# ASSIGNMENT BRIEF

| | | | | | |
|---|---|---|---|---|---|
| **Module Code** | COM6008M | **Module Tutor** | Dr Hamed Balogun | | |
| **Module Title** | Cyber Crime and Security | | | | |
| **Level** | 6 | **Credit Value of Module** | 20 | | |
| **Assessment Task** | Portfolio – Theory, Practical and Problems Solving | | | | |
| **Assessment No** | 1 | **of** | 1 | **Weighting** | 100% |
| **Type of Submission** | Portfolio | | | | |
| **Method of Submission** | Moodle | | | | |
| **Publication Date** | 15th March, 2024 | | | | |
| **Due Date** | 17th May 2024 | | | | |
| **Expected Feedback Date** | 10th June 2024 | | | | |

**Learning Outcomes**

LO 1. Critically evaluate and apply advanced concepts, technologies and approaches to cybercrime security computing problems.

LO 2. Apply conceptual professional, moral, ethical and legal frameworks to cybercrime security.

LO 3. Critically evaluate areas where digital evidence can exist, can be recovered, analysed for criminal investigation and presented.

LO 4. Critically and accurately apply established techniques utilizing the main tools, methods and procedures used for cybercrime security computing.

**Assignment Description**

## Marks allocation for the Assessment

There are four sections in this assessment, with each section carries marks as follows:
Part 1: Ethical issues of Cybersecurity 20%
Part 2: Digital Forensics and Applied Cryptography 30 %
Part 3: Packet Sniffing & Spoofing Attacks, and countermeasures 20%
Part 4: TCP/IP Attacks and Countermeasures 10%
Part 5: Applied Cryptography 10%
Report: Practical report 10%

## What you need to submit

For section 1, you are to summarize your answers, findings, and constructive arguments and screenshots of the solutions.

For sections 2,3,4 and 5, you are to provide the screenshots with specific commands, sources code, and a brief illustration of how you solve the given problems. The marking criteria for these sections are accuracy and or relevant to the correct solutions.

Your assessment report will be graded on well you presented your report with all the required answers/screenshots and clear images/pieces of evidence of your answers and solutions and the quality of your answers.

# Part One - Ethical issues of Cybersecurity [20 marks]

**Problem 1.1**

Investigate what is known about the Russian cyber-attack on the United Kingdom and the cyber-attacks by “Anonymous” against Russia since when Russia invaded Ukraine. Did any of the attacks use things that you have learned about in this course? What could have been done to prevent a portion of the attack, if anything? [5 marks]

**Problem 1.2**

What kind of professional certifications and competence are required in the field of Cybersecurity/Penetration testing/Digital forensics (you are to choose only one from these three terms)? Does someone who has multiple certifications necessarily know more and have greater skills than someone who does not? What jobs are available to people with expertise in Cybersecurity or penetration testing or digital forensics? Using a career search website such as Monster.com or LinkedIn Job Search, find at least five jobs that require one of the certifications you mentioned earlier. [5 marks]

**Problem 1.3 – Detecting Cross Site Scripting vulnerabilities in web applications.** [5 marks]

Cross Site Scripting vulnerabilities allow attackers to spoof content, steal user cookies, and even execute malicious code on the user's browsers. There are even advanced exploitation frameworks such as Beef that allow attackers to perform complex attacks through JavaScript hooks. Web pen testers can use Nmap to discover these vulnerabilities in web servers in an automated manner. Your task is to use either of the following scripts or any of your choice to scan a web server looking for files vulnerabilities to Cross Site Scripting (XSS). You are required to use a free scan webserver or even your own webserver to complete this task. Make sure you write the result of your scanning into a file to enable you analyse the result of you scanning. http-unsafe-output-escaping If your target webserver is a PHP server, you may consider using the following script instead.

http-phpself-xss,httpunsafe-output-escaping

You are to explain the result of your findings whether you discover the vulnerabilities, or you did not.

**Problem 1.4 Finding SQL injection vulnerabilities in web applications.** [5 marks]

SQL injection vulnerabilities are caused by the lack of sanitation of user input, and they allow attackers to execute DBMS queries that could compromise the entire system. This type of web vulnerability is very common, and because each script variable must be tested, checking for such vulnerabilities can be a very tedious task. Fortunately, we can use Nmap to quickly scan a web server looking for vulnerable files for SQL injection. Your task is to search and find the sql-injection vulnerabilities nmap script to scan your chosen webserver. You are to explain your findings whether you have found any vulnerabilities or not. If you are not comfortable to using the nmap, you have an option to use any tool to scan for SQL injection vulnerabilities of your target. Make sure you write the result of your scanning into a file to enable you analyse the result of your scanning.

End of Part one

---

# Part 2 Digital Forensics [30 marks]

The objective of part is for you to demonstrate your learning about incident response and data acquisition, digital data recovery and data carving processes and techniques using forensics applications. You will also demonstrate your learning of the basic artifact analysis process, analyze memory dumps to discover ransomware traces, and perform swap analysis on digital evidence.

**Problem 2.1 Incident Response and Data Acquisition [10 marks]**

As part of the best practices of digital forensics investigation, we should be aware of and follow the rules, techniques, and procedures for obtaining evidence so that it is neither tampered with nor, in the worst-case situation, lost throughout any inquiry. Subsequently, we use either Hardware Write Blockers or Software Write Blockers to protect the devices (disc) we are investigating. Write blockers are devices that enable for the acquisition of data on a drive without causing the drive's contents to be mistakenly damaged. They accomplish this by allowing read commands to flow but blocking write commands, as their name implies.
You will use a Tableau Forensic SATA/IDE Bridge Kit and the SATA hard disc to complete the following task.

i. Create a forensic image of the disc **[5 marks]**
ii. Create MD5 or SHA1 hash of the disc **[2 marks]**
iii. Describe the challenges and benefit you encountered when running the experiment with the write blocker. **[3 marks]**

**Problem 2.2 [5 marks] – Digital file recovery and data carving**

In the process of Digital investigation, we use file carving to retrieve data and files from unallocated space using specific characteristics, such as the file structure and file headers, instead of traditional metadata created by or associated with filesystems. Generally, Data carving is quite a lengthy process and should be done using automated tools to save time. It also helps if the investigator has an idea of what file types, they are looking for to have a better focus and to save time.

In these tasks, you 'll be using a digital forensic tool-testing image, created by Nick Mikus specifically for testing data carving. The file is named **L2_Video.dd.bz2** and it is in the memory dump zipped file. The memory dump image zipped file can be downloaded from Moodle.

