OREGON STATE UNIVERSITY

CS 373

WINTER 2019

Week 4

Author:
Thomas Noelcke

Instructor:
D. Kevin McGrath

I. Overview

This week we are diving deeper into Vulnerabilities and Exploits. In these lectures we learned more about how attacks are carried out through vulnerabilities. In this write up will include any interesting things that I learned during lecture. I will then have another section were I list out the new terms that learned during the lecture.

II. Interesting Lecture Sections

In this section will discuss interesting topics I learned about during the lecture.

A. Introduction

This lecture is about what hacking really is. If we are comparing this to Harry Potter this isn't really defense against the dark arts but is rather the dark arts them selves. So I guess you would say that this is Moody's class. At it's core hacking isn't really doing something magical or new but rather it is just controlling a program in a way that it wasn't designed to be used. This is much like driving. If you come to an intersection you can go one of two ways left or right. But what if you didn't and you went strait? What would happen? This essentially hacking.

B. Types of Vulnerabilities

There are really two general types of vulnerabilities. Control related vulnerabilities where you try and take control of a program. There are also configuration related vulnerabilities. These are where the user configures there system in a way where it isn't secure. This is the low hanging fruit of the venerability world. In this lecture we will focus on the former.

C. Backgound

In the early days of the internet hacking was kind of a hippy thing. Hacking wasn't very serious and it wasn't really a very main stream thing. Today things have changed. Today hacking is a very serious thing. So serious in fact that governments have their own special forces of the military that hack stuff. The type of stuff that we are going to be learning is the kind of stuff that those cyber armies are also doing. We need to be careful when we are trying to learn this stuff on our own. This is the type of stuff that can get us into serious legal trouble.

D. Bug Bounty Software

Bug bounty program is where if you find a vulnerability and report it to the company they will pay you for finding this information. There was an IOS bug that paid out 500k for one vulnerability. The lecture had found a Samsung bug that paid out 5k. This is a serious business.

E. Popular trends in hacking

Today the networks of most large companies are fairly hardened. This makes it difficult to attack organizations from the out side. As a result hackers are now focusing on using social engineering to get inside the network first and then use patient zero machine to attack other points with in the same network. This is often done through a users browser. Hackers are using vulnerabilities in the browser to take control over execution of the code in the browser.

F. WinDB

This the windows equivalent of GDB. It allows you on a windows system to freeze execution of a program and interact with the program. This will also allow you to look at memory and registers. We are going to test out this tool using a lab by running bad activex script in the browser. We will then use WinDB to observe this piece of code running.

G. I'm Calling it in this week

I regret to inform who ever may be reading this that this write has to end early. I've been fighting the flu all weekend and it has caused me to get behind. So rather than let that derail me I took what notes I could and turned this write up in. I full accept that I may get a poor score on this write up but at least I won't get behind on subsequent write ups. I do have to say though it makes me sad I had to get sick now because this was probably one of the topics I was most interested in. I plan to finish the lectures and will probably even add more notes to this write up.

III. TERMS

In this section I will list out new terms that learned during the lectures and labs.

-