Building a Penetration Testing Device for Black Box using Modified Linux for Under $50

Young B. Choi
Department of Science, Technology, and Mathematics
Regent University
Virginia Beach, VA 23464-9800
USA

Kenneth P. LaCroix
Department of Science, Technology, and Mathematics
Regent University
Virginia Beach, VA 23464-9800
USA

***Abstract*—This study analyzes the use of a Raspberry Pi (RPi) as part of a Penetration Tester's toolkit. The RPi's form factor, performance to cost ratio, used in conjunction with modified Linux, allows the RPi to be a very versatile product. Whatsmore, the RPi retails for $35 and is available from many hobby shops and on Amazon.com. Included in this research is the use of a virtual lab where the RPi is attached using an Ethernet connection. Simple attacks are carried out with a few suggestions for preventing this scenario from playing out in the real world.**

***Keywords*—Penetration Testing; Black Box; White Box; Modified Linux; Raspberry Pi (RPi); Kali Linux**

I. Introduction

The RPi is a system board that runs on the ARM architecture and includes Raspbian, which is a modified version of Debian. The board is used for many purposes and is very popular in the maker community. Notable projects include a DIY cell phone, Quadcopter, and Smart Mirror [1]. While not released or designed with malicious intentions in mind, the RPi can nonetheless be used for such purposes. The system is an ARM computer, which can draw upon the freely available Linux ecosystem to install additional applications, such as those included in the Kali Linux system image, which will be used later in a demonstration.

II. Raspberry Pi

A. Raspberry Pi Form Factor

The RPi is roughly the scale of a credit card which allows the Penetration Tester (pen tester) to leverage the size in an on-site install. For example, the board could be mounted in a real Cisco switch or hub with the RPi plugged into a port [2]. The RPi could also be fitted into a power brick such as those used for printers or a fully functioning power strip. The advantage is that no one is likely to question or inspect a legitimate looking piece of networking or office equipment in the day-to-day bustle of the modern fast paced world environment. Left undisturbed and a constant power source, the RPi could sit on a network until discovered or malfunctions, which could be several months or longer. The pen tester could even implement a TXT system that executes commands [3].

B. Raspberry Pi Specifications

For its size and price, the RPi offers the power that a pen tester would need from an onsite drop box. A drop box is a term used for describing a computer system that is temporarily installed on site in which the tester uses to carry out the attack. An example of a drop box Operating System is PwnPi, which like the ARM version of Kali Linux, is intended for the Raspberry Pi [4]. The RPi v3 has a Quad-Core Cortex-A53 CPU @ 1.2Ghz, 1GB RAM, 1x Fast Ethernet, 802.11N, Bluetooth, and HDMI. See **Figure 1** [5].

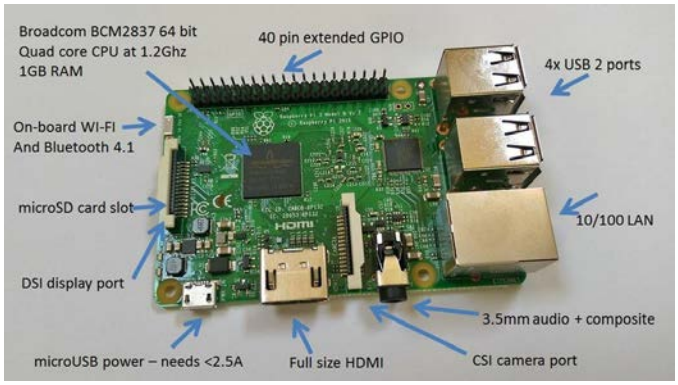

Fig. 1. RPi Overview [6]

III. Penetration Testing

A. Kali Linux

Kali is Linux distribution that is focused on penetration testing and includes several hundred open source tools crafted to the task of a pen test. The distribution is available for download and has specific versions such as those for the RPi and Motorola Nexus platforms. Kali's predecessor was Backtrack which was a convergence of three other pen testing distributions [7]. Both Kali and now the defunct Backtrack have a patched kernel to support Wi-Fi injection, which is the process of spoofing packets, so they appear to that of regular network traffic. The process of getting Kali Linux on a Secure Digital (SD) card is straightforward and not complicated, but not covered in this paper. The process mostly involves transferring a Kali Linux system images to the SD card and booting up the RPi to update and install packages.

