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

EXAMPLE SOLUTIONS + grading rubric

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.

   Solution: Caching authentication tokens for too long can violate the Complete Mediation principle because it avoids re-validating user permissions with each access attempt. If a user's permissions change, a cached token might still grant access based on outdated permissions, leading to unauthorised access. To adhere to Complete Mediation, it's important to periodically re-validate tokens against current user status and permissions.

   (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

   Solution: Segregating duties among the development, QA, and operations teams, would ensure that different aspects of the software release process are handled by specialised teams with appropriate oversight, minimising the risks of errors and malicious code being deployed.

   (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.

   Solution: Both a password and a security question are examples of authentication via "something only you know" method, so it is NOT a legitimate example of MFA.

(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.

Solution: Type-II errors means authenticating users that should not be authenticated, which is more dangerous (from the security standpoint) than not authenticating users that should be (type-I error) which are rather a nuisance than a major security issue.

(e) Ping-of-Death is an example of which of the following attacks?

A. Cache poisoning

B. Sniffing

C. Spoofing

D. DoS

E. MitM

Solution: Denial-of-Service. (although it is NOT a volumetric one, but rather, protocol-based)

(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;`

Solution: "WITH GRANT OPTION" means now **`alice`** can pass the "insert" privilege to other roles or users at their discretion.

(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)

Solution: `chgrp` does not require set-uid because changing the group ownership should be a controlled action permitted to a user only over files they own.

(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
```

Solution: Option "A" is wrong because `bob` is a member of `staff`, who have write permission to the `CYBR371` directory.

Option "B" is wrong because the primary group of `bob` is `tutors`, which will be his real group upon logging in. Any newly created file or directory has that user as the owner and the real group of that user as the group owner. The group owner of the file would have been `staff`, which is the group owner of the

directory `CYBR371`, if the "setgid" special permission on the directory was set (which is not!).
Option "E" is wrong because the permissions are consistent with the umask but if it was a newly created directory not a file.
Option "D" is wrong for reasons covered for options "B" and "E".

(i) Which one of the following is NOT 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`**.

Solution: Using a hub instead of a switch means the attacker has it easier to access all hosts on the network via broadcast.

(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.

Solution: Don't confuse SYN cookies with application layer cookies!

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.

Solution: Many options possible. For example, consider some sensitive data that is encrypted at rest and in transit, access is controlled through multi-factor authentication, and all activities are monitored by an anomaly detection system. This is coupled with regular security training for employees and robust incident response protocols, as well as taking regular backups.

(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 one option, the most relevant one. No explanation is necessary.)

i. Firewalls **B**

ii. Access Control **B**

iii. Honeypots **A**

iv. Installing security patches as soon as they are released **B**

(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.

Solution: Neither: not BLP, because *Alice* can write down to `questions.pdf`. Not Biba either, because *Alice* can read down from `questions.pdf`.

(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).

Solution: With ABAC, you can set conditions that are related to the attributes of the subject (beyond just their role), object, or the environment. For instance, an ABAC rule can be give access to a patient record to a doctor is the doctor is assigned to that patient, AND if the patient has done the admission process OR is in critical condition, AND the time is within the working hours of that doctor.

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

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.

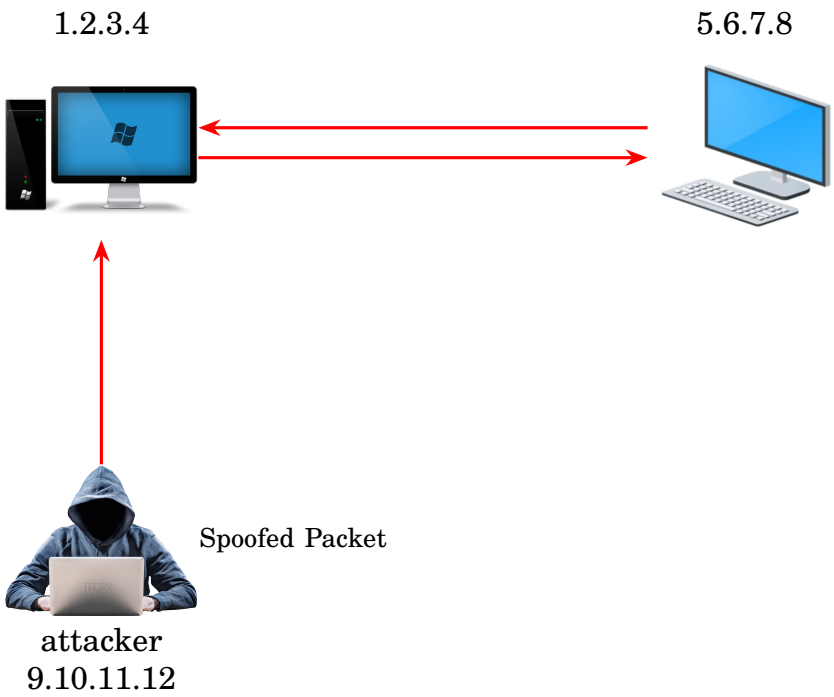
Fill in the following detail about the spoofed packet that the attacker sends.

i. Source IP address: **5.6.7.8**

ii. Source UPD port number: **7**

iii. Destination IP address: **1.2.3.4**

iv. Destination UPD port number: **19**



Solution: The port numbers 7 and 19 can also be other way around too, but not the source and destination IP addresses. In fact, both source and destination port numbers can be set to 19 too. Less effective but still a valid solution, both source and destination port numbers can also be set to 7 too.

End of Questions.