KompyuterM3chakrs

Week of (Date):

Team Members Active this Week:

Melanie Growley

Keren Angeles

Nathan Bellew

Weekly Update of Project/Research (Summarized by Team Lead):

Main Projects: Husqavarna Hack, Meccano Robot Hack.

Sub Projects: Capture the Flag: Janos, Hackertest.

Main Goal: Buffer Overflow

Each student worker has slowly come to the understanding of how the Buffer Overflow works, and will continue to learn throughout the next week through examples.

We have used sources form Hacking the Art of Exploitation, which has given us some sample problems to create Buffer Overflows with.

Name: Nathan Bellew Hours worked this week:

Please explain in detail what you worked on this week.

In order to crack a company machine we need to first understand how to hack simple programs, our sub projects will help launch us to our ultimate goal. So far this week we discussed the many ways Buffer Overflow is used to break into systems and how we can create them. The Buffer Overflow is one of the highlights of the Janos CTF, and so it would be nearly impossible to complete it without covering it. By the end of the week we should have a few positive tests to show how buffer overflow exists.

What are the outcomes of your research and time for the week?

Each student worker now has a base understanding of the memory stored in the HEAP and STACK of a computer, and how if used incorrectly, can cause severe security problems in the computer.

Please describe any roadblocks or difficulties you experienced in your research this week.

As always our biggest roadblock continues to be the lack of computer knowledge and the difference of Operating system. This roadblock is not easily fixed with something like a virtual machine, due to the network setup, even with a virtual machine, we are still unable to create proper work. We found a few work arounds with the Windows Subsystem for Linux, but it is still far from perfect. As each day passes it does appear that the growth in knowledge is slow building.

What are your next steps moving forward?

Currently the methods for teaching the new student workers the hacking techniques, is a lecture method with examples. Assignments may need to be assigned during the last hours of work to ensure they are maintaining the lesson of each day.

Name: Melanie Grumley Hours worked this week:

Please explain in detail what you worked on this week.

We worked on a hacking game called Capture the Flag. Nathan has been going through each level and explaining how to hack each one.

What are the outcomes of your research and time for the week?

I have a better understanding of what vulnerabilities to look for when we go to hack the lawn mower.

Please describe any roadblocks or difficulties you experienced in your research this week.

I have no experience doing anything like hacking or getting into the internals of computer software so that is going to be my biggest roadblock throughout this entire project. This week in particular, I have also fallen behind on homework for a summer class so I haven't been able to come into work.

What are your next steps moving forward?

Pay attention and learn what I can during work hours.

Name: Keren Angeles Hours worked this week:

Please explain in detail what you worked on this week.

This week are working on a Capture-the-Flag project. The goal of capture the flag is to learn to look for vulnerabilities in a given piece of code and learn how to exploit those. We learned about manipulating $PATH in order to run the code we want to access a password. We also learned how to manipulate cookies from a local host.

What are the outcomes of your research and time for the week?

The point of the CTF exercise was to learn different vulnerabilities in programs and softwares so that we can apply this knowledge later on when we try to hack the auto-mower.

Please describe any roadblocks or difficulties you experienced in your research this week.

Some of the roadblocks were the new terminologies that we learned

such as pointer manipulation, little endian notation, buffer overflow, and segmentation faults. We also learned how to implement them which was at time difficult at times to understand the concept

What are your next steps moving forward?
Our next steps moving forward are to finish the CTF practice up to
the last level and the next step would be to also learn more about how to use a Raspberry Pi