B. White Box

White box pen testing is an authorized security audit of a system(s). Prior knowledge has been granted, and the appropriate assurances are in place for either an inside person or a third party to try and hack or assess the target. White box testing is "overt" [8] in the sense that since prior authorization

has been granted and the companies IT personnel know you are coming, the attacker can be as loud and visible as need be to perform the assessment. In other words, the attacker can run deafening attacks such as port scanning and brute forcing.

C. Black Box

This form testing is the opposite of White Box. An attacker who is performing a Black Box pen test needs to have stealth and not have their cover blown. Access has been granted by those at the top of the company, but lower level employees are not aware. For example, an agent participating in this type of test is bound by law but has been given permission to enter the building to try and infiltrate a system or network. An attack vector might be for the agent to bring an RPi onsite and find a good Ethernet jack. The agent would then hook up and hide the RPi using the methods discussed earlier. The agent could then communicate with the machine either through the Internet, TXT messages or SSH for example, or locally via Wi-Fi.

IV. Lab

For our research and demonstration of pen testing, a home lab was set up. The lab consists of six Virtualized Machines (VMs): 1x Windows Server 2012, 1x Windows 8, 1x Windows 7 and 3x Windows XP. The host computer is a Windows 10 eight-core system with 16GB of RAM. For DHCP, a hardware router hands out both static and dynamic IP's in the 172.16.42.1/24 range. A hardware managed switch is used with one Ethernet running from the host to the switch, all of the VM's are set to bridge the one Ethernet connection. The raspberry pi will be the attack and configure to establish a connection out of the network to a relay machine. See **Figure 2**.

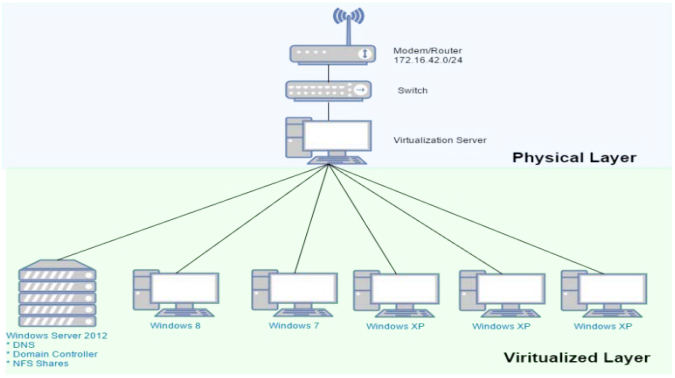

Fig. 2. Lab Network Layout

A. Boise Automotive Repair Group (BARG)

For our research, a fictitious company, BARG, was created. BARG is currently a one site facility with five employees. The employees are a CEO, VP, Sales Manager, Office Personnel and Accounting Manager. BARG does not have a dedicated IT staff, rather the company's IT is outsourced to an unnamed company. The outsourced IT company supplied BARG with five machines and a Windows Server 2012.

B. Attack Senarios with Bring Your Own Device (BYOD) and Small Business

Tacitly it is known that most small businesses have a small budget. To reduce cost and increase employee happiness [9] a company may wish to institute a BYOD policy. Such a system will allow and encourage company employees to bring their technology into the business setting to access company information; sometimes that information may be critical such as confidential records, databases, etc. BYOD devices will need a way to access this information, usually via Wi-Fi or Ethernet. The RPi has both Ethernet and Wi-Fi.

V. Hacking Phases

There are five phases of hacking: Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Cover Tracks [10]. During phase one, the hacker may employ various reconnoitering tactics. For example, the attacker may dumpster dive, physically visit the victim, search the Internet for information, etc. The second phase involves using tools that scan the victim from the Internet or internally on the LAN for vulnerabilities or open ports. The third step involves taking information such as vulnerabilities found and exploiting them. An attacker may use custom code premade exploits or even a Denial of Service (DoS) or Buffer Overflow, the attacks might be active or passive [11]. The fourth phase involves actions an attacker would use to keep the new access to the machine or network as long as it is needed. A backdoor such as Trojan might be utilized. The fifth and last step involves steps the attacker would use to erase evidence that an intrusion occurred. Evidence can come in many forms such as system logs, packet captures, binaries, etc.