You are to use ***foremost*** data carving application to investigate the image.
If foremost is not listed in or installed on your version of Kali Linux, install it by typing.
**sudo apt-get install foremost.**
Once foremost is successfully installed, you can use the following foremost's syntax to carve the 11-carve-fat.dd image. Make sure you extracted the file.

```
foremost -i (forensic image) -o (output folder) -options
```

**Where**

- **-i Input**
- **-o Output**

> **Tip:**
> For quick access to some of the commands in Foremost, you can use `foremost -h`.

Once the processes of data carving are complete, you can navigate to your output folder to view the findings. You are to include the evidence of data carving process with the carved items, categorized by file type, along with an audit.txt file that contains details of the findings.
Once you're in the same directory as the extracted **L0_Graphic.dd** file that you have just downloaded, you may use the following syntax to carve files. The following syntax illustrate how you can recover only avi files from the image.

```
foremost -t avi -i L2_Video.dd -o Recovered_AVI
```

i. Now, use the same syntax to recover (i) AVI files, (ii) mov files and (iii) wmv files. **[3 marks]**

ii. Install and use **Scalpel** to carve all the files in **L0_Graphic.dd** image that you have downloaded. You are to include the evidence of accomplished tasks and the screenshot of the Log file. **[1 mark]**

iii. Comment on the differences between the **Scalpel** and **foremost in terms of data carving.** **[1 mark]**

# A case study - Incident Response and Data Acquisition

A user in your organisation suspects that her computer is infected with a Malware after she open an attachment that she received via email. Your manager assigned the incident to you and advise you to apply digital forensic method to investigate the affected machine.
Since the Memory (RAM) stores valuable information about the runtime state of the processes/systems, as a first responder to the vent, what are the things you need to do to find and extract forensics artifacts from the computer's RAM. **[2 marks]**
In the context of digital evidence acquisition and preservation, describe the process of Chain of custody (CoC) and how it helps ensures the integrity of digital evidence and provides a level of accountability. **[3 marks]**

### Problem 2.4 [10 marks] – Malware Analysis

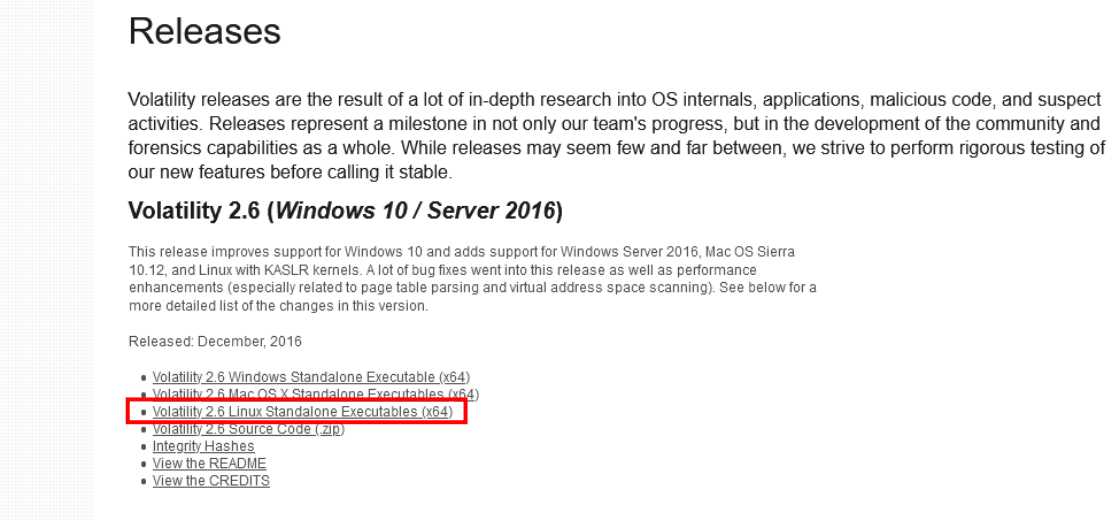
This task is the continuation of task 2 - the provided case study.
You are to use the link below to download and extract the memory dump of the machine you are investigating.
https://mega.nz/file/Au5xlCAS#KX5ZJKYzQgDHSa72lPFwqKL6CsZS7oQGbyyQrMTH9XY

The password for the malware is infected
If you are having difficulties downloading the file from the provided link, you can locate the same memory dump image in a folder called "Memory dump" on the Module page. The name of the image is 'WannaCry.' Now that you have the Memory image to be investigated, you are ready to go. But to do that, you need to download and install Volatility to help you do the investigations.

The Volatility Framework is an open source, cross-platform, incident response framework that comes with many useful plugins that provide the investigator with a wealth of information from a snapshot of memory, also known as

a memory dump. You may use the following link to download the Volatility that is compatible with your operating system. If you are using Kali Linux, you may consider downloading the Volatility 2.6 Linux Standalone_Executable as indicated below.

- http://www.volatilityfoundation.org/releases




To view the options within Volatility, type in volatility –h. If Volatility does not start, or a command not found error is returned, install the Volatility Framework by typing apt-get install volatility. During the installation, you will be prompted to press Y (yes) to download the files required for the installation. Depending on your OS, the Python compiler installed on your machine or the version of the volatility you are using. Sometimes you may encounter an error while installing the volatility. You use the following example to grab the latest release of the Volatility Framework from the GitHub and install it on your machine.

```
                                          Grab latest release of Volatility
$ cd
$ git clone
https://github.com/volatilityfoundation/volatility.git

$ cd volatility                           Preliminary setup
$ python setup.py build                   and then sanity check
$ python vol.py --info
```

After you successfully installed the Volatility on your Machine, you can then use the Volatility plugins to investigate the image you are working on. Recall, you may need to get the image information to enable you conduct the experiment as indicated below.

```
└─$ sudo ./volatility -f wcry.raw imageinfo
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/aminu/Desktop/volatility/wcry.raw)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x8054cf60L
        Number of Processors : 1
    Image Type (Service Pack) : 3
               KPCR for CPU 0 : 0xffdff000L
            KUSER_SHARED_DATA : 0xffdf0000L
          Image date and time : 2017-05-12 21:26:32 UTC+0000
    Image local date and time : 2017-05-13 02:56:32 +0530
```

