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

Student Name Surname:	**Number:**			**Signature:**	
Course: BLM4011 Gr1,2,3	**Date/Time: 03/02/2022 11:00**			**Duration: 75 min.**	
Exam. Type: Final	**MidT 1**	**MidT 2**	**MakeUp**	**Final**	**MUFinal ☒**
Instructors: Prof. Dr. Hasan Hüseyin BALIK					

QUESTIONS

Q1) RFC 791, the IPv4 protocol specification, describes a reassembly algorithm that results in new fragments overwriting any overlapped portions of previously received fragments. Given such a reassembly implementation, an attacker could construct a series of packets in which the lowest (zero-offset) fragment would contain innocuous data (and thereby be passed by administrative packet filters) and in which some subsequent packet having a nonzero offset would overlap TCP header information (destination port, for instance) and cause it to be modified. The second packet would be passed through most filter implementations because it does not have a zero fragment offset. Suggest a method that could be used by a packet filter to counter this attack.? **(20p)**

If the router's filtering module enforces a minimum fragment offset for fragments that have non-zero offsets, it can prevent overlaps in filter parameter regions of the transport headers..

Q2) Can you propose some rules which could be used to distinguish “suspicious activities” from normal user behavior on a system for some organization? **(20p)**

'Normal' behavior would generally involve users creating, using or deleting files belonging to either the individual user or to a group to which they belong. Normal behavior would not involve attempting to gain superuser or root privileges or in any other way altering the operating system or attempting to perform what could be considered administrator functions.

- bad or repeated login attempts
- copying large numbers of files to either external media or remote locations
- attempts to access system files or log files
- accessing directories, files or programs that are not usually accessed
- changing security settings attempts to become a superuser using the su or sudo commands

Q3) List some problems that may result from a program sending unvalidated input from one user to another user. **(20p)**

Problems that may result from a program sending unvalidated input from one user to another user if the output does not conform to the expected form and interpretation by the recipient. A program may accept input from one user, save it, and subsequently display it to another user. If this input contains content that alters the behavior of the program or device displaying this data, and it is not adequately sanitized by the program, then an attack on the user is possible. Examples include embedding terminal (e.g.. VT100) “escape sequences”, or Javascript script code in an XSS attack..

Q4) List and briefly define the two types of honeypots that may be deployed. **(20p)**

Honeypots are typically classified as being either a:

- Low interaction honeypot: a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems.
- High interaction honeypot: a real system, with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers.

Q5) Suggest a way of implementing protection domains using both access control lists and capability tickets? **(20p)**

Hepinize sınavınızda başarılar dilerim.

- access control lists: We could implement "subject" objects that are not associated with any user. The subject would be a protection domain and would have all the privileges that subject has in the access control lists. An operation on the subject object would be to allow the process to 'become" that subject. Being that subject would be equivalent to being in that protection domain.
- capability tickets: It is only necessary to change the system so that sets of capabilities can exist independent of a process, and a process can run in a protection domain. There would be a capability to enter each protection domain, and only processes holding that capability would be allowed to enter. You could have some capabilities associated with the process and some with the protection domain it is running in.

Hepinize sınavınızda başarılar dilerim.