German International University
Faculty of Informatics and Computer Science
Dr. Marwa Zamzam
Eng. Zyad Mostafa

Ethical Hacking and Peneteration Testing, Spring 2024
Assignment 4

1 Description

Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information. For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems.

If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store, and overwrite areas that hold executable code, replacing it with their own code. For example, an attacker can overwrite a pointer (an object that points to another area in memory) and point it to an exploit payload, to gain control over the program.

2 Guidelines

Netstart is a Linux box, running a WINE Application vulnerable to Buffer Overflow.

1. Install the machine from this link:
   `https://bit.ly/3K9pNTB`
2. Download the files you will debugging and the python script from this link:
   `https://bit.ly/3JMXedx`
3. Use the python code in the spiking phase and modify it throughout the other phases
   `https://bit.ly/3JMXedx`

German International University
Faculty of Informatics and Computer Science
Dr. Marwa Zamzam
Eng. Zyad Mostafa

3 Deliverables

You are required to submit a pdf file including:-

1. Buffer overflow exploitation using Immunity debugger.
2. Screenshots of each step (information gathering,scanning and exploitation) and a description at each screenshot.

4 Submission

- You should submit your file at the following link:
  https://forms.office.com/r/NRMuJtMS9k
- The filename should be of form <ID_Name>.
  For example: 1001234_Adam_Smith.ctb
- Online submission is due on Monday, April 1, by 11:59 pm.