Now that you have the information you need to investigate the image, do the following. As an example, see the following example of the Volatility output of process list plugin.

```
└─$ sudo ./volatility --profile=WinXPSP2x86 -f 0zapftis.vmem pslist volatility Foundation Framwwork 2.6
[sudo] password for aminu:
Volatility Foundation Volatility Framework 2.5
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x819cc830 System                    4      0     55      162 ------      0
0x81945020 smss.exe                536      4      3       21 ------      0 2011-10-10 17:03:56 UTC+0000
0x816c6020 csrss.exe               608    536     11      355      0      0 2011-10-10 17:03:58 UTC+0000
0x813a9020 winlogon.exe            632    536     24      533      0      0 2011-10-10 17:03:58 UTC+0000
0x816da020 services.exe            676    632     16      261      0      0 2011-10-10 17:03:58 UTC+0000
0x813c4020 lsass.exe               688    632     23      336      0      0 2011-10-10 17:03:58 UTC+0000
0x81772ca8 vmacthlp.exe            832    676      1       24      0      0 2011-10-10 17:03:59 UTC+0000
0x8167e9d0 svchost.exe             848    676     20      194      0      0 2011-10-10 17:03:59 UTC+0000
0x817757f0 svchost.exe             916    676      9      217      0      0 2011-10-10 17:03:59 UTC+0000
0x816c6da0 svchost.exe             964    676     63     1058      0      0 2011-10-10 17:03:59 UTC+0000
0x815daca8 svchost.exe            1020    676      5       58      0      0 2011-10-10 17:03:59 UTC+0000
0x813aeda0 svchost.exe            1148    676     12      187      0      0 2011-10-10 17:04:00 UTC+0000
0x817937e0 spoolsv.exe            1260    676     13      140      0      0 2011-10-10 17:04:00 UTC+0000
0x81754990 VMwareService.e        1444    676      3      145      0      0 2011-10-10 17:04:00 UTC+0000
0x8136c5a0 alg.exe                1616    676      7       99      0      0 2011-10-10 17:04:01 UTC+0000
0x815c4da0 wscntfy.exe            1920    964      1       27      0      0 2011-10-10 17:04:39 UTC+0000
0x813bcda0 explorer.exe           1956   1884     18      322      0      0 2011-10-10 17:04:39 UTC+0000
0x816d63d0 VMwareTray.exe          184   1956      1       28      0      0 2011-10-10 17:04:41 UTC+0000
0x8180b478 VMwareUser.exe          192   1956      6       83      0      0 2011-10-10 17:04:41 UTC+0000
0x818233c8 reader_sl.exe           228   1956      2       26      0      0 2011-10-10 17:04:41 UTC+0000
0x815e7be0 wuauclt.exe             400    964      8      173      0      0 2011-10-10 17:04:46 UTC+0000
0x817a34b0 cmd.exe                 544   1956      1       30      0      0 2011-10-10 17:06:42 UTC+0000
```

1. Generate the Hash of the image using the SHA256 Hash algorithm for integrity checking. **[2 marks]**
2. What does the number 2 mean in the name of SHA-2? What does the number 256 means in the name of SHA-256? **[2 marks]**
3. Use the following plugins to investigate the memory image. You are to research and explain the output of each plugin **[4 marks],** with each plugin 0.5 marks]. An example of the output for the ***plist*** is provided.
    i. pslist, ii. pstree iii. psscan iv. psxview v. connscan vi. Sockets
    vii. hivescan viii. hivelist
4. Volatility can produce a list of timestamped events, which is essential to any investigation. To produce this list, use the ***timeliner*** plugin to produce the timeline of the event. Explain your finding **[2 mark].**

**End of part two**

---

# Part 3 - Network Security: Packet Sniping and Spoofing [20 Marks]

**Problem 3.1** [3 marks]

In cyberwars between two counties, the root DNS servers of each side will be primary targets. If country A can bring down all the root servers of country B, A can effectively cut off the communication between B and the outside world. Assume that your job is to manage the root DNS server for country B, which is a small country that does not have sufficient resources to defend against large-scale DDoS attacks from its powerful foe. What can you do?

**Problem 3.2** [2 marks]
In one or two paragraphs discuss the ethical and legal issues surrounding the use of packet sniffing in cyber security.

**Problem 3.3** [2 marks]
What are the different types of packets sniffing tools available to an attacker? Explain the features and capabilities of each tool.

**Problem 3.4** [2 marks]
What are the common methods used to prevent packet sniffing attacks in a network? Explain each method.

**Problem 3.4** [2 marks]
Write a spoofing program. Please write your own packet spoofing program in any programming language of your choice. You need to provide evidence (e.g., Wireshark packet trace) to show that your program successfully sends out spoofed IP packets.

## Practical

Packet sniffing and spoofing are two important concepts in network security; they are two major threats in network communication. Being able to understand these two threats is essential for understanding security measures in networking. There are many packets sniffing and spoofing tools, such as Wireshark, Tcpdump, Netwox, Scapy, etc. So far in this class, we have been using Wireshark to analyse network protocols and security protocols. However, there are other tools that are widely used by security experts, pen testers as well as by attackers. Being able to use these tools is important for a student of Cyber security, but what is more important is to understand how these tools work, i.e., how packet sniffing, and spoofing are implemented in software.

The objective of this task is two-fold: learning to use the tools and understanding the technologies under-lying these tools. For the second object, students will write simple sniffer and spoofing programs, and gain an in-depth understanding of the technical aspects of these programs. This lab covers the following topics:

- Scapy
- Sniffing using the pcap library
- Raw socket

**Lab environment.**

For this lab
You need an attacker machine and a victim machine. If you are using virtual machines, make sure the two VMs have different IP addresses.

## Using Tools to Sniff and Spoof Packets

Many tools can be used to do sniffing and spoofing, but most of them only provide fixed functionalities. Scapy is different: it can be used not only as a tool, but also as a building block to construct other sniffing and spoofing tools, i.e., we can integrate the Scapy functionalities into our own program. In this set of tasks, we will use Scapy for each task.

To use Scapy, we can write a Python program, and then execute this program using Python. See the following example. We should run Python using the root privilege because the privilege is required for spoofing packets. At the beginning of the program (Line À), we should import all Scapy's modules.

```
$ view mycode.py
#!/bin/bin/python

from scapy.all import *     ①

a = IP()
a.show()

$ sudo python mycode.py
###[ IP ]###
  version   = 4
  ihl       = None
  ...
```

We can also get into the interactive mode of Python and then run our program one line at a time at the Python prompt. This is more convenient if we need to change our code frequently in an experiment.

```
$ sudo python
>>> from scapy.all import *
>>> a = IP()
>>> a.show()
###[ IP ]###
  version   = 4
  ihl       = None
  ...
```

Sniffing Packets

Wireshark is the most popular sniffing tool, and it is easy to use. We will use it throughout the entire lab. However, it is difficult to use Wireshark as a building block to construct other tools. We will use Scapy for that purpose. The objective of this task is to learn how to use Scapy to do packet sniffing in Python programs. A sample code is provided in the following:

```
#!/usr/bin/python
from scapy.all import *

def print_pkt(pkt):
  pkt.show()

pkt = sniff(filter='icmp',prn=print_pkt)
```

**Problem 2.1.** The above program sniffs packets. For each captured packet, the call back function print pkt() will be invoked; this function will print out some of the information about the packet. Run the program with the root privilege and demonstrate that you can indeed capture packets. After that, run the program again, but without using the root privilege; describe and explain your observations. [2 marks]

```
// Run the program with the root privilege
$ sudo python sniffer.py

// Run the program without the root privilege
$ python sniffer.py
```

**Problem** 2.2. Usually, when we sniff packets, we are only interested certain types of packets. We can do that by setting filters in sniffing. Scapy's filter use the BPF (Berkeley Packet Filter) syntax; you can find the BPF manual from the Internet. Please set the following filters and demonstrate your sniffer program again (each filter should be set separately). [2 marks]

- Capture only the ICMP packet.
- Capture any TCP packet that comes from a particular IP and with a destination port number 23.
- Capture packets comes from or to go to a particular subnet. You can pick any subnet, such as 128.230.0.0/16; you should not pick the subnet that your VM is attached to.

