Vanier College

Computer Science Department

420-321-VA Unix

Winter 2024

Final Project: *Pen-Test Journal*

Submitted by

Student Name: _Karl_____ _Alvarado_____
First name **Last name**

Student ID: _6211078_

Week of 28/4/2024

This week, the work on our project consisted of discussions, research, and preparation. The focus of our discussions were the objectives of the project, which is to perform penetration tests using Kali Linux and Parrot Security OS, with the goal of understanding various tools and techniques of these tests.

The research and preparation tie in together, as the "research" was just several YouTube tutorials on the setup and basic operations of Kali Linux and Parrot Security. The tutorials were helpful in getting us comfortable with the basics. Along with the videos, we downloaded the ISO files of both operating systems. We then created bootable USB drives for each OS by following the video tutorials.

Week of 5/5/2024

This week, our focus in both Kali Linux and Parrot Security OS centered on delving deeper into penetration testing. I collaborated with the others in their respective OS's (Trevor: Kali, Nat: Parrot). We were testing the Metasploit framework across both operating systems. This extensive testing was to get a good feel of Metasploit so that the hack plan whould be straightforward.

Week 3

This week, we setup our Metasploitable 2 as our target for the penetration tests. On the Kali side of things, this was only figured out after hours of failed hacking attempts when trying to hack into the Metasploit console. With the target now setup, the decided attack was to use TigerVNC after scanning the vulnerabilities with Nessus. This gave us the ability access & run commands remotely on the target's shell. We figured that the easiest way to showcase this was to run some simple commands that creates & reads files.

For Parrot, it took a little bit to setup, since there were mistakes when it came to setting the right processor core for Metasploitable 2 and logging in. After that was handled though, we set the Network Configuration to Host-Only Networking, and then we were ready to start the hack. Metasploit was used on ParrotOS to exploit the vsftpd 2.3.4 backdoor vulnerability on Metasploitable2, which opened a command shell on the victim machine. Many commands were executed to scope our level of access and other information about the target, such as whoami, which confirmed root access. We used the wall command to remotely display a message in Metasploitable2 console, confirming a successful breach.

GitHub Link

YouTube Videos:

https://www.youtube.com/watch?v=8ucrQ6Tj2js&pp=ygUYaG93IHRvIHN0YXJ0IHBlbnRlc3Rpbmcg

https://www.youtube.com/watch?v=B7tTQ272OHE&pp=ygUYaG93IHRvIHN0YXJ0IHBlbnRlc3Rpbmcg

Link for ISO files:
https://www.osboxes.org/kali-linux/

https://sourceforge.net/projects/metasploitable/files/latest/download

https://www.tenable.com/downloads/nessus?loginAttempted=true

https://www.osboxes.org/parrot-security-os/