YILDIZ TECHNICAL UNIVERSITY
FACULTY of ELECTRICAL & ELECTRONICS ENG. / DEPT. of COMPUTER ENGINEERING

Student Name Surname:	**Number:**			**Signature:**	
Course: BLM4011 Gr1,2	**Date/Time: 26/01/2023 11:00**			**Duration: 60 min.**	
Exam. Type:	**MidT 1**	**MidT 2**	**MakeUp**	**Final**	**MUFinal ☒**
Instructors: Prof. Dr. Hasan Hüseyin BALIK					

Q1 UNIX treats file directories in the same fashion as files; that is, both are defined by the same type of data structure, called an inode. As with files, directories include a nine-bit protection string. If care is not taken, this can create access control problems. For example, consider a file with protection mode 644 (octal) contained in a directory with protection mode 730. How might the file be compromised in this case? **(25p)**

A1) Suppose that the directory **d** and the file **f** have the same owner and group and that **f** contains the text something. Disregarding the superuser, no one besides the owner of **f** can change its contents, because only the owner has write permission. However, anyone in the owner's group has write permission for **d**, so that any such person can remove **f** from **d** and install a different version, which for most purposes is the equivalent of being able to modify **f**.

Q2) Assume you receive an e-mail, which appears to come from your bank, includes your bank logo in it, and with the following contents:
"Dear Customer, Our records show that your Internet Banking access has been blocked due to too many login attempts with invalid information such as incorrect access number, password, or security number. We urge you to restore your account access immediately, and avoid permanent closure of your account, by clicking on this link to restore your account. Thank you from your customer service team."
What form of attack is this e-mail attempting? What is the most likely mechanism used to distribute this e-mail? How should you respond to such e-mails? **(25p)**

A2) A **phishing** attack uses a spam e-mail to exploit social engineering to leverage user's trust by masquerading as communications from a trusted source, that may direct a user to a fake Web site, or to complete some enclosed form and return in an e-mail accessible to the attacker. A more dangerous variant of this is the **spear-phishing** attack. This again is an e-mail claiming to be from a trusted source. However, the recipients are carefully researched by the attacker, and each e-mail is carefully crafted to suit its recipient specifically, often quoting a range of information to convince them of its authenticity. This greatly increases the likelihood of the recipient responding as desired by the attacker..

Q3) User "ahmed" owns a directory, "stuff," containing a text file called "ourstuff.txt" that he shares with users belonging to the group "staff." Those users may read and change this file, but not delete it. They may not add other files to the directory. Others may neither read, write, nor execute anything in "stuff." What would appropriate ownerships and permissions for both the directory "stuff" and the file "ourstuff.txt" look like? (Write your answers in the form of "long listing" output in linux.)? **(25p)**

A3)
```
drwxr-x---    2 ahmed staff    0 Jul 21 07:58 stuff
-rw-rw----    1 ahmed staff    0 Jul 21 08:00 ourstuff
```

Q4) IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. CSPs typically approach this risk by using isolated VMs for individual clients. This approach is still vulnerable to attack, by both insiders and outsiders, and so can only be a part of an overall security strategy. Suggest 5 countermeasures. **(25p)**

A4) (1) implement security best practices for installation/configuration; (2) monitor environment for unauthorized changes/activity; (3) promote strong authentication and access control for administrative access and operations; (4) enforce SLAs for patching and vulnerability remediation; and (5) conduct vulnerability scanning and configuration audits.

Hepinize sınavınızda başarılar dilerim.