Spoofing ICMP Packets

As a packet spoofing tool, Scapy allows us to set the fields of IP packets to arbitrary values. The objective of this task is to spoof IP packets with an arbitrary source IP address. We will spoof ICMP echo request packets and send them to another VM on the same network. We will use Wireshark to observe whether our request will be accepted by the receiver. If it is accepted, an echo reply packet will be sent to the spoofed IP address. The following code shows an example of how to spoof an ICMP packets.

```
>>> from scapy.all import *
>>> a = IP()                    ①
>>> a.dst = '10.0.2.3'          ②
>>> b = ICMP()                  ③
>>> p = a/b                     ④
>>> send(p)                     ⑤
.
Sent 1 packets.
```

In the code above, Line À creates an IP object from the IP class; a class attribute is defined for each IP header field. We can use ls(a) or ls(IP) to see all the attribute names/values. We can also use a.show() and IP.show() to do the same.

```
>>> ls(a)
version    : BitField (4 bits)       = 4               (4)
ihl        : BitField (4 bits)       = None            (None)
tos        : XByteField              = 0               (0)
len        : ShortField              = None            (None)
id         : ShortField              = 1               (1)
flags      : FlagsField (3 bits)     = <Flag 0 ()>     (<Flag 0 ()>)
frag       : BitField (13 bits)      = 0               (0)
ttl        : ByteField               = 64              (64)
proto      : ByteEnumField           = 0               (0)
chksum     : XShortField             = None            (None)
src        : SourceIPField           = '127.0.0.1'     (None)
dst        : DestIPField             = '127.0.0.1'     (None)
options    : PacketListField         = []              ([])
```

The / operator is overloaded by the IP class, so it no longer represents division; instead, it means adding b as the payload field of a and modifying the fields of a accordingly. As a result, we get a new object that represent an ICMP packet. We can now send out this packet using send() in Line 5. Please make any necessary change to the sample code, and then demonstrate that you can spoof an ICMP echo request packet with an arbitrary source IP address.

**Problem** 2.3: Traceroute [3 marks]

The objective of this task is to use Scapy to estimate the distance, in terms of number of routers, between your VM and a selected destination (any destination of your choice). This is basically what is implemented by the traceroute tool. In this task, we will write our own tool. The idea is quite straightforward: just send an packet (any type) to the destination, with its Time-To-Live (TTL) field set to 1 first. This packet will be dropped by the first router, which will send us an ICMP error message, telling us that the time-to-live has exceeded. That is how we get the IP address of the first router. We then increase our TTL field to 2, send out another packet, and get the IP address of the second router. We will repeat this procedure until our packet finally reach the destination. It should be noted that this experiment only gets an estimated result, because in theory, not all these packets take the same route (but in practice, they may within a short period of time). The code in the following shows one round in the procedure.

```
a = IP()
a.dst = '1.2.3.4'
a.ttl = 3
b = ICMP()
send(a/b)
```

If you are an experienced Python programmer, you can write your tool to perform the entire procedure automatically. If you are new to Python programming, you can do it by manually changing the TTL field in each round and record the IP address based on your observation from Wireshark. Either way is acceptable, as long as you get the result.

Sniffing and-then Spoofing

In this task, you will combine the sniffing and spoofing techniques to implement the following sniff-and-then-spoof program. You need two VMs on the same LAN. From VM A, you ping an IP X (any machine of your choice). This will generate an ICMP echo request packet. If X is alive, the ping program will receive an echo reply, and print out the response. Your sniff-and-then-spoof program runs on VM B, which monitors the LAN through packet sniffing. Whenever it sees an ICMP echo request, regardless of what the target IP address is, your program should immediately send out an echo reply using the packet spoofing technique. Therefore, regard-less of whether machine X is alive or not, the ping program will always receive a reply, indicating that X is alive. You need to use Scapy to do this task. In your report, you need to provide evidence to demonstrate that your technique works.

Writing Packet Sniffing Program

Sniffer programs can be easily written using the pcap library. With pcap, the task of sniffers becomes invoking a simple sequence of procedures in the pcap library. At the end of the sequence, packets will be put in buffer for further processing as soon as they are captured. All the details of packet capturing are handled by the pcap library. See the sample code in the following (see the book for detailed explanation).

```
#include <pcap.h>
#include <stdio.h>

/* This function will be invoked by pcap for each captured packet.
   We can process each packet inside the function.
 */
void got_packet(u_char *args, const struct pcap_pkthdr *header,
        const u_char *packet)
{
   printf("Got a packet\n");
}

int main()
{
  pcap_t *handle;
  char errbuf[PCAP_ERRBUF_SIZE];
  struct bpf_program fp;
  char filter_exp[] = "ip proto icmp";
  bpf_u_int32 net;

  // Step 1: Open live pcap session on NIC with name eth3
  //         Students needs to change "eth3" to the name
  //         found on their own machines (using ifconfig).
  handle = pcap_open_live("eth3", BUFSIZ, 1, 1000, errbuf);

  // Step 2: Compile filter_exp into BPF psuedo-code
  pcap_compile(handle, &fp, filter_exp, 0, net);
  pcap_setfilter(handle, &fp);

  // Step 3: Capture packets
  pcap_loop(handle, -1, got_packet, NULL);

  pcap_close(handle);   //Close the handle
  return 0;
}
```

Read the tutorial in the following link about packet sniffing using C programming language. The tutorial is available at http://www.tcpdump.org/pcap.htm

Task 2.4 You are to write a sniffer program to print out the source and destination IP addresses of each captured packet. You can type in the above code or download the provided sample code. You should provide screenshots as evidence to show that your sniffer program can run successfully and produces expected results. [2 marks]

