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

Student Name Surname:	**Number:**			**Signature:**	
Course: BLM4011 Gr1,2,3	**Date/Time: 11/01/2022 13:00**			**Duration: 90 min.**	
Exam. Type: Final	**MidT 1**	**MidT 2**	**MakeUp**	**Final ☒**	**MUFinal**
Instructors: Prof. Dr. Hasan Hüseyin BALIK					

QUESTIONS

Q1) It is recommended that when using BitLocker on a laptop, the laptop should not use standby mode, rather it should use hibernate mode. Why? **(15p)**

When using BitLocker on a laptop, the laptop should not use standby mode, rather it should use hibernate mode. This is because Hibernate writes memory to the computer’s disk drive, which means the computer's memory content, is protected by bitlocker. Standby simply keeps the computer in a very low power state, and memory is maintained and not protected by BitLocker.

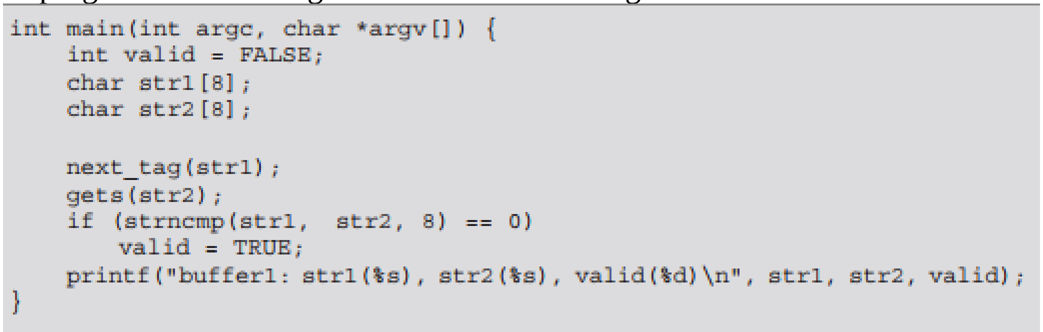
Q2) Suppose you operate an Apache-based Linux Web server that hosts your company’s e-commerce site. Suppose further that there is a worm called “WorminatorX,” which exploits a (fictional) buffer overflow bug in the Apache Web server package that can result in a remote root compromise. Construct a simple threat model that describes the risk this represents: attacker(s), attack-vector, vulnerability, assets, likelihood of occurrence, likely impact, and plausible mitigations. **(15p)**

Assets: website availability, system availability, local network integrity (integrity of other systems the attacker may reach via compromised web server), corporate data, customer data, website availability, ecommerce business activity (immediate revenue), company reputation (future revenue)
Vulnerability: buffer-overflow in Apache
Attack-vector: the worm “WorminatorX” (that multiple exploits may target the same vulnerability -- this is just the one we know about)
Attackers: competitors, thieves, identity thieves, website defacers (vandals), disgruntled ex-employees, the Byelorusan mob, etc. -- public web sites can be prey to any Internet-connected type of attacker
Likelihood of Occurrence: High (or synonyms thereof) – Internet worms spread very far very quickly
Likely Impact: High -- complete exposure/loss of any or all affected assets to any potential attacker
Plausible Mitigations: Patch the Apache vulnerability; if no patch is available, protect Apache with SELinux or AppArmor; or run Apache in a chroot jail (Note that Apache already runs as an unprivileged user, by default -- presumably the WorminatorX vulnerability depends on some other privilege-escalation vulnerability)

Q3) Define the principle of least privilege. **(10p)**

The principle of least privilege states that programs should execute with the least amount of privileges needed to complete their function.

