THE UNIVERSITY OF NEW SOUTH WALES, CANBERRA

AUSTRALIAN DEFENCE FORCE ACADEMY

2022 SEMESTER 1 – Examination

Course Code:	ZEIT2104
Course Name:	Computers and Security
Paper No.:	Final Exam
Time Allowed:	3 Hours
No of Questions on Paper:	5 Questions. 1 Question per page, but questions can be answered in any order. • **Question 1** – 14 Marks • **Question 2** – 20 Marks • **Question 3** – 22 Marks • **Question 4** – 18 Marks • **Question 5** – 26 Marks
No of Questions to be Answered:	5 of 5 Questions
Maximum total marks for exam:	100

Answers must be typed directly into Moodle. This is an Open Book exam. Candidates may bring any materials into the room.

By undertaking this Final Exam I declare that:

- This assessment item is entirely my own original work, other than where explicitly acknowledged to be otherwise.
- This assessment item, or part thereof, has not been published anywhere or provided to any other person other than to the assessor of this assessment for the purposes outlined in the assessment rules.
- The preparation of this work has been completed in accordance with the UNSW Student Code of Conduct, and is a true representation of my current capabilities in this course.

I understand that:

- The assessor of this assessment item may, for the purpose of assessing this item, reproduce this assessment item and provide a copy to another member of the University.
- The assessor may communicate a copy of this assessment item to a plagiarism checking service (which may then retain a copy of the assessment item on its database for the purpose of future plagiarism checking).

Question 1 (14 Marks in total)

This question is about "Incident report on the breach of the Australian National University's administrative systems" (https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf).

a) Several times, the incident report discusses the role of ANU's firewalls. Explain if these are network-based or host-based firewalls. **(2 Marks)**

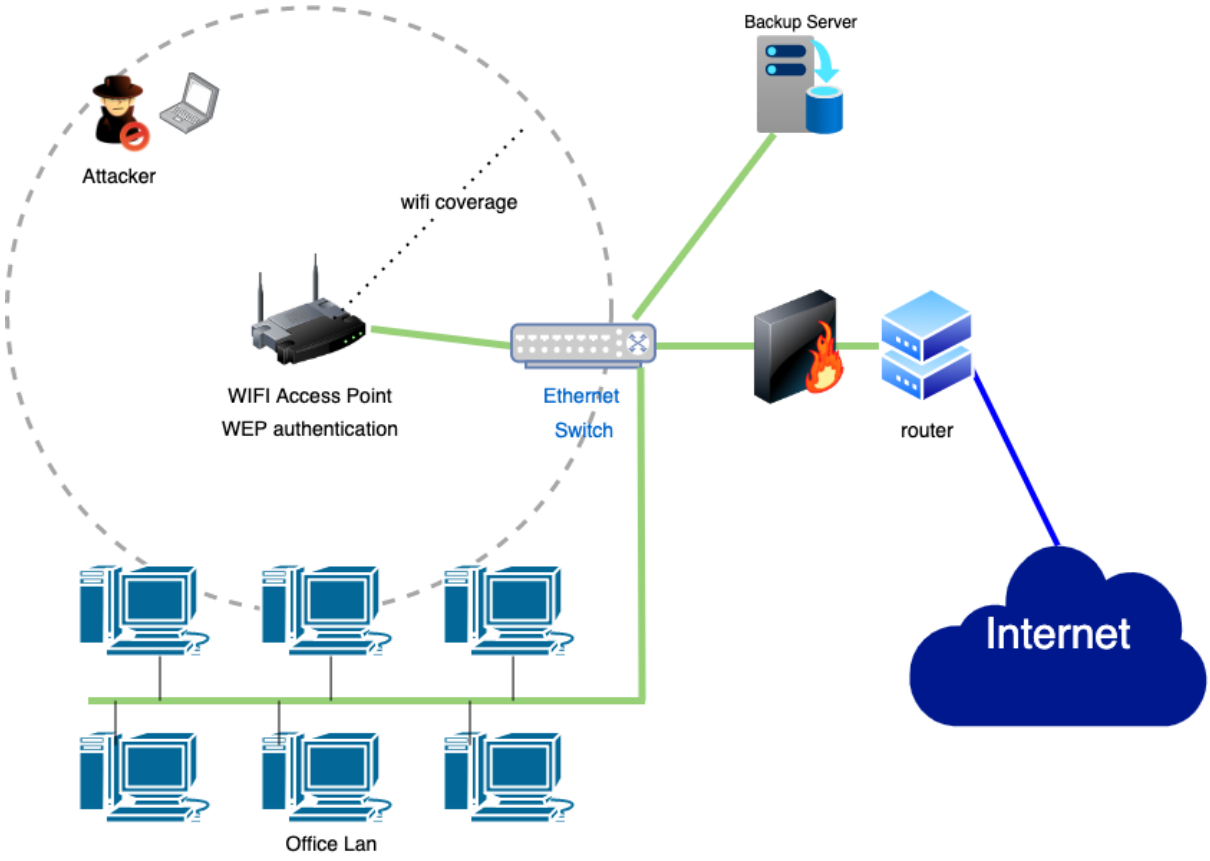
b) On p4, the report describes the events on 12-14 November 2018 as follows: "It is probable that the actor used credentials gained on 9 November to successfully access an Internet-facing webserver used by one of the University's schools. The actor successfully created a webshell on this webserver which was then used, over two days, to conduct command and control (C2) operations through what is known as a TOR exit node. These activities were likely designed to set up infrastructure and tools to be used throughout the actor's campaign." Explain which of these activities are covered by which phase(s) of the Lockheed-Martin Cyber Kill Chain. **(5 Marks)**