**End of part three**

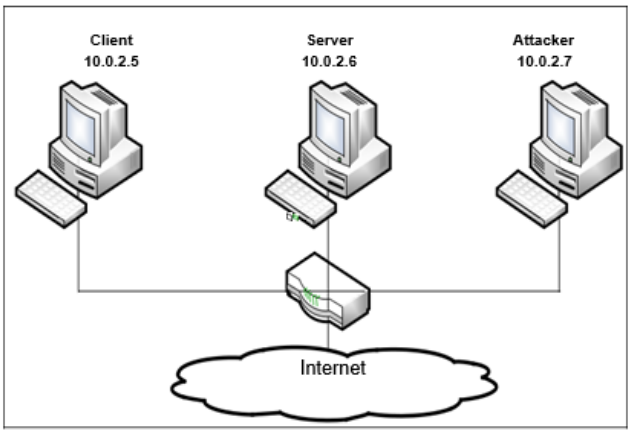
---

# Section 4 - TCP/IP Attacks and Countermeasures [10 marks]

The learning objective of this section is for students to gain first-hand experience on vulnerabilities, as well as on attacks against these vulnerabilities. The vulnerabilities in the TCP/IP protocols represent a special genre of vulnerabilities in protocol de-signs and implementations; they provide an invaluable lesson as to why security should be designed in from the beginning, rather than being added as an afterthought. Moreover, studying these vulnerabilities help students understand the challenges of network security and why many network security measures are needed. In this lab, students will conduct several attacks on TCP. In the second part of this section, you will gain the insights on how firewalls work by playing with firewall software and implement a simplified packet filtering firewall.

## Lab Environment

Network Setup. To conduct this lab, students need to have at least 3 machines. One computer is used for attacking, the second computer is used as the victim, and the third computer is used as the observer. Students can set up 3 virtual machines on the same host computer, or they can set up 2 virtual machines, and then use the host computer as the third computer. For this lab, we put all these three machines on the same LAN, the configuration is shown in the Figure below – Environment Setup.




Environment Setup

Netwox Tools. We need tools to send out network packets of different types and with different contents. We can use Netwag to do that. However, the GUI interface of Netwag makes it difficult for us to auto-mate the process.
Netwox consists of a suite of tools, each having a specific number. You can run a command like following (the parameters depend on which tool you are using).

If you are not sure how to set the parameters, you can look at the manual by issuing "netwox number --help". You can also learn the parameter settings by running Netwag: for each command you execute from the graphic interface, Netwag actually invokes a corresponding Netwox command, and it displays the parameter settings. Therefore, you can simply copy and paste the displayed command.

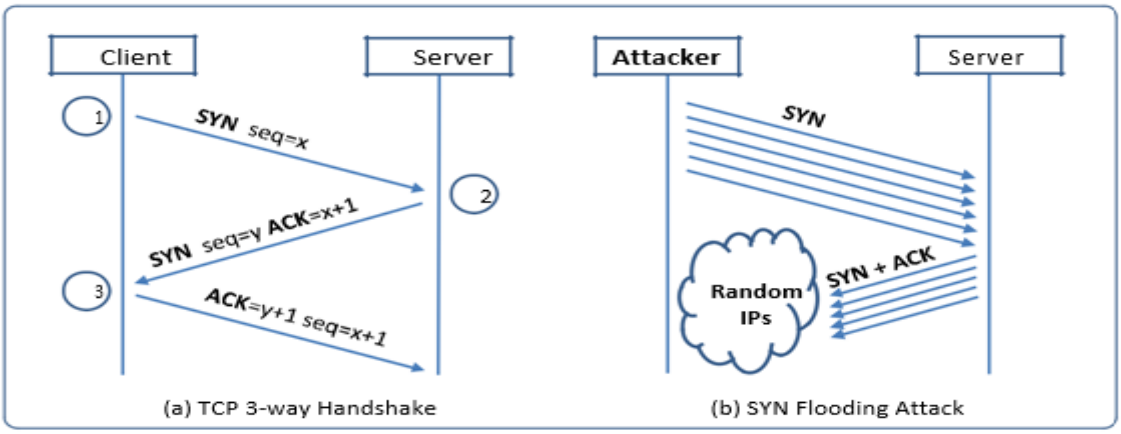
Scapy Tool. Some of the tasks in this lab can also be conducted using Scapy, which is a powerful interac-tive packet manipulation program. Scapy is very well maintained and is widely used; while Netwox is not being maintained any more. There are many online tutorials on Scapy; we expect students to learn how to use Scapy from those tutorials.

## Lab Tasks

In this lab, students need to conduct attacks on the TCP/IP protocols. They can use the Netwox tools and/or other tools in the attacks. All the attacks are performed on Linux operating systems. However, instructors can require students to also conduct the same attacks on other operating systems and compare the observations.

To simplify the “guess” of TCP sequence numbers and source port numbers, we assume that attackers are on the same physical network as the victims. Therefore, you can use sniffer tools to get that information. The following is the list of attacks that need to be implemented.

### Problem 4.1: SYN Flooding Attack [ 2 marks]




SYN Flooding Attack

SYN flood is a form of DoS attack in which attackers send many SYN requests to a victim’s TCP port, but the attackers have no intention to finish the 3-way handshake procedure. Attackers either use spoofed IP address or do not continue the procedure. Through this attack, attackers can flood the victim’s queue that is used for half-opened connections, i.e. the connections that has finished SYN, SYN-ACK, but has not yet gotten a final ACK back. When this queue is full, the victim cannot take any more connection. Figure 2 illustrates the attack.
The size of the queue has a system-wide setting. In Linux, we can check the setting using the following command:

```
$ sudo sysctl -q net.ipv4.tcp_max_syn_backlog
```

We can use command "netstat -na" to check the usage of the queue, i.e., the number of half-opened connection associated with a listening port. The state for such connections is SYN-RECV. If the 3-way handshake is finished, the state of the connections will be ESTABLISHED.
In this task, you need to demonstrate the SYN flooding attack. You can use the Netwox tool to conduct the attack, and then use a sniffer tool to capture the attacking packets. While the attack is going on, run the "netstat -na" command on the victim machine, and compare the result with that before the attack. Please also describe how you know whether the attack is successful or not.

The corresponding Netwox tool for this task is numbered 76. Here is a simple help screen for this tool.
You can also type "netwox 76 --help" to get the help information.ki

Listing 1: The usage of the Netwox Tool 76

```
Title:  Synflood
    Usage: netwox 76 -i ip -p port [-s spoofip]
    Parameters:
    -i|--dst-ip ip              destination IP address
    -p|--dst-port port          destination port number
    -s|--spoofip spoofip        IP spoof initialzation type
```

SYN Cookie Countermeasure: If your attack seems unsuccessful, one thing that you can investigate is whether the SYN cookie mechanism is turned on. SYN cookie is a defense mechanism to counter the SYN flooding attack. The mechanism will kick in if the machine detects that it is under the SYN flooding attack. You can use the sysctl command to turn on/off the SYN cookie mechanism:

$ sudo sysctl -a | grep cookie  (Display the SYN cookie flag)
$  sudo sysctl -w net.ipv4.tcp_syncookies=0 (turn off SYN cookie)
$  sudo sysctl -w net.ipv4.tcp_syncookies=1 (turn on  SYN cookie)

Please run your attacks with the SYN cookie mechanism on and off, and compare the results. In your report, please describe why the SYN cookie can effectively protect the machine against the SYN flooding attack. If your instructor does not cover the mechanism in the lecture, you can find out how the SYN cookie mechanism works from the Internet.

