Malware Analysis (CS6038)

Week 02.2 Malware Labs cont. & Sandboxing

Scott Nusbaum
nusbausa@ucmail.uc.edu

January 24, 2019

University of CINCINNATI

Overview

- Homework 1
- VirtualBox Networking
- Kali Linux
- Metasploit
- Sandboxing
  - Cuckoo
  - VirusTotals

University of CINCINNATI

Homework 1

- Assignment
- Due Feb 7, 2019

University of CINCINNATI

VirtualBox Networking

- Demo:
  - Review the GUI Networking settings

University of CINCINNATI

Kali Linux

- https://www.kali.org/

Kali Linux[3] is a Debian-derived Linux distribution designed for digital forensics and penetration testing.[4][5][6][7] It is maintained and funded by Offensive Security Ltd. It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of BackTrack, their previous information security testing Linux distribution based on Knoppix. The third core developer Raphaël Hertzog joined them as a Debian expert.[8][9][10][11][12]

University of CINCINNATI

Demo Kali Linux

- Overview of Kali Installation
- Walk through some of the different programs installed by default
- Show how to change password
- Show how to update the install packages
- Show how to set a static IP address
- Show how to use Metasploit
- Show Wireshark and communication between guests
- Snapshot

University of CINCINNATI

Sandboxing

In computer security, a "sandbox" is a security mechanism for separating running programs, usually in an effort to mitigate system failures or software vulnerabilities from spreading. It is often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users or websites, without risking harm to the host machine or operating system.[1] A sandbox typically provides a tightly controlled set of resources for guest programs to run in, such as scratch space on disk and memory. Network access, the ability to inspect the host system or read from input devices are usually disallowed or heavily restricted.

In the sense of providing a highly controlled environment, sandboxes may be seen as a specific example of virtualization. Sandboxing is frequently used to test unverified programs that may contain a virus or other malicious code, without allowing the software to harm the host device.[2] Wikipedia

University of CINCINNATI

Sandboxing

- Local
  - Single Standalone VM
  - Cuckoo
- Online
  - VirusTotal
  - Hybrid Analysis

University of CINCINNATI

Stand Alone Sandbox

- Demo DevWin7

University of CINCINNATI

Cuckoo Sandbox

- About Cucko Sandbox
- Setting up Cuckoo
- Cuckoo with ProxMox

University of CINCINNATI

Demo Cuckoo

- Walk through the UI
- Submit Malware sample
- Walk through result
- Open VM after to see or extract artifacts

University of CINCINNATI