c) Apparently (also on p4), "the actor sent out four spearphishing emails, to ANU users, to try and gain … hashes", where the report defines hashes as "a one-way mathematically altered version of a password designed to ensure the confidentiality of credentials." Explain why gaining hashes could be an interesting objective for the malicious actor, despite the related passwords being mathematically altered one-way. **(4 Marks)**

d) On p11 it says that "the actor was able to, in several cases, avoid detection by altering the signatures of more common malware used during the campaign." Does this mean that the actor created zero-day attacks? Justify your answer **(3 Marks)**

Question 2 (20 Marks in total)

Consider the example small-company network as shown below. The network includes a small LAN, a backup server, a switch, a router, a firewall, and a WiFi access point to provide connectivity to the employees' mobile devices. The WiFi coverage is shown by the dashed circle. An Attacker is located not far from the company network, and aims to get unauthorised access to the Backup Server.



a) Briefly describe the technical reconnaissance steps the attacker is likely to take before they can achieve their aim and name a tool for each of these steps. **(4 Marks)**

b) Describe the most likely attack vector that will give the attacker initial access to the company network. **(3 Marks)**

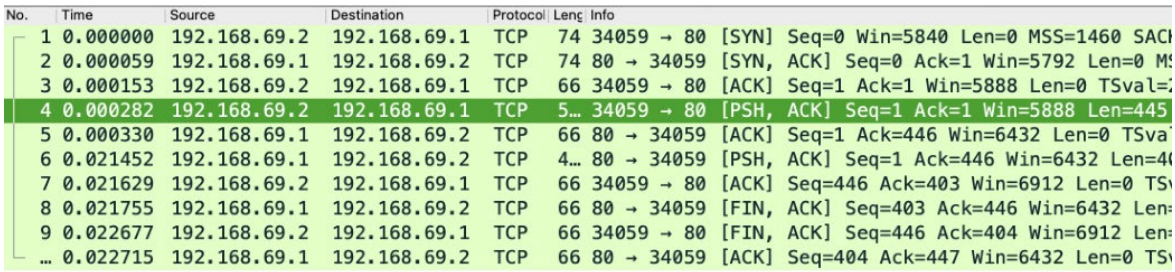
c) Briefly list and describe tools which the attacker is likely to use for exploitation. **(4 Marks)**

d) Describe a way in which the attacker can gain persistence in the network after having achieved initial access. **(3 Marks)**