VI. Attack on BARG

In our research, we will assume that BARG has gone to an outside source and hired the services of a security consultant. BARG's CEO agrees that a small scale black box test would be needed to understand the need for tighter information security controls. The expert hired for the job, hereafter "the attacker," argues that by exposing the bad security practices, management at BARG will be motivated to spend the limited money they have to increase their network and computer security. Before the consultant was hired, BARG instituted the BYOD policy, and all employees were allowed to attach their technology via wired or wireless access. Since this is a black box test, the consultant does not know anything about BARG's network or computers.

A. Phase 1 – Reconnaisance

Upon cursory inspection during a site visit posing as a customer, the attacker notices several Ethernet and power jacks that he could use to plug in and power an RPi. For example, a VOIP phone often has a USB and Ethernet ports. An attack route is identified, and the attacker prepares the RPi. After the RPi is set up, the attacker returns to the BARG office and poses as a custodian and is not questioned by the staff as they leave for the day. Dressing the part and having a believable story is an example of social engineering as people

are often more trusting of a person if they are dressed in the appropriate attire and look official. The RPi is installed and set to create a reverse SSH tunnel [12] to an intermediary under the control of the attacker.

B. Phase 2 – Scanning

Nmap and Metasploit are two open source pen test tools that are user-friendly. Nmap is a port scanner with various scan profiles such as "Stealth" and scanning of all ports on a host, not just the regular 1000 that are usually examined. Metasploit is a framework that includes the ability to execute exploits on vulnerabilities and more. The structure also includes the Meterpreter shell which can connect back from the victim to the attacker. From the RPi, Nmap can be used, and the results can be written to file, See **Figure 3**.

Scanning is about information gathering, so the attacker will want to know as much as possible about the network and the computers connected. One way to fingerprint the Operating System that the computer is running is via the Server Message Block (SMB) protocol that Windows uses to communicate with other computers on the network. SMB can be used for file sharing and printing, among other tasks. SMB runs at the application layer or presentation layer. Metasploit has a module for this purpose, see **Figure 4**. From the scan, we can see that one of the computers is running Microsoft Windows XP SP3 which has since been unsupported by Microsoft, which could mean that this equipment is not properly patched. Unpatched systems can contain vulnerabilities that could be exploited.

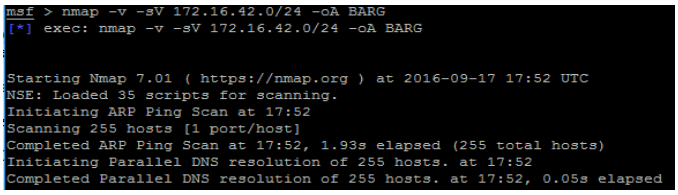

Fig. 3. Using Nmap in Metasploit

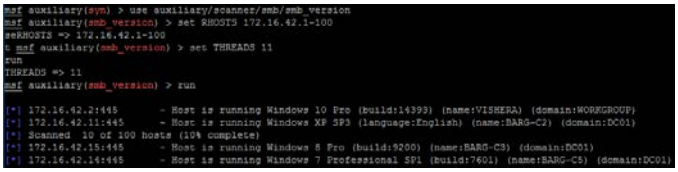

Fig. 4. SMB Version Scan from Metasploit

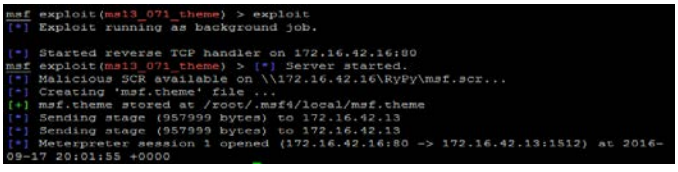

Fig. 5. Exploiting MS13_071 to Gain Access

C. Phase 3 – Gaining Access

The attacker gained access to the Windows XP machine using MS13-071, which is detailed in a security bulletin on the Microsoft website [13]. This exploit relies on a vulnerability in how Windows handles theme files in Windows XP and Windows Server 2003. The vulnerability specifically occurs when an item is specially crafted to call a malicious screensaver file, which can be a backdoor or virus [14]. The theme file can be stored on a network share where a user can be socially engineered to install the theme. Other social engineering examples are posing as a member of IT in which the user is instructed to launch the file, spamming or phishing the file via email and so on. For the exploit to be successful, the theme needs to be run by the user and cannot be executed remotely. Once access is gained, Meterpreter offers complete control of the machine. The attacker can create, delete, modify files, take screenshots, and so on. See **Figure 5**.

