VICTORIA UNIVERSITY OF
WELLINGTON
TE HERENGA WAKA

CYBR 371: SYSTEM & NETWORK SECURITY
2024/T1 – Dr Arman Khouzani, Dr Mohammad Nekooee

- - - - - - - - - - - - - - - -

Midterm Test (20%) — April 17, 2024
Duration: 40 Minutes

- - - - - - - - - - - - - - - -

FULL NAME: ....

STUDENT ID: ....

Question:	1	2	Total
Points:	10	10	20
Score:			

Leave this table blank!

- Do not start (do not turn over this page) until instructed to do so.

- Write down your student name and ID in the designated space above.

- Have your student ID card available in front of you. You may be checked during and/or at the end of the test.

- This is a closed-book, closed-resources test.

- Calculators or any other electronics are NOT permitted.

- Your phone should be turned off and stowed away during the test.

- You must hand over your manuscript at the end of the test.

- You can leave as soon as you finish. Just raise your hand and we will come to you to check your ID and collect your manuscript. Be courteous to others still taking the test, so please exit as quietly as possible.

- Plagiarism will not be tolerated: do not risk its major consequences. If you consult any material or individual other than the instructors or invigilators during the test, that will constitute as plagiarism.

1. **Multiple Choice Questions**. Circle the correct answer. There is no penalty for a wrong answer, however, only one choice per each question should be marked.

   (a) Caching authorisation tokens for too long is (most clearly) a violation of which security principle?
      - A. Fail-safe Defaults
      - B. Complete Mediation
      - C. Economy of Mechanism
      - D. Least Common Mechanism
      - E. Segregation (separation) of Duties.

   (b) In a small software company, the development team is responsible for the entire life-cycle of an application, including writing code, testing it, and deploying it to production servers. This streamlined approach is adopted to speed up the release process. This is (most directly) a violation of which security principle?
      - A. Fail-safe Defaults
      - B. Complete Mediation
      - C. Economy of Mechanism
      - D. Least Common Mechanism
      - E. Segregation (separation) of Duties

   (c) Which one of the following is NOT an example of multi-factor authentication?
      - A. Using a PIN number with your debit card to withdraw money from an ATM.
      - B. Receiving a verification code on your phone that you use along with your password to log in.
      - C. Employing a retina scan along with a security token to authenticate.
      - D. Using voice recognition and an implanted chip in your hand to enter a building.
      - E. Using a security question and a password to log into an online account.

   (d) Which one of the following statements is correct?
      - A. 2-factor authentication is more secure than single-factor authentication because it results in "mutual authentication".
      - B. An authentication method that has no type-I error rate at all but has 10% type-II error rate is more dangerous than an authentication method that has 10% type-I error rate but no type-II errors.
      - C. Different users that are successfully authenticated can be thought of as having the same level of authorisation.
      - D. Using your student ID card to tap and unlock a door on campus is an example of multi-factor authentication.
      - E. Once a user successfully authenticates, they can be given access to the authentication logs.

   (e) Ping-of-Death is an example of which of the following attacks?
      - A. Cache poisoning

B. Sniffing

C. Spoofing

D. DoS

E. MitM

(f) Which one of the following Oracle statements best demonstrates the usage of discretionary access control (DAC)?

    A. `GRANT SELECT ON grades TO PUBLIC;`

    B. `CREATE ROLE lecturer; GRANT UPDATE ON grades TO lecturer;`

    C. `GRANT ALL PRIVILEGES ON grades TO bob;`

    D. `GRANT lecturer TO alice;`

    E. `GRANT INSERT ON grades TO alice WITH GRANT OPTION;`

(g) The executable file of each of the following Linux programs is owned by '**root**'. Which one of them must NOT be a set-uid programme?

    A. `chgrp` (used to change the group ownership of a file)

    B. `newgrp` (used to log in to a new group, i.e., to change your real group to another group that you are a member of)

    C. `mount` (used to mount to a filesystem, e.g., attaching a USB)

    D. `sudo` (used to run programs with elevated privileges)

    E. `chsh` (allows a user to change their own preferred login shell)

(h) Suppose the output of **`ls -l /opt/CYBR371`** is the following:

```
drwxrwxr-x  2  alice  staff  4096  Apr 17 15:00   CYBR371
```

So `CYBR371` is a directory owned by user `alice` and group `staff`, with permissions set to `rwxrwxr-x`. Also, the output of the command **`id bob`** is:

```
uid=1002(bob) gid=1003(tutors) groups=1003(tutors),1004(staff),
1005(gamers)
```

and the output of the command **`umask`** is:

```
0022
```

No extended ACL is used. Suppose now the user `bob` logs in and enters the following commands in the terminal:

```
cd /opt/CYBR371
touch README.md
```

Which one of the following statements is correct?

