

Abstract

The problem is that companies are constantly being attacked by hackers and they lose sensitive information that can cause stolen identities, bank accounts, private company information, etc. In order to practice keeping hackers out, cyber security experts have been practicing breaking into systems. This activity is generally referred to as penetration testing. This poster describes some of the challenges our team experienced while building a penetration testing lab for the SWOSU College Cyber Defense (CCDC) team. The goal of this research is to show how easy it is to use an inexpensive *Raspberry Pi* for penetration testing for beginners as well as experts looking for alternative methods. By researching the book *Penetration Testing with Raspberry Pi* by Michael McPhee and Jason Beltrame, I want to show the benefits of using this software and how to perform this type of test in order to protect sensitive information. In turn, this will keep businesses from losing customers and minimizing the amount of exploits in software's.

What is Penetration Testing?

Penetration testing is a security exercise performed by professional cyber security experts that are hired by a company. The job of a pen tester is to find the security exploits within a company's security system. Think of a criminal that is hired by a company to steal information from their own company. Penetration testing has been beneficial to many companies because they discover the vulnerabilities within their systems, which helps the company patch these exploits. Typically companies hire cyber security personnel that has no prior relation to the company. There are three main types of penetration testing, such as: white box, black box and gray box. White box pen testing has full knowledge of the company's system, black box pen testing has no knowledge, while gray box pen testing has some knowledge.

What is Kali Linux?

Kali Linux is a Debian-based Linux distribution that focuses on penetration testing and security auditing. Kali is meant for offensive security and is a great tool for many information security tasks. Kali is maintained by Offensive Security, a leading information security training company.

Methodology

Equipment

- Raspberry Pi
- SD Card
- Mouse and Keyboard

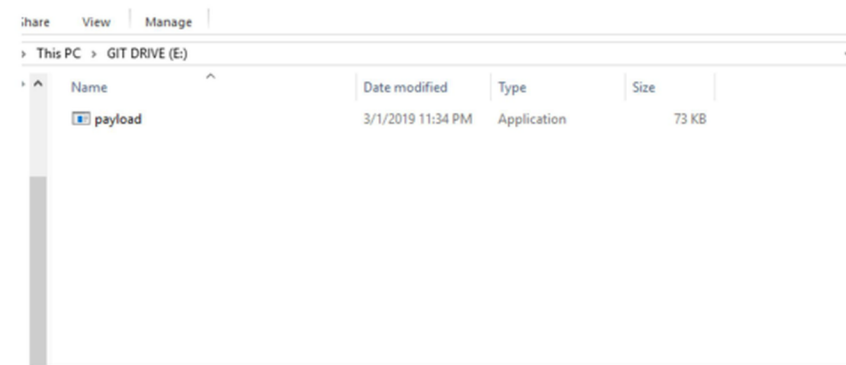
Software

- Kali Linux
- Metasploit
- Separate computer (victim)

Process

Downloading all of the software for the Raspberry Pi will took quite some time, since it is only a small computer. Once I installed Kali Linux to it's most current version I opened Metasploit from the command line and began to generate the payload. There are a few payloads to choose from, but I decided to use the command line tool, *msfvenom*. I generated a payload that was simply named *payload.exe*, naming a payload can be crucial when performing penetration testing. The file required the victim to execute the application to allow a backdoor for remote access from the Raspberry Pi. I uploaded the payload file onto a USB flash drive and was able to execute the file, giving me remote access to the infected system.

Output of a Successful Trial



A screenshot of the payload on the infected system via USB.

Why Use a Raspberry Pi?

A Raspberry Pi is a small computer that only the size of a credit card. It is also affordable for any technology enthusiast as the Raspberry Pi only costs \$35. The portability and accessibility to these pi's are why so many technology enthusiasts use these for small projects. I personally have used the Raspberry Pi for hosting a server for video games and this device is simple to use.

Creating a Portable Penetration Testing Pi



A writer from Null Byte, known as Mkilic, created a portable penetration testing box just under \$100. The design is very simple but offers a way to have a portable penetration testing box that has easy access and can be disposed of quickly. Mkilic build includes: a Raspberry Pi, a Makerfire 7" LCD screen, a Rii mini wireless keyboard and mouse, a PNY battery pack, a micro SD card, a 12V 2A DC power adapter, and an HDMI cable.



Mkilic then uses tape and velcro to hold everything inside of the lunchbox. The keyboard and mouse are integrated into one but it is completely wireless, offering the easy accessibility of navigating through the penetration testing box. There are plenty of other ways to build a small penetration testing box for the Raspberry Pi, some can be cheap while other can be fairly expensive.

Works Cited

- *Penetration Testing with Raspberry Pi*. 2nd ed., Packt Publishing Ltd. 2016.
- <https://null-byte.wonderhowto.com/how-to/build-portable-pen-testing-pi-box-0167629/>
- <https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/>
- <https://resources.infosecinstitute.com/the-types-of-penetration-testing/>
- <https://docs.kali.org/introduction/what-is-kali-linux>