Group 8 Final Project Proposal

By Cory Lagor (v89h865), Micheal Wetherbee (z93r546), Michael Utt (p41r185), Emilia Bourgeois (n37n792)

Overview

Our group is looking at vulnerabilities that exist within certain versions of the Linux operating system, particularly Ubuntu 16.04 & 12.04. Exploit creation and patching work for the vulnerabilities will be done on virtual machines so as to safeguard our own computers from the effects of said exploits. Exploits and patches in code form will be written in C and/or Python. A final report will be written collaboratively and exported as a pdf. A final demo of our project will be made in the form of a video.

Attacks

Dirty Cow

Dirty COW(dirty copy on write) is an exploit used to change someone's read permission to a write permission in a file, this can be used to gain root access to a computer. This is done by exploiting a race condition in the implementation of the copy-on-write mechanism in the kernels memory-management.

Heartbleed

Heartbleed is caused by a flaw in OpenSSL, an open source code library that implemented the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. This vulnerability is present in the OpenSSL version 1.0.1f.

Spectre

Spectre is an attack that exploits many modern amd and intel processors. The CPUs themselves have a vulnerability that allows malicious programs to break intra-process and inter-process isolation.

Buffer-Overflow Vulnerability

A buffer-overflow vulnerability occurs when a program writes data to space beyond the boundaries of a pre-allocated buffer. An attacker could change the flow control of a program and cause all kinds of damage.

Logistics

Rough Schedule:
10/23/2020 - Complete and upload proposal for project.

11/1/2020 - Have completed the attack for your exploit.
11/12/2020 - Have completed the patch to the best of your ability.
11/15/2020 - Present on our findings and implementation of each exploit

Division of Labor: For division of labor each member will complete the exploitation and patching of one vulnerability to the Linux build we have chosen. If a member becomes stuck on a part the other 3 members will pitch in to solve it. If for whatever reason a vulnerability is unsolvable within the bounds of what our group is capable of, that vulnerability shall be abandoned. The chooser of that exploit will become auxiliary for the other 3 exploits and each other exploit will be completed to a more in depth degree then if we were to have four exploits.