The University of Sydney
School of Computer Science
Dr Suranga Seneviratne
Senior Lecturer - Security

THE UNIVERSITY OF SYDNEY

INFO3616/CSEC3616/CSEC5616 — S2 2025
Assignment - 3

This is an **individual** assignment.

This assignment worths 10% of the final marks of the course and covers the content of Weeks 7-10 (inclusive).

Submit your final report as a `PDF` and the certificate in Q1 as a `zip` file in Canvas. In Canvas, under Assignment 3, you will find two links to submit your report and the certificate separately.

Please read the below instructions carefully.

***** IMPORTANT *****

1) **Note the answer release date:** Please note the answer release date mentioned below. Any submission after that will get zero marks, instead of a late penalty.

2) **Typeset reports only:** We accept only typeset answers. Any hand written answers will get zero marks. This is because we can't do plagiarism checks for hand written answers.

3) **DO NOT repeat questions:** In your answer sheet DO NOT repeat the questions. Simply include the question number and your answer only. If you include question text in your answer sheet, your TurnItIn score will be high and there will be additional checks. This will cause a delay in releasing your marks. **We will also impose a penalty of 10% of the total marks.**

***** SUBMISSION *****

Final Report and Artefacts: Due by Sunday the 26th of October, 2025 11:59 PM

Simple Extensions: For this assignment, you can apply for simple extensions following the university process. If your request is **approved**, the revised deadline will be **31st of October, 2025 11:59 PM**. Please note that you have do it yourself and no need to contact the unit of study co-ordinator for this. We will get an automatic email from the system if your request was approved. Also note that, this system is not connected with Canvas, therefore it is normal for you the see the old deadline in Canvas, even if your simple extension was approved.

****Simple Extensions Update 06/10/2025**** - Please refer to the Week 5 announcements on Ed for updated information regarding simple extensions (i.e., the same arrangement as Assignment 1 and Assignment 2).

Answer release: The answers to this assignment will be automatically released on the **3rd of November 00:00 AM**. Any submissions after that will get **zero marks**. If you have a legitimate reason that requires an extension beyond that you will need to go through the university special considerations process. If approved, what you will be grant is a mark adjustment not an extension.

1 Public Key Infrastructure and Transport Layer Security (25 marks)

a) Inspect a Certificate Chain (6 marks)

Inspect the given full-cert-chain.pem containing a chain of certificates using a tool such as openssl and complete the blanks in Figure 1. There are multiple ways to do this, you are free to use any method. Explain the method you used in your answer.

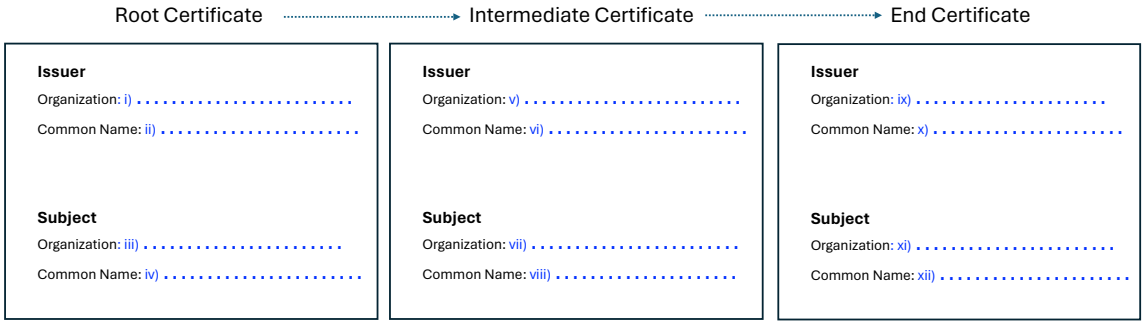

Figure 1: Certificate Chain

b) Study the given trace file `1.pcapng` and answer the following questions

You are given two `Wireshark` (https://www.wireshark.org/) traces taken while the homepage of The University of Sydney. The two traces are in `pcapng` (https://pcapng.com/) format. Your task is to install `Wireshark` software in you computer, inspect the traces, and answer the following questions.

i What are the source and destination IP addresses of the given communication? **(1 marks)**

ii Which one of these is a private IP address? Explain why a private IP address is used in this setting. **(1 marks)**

iii Explain the functionality of the first three packets of the trace file. **(1 marks)**

iv Draw and annotate a protocol diagram using the first six **TLS packets** of the trace (An example protocol diagram can be found in Slide 55 of Week 8 lecture slides). **(3 marks)**

v In one of the TLS packets from the server to client, you will see that there is messge called, `New Session Ticket`. Explain the purpose of that. **(1 marks)**

vi What is the agreed cipher suite between the client and the server. **(1 mark)**

vii Explain what cryptographic scheme/methods are used in the selected cipher stream for; *Key Exchange, Authentication, Encryption, Message Authentication.* **(2 marks)**

viii What are the last four bytes of the server's Diffie-Hellman public key. **(1 mark)**

c) A different trace

Study the given trace file `2.pcapng`. You will notice that the TLS protocol flow is different here. Explain why some TLS messages such as Server Certificate are not visible in plaintext format in this trace **(2 marks)**.

d) Build your own certificate chain

Make a three-level certificate chain of your own using `openssl`. For the Common Names (CN) use your Student ID and suffixes "Root", "Intermediate" and "End". You can use any value for the rest of the parameters. Collate the three certificates of one `pem` file and submit in the artefacts link (This is the second link in Canvas for Assignment 3). Include and explain the sequence of `openSSL` commands you used in the report. **(6 marks)**.

