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

Student Name Surname:	**Number:**			**Signature:**	
Course: BLM4011 Gr1,2	**Date/Time: 10/01/2023 09:00**			**Duration: 60 min.**	
Exam. Type: Final	**MidT 1**	**MidT 2**	**MakeUp**	**Final ☒**	**MUFinal**
Instructors: Prof. Dr. Hasan Hüseyin BALIK					

Q1 What is MiniSec and what are the requirements that MiniSec is designed to meet? **(30p)**

A1) MiniSec is an open-source security module that is part of the TinyOS operating system. MiniSec is designed to meet the following requirements:
Data authentication: Enables a legitimate node to verify whether a message originated from another legitimate node (i.e., a node with which it shares a secret key) and was unchanged during transmission.
Confidentiality: A basic requirement for any secure communications system. Replay protection: Prevents an attacker from successfully recording a packet and replaying it at a later time.
Freshness: Because sensor nodes often stream time-varying measurements, providing guarantee of message freshness is an important property. There are two types of freshness: Strong and weak. MiniSec provides a mechanism to guarantee weak freshness, where a receiver can determine a partial ordering over received messages without a local reference time point.
Low energy overhead: This is achieved by minimizing communication overhead and by using only symmetric encryption.
Resilient to lost messages: The relatively high occurrence of dropped packets in wireless sensor networks requires a design that can tolerate high message loss rates.

Q2) Why is logging important? What are its limitations as a security control? What are pros and cons of remote logging? **(20p)**

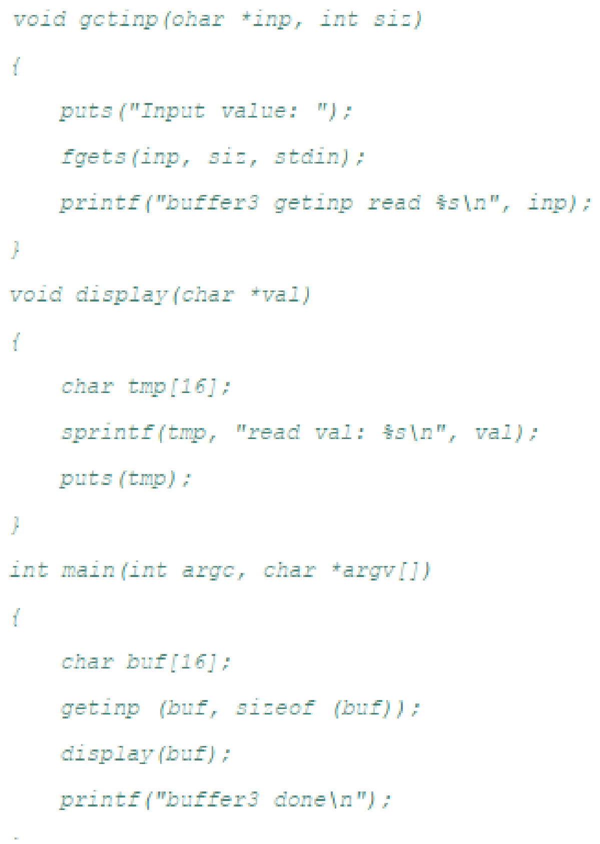
A2) Logs provide audit trails of system and application events, and are useful for identifying problems, analyzing security breaches, analyzing system/application failures. Logs may even, if monitored closely, provide an early warning of failures or attacks in progress. But logs only capture the level of detail

Q3) Define an injection attack. List some examples of injection attacks. What are the general circumstances in which injection attacks are found? **(20p)**

A3) An injection attack refers to a wide variety of program flaws related to invalid handling of input data, particularly when such input data can accidentally or deliberately influence the flow of execution of the program. Examples of injection attacks include: command injection, SQL injection, code injection, and remote code injection. There are a wide variety of mechanisms that can result in injection attacks. These include when input data is passed as a parameter to another helper program (command) or to a database system (SQL), whose output is then processed and used by the original program. Or when the input includes either machine or script code that is then executed/interpreted by the attacked system (code)

Hepinize sınavınızda başarılar dilerim.