D. Phase 4 – Maintaining Access

The attacker may want to have a persistence backdoor to the system where if the user reboots the machine or loses connection, a shell will reopen, allowing the attacker to continue to compromise the computer. Using the shell access gained earlier, Meterpreter offers a persistence option that starts a reverse Multi-Handler on the port specified, generates and uploads a Visual Basic file and modifies the system registry to auto launch the connection. The persistence program offers the ability to customize the port, the location of the payload, the interval a new connection is established and the IP address of the attacker's machine. Uploading and executing files are two standard features using Meterpreter. So another way to maintain access might be to upload another program like NetCat or a separate payload that is encrypted and thus undetectable. See **Figure 6**.

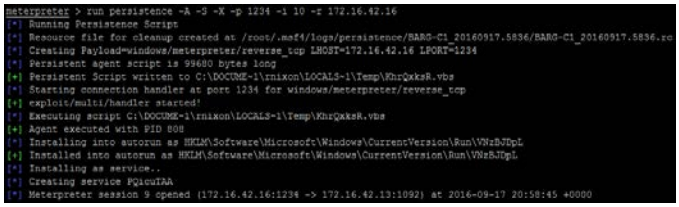

Fig. 6. Manipulating the System for Persistence Backdoor Access

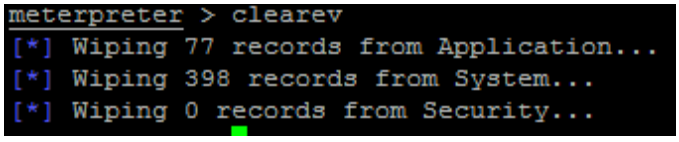

Fig. 7. Clearing the System Logs

E. Phase 5 – Erase Evidence of a Break-in

The final step of hacking involves the attacker erasing condemning evidence that the attacker was on a system or network. This last step is crucial as after a hack is discovered the first step is to image servers or computers to keep this data from being seen or recovered. The shell, previously opened, Meterpreter has a command, "clearev" which will delete the Windows logs including Application, Security, and System. Other actions the attacker may want to take is closing connections, wiping the attacking system, keeping communications to a minimum, etc. See **Figure 7**.

VII. Risks of a Relaxed Computer and Network Security Posture

The fictional company BARG hired a security consultant to help assess its security posture. However, many small

businesses do not have the funds to provide this service and may view it as a luxury to be able to have an expert come in. In fact, some small business may rely on family friends or the in-family "expert" to help set up the IT. The problem with this method, while cost effective, is that this person may not have the training or expertise to set up a proper small business network. Rather, the setup is a home network that is used for business. Setting up this way exposes the company to huge risks that at its worst can destroy and financially harm the business. For example, in 2013, CryptoWall, a malware that encrypts user files and demands a ransom payment, had over twenty-two thousand infections [15]. The cost of an infection of CryptoWall can be staggering, especially if the business didn't properly maintain backups.

VIII. Prevention

A. Network Isolation

One reliable avenue for prevention and protection in computer networking is network isolation. In the case of BARG, a first step might be separating conventional work computers and those that may have a connection to a guest Wi-Fi. Going further, BARG could implement VLANs for those work computers that hold especially sensitive data such as accounting, payroll, and customer databases.

B. User Education

Educating users on the importance of what viruses and malware are and their effects is tantamount. In the case of BARG, if the payroll computer was infected in 2013 with CryptoWall, there is little recourse but either restore from backups if they have them or pay the ransom as not doing so leaves the payroll data in an unusable state. Phishing is a grave threat to any company and some services such as https://knowb4.com can simulate Phishing to educate users. Uneducated users and weak network security only enhance malware such as CryptoWall's ability to infect and encrypt important files. Updating the firmware of devices is another preventative measure that can keep attackers, inside and outside of the network from exploiting vulnerabilities.