2 Marks & Spencer (M & S)-UK Data Breach (25 marks)

Read about the Marks & Spencer (M & S)-UK Data Breach that happened in April, 2025 and answer the following questions. There have been many new reports and expert commentary on this - you should be able to find many resources online.

Here are some links that will help you to get started.

- Marks & Spencer Breach: How a Ransomware Attack Crippled a UK Retail Giant
- M & S cyberattackers used a little-known but dangerous technique – and anyone could be vulnerable
- Clothing shortages, food waste and millions lost each day: inside the M & S cyber-attack chaos
- Threat Actor Analysis: Scattered Spider and the Marks & Spencer Cyber Incident

Answer the following questions. The indicative answer length is provided as a guide to show the level of detail expected. It is not a strict rule.

i. Briefly explain what happened. What was the impact and what data was breached? Explain the impact in terms of operational, financial, and reputational. *(Indicative answer length: 150-300 words).* **(5 marks)**

ii. How did the attackers obtain unauthorised access? Include how the initial entry was made and subsequent actions by the attackers. *(Indicative answer length: 100-150 words)* **(5 marks)**

iii. How did Marks & Spencer (M & S) respond when they came to know about the breach? This answer should cover not only technical aspects but also legal, customer relations, and public relations aspects. *(Indicative answer length: 150-250 words)* **(5 marks)**

iv. Explain two possible risks (i.e., to the impacted customers of M & S) associated with this data breach? *(Indicative answer length: 50-100 words)* **(5 marks)**

v. As of now it is unclear whether How did Marks & Spencer (M & S) has made the ransom payment or not. Discuss the pros and cons of paying the data ransom demanded by attackers in the context of the How did Marks & Spencer (M & S) data breach. Consider the legality of paying a ransom, the potential consequences for businesses and customers, and provide your opinion on whether paying the ransom is a viable option. *(Indicative answer length: 300-400 words)* **(5 marks)**

3 Conduct a Buffer Overflow Attack (25 marks)

In your Azure virtual machine, under `/home/tutorials/Assignment_3/` you will find a compiled C executable names `securevault`. The program contains three secrets. Conduct a series of buffer

overflow attacks using `gdb` and recover the secrets. Explain your process and payloads in the report. The markers must be able to copy paste your commands and verify whether your attack works. As this is a compiled program you can only run this on your Azure VM.

4 Firewalls (25 marks)

We will configure firewalls in this task. Figure 4 shows a possible firewall setup. Your goals are:

- For all hosts in the network, outgoing traffic is only allowed to TCP ports 80 (HTTP), 443 (HTTPS), and 25 (SMTP); plus UDP ports 53 (DNS).
- Incoming traffic is always allowed if there is an established connection, i.e. if the connection has been established from a host in the local network.
- Host 129.78.1.1 is reachable (incoming connection) from everywhere on port 80 and port 443.
- Host 129.78.1.2 is reachable (incoming connection) on port 22 (SSH) from 129.78.1.90
- In addition to the first rule, host 129.78.1.100 is allowed make outgoing connections to 172.217.167.110 using HTTP/3. (Read about HTTP/3 here and decide what port and protocol to use.)
- No other incoming traffic is allowed.

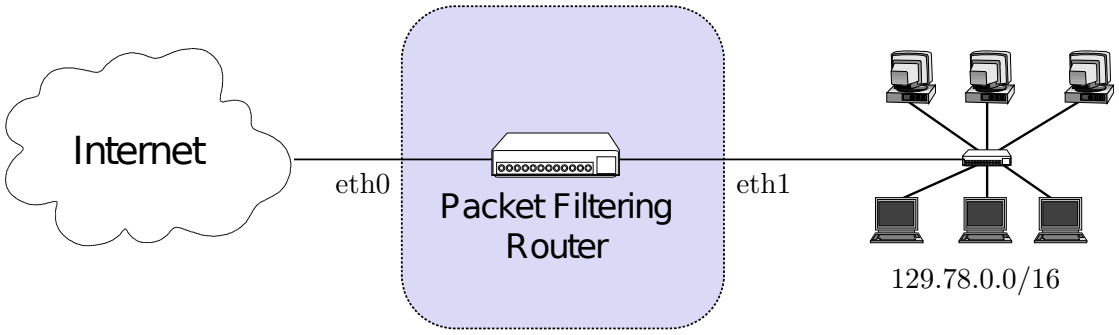

Figure 2: Firewall setup.

a) Configuring a stateful firewall (12 marks)

Write stateful rules in table form as shown in the lecture. A template is given in Table 1. You are free to add more rows to the table, if required.

However, do not add too many unnecessary rules. Implement the policies using as less rules as possible.

b) Converting to stateless filtering (13 marks)

Convert your rules to stateless filtering rules. A template is given in Table 3. Again you are free to add more rows to the table, if required.

However, do not add too many unnecessary rules. Implement the policies using as less rules as possible.

Rule	Incoming Interface	Src IP	Dst IP	Proto	Src Port	Dst Port	State	Action
A								
B								
C								
D								
E								
F								
G								

Table 1: Template for stateful filtering.

Rule	Iface	Src IP	Dst IP	Proto	Src Port	Dst Port	ACK	Action
A								
B								
C								
D								
E								
F								
G								

Table 2: Template for stateless filtering.