Note on Scapy: Although theoretically, we can use Scapy for this task, we have observed that the number of packets sent out by Scapy per second is much smaller than that by Netwox. This low rate makes it difficult for the attack to be successful. We were not able to succeed in SYN flooding attacks using Scapy.

### Problem 4.2: TCP RST Attacks on telnet and ssh Connections [ 3 marks]

The TCP RST Attack can terminate an established TCP connection between two victims. For example, if there is an established telnet connection (TCP) between two users A and B, attackers can spoof a RST packet from A to B, breaking this existing connection. To succeed in this attack, attackers need to correctly construct the TCP RST packet.

In this task, you need to launch an TCP RST attack to break an existing telnet connection between A and B. After that, try the same attack on an ssh connection. Please describe your observations. To simplify the lab, we assume that the attacker and the victim are on the same LAN, i.e., the attacker can observe the TCP traffic between A and B. To complete this task, you may choose either to use Netwox or Scapy.

Using Netwox. The corresponding Netwox tool for this task is numbered 78. Here is a simple help screen for this tool. You can also type "netwox 78 --help" to get the help information.

Listing 2: The usage of the Netwox Tool 78

```
Title: Reset every TCP packet
    Usage: netwox 78 [-d device] [-f filter] [-s spoofip]
    Parameters:
    -d|--device device              device name {Eth0}
    -f|--filter filter              pcap filter
    -s|--spoofip spoofip            IP spoof initialization type {linkbraw}
```

Using Scapy. If you choose to use Scapy to conduct the TCP RST attack. A skeleton code is provided in the following (you need to replace each @@@@ with an actual value):

```
#!/usr/bin/python
from scapy.all import *

ip  = IP(src="@@@@", dst="@@@@")
tcp = TCP(sport=@@@@, dport=@@@@, flags="@@@@", seq=@@@@, ack=@@@@)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
```

**Problem 4.3: TCP RST Attacks on Video Streaming Applications** [ 2 marks]

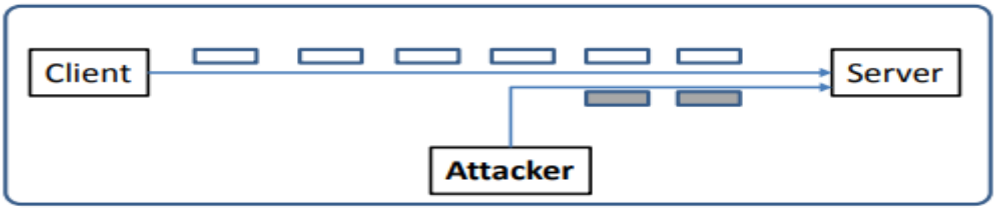
Let us make the TCP RST attack more interesting by experimenting it on the applications that are widely used in nowadays. We choose the video streaming application in this task. For this task, you can choose a video streaming web site that you are familiar with (we will not name any specific web site here). Most of video sharing websites establish a TCP connection with the client for streaming the video content. The attacker's goal is to disrupt the TCP session established between the victim and video streaming machine. To simplify the lab, we assume that the attacker and the victim are on the same LAN. In the following, we describe the common interaction between a user (the victim) and some video-streaming web site:

- The victim browses for a video content in the video-streaming web site, and selects one of the videos for streaming.

- Normally video contents are hosted by a different machine, where all the video contents are located. After the victim selects a video, a TCP session will be established between the victim machine and the content server for the video streaming. The victim can then view the video he/she has selected.

Your task is to disrupt the video streaming by breaking the TCP connection between the victim and the content server. You can let the victim user browse the video-streaming site from another (virtual) machine or from the same (virtual) machine as the attacker. Please be noted that, to avoid liability issues, any attacking packets should be targeted at the victim machine (which is the machine run by yourself), not at the content server machine (which does not belong to you). You only need to use Netwox for this task.

**Problem 4.4: TCP Session Hijacking** [ 3 marks]




TCP Session Hijacking Attack

The objective of the TCP Session Hijacking attack is to hijack an existing TCP connection (session) between two victims by injecting malicious contents into this session. If this connection is a telnet session, attackers can inject malicious commands (e.g. deleting an important file) into this session, causing the victims to execute the malicious commands. The TCP session Hijacking attack figure above depicts how the attack works. In this task, you need to demonstrate how you can hijack a telnet session between two computers. Your goal is to get the the telnet server to run a malicious command from you. For the simplicity of the task, we assume that the attacker and the victim are on the same LAN.

Using Netwox. The corresponding Netwox tool for this task is numbered 40. Here is part of the manual for this tool. You can also type "netwox 40 --help" to get the full help information. You may also need to use Wireshark to find out the correct parameters for building the spoofed TCP packet.

Listing 3: Part usage of netwox tool 40

```
Title:  Spoof Ip4Tcp packet
    Usage: netwox 40 [parameters ...]
    Parameters:
    -l|--ip4-src ip                Source IP
    -m|--ip4-dst ip                Destination IP
    -j|--ip4-ttl uint32            Time to live
    -o|--tcp-src port              TCP Source port number
    -p|--tcp-dst port              TCP Destination port number
    -q|--tcp-seqnum uint32         TCP sequence number
    -E|--tcp-window uint32         TCP window size
    -r|--tcp-acknum uint32         TCP acknowledge number
    -z|--tcp-ack|+z|--no-tcp-ack   TCP ack bit
    -H|--tcp-data data             TCP data
```

You can use Wireshark to figure out what value you should put into each field of the spoofed TCP packets. It should be noted in the TCP session hijacking section of the SEED book, the command listed there does not set all the fields of the TCP and IP headers.

In the netwox command above, the tcp-data part only takes hex data. If we want to inject a command string, which is typically represented as a human-readable ASCII string, we need to convert it into a hex string. There are many ways to do that, but we will just use a very simple command in Python. In the following, we convert an ASCII string "Hello World" to a hex string (the quotation marks are not included).

```
$ python
>>> "Hello World".encode("hex")
'48656c6c6f20576f726c64'
```

Using Scapy. Please also use Scapy to conduct the TCP Session Hijacking attack. A skeleton code is provided in the following (you need to replace each @@@@ with an actual value):

```
#!/usr/bin/python
from scapy.all import *

ip   = IP(src="@@@@", dst="@@@@")
tcp = TCP(sport=@@@@, dport=@@@@, flags="@@@@", seq=@@@@, ack=@@@@)
data = "@@@@"
pkt = ip/tcp/data
ls(pkt)
send(pkt,verbose=0)
```

# Part 5 Applied Cryptography [10 marks]

**Problem 5.1 [ 3 marks]**

RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure communication. The RSA algorithm first generates two large random prime numbers, and then use them to generate public and private key pairs, which can be used to do encryption, decryption, digital signature generation, and digital signature verification.

