CMP020X305: Cyber Security

Deploy a Sandboxed Network: Portfolio Lab 01 (of 6)

Set Date:	**27th January 2023**
Deadline:	10th February 2023 by 14:00 hours
Submission Points:	In-person lab demonstration
Submission Format:	In-person lab demonstration
Feedback and Marks:	Verbal and rubric feedback during the demonstration
Marking Scale (Lab):	Maximum 10.00 marks for Lab completion
Marking Scale (Wow Factor):	Maximum 6.66 marks for Lab completion
Learning Outcomes:	**LO2:** Investigate measures that can be taken by both individuals and organizations including governments to prevent or mitigate the undesirable effects of computer crimes and identity theft.

IMPORTANT: This is a living document and will be subject to changes and updates during the life cycle of the lab portfolio. Therefore, it is imperative that you check this document regularly!!

About this lab portfolio

In this lab, you are going to build a sandboxed network using Virtual Box and 5 virtual machines. A network diagram of what you will deploy is shown in Figure 1.

How will this portfolio be marked?

To receive a mark for this portfolio lab, you will need to demonstrate your sandboxed network and its functionality, in-person, in the lab. As part of the demonstration, you will receive verbal feedback and a mark and associated comment will be added to your Coursework Log Book.

Marks for awarded for a demonstration of lab completion in accordance with the specifications in this document. The **maximum mark for this lab portfolio is 10**. An **additional maximum mark of 6.66** can be awarded for "**Wow Factor**" that evidences appropriate, relevant and additional learning. Typically, wow factor demonstrates a self study contribution that extends or advances the core technical requirements of a lab portfolio.

Late Portfolio Submissions

For each week that a portfolio is late, a single mark will be deducted from the portfolio score that is awarded.

How will the sandboxed network be used?

You will use this sandboxed network throughout the module for practical labs, some of which count as contributions towards your coursework portfolio (worth 60% of the total module marks).

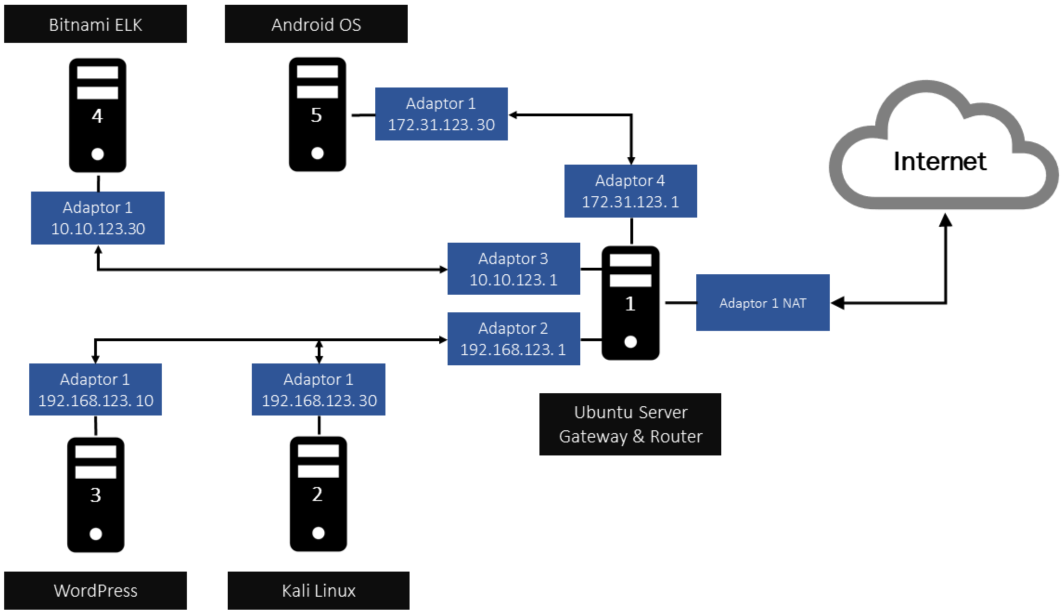

Figure 1: Sandboxed Network Diagram

Resources for this Portfolio Lab

This lab requires 5 virtual machines. Details for each machine are summarised in Table 1, Table 2, Table 3, Table 4 and Table 5 respectively.