    A. `bob` **cannot create any files inside the** `CYBR371` **directory, so the second command will fail with a "permission denied" message.**

    B. `README.md` **file is created as follows:**

```
-rw-r--r--  1  bob  staff  0  Apr 17 15:05   README.md
```

C. `README.md` file is created as follows:

```
-rw-r--r--   1  bob   tutors   0   Apr 17 15:05    README.md
```

D. `README.md` file is created as follows:

```
-rwxr-xr-x   1  bob   staff   0   Apr 17 15:05    README.md
```

E. `README.md` file is created as follows:

```
-rwxr-xr-x   1  bob   tutors   0   Apr 17 15:05    README.md
```

(i) Which one of the following is <u>NOT</u> a valid defence against ARP spoofing attacks?
   A. Using a hub instead of a switch (bridge).
   B. Enabling static ARP entries for critical systems.
   C. Deploying a network intrusion detection system (NIDS).
   D. Implementing port security on network switches.
   E. Employing a tool that keeps track of IP to MAC address pairings like **Arpwatch** or **Xarp**.

(j) How do SYN cookies work to mitigate SYN flood attacks?
   A. They encrypt the SYN packets, making them unreadable to attackers.
   B. They block all SYN packets from unknown sources.
   C. They encode the initial sequence number of a TCP connection to avoid allocating server resources for each connection attempt.
   D. They send a cookie to the client's browser to verify if it is a legitimate user.
   E. They work by limiting the rate that the attacker can send SYN packets.

2. **Short Answer Questions**.
   (a) Give a real-life example of using the "Defence in Depth" security principle. That is, provide a practical example that demonstrates compliance with the "Defence in Depth" security principle.

(b) Security controls (countermeasures) can be classified in one of the following categories based on their primary operational mechanism:

A: Detection

B: Prevention

C: Recovery

For each of the following security controls, determine which one of the above (A, B, or C) is the primary operational mechanism. (Only choose <u>one</u> option, the most relevant one. No explanation is necessary.)

   i. Firewalls _____

  ii. Access Control _____

 iii. Honeypots _____

 iv. Installing security patches as soon as they are released _____

(c) Suppose *Alice* (as the lecturer) is at security clearance level of "confidential" (level 1). *Bob* (as a student) has no security clearance (level 0). There are (only) two documents in the system: **questions.pdf**, which is not sensitive (security level 0), and **solutions.pdf**, which is labelled "confidential" (security level 1). Now, suppose the access control matrix is as the following:

	questions.pdf	**solutions.pdf**
Alice	**rw**	**rw**
Bob	**r**	**–**

Determine whether this system is compliant with the Bell-LaPadula model, Biba model, both, or neither. Briefly support your answer.

(d) Provide an explicit example of an access control scenario that can be implemented in Attribute-Based Access Control (ABAC) but not in Role-Based Access Control (RBAC).

(e) The attacker in the following figure wants to launch a UDP Ping Pong Attack.

1.2.3.4   5.6.7.8

Spoofed Packet

attacker
9.10.11.12
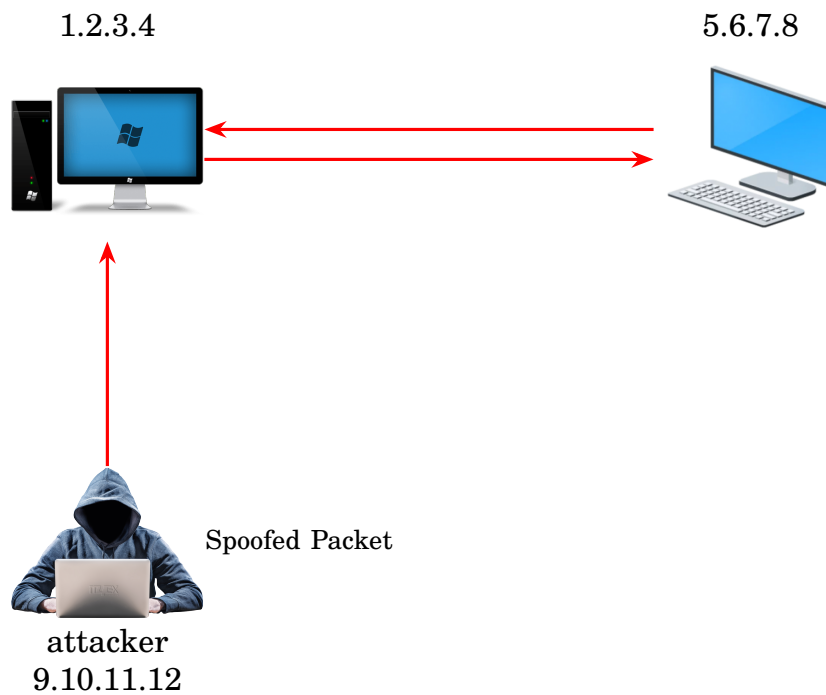
As a reminder, UDP port 7 is for the "Echo" service, which responds by sending an identical copy of the data back to the sender. Also, UDP port 19 is associated with the "Character Generator Protocol" (CHARGEN), which responds by sending a random character stream back to the sender.

Fill in the following detail about the spoofed packet that the attacker sends.

    i. Source IP address: _____

   ii. Source UPD port number: _____

  iii. Destination IP address: _____

   iv. Destination UPD port number: _____

End of Questions.