Penetration Testing Using A Raspberry Pi

Hagan Holsapple  
Southwestern Oklahoma State University

Devin Smoot  
Southwestern Oklahoma State University

Jeremy Evert  
Southwestern Oklahoma State University

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... Read More

Follow this and additional works at: https://dc.swosu.edu/cpgs_edsbt_bcs_student

Recommended Citation

Holsapple, Hagan; Smoot, Devin; and Evert, Jeremy, "Penetration Testing Using A Raspberry Pi" (2019). Student Research. 18.  
https://dc.swosu.edu/cpgs_edsbt_bcs_student/18

This Poster is brought to you for free and open access by the Business & Computer Science at SWOSU Digital Commons. It has been accepted for inclusion in Student Research by an authorized administrator of SWOSU Digital Commons. An ADA compliant document is available upon request. For more information, please contact phillip.fitzsimmons@swosu.edu.
Penetration Testing Using A Raspberry Pi

Southwestern Oklahoma State University

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.

Methodology

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raspberry Pi</td>
<td>Kali Linux</td>
</tr>
<tr>
<td>SD Card</td>
<td>Metasploit</td>
</tr>
<tr>
<td>Mouse and Keyboard</td>
<td>Separate computer (victim)</td>
</tr>
</tbody>
</table>

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.

Authors

Hagan Holsapple | Devin Smoot | Dr. Jeremy Evert | Department of Computer Science

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 MkIlc, 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. MkIlc 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.

Works Cited

- 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