Virtual Machine: 1	**Ubuntu Gateway & Router**
Use case(s)	- As an internet access gateway for Ubuntu 18.04, Android OS, Kali Linux and WordPress - As a router to connect 3 private networks (192.168.123.0/24; 10.10.123.0/24, 172.31.123.0/24) - As a network Firewall
RAM	2 GB

Virtual Machine: 1	**Ubuntu Gateway & Router**
CPUs	1
Operating System	Ubuntu 22.04
Network Adaptor 1	NAT
Network Adaptor 2	192.168.123.1
Network Adaptor 3	10.10.123.1
Network Adaptor 4	172.31.123.1
Source	A pre-built version is available from the BSc Level 6 Cyber Security Virtual Machines repository.
Username	student
Password	Student1

Table 1: Ubuntu Gateway & Router

Virtual Machine: 2	**Kali Linux**
Use case(s)	Workstation
RAM	4 GB
CPUs	2
Operating System	Debian
Network Adaptor 1	192.168.123.30
Source	A pre-built version is available from the BSc Level 6 Cyber Security Virtual Machines repository.
Username	kali
Password	kali

Table 2: Kali Linux

Virtual Machine: 3	**WordPress**
Use case(s)	Web Server (Content Management System)
RAM	2 GB
CPUs	1
Operating System	Ubuntu 14.04
Network Adaptor 1	192.168.123.10
Source	A pre-built version is available from the BSc Level 6 Cyber Security Virtual Machines repository.
Username	student
Password	Student1

Table 3: WordPress

Virtual Machine	**Bitnami ELK**
Use case(s)	- Data Analysis
RAM	8192 GB
CPUs	2
Operating System	Debian
Network Adaptor 1	172.31.123.40
Source	A pre-built version is available from the BSc Level 6 Cyber Security Virtual Machines repository.
Username	bitnami
Password	bitnami

Table 4: Bitnami ELK

Virtual Machine	**Android OS**
Use case(s)	- Android OS lab activities

Virtual Machine	**Android OS**
RAM	4 GB
CPUs	1
Operating System	Android
Network Adaptor 1	172.31.123.30
Source	A pre-built version is available from the BSc Level 6 Cyber Security Virtual Machines repository.
Username	root
Password	abc123

Table 5: Android OS

VirtualBox and UTM

This lab portfolio requires a Type 2 hypervisor, for example VirtualBox and UTM. Both are free and open source. For Windows and Linux PCs, use VirtualBox. Although Macs with Intel process can run VirtualBox; UTM for Macs works well with both Intel and Silicon M1 and M2 processors.

Using a Lab PC

VirtualBox has already been installed in the DB210, DB218 and DB323 computer labs. UTM for Mac users has been installed in DB080, DB081, DB110 and DB111.

Using your own Laptop or PC

You will need to download:

- VirtualBox (if you are using a Linux or Windows PC)
- UTM (if you are using a Mac)

If you plan to run this lab portfolio on your own laptop, you will need to have a **minimum of 16 GB of RAM**.

Lab Portfolio Requirements

1. **Copy the virtual machine .OVA files to your lab workstation or laptop**
   The virtual machines for this lab have been created for you and are available either via a USB (ask your instructor), or can be downloaded from here: BSc Level 6 Cyber Security Virtual Machines. NOTE: Downloading online is typically very slow as each virtual machine is a minimum of 1GB. Therefore, the recommended option for accessing each virtual machine is via a USB drive.
2. **Configure the network adaptors to use the IP addresses specified in Table 1, Table 2, Table 3, Table 4 and Table 5 respectively.**
   If you are not familiar with configuring IP address for Linux virtual machines, research the process. However, we will cover this in the lab session.
3. **Test that machines on the same subnet, can communicate with each other.** For example:
   - Use the ping command and test for appropriate responses
   - Use a browser to connect to to WordPress
   - Find the WordPress Admin URL and sign on
4. **Test that virtual machines on different subnets cannot communicate** .
   - Try pinging each machine for an appropriate response.
5. **Test to see if all virtual machines have internet access**.
   - You can test communications using the ping command.
   - Use a browser from your Kali Linux virtual machine.
   - Use the ping command from servers (e.g., try pinging 8.8.8.8).
6. **Demonstrate your completed work to your instructor. No demonstration, no marks!**
   In order to ensure that instructor time is not monopolised by a single student and that students fully own the responsibility for their portfolio labs, each student is permitted one formal demonstration period, after which, marks and an outcome will be added a student's Coursework Portfolio Log.

Wow factor suggestion!

It is feasible to pass this portfolio without completing any "wow factor". However, if you decide to take on this additional learning opportunity, the choice of what contribute is yours. Here is an example to consider:

- Deploy an additional virtual machine to your sandboxed network.
- It can be any operating system of your own choice.
- Think carefully about its relevance and how it might be used as part of your sandboxed network.
- consider which subnet you might add it to and why.

End of Lab Portfolio :-)