Let p, q, and e be three prime numbers. Let n = p*q. We will use (e, n) as the public key. Please calculate the private key d. The hexadecimal values of p, q, and e are listed in the following. It should be noted that although p and q used in this task are quite large numbers, they are not large enough to be secure. We

intentionally make them small for the sake of simplicity. In practice, these numbers should be at least 512 bits long (the one used here are only 128 bits).

p = F7E75FDC469067FFDC4E847C51F452DF
q = E85CED54AF57E53E092113E62F436F4F
e = 0D88C3

**Problem 5.2 [2 marks]**

In the RSA algorithm, since doing $(M^e)^d$ mod n and $(M^d)^e$ mod n always get the same result M. Bob decides to keep e as the private key and use e to do the decryption, and publish d as the public key, and use d to do the encryption. Is this safe?

**Task 5.3 [ 3 marks]**

In the Diffie-Hellman key exchange, Alice sends $g^x$ mod p to Bob, and Bob sends $g^y$ mod p to Alice. How do they get a common secret?

**Problem 5.4 [2 marks]**

A news report says that company XYZ's network was attacked by outsiders, who apparently sent a lot of spoofed ARP requests/responses from remote machines to the company's network, trying to launch ARP cache poisoning attacks. Please comment on whether this is fake news or not.

**Additional Information**

Reference Text

Chapter 15 - Du, W., 2019. *Computer & Internet Security: A Hands-on Approach*. Independently published.
Du, W., 2011. SEED: hands-on lab exercises for computer security education. *IEEE Security & Privacy*, *9*(5), pp.70-73.
Calderon, P., 2017. *Nmap: Network Exploration and Security Auditing Cookbook*. Packt Publishing Ltd.

**Assessment Regulations**

- Your attention is drawn to the University policy on cheating and plagiarism. Penalties will be applied where a student is found guilty of academic misconduct, including termination of programme (Policy link).
- You are required to keep to the word limit set for an assessment and to note that you may be subject to penalty if you exceed that limit. (Policy link). You are required to provide an accurate word count on the cover sheet for each piece of work you submit.
- For late or non-submission of work by the published deadline or an approved extended deadline, a mark of 0NS will be recorded. Where a re-assessment opportunity exists, a student will normally be permitted only one attempt to be re-assessed for a capped mark. (Policy link).
- An extension to the published deadline may be granted to an individual student if they meet the eligibility criteria of the Exceptional Circumstances policy.

**Summary Feedback**

| | | | |
|---|---|---|---|
| **First Marker:** | | **Date:** | |
| *First marker feedback* | | | |
| **Second Marker:** | | **Date**: | |
| *Second marker feedback (if applicable)* | | | |
| | **Provisional mark:** | | |

| | PASS GRADES | | | | | FAIL GRADES | |
|---|---|---|---|---|---|---|---|
| | (100-85) | (84 - 70) | (69 - 60) | (59 - 50) | (49 - 40) | (39 - 20) | (19 - 0) |
| **SUMMARY DESCRIPTOR:** Learning accredited at **Level 6 (UG)** will reflect the ability to critically review, consolidate and extend a systematic and coherent body of knowledge, utilising specialised skills across an area of study. | | | | | | | |
| | **General Characteristics (UG)** | | | | | | |
| **Knowledge & understanding**<br>PLO(s): Enter "All" or specific PLO(s). If N/A: Delete row | Subject knowledge and conceptual understanding beyond expectation(s) of the level of study. | Subject knowledge and conceptual understanding that evidences a breadth/depth of reading/research significantly beyond set material. | Detailed subject knowledge and conceptual understanding relevant to the level of study and demonstrating development beyond set material. | Subject knowledge and conceptual understanding consistent with taught content. | Replication of taught content with limited demonstration of conceptual understanding. | Insufficient knowledge and understanding of the subject and its underlying concepts. | Little or no evidence of knowledge and understanding of the subject and its underlying concepts. |
| **Originality**<br>PLO(s): | Originality of thought, and/or independence beyond the expectation(s) of the level of study. | Strong and sustained originality of thought and/or evidence of significant independent study. | Strong examples(s) of originality of thought and/or evidence of wide-ranging independent study. | Sound evidence of originality of thought and/or clear evidence of study independent of set/ recommended material. | Limited evidence of originality of thought and/or study independent of set/recommended material. | Very limited originality of thought and/or evidence of study independent of set/recommended material. | No originality of thought and/or evidence of independent study. |
| **Higher cognitive skills**<br>PLO(s): | Critical analysis/ evaluation /synthesis and/ or problem solving skills beyond expectation(s) of the level of study. | Sustained and coherent critical analysis/ evaluation/ synthesis and/or problem solving, demonstrating very high skill(s) relevant to the level of study and beyond. | Evidence of high level critical analysis/ evaluation/ synthesis and/or problem solving skills relevant to the level of study. | Sound critique, synthesis and/or problem solving skills relevant to the level of study. | Limited analysis, evaluation or critique and/or problem-solving relevant to the level of study. | Very limited analysis, evaluation critique and/or problem solving skills, evidenced through work that is mostly descriptive. | Little or no evidence of relevant analysis, evaluation, critique and/or problem-solving. |
| **Use of subject-specific methods/ techniques**<br>PLO(s): | Exceptional demonstration of subject-specific methods/ techniques beyond expectation(s) of the level of study. | Sophisticated demonstration of subject-specific methods/ techniques relevant to the level of study. | Consistently skilled and accurate use of subject-specific methods/ techniques relevant to the level of study. | Skilled use of subject-specific methods/ techniques relevant to the level of study. | Adequate use of subject-specific methods/ techniques relevant to the level of study. | Inadequate use of subject-specific methods/ techniques relevant to the level of study. | Little or no use of subject-specific methods/ techniques relevant to the level of study. |
| **Written and/or oral communication and adherence to academic conventions**<br>PLO(s): | Professional, sophisticated/ innovative communication, with exceptional clarity and/or audience-engagement, and exemplary academic conventions. | Professional communication, that holds the attention of its reader/audience throughout, and demonstrates academic conventions that are accurate and relevant to the level of study/ beyond. | Fluent and coherent communication, which demonstrates consistent and accurate academic conventions. | Mostly fluent and coherent communication; demonstration of appropriate academic conventions, which may include some errors or inconsistencies. | Communication that is difficult to follow at times because of poor clarity/structure; inconsistent demonstration of academic conventions. | Limited clarity and/or structure in communication, and/or inadequate demonstration of academic conventions. | Highly limited clarity and/or structure in written and/or oral communication. Inadequate demonstration of academic conventions. |
| **Practical and/or professional skills**<br>PLO(s): | Exceptional and insightful demonstration/ application of practical and/or professional skills relevant and level of study. | Very high degree of competence and confidence in the demonstration/ application of practical and/or professional skills relevant to the level of study. | High degree of competence and confidence in the demonstration/ application of practical and/or professional skills relevant to the level study. | Competent in the demonstration/ application of practical and/or professional skills relevant to the level, with evidence of developing confidence. | Competent demonstration/ application of practical and/or professional skills relevant to the level of study. | Development required in order to demonstrate competence in practical and/or professional skills relevant to the level of study. | Significant development required in order to demonstrate competence in practical and/or professional skills relevant to the level of study. |
| **Team work**<br>*as a leader or team member*<br>PLO(s): | Exceptional contribution in support of successful team outcome(s), and an insightful and critical appreciation of individual and/ or collaborative performance. | Contribution to teamwork that significantly influenced successful team outcome(s) and a critical appreciation of individual and/or collaborative performance. | Strong and sustained contribution in support of successful team outcome(s) and a comprehensive appreciation of individual | Professional contribution to successful team outcome(s) and a developing appreciation of individual and/or collaborative performance. | Adequate contribution to successful team outcome(s), and an appreciation of individual and/or collaborative performance that may be | Limited contribution to successful team outcome(s), and an appreciation of individual and/or collaborative performance that is inadequately evidenced. | Negligible (or no) contribution to successful team outcome(s). |