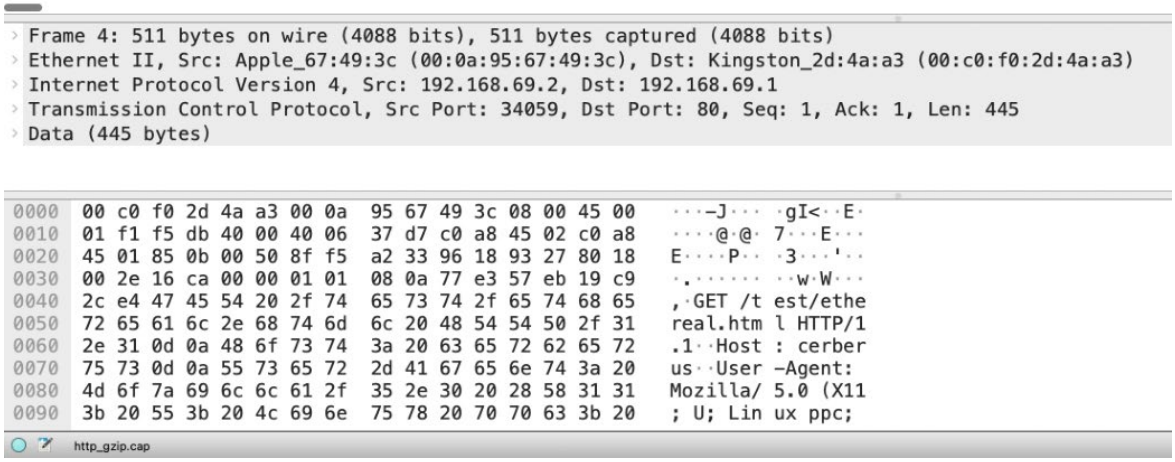
e) List and describe two preventive network controls and one detective network controls that would significantly improve the security of this network. **(6 Marks)**

Question 3 (22 Marks in total):

The figure below shows a screenshot of Wireshark after capturing a TCP session. Use this figure to answer the following questions.



No.	Time	Source	Destination	Protocol	Leng	Info
1	0.000000	192.168.69.2	192.168.69.1	TCP	74	34059 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK
2	0.000059	192.168.69.1	192.168.69.2	TCP	74	80 → 34059 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MS
3	0.000153	192.168.69.2	192.168.69.1	TCP	66	34059 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=2
4	0.000282	192.168.69.2	192.168.69.1	TCP	5…	34059 → 80 [PSH, ACK] Seq=1 Ack=1 Win=5888 Len=445
5	0.000330	192.168.69.1	192.168.69.2	TCP	66	80 → 34059 [ACK] Seq=1 Ack=446 Win=6432 Len=0 TSva
6	0.021452	192.168.69.1	192.168.69.2	TCP	4…	80 → 34059 [PSH, ACK] Seq=1 Ack=446 Win=6432 Len=4
7	0.021629	192.168.69.2	192.168.69.1	TCP	66	34059 → 80 [ACK] Seq=446 Ack=403 Win=6912 Len=0 TSv
8	0.021755	192.168.69.1	192.168.69.2	TCP	66	80 → 34059 [FIN, ACK] Seq=403 Ack=446 Win=6432 Len=
9	0.022677	192.168.69.2	192.168.69.1	TCP	66	34059 → 80 [FIN, ACK] Seq=446 Ack=404 Win=6912 Len=
…	0.022715	192.168.69.1	192.168.69.2	TCP	66	80 → 34059 [ACK] Seq=404 Ack=447 Win=6432 Len=0 TSv



```
› Frame 4: 511 bytes on wire (4088 bits), 511 bytes captured (4088 bits)
› Ethernet II, Src: Apple_67:49:3c (00:0a:95:67:49:3c), Dst: Kingston_2d:4a:a3 (00:c0:f0:2d:4a:a3)
› Internet Protocol Version 4, Src: 192.168.69.2, Dst: 192.168.69.1
› Transmission Control Protocol, Src Port: 34059, Dst Port: 80, Seq: 1, Ack: 1, Len: 445
› Data (445 bytes)
```

```
0000  00 c0 f0 2d 4a a3 00 0a  95 67 49 3c 08 00 45 00   ···-J··· ·gI<··E·
0010  01 f1 f5 db 40 00 40 06  37 d7 c0 a8 45 02 c0 a8   ····@·@· 7···E···
0020  45 01 85 0b 00 50 8f f5  a2 33 96 18 93 27 80 18   E····P·· ·3···'··
0030  00 2e 16 ca 00 00 01 01  08 0a 77 e3 57 eb 19 c9   ·.······ ··w·W···
0040  2c e4 47 45 54 20 2f 74  65 73 74 2f 65 74 68 65   ,·GET /t est/ethe
0050  72 65 61 6c 2e 68 74 6d  6c 20 48 54 54 50 2f 31   real.htm l HTTP/1
0060  2e 31 0d 0a 48 6f 73 74  3a 20 63 65 72 62 65 72   .1··Host : cerber
0070  75 73 0d 0a 55 73 65 72  2d 41 67 65 6e 74 3a 20   us··User -Agent:
0080  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28 58 31 31   Mozilla/ 5.0 (X11
0090  3b 20 55 3b 20 4c 69 6e  75 78 20 70 70 63 3b 20   ; U; Lin ux ppc;
```

http_gzip.cap

a) What are the IP addresses and port numbers of the TCP client and server? **(2 Marks)**

b) What are the packet numbers (to be found in the left-hand column of the top half of the figure) of the packets that established the TCP connection? Justify your answer. How is this step called? **(3 Marks)**

c) What are the packet numbers of the packets that closed the TCP connection? Justify your answer. **(2 Marks)**

d) What is the application layer protocol that is carried over this TCP session? Provide two reasons that justify your answer. **(3 Marks)**

e) What is the user service that is supported by this session? Justify your answer. **(2 Marks)**

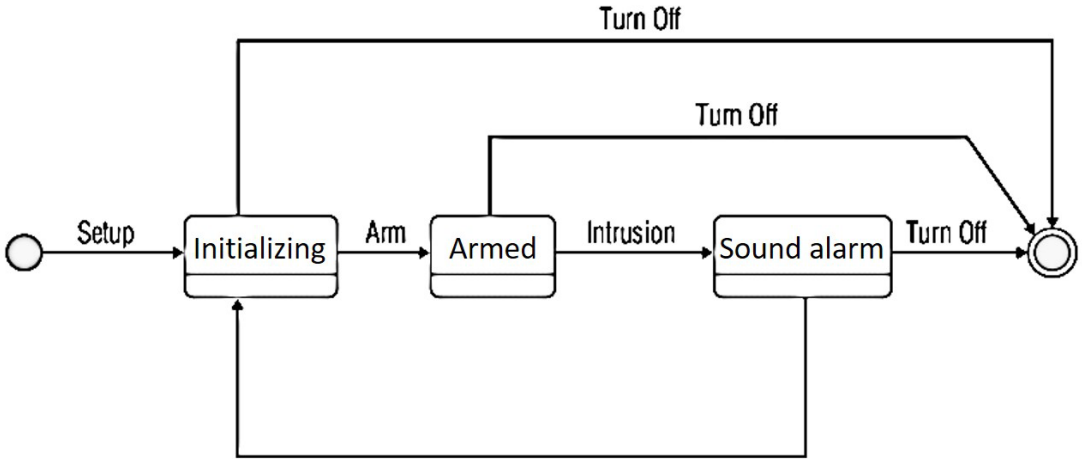
f) What are the Data Link and Network Layer protocols used in this session? **(2 Marks)**

g) Unfortunately, an adversary has been able to capture these packets. Explain what measures the client and host have taken to protect the confidentiality of the data communicated. **(2 Marks)**

h) What information about the network, the connected devices, and the software running on the client and the server can the adversary obtain from this capture as part of their reconnaissance activity? **(6 Marks)**

Question 4 (18 Marks in total):

Consider the state diagram for a simple burglar alarm as shown below. The alarm has 4 authorized states: “Initializing”, “Armed”, “Sound Alarm”, and “Off”, and authorized state transitions as shown in the diagram.



The alarm has three authorized users: the owner, the other family member in the house, and the home security company. The alarm is connected to Internet, by which all authorized users can gain remote access to the system, e.g. via a phone app to the remote management interface. Only the owner is permitted to switch the alarm off using the remote management interface. If anybody else tries to switch the alarm off via the remote management interface, this would be detected as an intrusion (other family members can switch the alarm off by means of physically typing a pin-code on the device itself).

a) A burglar has asked a hacker for help. The hacker manages to gain remote access to the system, but only as an “other family member” and without possibilities to escalate privileges. Turning the alarm off is therefore not an option. However, the hacker found a very useful hidden state transition (i.e. not shown in the diagram) they could trigger. Which state transition would that be? **(2 Marks)**

b) The hacker is not actually a family member. To which group of threat actors does this hacker most likely belong? Would this be different if the hacker would have been a real other family member? Justify your answer. **(4 Marks)**

c) Access control to the system is governed by the Bell-LaPadula information flow model. The highest security level is for the home security company. They can read the remote management interfaces of all burglar alarms in town. The middle security level is for the owner. The owner can read and write the remote management interface of the burglar alarm they own. The lowest security level is for the other family member. They can read the remote management interface but cannot write.

   i) Discuss if the ability of the other family member to read the remote management interfaces is a violation of the “no read up” rule. **(3 Marks)**

ii) Discuss if the ability of the owner to write the remote management interface is a violation of the *-property. **(3 Marks)**
iii) Discuss the advantages and disadvantages of applying the Bell-LaPadula model to this system with these particular users. **(6 Marks)**

Question 5 (26 Marks in total)

Bob is a field officer of an intelligence unit that gathers information close to the front. Bob and the base officer Alice have decided to communicate using satellite connectivity. Bob has a small laptop with limited power and computing resources that can be connected to the satellite network and send real-time information (including messages, photos and video) to Alice, and receive orders. The software of this laptop supports AES, RSA, and SHA-256.

a) Information exchange between Bob and Alice needs to be confidential. Which algorithms supported by the laptop could be used for that? Justify your answer. **(4 Marks)**

b) Bob needs to be sure that messages from Alice are not modified on the fly. Given the algorithms supported by the laptop, describe how Alice can protect the integrity of messages to Bob. **(4 Marks)**

c) How Bob also has to be sure that the message is from Alice. Given the algorithms supported by the laptop, describe how Bob can authenticate the sender of the message, that is Alice. **(4 Marks)**

d) After the first day, Bob and Alice found that encrypting the video requires too much resources from the laptop. Therefore, Alice asks Bob to just protect the video messages' integrity. Given the algorithms supported by the laptop, describe how Bob can protect the video messages' integrity **(2 Marks)**.

e) Describe how the communication can be protected against man-in-the-middle attacks. You may have to make reasonable assumptions regarding further capabilities of the laptop and/or network. **(6 Marks)**

f) The intelligence unit is in fact an international collaboration between different AUKUS partners. Alice is from the US and Bob is from Australia. One is using AES according to FIPS 197 and the other is using AES according to ISO/IEC 18033-3:2010.
   i. Who is most likely the one that uses AES according to FIPS 197? Justify your answer. **(2 Marks)**
   ii. Do you expect this difference in implementations to be an issue? Justify your answer. **(4 Marks)**

END OF EXAM