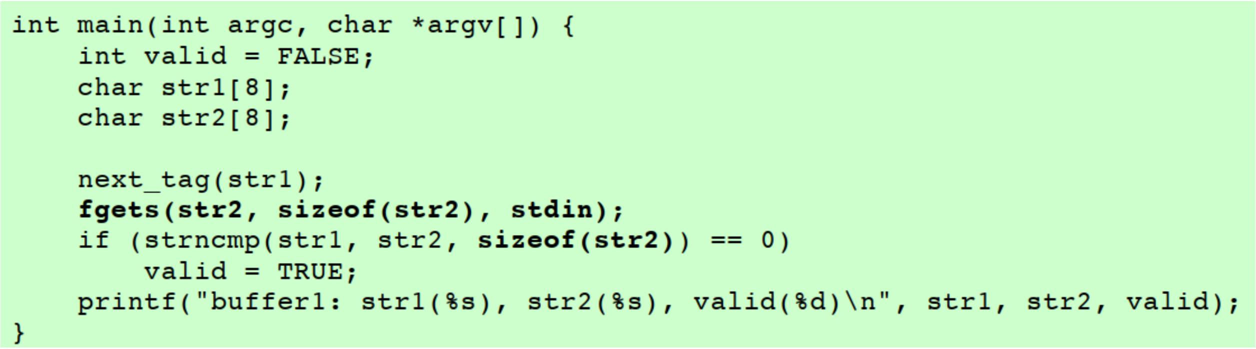
Q4) Rewrite the program shown in Figure 1 so that it is no longer vulnerable to a buffer overflow. **(15p)**



```
int main(int argc, char *argv[]) {
    int valid = FALSE;
    char str1[8];
    char str2[8];

    next_tag(str1);
    gets(str2);
    if (strncmp(str1,  str2, 8) == 0)
        valid = TRUE;
    printf("buffer1: str1(%s), str2(%s), valid(%d)\n", str1, str2, valid);
}
```

Figure 1.



```
int main(int argc, char *argv[]) {
    int valid = FALSE;
    char str1[8];
    char str2[8];

    next_tag(str1);
    fgets(str2, sizeof(str2), stdin);
    if (strncmp(str1, str2, sizeof(str2)) == 0)
        valid = TRUE;
    printf("buffer1: str1(%s), str2(%s), valid(%d)\n", str1, str2, valid);
}
```

Q5) How does an IPS differ from a firewall? **(10p)**

An IPS blocks traffic, as a firewall does, but makes use of the types of algorithms developed for IDSs.

Q6) Consider the first step of the common attack methodology we describe, which is to gather publicly available information on possible targets. What types of information could be used? What does this use suggest to you about the content and detail of such information? How does this correlate with the organization's business and legal requirements? How do you reconcile these conflicting demands? **(15p)**

Types of publicly available information that could be used by an attacker include: information required by law such as business registration and contact details or share registration details; contact information in phone books, DNS entries, network registration and WHOIS details; publicity and contact details provided by an organization on their website, or in publications handed out to the public. This suggests that from a security perspective, the content and detail of such information should be minimized. But this may well conflict with the organization's business and legal requirements to make this information available? It can be very difficult to reconcile these conflicting demands, though the appropriate balance may be suggested by the results of a risk assessment of the organization which may identify which types of information may be particularly dangerous. It may be possible to remove details of individual's names and positions, which would be of use in a spear-phishing attack, and use generic position details instead.

Q7) Assume you receive an e-mail, which appears to come from a senior manager in your company, with a subject indicating that it concerns a project that you are currently working on. When you view the e-mail, you see that it asks you to review the attached revised press release, supplied as a PDF document, to check that all details are correct before management release it. When you attempt to open the PDF, the viewer pops up a dialog labeled "Launch File" indicating that "the file and its viewer application are set to be launched by this PDF file." In the section of this dialog labeled "File," there are a number of blank lines, and finally the text "Click the 'Open' button to view this document." You also note that there is a vertical scroll-bar visible for this region. What type of threat might this pose to your computer system should you indeed select the "Open" button? How could you check your suspicions without threatening your system? What type of attack is this type of message associated with? How many people are likely to have received this particular e-mail? **(15p)**

If you should open the PDF attachment, then it could contain malicious scripting code that could run should you indeed select the 'Open' button. This may be either worm (specifically exploiting a client-side vulnerability), or trojan horse code. You could you check your suspicions without threatening your system by using the scroll bar to examine all the code about to be executed should you select the 'Open' button, and see if it looks suspicious. You could also scan the PDF document with suitable, up-to-date anti-virus software for any signs of malware – though this will not detect unknown, zero-day exploits. This type of message is associated with a spear-phishing attack, given that the email was clearly crafted to suit the recipient. That particular e-mail would only have been sent to one or a few people for whom the details would seem plausible.

Q8) It was stated that the inclusion of the salt in the UNIX password scheme increases the difficulty of guessing by a factor of 4096. But the salt is stored in plaintext in the same entry as the corresponding ciphertext password. Therefore, those two characters are known to the attacker and need not be guessed. Why is it asserted that the salt increases security? **(10p)**

Without the salt, the attacker can guess a password and encrypt it. If ANY of the users on a system use that password, then there will be a match. With the salt, the attacker must guess a password and then encrypt it once for each user, using the particular salt for each user.

Hepinize sınavınızda başarılar dilerim.