heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

Seoul National University
College of Engineering
Dept. of Computer Science and Engineering

Introduction to Social Networks

Summer University 2017
Seoul, Republic of Korea

Alexandre Karlov

Swift Tools

Tools

- So what are the best tools to be an ultimate hacker ?
- Which OS to use ? Windows, Linux or OSX ?
- Will go through some of them during these days

Recommendations

- What do you use?
  - Windows
  - Linux
  - OS X

- Recommendation is to have all three of them, or at least Windows and Linux
  - Don't think of them as different operating systems
  - Think of them as set of tools
- Setup a virtualized environment on you machine (VMWare)
  - Deploy images of Windows and Linux boxes so that you can easily switch between
- Today's average Portable PC
  - Can easily run several OS in parallel
  - Images allow easily to backup, roll-back and deploy a fresh/clean version of the OS (especially relevant for malware analysis)

Kali

- The Kali linux distribution which superseded historical BackTrack (BT) linux is seen as a de-facto standard platform to help you with your pentest tasks
  - Debian-based distribution
  - More than 300 tools for pentest and data forensics
  - Active online support community

If you are an Arch Linux fan, you might want to give BlackArch a try

Kali

- Download from www.kali.org
  - Either an ISO from http://www.kali.org/downloads/
  - VMWare image from http://www.offensive-security.com/kali-linux-vmware-arm-image-download/
    - Download, unzip (7z x Kali-Linux-2017.1-vm-amd64.7z) and open the image in VMPlayer
    - default username and password: root/toor
    - remember to change the root password
    - apt-get update && apt-get upgrade

Kali - non root user

- When installed, Kali linux uses root user for all tasks
- It is a good security practice to add an additional user with non-root privileges
  - **useradd -m noroot**
    passwd noroot
    usermod -a -G sudo noroot
    chsh -s /bin/bash noroot
  - Replace the **noroot** by whatever you prefer

Kali - Install Multiarch support

- By default Kali comes with 64 bit architecture
  - sudo dpkg --add-architecture i386
    sudo apt-get update
    sudo apt-get upgrade
  - Enables 32-bit support
  - Useful for applications supporting only 32-bit

pwntools

- a framework for CTF and exploit development
- allows rapid prototyping and development
- client-server interaction
  - to interact with all kind of services (web, binary, etc...)
- process interaction
- assembly and elf manipulation
- GDB debugging helpers

pwntools

- Go read:
  - http://docs.pwntools.com/en/stable/index.html
    - or if you prefer a PDF:
      - https://media.readthedocs.org/pdf/pwntools/stable/pwntools.pdf
- Online demo:
  - https://demo.pwntools.com/