Portable Pen-testing Box

Saint Leo University
COM 497 - Capstone Project
Dr. Vyas Krishnan

Authors:

Hashim Alsalman , Khalid Alalshaykh,

i. Introduction

Portable Pen-testing Box, What is it?

It is penetration testing tool that is using Raspberry Pi 2 as a core hardware component for implementing the maximum capabilities, which other pen-testing tools may not reach. Mobility is a main subject in this small device, since it gets its power through micro-USB input like many smart phones do.

ii. Hardware

What is Raspberry pi 2?

RP2 model B is a credit card-sized single board computer. It was introduced in February 2015. It has:

- A 900MHz quad-core ARM Cortex-A7 CPU
- 1GB RAM
- 4 USB ports
- 40 GPIO pins
- Full HDMI port
- Ethernet port
- Combined 3.5mm audio jack and composite video
- Camera interface (CSI)
- Display interface (DSI)
- Micro SD card slot
- VideoCore IV 3D graphics core

Device Name	Device Description	Cost
Raspberry pi 2	*Single board computer	$35
Wireless Adapter	Realtek 8191 300Mbps 802.11n/g/b USB Wireless WIFI LAN Network Card Adapter	$8.50
SDHC Memory	32GB UHS-I/Class 10 Micro SDHC Memory Card Up to 48MB/s	$9.99
PiTFT	3.5" display with 480x320 16-bit color pixels	$44.99
Charger Power	AA Battery Portable Charger Power Pack Power Supply	$9.99
Case for RP2	Clear Case for Raspberry Pi 2 Model	$9.50
Remote Control Keyboard	Raspberry pi Mini Wireless Handheld Remote Control Keyboard with Multi-Touch Touchpad	$8.50
	Total Cost	$126.47
	Total without case, PiTFT, RC Keyboard	$63.48

Challenges**:**

- Raspberry pi 2 is just released so we had to wait long time to get it.
- Finding the best in the market with affordable price
- We had to buy several touchscreens to find the one that works perfectly with new Raspberry pi 2

iii. Software

This section will cover only the fundamental software and application that are related to penetration testing, drivers and some additional software are not listed.

Operating System

- Raspbian OS
- Debian wheezy
- Kernel version:3.18
- Copy : 2015-02-16
- Free operating system based
- Comes with over 35,000 packages

Challenges:

- Dealing with Linux based system and learning its commands.
- We had to install and test several operating systems before we decide which one is the best to the project.
- Raspbian OS just released its version that supports Raspberry pi 2, so we faced some bugs and problems.

System Management

1. Webmin :

Web-based system configuration tool for system administration. Using any web browser, it is easy to setup user accounts, Apache, DNS, file sharing and more other tasks.

Version: 1.740

Dependencies:

- perl
- libnet-ssleay-perl
- openssl
- libauthen-pam-perl
- libpam-runtime
- libio-pty-perl
- apt-show-versions
- python

Download Link:

- http://prdownloads.sourceforge.net/webadmin/webmin_1.740_all.deb

Challenges:

- Long process to install and configure.
- Not assessable from outside the network, PageKite solved the problem.
- A problem related to the SSL, solved by disabling it.

2. PageKite :

A reverse proxy tool that connects the PI2 to the public Internet. It makes it possible to connect to the PI2 from anywhere even if it connected to a privet network with dynamic IP.

Version: 0.5.4

Dependencies:

- python-socksipychain (>= 2.0)

Download Link:

- http://apt.he.pagekite.me/

Challenges:

- Long process to configure.
- Writing and editing files to make it works properly.

3. Postfix :
   Mail transfer agent (MTA), makes it possible to send emails directly from the command line using Gmail SMTP configurations.

Version: 3.0

Dependencies:

- mailutils
- libsasl2-2
- ca-certificates
- libsasl2-modules

Challenges:

- complicated, hard to configure.

Penetration Testing Tools

1. OpenVas:
   Services &Tools for vulnerability scanning and vulnerability management

Version: 7.0.4

Dependencies:

- libmicrohttpd-dev
- libxml2-dev
- xsltproc
- libxslt1-dev
- pkg-config
- flex
- cmake
- libssh-dev
- sqlite3
- libsqlite3-dev
- libgnutls28-dev
- libgcrypt11-dev
- libglib2.0-dev
- libpcap-dev
- libgpgme11-dev
- uuid-dev bison
- libksba-dev
- nmap

- rpm
- doxygen
- libgnutlsxx27
- libgnutls-dev
- libghc-gnutls-dev

Download Link:

- http://wald.intevation.org/frs/download.php/1722/openvas-libraries-7.0.4.tar.gz
- http://wald.intevation.org/frs/download.php/1726/openvas-scanner-4.0.3.tar.gz
- http://wald.intevation.org/frs/download.php/1730/openvas-manager-5.0.4.tar.gz
- http://wald.intevation.org/frs/download.php/1734/greenbone-security-assistant-5.0.3.tar.gz
- http://wald.intevation.org/frs/download.php/1633/openvas-cli-1.3.0.tar.gz

Challenges:

- No clear instruction found, very advance tool.
- Very long process installing and configuration.
- Not programmed to work in Raspbian OS, so we had to do a lot of file changes, write new codes, and create new files.
- Dependencies files and applications needed some changes.
- Takes time to load.
- A new version released that needed new dependencies.

