

LONDON METROPOLITAN UNIVERSITY**PROFESSIONAL WORK PLACEMENT****LEARNING LOG**

YOUR ID:19031311




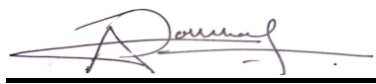
YOUR NAME : Himanshu Pandey



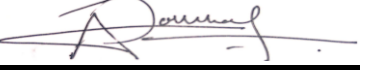
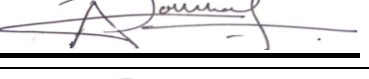
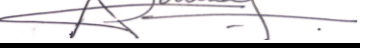
YOUR COURSE: Work Related Learning (WRL) Module

YOUR WRL TUTOR: Ravi Chandra Gurung/Bibek Khanal

PLACE OF WORK (Company Name): Variav Technology Security Pvt Ltd

DATES OF ENTRIES IN LEARNING LOG:

| Log Index | Start Date | End Date | Company Supervisor Signature |
|-----------|------------|------------|--|
| Log 1 | 21/09/2021 | 30/09/2021 |  |
| Log 2 | 31/10/2021 | 22/10/2021 |  |
| Log 3 | 24/10/2021 | 31/11/2021 |  |
| Log 4 | 02/11/2021 | 12/11/2021 |  |

| | | | |
|-------|------------|------------|--|
| Log 5 | 14/11/2021 | 26/11/2021 |  |
| Log 6 | 29/11/2021 | 10/12/2021 |  |
| Log 7 | 12/12/2021 | 21/12/2021 |  |
| Log 8 | 22/12/2021 | 31/12/2021 |  |
| Log 9 | 2/01/2022 | 7/01/2022 |  |

LEARNING LOG 1

For the period **21st September 2021** (start date) to **30th September 2021** (end date)

What have I done? (relate tasks to Learning Outcomes) (L01,L02,L03,L04)

As we can know that from last 2 year we facing problem from the virus called Covid -19. Due which we were not able to step out the house and many company had the started telling their employees to do their work online (work from their home). At the very first day of the meeting we had the group discussion with the supervisor (Lo2, L03). Where the supervisor told us that we will divided you in the group of three where the topics where GRC, SOC, VAPT. The group was made by the supervisor itself. The necessary information was made by the supervisor about the internship like all the work given by the supervisor should be completed on time, activities and many more information was provided. And the very next we had an emailed that we will be having our internship class and we were given the topics on which we will be having the class like Assets, Threats, CIA, service industry and many more topics were discussed in the class. On the third day we got an email from the supervisor that we need to write the report on the topic of governance, risk, and compliance (GRC). (L01,L04)

What I did well (refer to skills used)

I was able to give answer asked by the supervisor. I was able to note down the information which I was not able to find before joining the internship meeting.

What I could improve on (i.e. skills I want to improve)

I need to improve in my research skills

Action I can take to improve my skills and learning (make these "SMART"):

GOAL: To enhance my speaking and writing abilities.

ACTION: Practice speaking and writing skills, and ask instructor and friends for advice on how to improve speaking and writing abilities.

Timing:

LEARNING LOG 2

For the period 30th September 2021 (start date) to 9th October 2021 (end date)

What have I done? (relate tasks to Learning Outcomes)

On the first day of the second week, we discussed about Governance Risk and Compliance (GRC) which we were given to write the report on it in the previous meetings. In this subject again we had to do many research because our supervisor were unsatisfied with our researched answer. And furthermore, he added some of the topics related to GRC like what are GRC key roles, it's certification and importance? On the third day the supervisor asked us about the topic what must done research and speak about our research and get the next topic for next class. On the fifth day we were asked by the supervisor and the topic was given to make reports on the particular research terms.

What I did well (refer to skills used)

I was able to give answer asked by the supervisor. I was able to note down the information which I was not able to find it.

What I could improve on (i.e. skills I want to improve)

I need to improve more in my research skills.

Action I can take to improve my skills and learning (make these "SMART"):

GOAL: To improve myself in research skills.

Action: Practicing all of the research skills and enhancing those research skills by help of our teacher and friends.

Timing: 11th October.

LEARNING LOG 3

For the period 21st September 2021 (start date) to 29th September 2021 (end date)

What have I done? (relate tasks to Learning Outcomes) (L01,L04)

On the first day of the week, we had to give the research work which was given last week and answer the question which was asked by the supervisor and topic was IS Audit and rules in organization and at last we were given another research for homework and the topic was domain of cyber security. In third day, we were asked by the supervisor that how many domains of cyber security are there and their importance to everyone in class and the next topic was given for the research and the topic was cyber security scenario in world and Nepal. In fifth day or last day of the week the supervisor asked about the topic and next topic was given for research and the topic was mitigation of cyber-attack.