C. Backups

Properly verified backups can keep a company from experiencing the worst day of its existence or just become a disruption. Everybody, including everyday users, should have a scheduled backup system in place, not only to guard against intruders, malware, and viruses but also to cover for unexpected events including fires and flooding. For BARG, a Network Attached Storage (NAS) with disk redundancy and physical or cloud offsite backups would help protect vital information.

D. Physical Security

In the case of BARG, where the attack vector was the initial install of a miniaturized computer, physical security is one way to prevent this from occurring, but admittedly hard when you are an auto repair facility with customers coming in and out. Cameras offer a vital option as a deterrent as well as vigilant staff to ensure that if something looks out of place, bring it to the attention of IT.

IX. Conclusion

In conclusion, the RPi is an example of a physical device that once attached to a network can reconnoiter, attack, pilfer and hack into devices via Metasploit and other tools. The size of the RPi is advantageous to an attacker because the unit can easily be disguised in power bricks, hidden behind plants and desks. Unknowledgeable users are unlikely to question the device so long as the installation does not cause problems or is incredibly evident. As computers continue to miniaturize, the threat will grow. And as technology is ubiquitous today, every business has an interest in having the right controls and procedures in place such as backups, user education, upgrading and maintaining hardware and software.

References

[1] Crider, M. (2016, May 10). Think the Raspberry Pi is underpowered? Here's 10 projects that prove you wrong. Retrieved September 15, 2016, from http://www.digitaltrends.com/computing/raspberry-pi-projects/

[2] Muniz, J., & Lakhani, A. (2015). Penetration Testing with Raspberry Pi. Packt Publishing.

[3] Paganini, P. (2013, June 22). Raspberry Pi as physical backdoor to office networks. Retrieved September 15, 2016, from http://securityaffairs.co/wordpress/15471/hacking/raspberry-pi-as-physical-backdoor.html

[4] Abramov, E., Kobilev, M., & Makarevich, O. (2013, November). Using quadrocopter as a pentest tool. *In Proceedings of the 6th International Conference on Security of Information and Networks (pp. 404-407)*. ACM. Chicago

[5] Raspberry Pi 3 is out now! Specs, benchmarks & more - The MagPi Magazine. (2016, March 12). Retrieved September 16, 2016, from https://www.raspberrypi.org/magpi/raspberry-pi-3-specs-benchmarks/

[6] Scargill, P. (2016, March 01). Scargill's Tech Blog. Retrieved December 25, 2016, from http://tech.scargill.net/raspberry-pi-3-grand-opening/

[7] Ali, S. (2014). *Kali linux: Assuring security by penetration testing*. Place of publication not identified: Packt Publishing Limited.

[8] Engebretson, P. (2013). The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier.

[9] Madzima, K., Moyo, M., & Abdullah, H. (2014, August). Is bring your own device an institutional information security risk for small-scale business organisations? In 2014 Information Security for South Africa (pp. 1-8). IEEE.

[10] Prasad, M. R., & Manjula, B (2014, November). Ethical Hacking Tools: A Situational Awareness. *IJETCSE SSN, 0976-1353*.

[11] Mortensen, Casey, Ryan Winkelmaier, and Jun Zheng. "Exploring Attack Vectors Facilitated by Miniaturized Computers." Proceedings of the 6th International Conference on Security of Information and Networks - SIN '13 (2013): 203-09. ACM Digital Libary. Web. 8 Sept. 2015. < http://dl.acm.org/citation.cfm?id=2527002&CFID=711358533&CFTOKEN=65687872>

[12] Jack. (2013, May 08). Raspberry Pi: Phoning Home Using a Reverse Remote Ssh Tunnel. Retrieved September 16, 2016, from https://www.tunnelsup.com/raspberry-pi-phoning-home-using-a-reverse-remote-ssh-tunnel

[13] Microsoft Security Bulletin MS13-071 - Important. (2013, September 10). Retrieved October 27, 2016, from https://technet.microsoft.com/en-us/library/security/ms13-071.aspx

[14] Vazquez, J. (2013, September 25). Change the Theme, Get a Shell: Remote Code Execution with MS13-071. Retrieved September 17, 2016, from https://community.rapid7.com/community/metasploit/blog/2013/09/25/change-the-theme-get-a-shell

[15] Jarvis, K. (2013, December 18). Cryptolocker Ransomware. Retrieved September 19, 2016, from https://www.secureworks.com/research/cryptolocker-ransomware