2. Metasploit:
   Exploit development framework.

Version: 4.11.1

Dependencies:

- build-essential
- libreadline-dev
- libssl-dev
- libpq5
- libpq-dev

- libreadline5
- libsqlite3-dev
- libpcap-dev
- openjdk-7-jre
- subversion git-core
- autoconf
- postgresql
- pgadmin3
- curl
- zlib1g-dev
- libxml2-dev
- libxslt1-dev
- vncviewer
- libyaml-dev
- ruby2.2.1
- nmap
- pcaprub
- wirble
- pg
- sqlite3
- msgpack
- activerecord
- redcarpet
- rspec
- simplecov
- yard
- bundler
- pcaprub

Download Link:

https://github.com/rapid7/metasploit-framework.git

Challenges:

- No clear instruction found, very advance tool.
- Very long process installing and configuration.
- Not programmed to work in Raspbian OS, so we had to do a lot of file changes, write new codes, and create new files.
- Dependencies files and applications needed some changes.
- Takes time to load.
- A new version released that needed new dependencies.

- The new version nedded Ruby version 2.2.1 which doesn’t work in Raspbian OS, se we had to install Ruby version 2.2.1 manually and that caused a lot of problem with other applications installed previously. Each application edited to take the old Ruby.

3. Nmap:
   Is a security scanner.

Version: 6.47

Dependencies:

- fontconfig
- fontconfig-config
- fonts-droid
- fonts-liberation
- ghostscript
- gnuplot
- gnuplot-nox
- groff gsfonts
- hicolor-icon-theme
- imagemagick
- imagemagick-common
- libavahi-client3
- libavahi-common-data
- libavahi-common3
- libblas3
- libblas3gf
- libcairo2
- libcroco3
- libcups2
- libcupsimage2
- libdatrie1
- libdjvulibre-text
- libdjvulibre21
- libexiv2-12
- libfontconfig1

Challenges:

- Understanding and doing the installation process.

4. Wireshark
   Packet sniffer/analyzer.

Version: 4.7.2

Dependencies:

- build-essential
- automake
- autoconf
- libgtk2.0-dev
- libglib2.0-dev
- libpcap0.8-dev
- flex
- bison

Challenges:

- Understanding and doing the installation process.

5. TCPdump
   Packet sniffer/analyzer.

Version: 4.7.4

Dependencies:

- Directly installed

Challenges:

- Understanding and doing the installation process.

6. Tshark
   Packet sniffer/analyzer.

Version: 4.7.2

Dependencies:

- Directly installed

Challenges:

- Understanding and doing the installation process.

7. Netcat:
   A network analysis tool

Version: 1.10

Dependencies:

- ○ Directly installed

Challenges:

- Understanding and doing the installation process.

8. MTR
   Network diagnostic tool

Version: 0.92

Dependencies:

- ○ Directly installed

Challenges:

- Understanding and doing the installation process.

iv. Scanning script

We coded a scanning script that described as following:

- ○ Bash script
- ○ Scan the network looking for live hosts IPs.
- ○ Create file contains the Live IPs.
- ○ Create targets on OpenVas based on IPs.
- ○ Create separate scanning task for each target.
- ○ Start each scanning task.
- ○ Send email contains the result of each scanning task (if it contains vulnerabilities only)
- ○ Added as cron job, to work once a day.

Challenges:

- Learning Bash scripting

- Learning XML
- Scan the network for live IPs and get the result as quick as possible, solved by using ping with specific parameters
- Communicating with OpenVas using bash script.
- Storing XML files and getting specific information from them.
- Handling errors.

v. Connection

The Portable Pen-testing Box can be accessed remotely using several types of connections as following:

- Webmin : wm.com497.pagekite.me
- SSH : ssh.com497.pagekite.me
- OpenVas : ov.com497.pagekite.me

vi. Conclusion

Raspberry Pi 2 offers a lot of features that attract computer science majors. Its small size, low-cost, and capabilities make it very powerful tool for penetration testing. Although installing applications on it is not as easy as it is in the other known operating systems, it is still very stable and efficient.