I start to research about cyber security and their domain, and write a report. In our third meeting, first we discuss about cyber security and its domain. Sami Shrestha ma'am ask us alphabetically, I was able to answer the questions. She asks to send the task in email. I had emailed my report to Richa Nepal (LO1).

What I did well (refer to skills used)

I was able to research the given topic properly and explained it in the meeting in the presence of supervisor. I noted down the sub-topic which I could not find while researching the topics.

What I could improve on (i.e. skills I want to improve)

I could improve my research skill of topic's sub-topics and my explanation skills.

Action I can take to improve my skills and learning (make these "SMART"):

GOAL: To improve myself in researching topics and explaining it.

ACTION: work on researching and gave an explanation on topic in meeting.

Timing: 1

LEARNING LOG 4

For the period 21st September 2021 (start date) to 29th September 2021 (end date)

What have I done? (relate tasks to Learning Outcomes)

As our dashain vacation ends our regular internship class begin and on the first day of the week, we had to give the research work which was given last week and answer the question which was asked by the supervisor and topic was mitigation of the cyber-attack and at last we were given another research for homework and the topic was ISO policies. In third day, we were asked by the supervisor the ISO policies are there and their importance to everyone in class and the next topic was given for the research and the topic was 27001: ISO. In fifth day, the supervisor asked about the topic and next topic was given for research and the topic was Data centre. The last day of the class the supervisor asked about the topic and asked to give the feedback back about the GRC class. After discussion was complete Richa ma'am give us a new task "Business impact analysis, benefit after doing BIA".

What I did well (refer to skills used)

I was able to get a various knowledge while researching about the topics and discuss well with group member and supervisor in the meeting.

What I could improve on (i.e. skills I want to improve)

I could improve the knowledge about the given topic and discuss with the group members.

Action I can take to improve my skills and learning (make these "SMART"):

GOAL: To improve knowledge of the given topic and work with the team member.

ACTION: discussed with the group member and researched the given topic properly.

Timing: 25th November.

LEARNING LOG 5

For the period **21st September 2021** (start date) to **29th September 2021** (end date)

What have I done? (relate tasks to Learning Outcomes) (L01,L04)

We begin our SOC session after finishing our GRC session, which is supervised by Mr. Rishitosh Ghatani. He does not teach courses; instead, he gives out tasks via email and ask to completed and send via email. While installing the software we have to take a screenshot about the process of creating the virtual environment and make a report on it. In the third week our supervisor provided a reference video to watch it and answer the question which is related to video which needs to submit in next week. We must do the assignment on our own. By doing some web research. We must conduct research, write a report, and submit it before moving on to the next job so I had researched Asset, Threat, Vulnerability, CIA, Attack methods, Adaptive Security Strategy, and other topics for this work and delivered it to my supervisor on time.(L01,L04).

What I did well (refer to skills used)

I was able to get a various knowledge while researching about the topics and discuss well with group member and supervisor in the meeting.

What I could improve on (i.e. skills I want to improve)

I could improve the knowledge about the given topic and discuss with the group members and also I could improve my research skills, understand about the technical terms and know the basic commands of the related topics.

Action I can take to improve my skills and learning (make these “SMART”):

GOAL: I could improve my technical skills, understand about the technical terms and know the basic commands.

ACTION: doing research about the topic, watching the tutorials of the mentioned tools which was discussed by the supervisor.

Timing: 28th December 2021Timing: 28th December 2021.

LEARNING LOG 6

For the period 21st September 2021 (start date) to 29th September 2021 (end date)

What have I done? (relate tasks to Learning Outcomes) (L01,L04,L06)

In our second work, supervisor give us a another task on next Sunday. In that task I have install VMware, setup that VMWare and install two Linux machine and one windows machine. Inside of Linux (ubuntu) I have install Nagios, cacti snort, inside of windows 7 I have installed glasswire and Wireshark. After completing the installation and setup process I have run the recon tool Nessus, Nagios and Nmap into victim machine window7(LO6). I also have created report of all the task and submit to supervisor (LO1). At the third week I have research and create report on topic gathering intelligence types: Human Intelligence (HUMINT), Intelligence (SIGINT), Imagery Intelligence (IMINT), Geospatial Intelligence (GEOINT), Measurement and Signatures Intelligence (MASINT), Telemetry Intelligence (TELINT), Open-Source Intelligence (OSINT) (LO4). I also have research and report about cyber treat intelligence and gathering information of Ip address. (L06)

We were assigned the responsibility of creating a virtual environment and deploying three virtual machines (Linux, kali linux, and windows 7), with kali linux acting as the attacker and windows 7 acting as the victim. Then we had to make sure that each virtual machine could communicate with each other. Following that, we had to conduct recon assaults. The final objective was to produce proper documentation of the logs generated by the Nagios server and Victim computer. This was the only project that took me more than a week to complete. To do the task, I had to enlist the support of my friends and my teacher.

