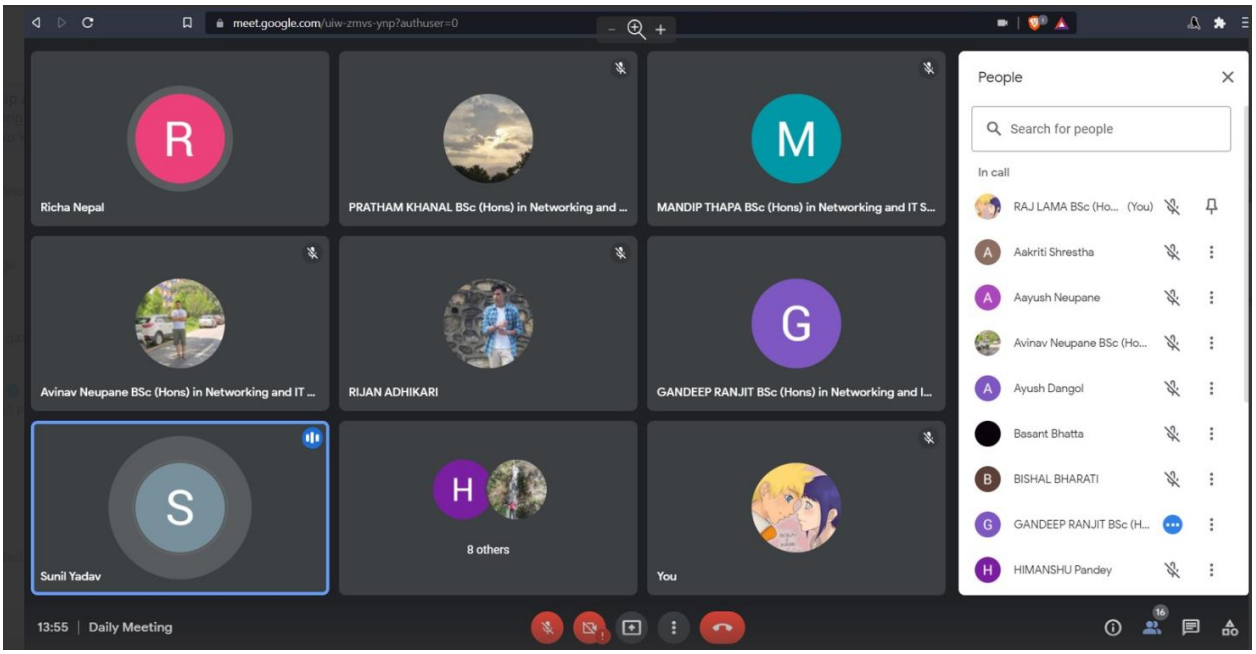
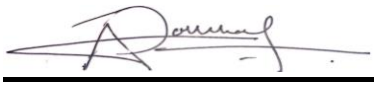


Figure 56 GRC class screenshot



Supervisor Signature