# ENPM695 – Secure Operating Systems

# Homework – 2

*Author – Syed Mohammad Ibrahim*

*UMD ID:* *iamibi*

*UID: 118428369*

*Email:* [*iamibi@umd.edu*](mailto:iamibi@umd.edu)

1. Address Space Layout Randomization is designed to make stack smashing attacks harder. Explain how Address Space Layout Randomization works (10 points). Describe an attack of how Address Space Layout Randomization can be circumvented (10 points)

A. Address Space Layout Randomization (ASLR) introduced into Linux from kernel version 2.6.12 works on the principle of randomizing the memory address space of a process that is currently loaded in the memory. This essentially involves randomizing the address space of Stack, Heaps, Internal Libraries, etc. Because of ASLR, the attacker now needs to know the process exact memory address which keeps on changing on every run making it hard for them to perform any kind of attack.

The following example demonstrates how ASLR can be bypassed. The program is written in C programming language and the exploit script is written in perl language. The Operating system is Linux 32-bit with little-endian architecture.

A screenshot of a computer

Description automatically generated

As it can be seen from the above program, the ASLR is currently ON and we were still able to exploit the program with exit(0) function call. This exploit is based on the concept of Ret2ESP where we find the address of “jmp \*%esp” and use that in our exploit script. The exploit mainly comprises of a return address, padding – to fill up the buffer and shell code which in our case is of exit(0) function call.

2. Executable Stack Protection is another technology which can be used to protect against stack smashing attacks. Explain how ESP works (10 points). Provide an example of a class of attacks that can circumvent ESP (5 points). Describe how this class of attacks work (10 points)

A.

3. You are tasked with hacking the President’s Twitter Account. Develop an attack tree that details the various options and pathways to achieve that result (15 points)

4. Given the network diagram below – develop a threat model diagram and an attack surface analysis for this system detailing the following information (20 points):

a. STRIDE elements for each component

b. For the web server in particular, develop a “back-of-the-envelope” attack surface from both an internal network perspective as well as an external network perspective using the following information:

i. open ports: 22, 111, 80, 443, 8080;

ii. operating system: Ubuntu Server 16.0.4 with the following software installed

1. SSHd (TCP/22)

2. Postfix (TCP/25)

3. Bind (TCP & UDP/53)

4. Rpcbind (TCP/111)

5. Apache (TCP/80, TCP/443)

6. MySQL (TCP/3306)

7. Tomcat (TCP/8080)

8. Webmin (TCP/10000) – accessible from Management server only

iii. The firewall provides external access to ports 22, 80, and 443

c. Potential threats derived from the threat model (list at least 5 potential threats)

5. Define the various parts of the DREAD scoring system. What does each part of the DREAD scoring indicate? (5 points)

6. A threat has the following components of the overall DREAD score:

a. Discoverability – 3

b. Reproducibility – 3

c. Damage Potential – 2

d. Exploitability – 3

e. Affected Users – 1

Calculate the overall DREAD score. Describe the characteristics of each component (i.e. is it high, low, etc.). Is this threat a high, medium or low threat? (note: consider the overall scale of DREAD) (15 points)