Q4) Rewrite the function shown blow so it is no longer vulnerable to a stack buffer overflow. **(20p)**

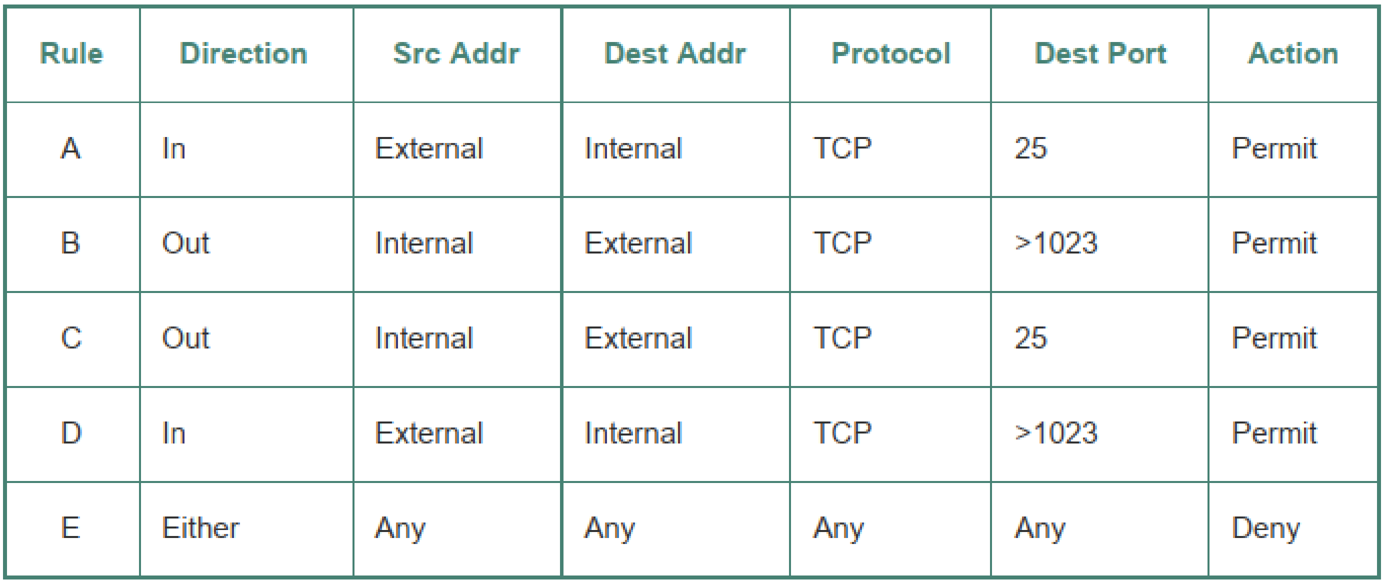


```
void getinp(char *inp, int siz)
{
    puts("Input value: ");
    fgets(inp, siz, stdin);
    printf("buffer3 getinp read %s\n", inp);
}
void display(char *val)
{
    char tmp[16];
    sprintf(tmp, "read val: %s\n", val);
    puts(tmp);
}
int main(int argc, char *argv[])
{
    char buf[16];
    getinp (buf, sizeof (buf));
    display(buf);
    printf("buffer3 done\n");
```

A4)

```
void display(char *val)
{
    char tmp[16];
    snprintf(tmp, sizeof(tmp), "read val: %s\n", val);
    puts(tmp);
}
```

Q5 SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following rule set:

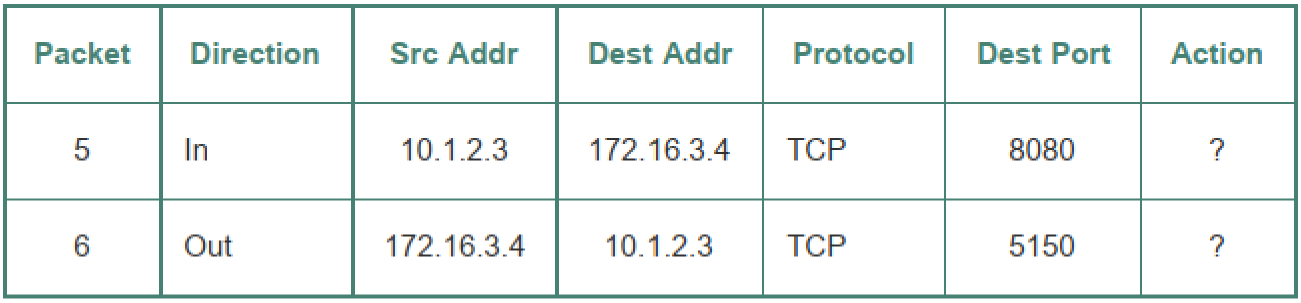


Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

a. Describe the effect of each rule. **(15p)**

Hepinize sınavınızda başarılar dilerim.

b. Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4) in order to carry out an attack. Typical packets are as follows:



Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
5	In	10.1.2.3	172.16.3.4	TCP	8080	?
6	Out	172.16.3.4	10.1.2.3	TCP	5150	?

Will the attack succeed? Give details. **(15p)**

A5)

a. Rules A and B allow inbound SMTP connections (incoming email) Rules C and D allow outbound SMTP connections (outgoing email) Rule E is the default rule that applies if the other rules do not apply.

b. The attack could succeed because in the original filter set, rules B and D allow all connections where both ends are using ports above 1023.