| | PASS GRADES | | | | | FAIL GRADES | |
|---|---|---|---|---|---|---|---|
| | (100-85) | (84 - 70) | (69 - 60) | (59 - 50) | (49 - 40) | (39 - 20) | (19 - 0) |
| **SUMMARY DESCRIPTOR:** Learning accredited at **Level 6 (UG)** will reflect the ability to critically review, consolidate and extend a systematic and coherent body of knowledge, utilising specialised skills across an area of study. | | | | | | | |
| | **General Characteristics (UG)** | | | | | | |
| | | | and/or collaborative performance. | | limited or partial and/or overly subjective. | | |

| | PASS GRADES | | | | FAIL GRADES | | |
|---|---|---|---|---|---|---|---|
| | (100-85) | (84 - 70) | (69 - 60) | (59 - 50) | (49 - 40) | (39 - 20) | (19 - 0) |
| **Overarching indicators:** | All learning outcomes/assessment criteria have been achieved to an exceptionally high level, beyond that expected at Level 7, with features consistent with Level 8 (doctoral study). | All learning outcomes/assessment criteria have been achieved to a high standard, and many at an exceptionally high level. | All learning outcomes/assessment criteria have been met fully, at a good or very good standard. | All learning outcomes/assessment criteria have been met. | One or more of the learning outcomes/assessment criteria have not been met. | A significant proportion of the learning outcomes/assessment criteria have not been met. | Most of the learning outcomes/assessment criteria have not been met. |
| SUMMARY DESCRIPTOR: Learning accredited at Level 7 (Master's) will reflect the ability to display mastery of a complex and specialised area of knowledge and skills, employing advanced skills to conduct research or advanced technical/professional activity, accepting accountability for related decision-making, including use of supervision. | | | | | | | |
| **Assessment criteria** | **General characteristics** | | | | | | |
| **Subject knowledge & understanding**<br>PLO(s): Enter "All" or specific PLO(s). | Exceptional subject knowledge and conceptual understanding at the forefront of the discipline. Authoritative approach to complexity. | Comprehensive subject knowledge and conceptual understanding, informed by recent developments in the discipline, demonstrating reading/research at significant depth/breadth. Informed & confident approach to complexity. | Detailed subject knowledge and conceptual understanding demonstrating purposeful reading/research. Developing awareness of complexity. | Broad subject knowledge and conceptual understanding, demonstrating directed reading/research. Some awareness of complexity. | Reproduction of taught content and/or tendency to describe or report facts rather than demonstrate complex ideas. Any errors or misconceptions are outweighed by the overall degree of knowledge & understanding demonstrated. | Insufficient evidence of knowledge and understanding of the subject and its underlying concepts. | Little or no evidence of knowledge and understanding of the subject and its underlying concepts. |
| **Higher cognitive skills & originality**<br>PLO(s): Enter "All" or specific PLO(s). | Rigorous and sustained criticality, independent thinking and original insight; convincing conclusions and/or application to practice. | Strong and sustained criticality and independent thinking/original insight; persuasive conclusions and/or application to practice. | Detailed criticality and evidence of independent thinking/original insight; logical and sustained conclusions and/or application to practice. | General criticality and some evidence of independent thinking; logical conclusions and/or application to practice. | Limited criticality and independent thought, leading to conclusions and/or application to practice that is poorly supported. | Mainly descriptive and/or inadequately supported conclusions and/or application to practice. | Little or no evidence of criticality and independence of thought. |
| **Advanced technical, professional and/or research expertise**<br>PLO(s): Enter "All" or specific PLO(s). | Exceptional demonstration of advanced technical, professional and/or research expertise. Innovative. Work may challenge the existing boundaries of knowledge and/or practice. | Purposeful, systematic and sophisticated demonstration of advanced technical, professional and/or research expertise. | Purposeful, systematic and skilled demonstration of advanced technical, professional and/or research expertise. | Skilled demonstration of advanced technical, professional and/or research expertise. | Developing expertise. Inconsistent demonstration of advanced technical, professional and/or research conduct. | Limited demonstration of advanced technical, professional and/or research conduct. | Little or no demonstration of advanced technical, professional and/or research conduct. |
| **Written and/or oral communication** [e.g. of information, results of research, ideas, concepts and arguments etc] **and adherence to academic conventions**<br>PLO(s): Enter "All" or specific PLO(s). | Professional, sophisticated/innovative communication, with exceptional clarity and/or audience-engagement, and exemplary academic conventions. | Professional and fluent communication, that holds the attention of its reader/audience throughout and which demonstrates academic conventions that are accurate and relevant to the level of study/beyond. | Fluent and coherent communication, which demonstrates consistent and accurate academic conventions. | Mostly fluent and coherent communication; demonstration of appropriate academic conventions, which may include some errors or inconsistencies. | Communication that is difficult to follow at times because of poor clarity/structure; inconsistent demonstration of academic conventions. | Limited clarity and/or structure in communication, and/or inadequate demonstration of academic conventions. | Highly limited clarity and/or structure in written and/or oral communication. Inadequate demonstration of academic conventions. |