What I did well (refer to skills used)

I was able to complete all the tasks and create the virtual environment after being assigned all of the questions.

What I could improve on (i.e. skills I want to improve)

My practical understanding and use of a linux-based operating system might undoubtedly be improved.

Action I can take to improve my skills and learning (make these “SMART”):

GOAL: I could improve my technical skills, understand about the technical terms and know the basic linux-based commands.

ACTION: doing research about the topic, watching the tutorials of the linux-based commands.

Timing: 28th December 2021.

LEARNING LOG 7

For the period **21st September 2021** (start date) to **29th September 2021** (end date)

What have I done? (relate tasks to Learning Outcomes) (L01,L04,L06)

The first portion of the second assignment, a study paper on cyber security, intelligence, intelligence tools, and tools to detect malicious ips, was provided to us during the third week of our SOC internship. The assignment had a deadline of November 23rd. Because of the extensive process of locating malicious IP addresses, it took me 5 days to complete the project, and I was only able to submit it on November 23rd, the sixth day.

We were assigned the duty of gathering Threat Intelligence material for the second half of the 3rd assignment, which was due on December 1st. We needed to obtain information regarding OSINT, or open source intelligence, in particular. More precisely, we needed to acquire knowledge on OSINT, or Open-Source Intelligence, as well as its flow chart, tools, and procedures, and put up a system to restrict investigation exposure. Descriptive descriptions of cyber threat intelligence, attack flow, and Advanced Persistent Threats were the second topic.

On the 6th of December, we received the fourth and last work for the SOC. The assignment was to write a report on the CSIRT, its function and responsibilities, the NIST and SANS Incident Response Frameworks, and their differences. We were also quizzed on frequent blunders in cyber event response and archiving, as well as the necessity of both. On December 10th, I turned in my work and gave a presentation.

What I did well (refer to skills used)

I was able to complete all the tasks and create the virtual environment after being assigned all of the questions.

What I could improve on (i.e. skills I want to improve)

My practical understanding and use of a linux-based operating system might undoubtedly be improved.

Action I can take to improve my skills and learning (make these “SMART”):

GOAL: I could improve my technical skills, understand about the technical terms and know the basic linux-based commands.

ACTION: technical research on the provided tools, watching tutorials and gathering more tricks and terms related to the linux-based commands.

Timing: 28th December 2021.

LEARNING LOG 8

For the period 21st September 2021 (start date) to 29th September 2021 (end date)

What have I done? (relate tasks to Learning Outcomes) ((L07,L08,L09)

First day of the week, we discussed about the topics which we are going to learn in the VAPT department. Our supervisor Mr Prem Basnet introduced the topics such as phases of VAPT, lab setup ,metasploitable 2, web bwapp ,SQL injection, XSS ,CSRF ,broken authentication ,brute force ,Shodan search, bug bounty platform, HTB hack the box etc. and then we learn the basic brief introduction of VAPT, its phases and the tools used in VAPT and we were given the task to research briefly and write the report in the same topic and submit it before the next class resumes.

At the first day

I went there with the proper research and communicated with my supervisor which define that I am good at professionals' skills. I used to maintain the notes and takes the screenshot of the topic that was discussed in meeting.

What I did well (refer to skills used)

I was able to complete all the tasks and create the virtual environment after being assigned all of the questions.

What I could improve on (i.e. skills I want to improve)

I could improve the technical skill in VAPT with the different methods.

Action I can take to improve my skills and learning (make these "SMART"):

GOAL: To improve myself technically and practically

ACTION: downloading the setup for VAPT (kali Linux, Nmap, reengine, and other essential

Timing:

LEARNING LOG 9

For the period 21st September 2021 (start date) to 29th September 2021 (end date)

What have I done? (relate tasks to Learning Outcomes) (L07,L08,L09)

On the next class we discussed about the topics Nmap, Zen map, Shodan and others scanning tools and in second day we were taught about the discussed topic of the first day to check the port whether it is open or closed and practice by ourselves. And in third day we discussed about Shodan, it is the software which help to check who is connected to local network. So, we learned it and did it practically. And on the next day we discussed about to use hping3 (software which helps to sends the custom ICMP/UDP/TCP packets) and its practical. Next day we learned about LBD (load balancing tool) (Software that helps to balance the traffic in different servers maintain the performance and reliability. On the last day of week our supervisor gave a description (revision) of the whole week which we studied in the last class of VAPT.

What I did well (refer to skills used)

I knew to use some of the tool and research about the tools write the notes and save the screenshot about the tools

What I could improve on (i.e. skills I want to improve)

I could improve the technical skills to uses the tools properly.

Action I can take to improve my skills and learning (make these "SMART"):

GOAL: To improve myself to use installed tools.

ACTION: Installed required tools and practices with that tool.

Timing: