

School of

# Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

## CYBR 171 T1 2023

Ngā whakapūtanga o Te Haumaruru rorohiko  
Cybersecurity Fundamentals

---

**Week 12 – Recap, Test revision, and Q/As**

# What are we going to cover?

---

- Coverage – examined on weeks 7-12 content, not only what is listed on today's slides!
- Format & information
- Preparation tips



# FORMAT & INFORMATION

---



# Format

---

- TWO hour
- Section A THIRTY multi-choice questions (1 mark each). /30
- Section B has TEN multi-choice questions (2 marks each) /20
- Section C has FIVE written short answer questions (5 marks each) /25

# Information

---

- **When is the test?**
  - Friday 9 June (both in-person and distance students)
  - In-person: 9:30-11:30 am New Zealand Time
  - Distance students: 9:30-11:30 “***New Zealand Time***”
- **Where?**
- The test will be in different rooms based on the surname
- MCLT102: A – Chi
- KKLT303: Cho – Kau
- MCLT101: Kav – Ph
- MCLT103: Pi – Z
- Distance students: ZOOM

# Distance Students

---

- If you do **NOT** see your ID below, then you are assumed to do the test “**in-person**”

300379210		
300635306		

# In-person students

---

***BRING YOUR STUDENT ID (or an alternative photo ID, e.g., passport or driver licence, if the student ID is not available)***

# Student name and ID

---

Joe Bloggs

3	0	0	1	3	9	6	4	2
●	●	●	●	●	●	●	●	●
(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)
(2)	(2)	(2)	(2)	(2)	(2)	(2)	(2)	(2)
(3)	(3)	(3)	(3)	(3)	(3)	(3)	(3)	(3)
(4)	(4)	(4)	(4)	(4)	(4)	(4)	(4)	(4)
(5)	(5)	(5)	(5)	(5)	(5)	(5)	(5)	(5)
(6)	(6)	(6)	(6)	(6)	(6)	(6)	(6)	(6)
(7)	(7)	(7)	(7)	(7)	(7)	(7)	(7)	(7)
(8)	(8)	(8)	(8)	(8)	(8)	(8)	(8)	(8)
(9)	(9)	(9)	(9)	(9)	(9)	(9)	(9)	(9)
(0)	(0)	(0)	(0)	(0)	(0)	(0)	(0)	(0)





# COVERAGE

---



Week 7

# **WEB SECURITY**

# Web security

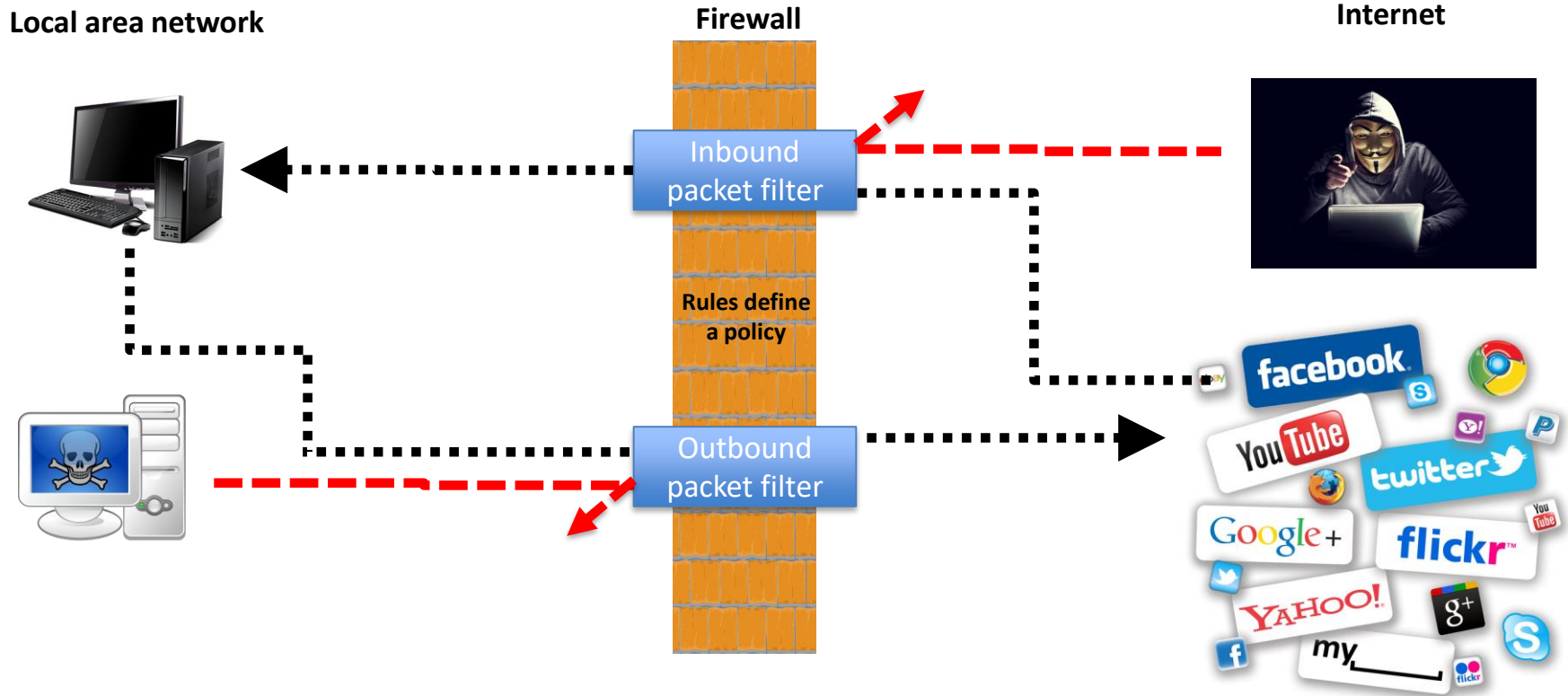
---

- Structure of a typical web application
- Universal Resource Identifier – URI
- HTTP verbs – GET and POST
- Steal the cookie
- SQL injection
- Path traversal
- Cookies and their security (XSS and CSRF)
  - Secure flag
  - Lab 4

Week 8


# **NETWORK SECURITY DEFENCES**

# How a firewall works




# Configurations (policies)

- Example: Specific machine



Direction	Source IP	Source Port	Destination IP	Destination Port	Action
Inbound	W.X.Y.Z	*	*	*	allow
Outbound	*	*	W.X.Y.Z	>1023	allow
*	*	*	*	*	block

- Example: Specific service



Direction	Source IP	Source Port	Destination IP	Destination Port	Action
Outbound	*	*	*	80	allow
Outbound	*	*	*	443	allow
Inbound	*	*	*	> 1023	allow
*	*	*	*	*	block

# Firewalls and others

---

- Firewalls
- Virtual Private Networks and how to secure the tunnels
- Onion routing (TOR)

# IDS/IPS and Honeypots

---

- Types of IDS
  - Network-based IDS vs Host-based IDS
  - Passive vs reactive
- Detection techniques
  - Anomaly detection
  - Misuse detection
- Honeypots
  - What are they?
  - What for?

History of IDS





Week 9

# **SOCIAL ENGINEERING**

# Social engineering

---

- Examples of social engineering attacks (non-exhaustive).
  - Phishing, whaling, tailgating, pretexting, spamming, quid pro quo, Spanish prisoner ...
- why do they work?
- what we know from experimental evidence
  - Solomon Asch
  - Stanley Milgram
  - Philip Zimbardo

Week 10

# **PROTECTION MODEL & PHYSICAL SECURITY**

# Protection Model

---

- Protection model and the principle of defence in depth
  - Deter
  - Detect
  - Alarm
  - Delay
  - Respond

# Physical protection

---

- Safety vs security
- Physical Protection System **Integration Objectives**
- Physical Security Vulnerabilities
  - Methods of breaking into a building and countermeasures
- Remarks

Week 11

# **INCIDENT RESPONSE ETHICAL AND LEGAL**

# Ethical aspects

---

- The differences between Ethics and law
- Types of computer crimes
- Types of property and intellectual property
- Privacy
- Ethical Issues
- Codes of ethics vs The Rules

# Incident response process

---





# Incident response and forensics

---

- Incident response **process**
  - Preparation
  - Detection
  - Analysis
  - Containment
  - Eradication and Recovery
  - Post incident activity
- Incident response Team
  - Who does what in incident response scenarios
- Plans and processes (**Playbooks**)

Week 12

# **DIGITAL FORENSICS**

# Digital forensics

---

- Types of evidence and admissibility
- Digital forensics process
  - Identification
  - Preservation
  - Collection
  - Examination
  - Presentation
- Chain of custody

Digital Forensics  
Lab and Tools





# PREPARATION TIPS

---



# Tips

---

- Review 2018 and 2019 exams
- Office hours for next week
  - **Harith**: Tuesday 6 June 11am – 12pm
    - **CO129** and
    - **Zoom**: <https://vuw.zoom.us/my/alsahaf>)
  - **Lisa**: Wednesday 7 June 1pm – 2pm
    - **CO127**