Intro to Metasploit

Who am I

- Trevon (blackmanta)
- Graduate Student
- Linux Junky
- HackerNews Lurker

Announcements

https://github.com/49thSecurityDivision/EducationScripts

What is penetration testing

What is Metasploit

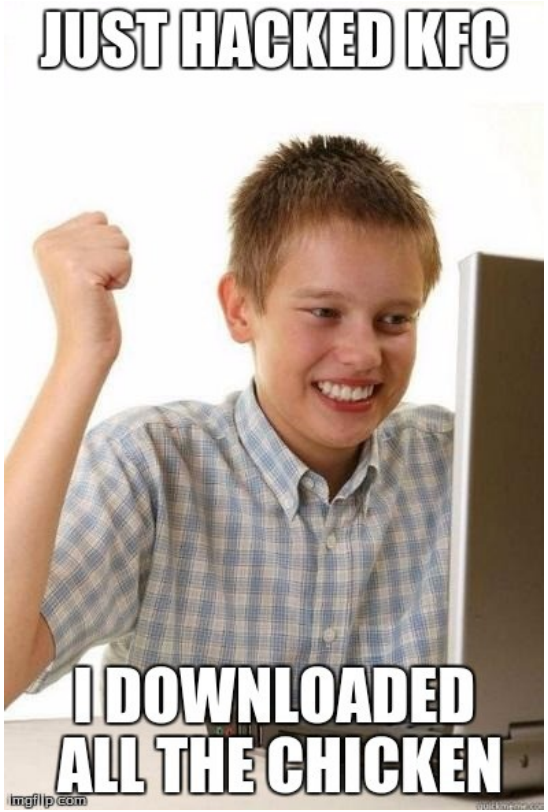
- Security tool and Framework
- Pentesting Aid

Similar Tools

- Web focused
  - Burp Suite, OWASP Zap, BeEF
- Vulnerability assessment
  - Cobalt Strike, OpenVas

Understanding Vulnerabilities

- Bugs in programs
- Vulnerability != Exploit



Why use these tools?

Enter Vulnhub

- Need practice?
  - https://www.vulnhub.com/
  - Metasploitable 3
- Machine for personal practice
  - bossplayersCTF

How to start

- Install metasploit
  - Getting started with metasploit (install vagrant on host machine)
    - vagrant init rapid7/metasploitable3-win2k8 --box-version 0.1.0-weekly
    - apt install metasploit-framework msfpc armitage
- Configure networking

Metasploit continued

- Armitage is the GUI version
- In terminal
  - sudo msfdb init
  - sudo systemctl enable postgresql

Configuring networking

- Connect Host-only adapter
  - For debian VM and metasploitable 3
    - **METASPLOITABLE USES NAT NETWORKING BY DEFAULT, PLEASE CHANGE TO HOST-ONLY**
- What is the IP for metasploitable 3
  - ipconfig (windows)
  - ifconfig or ip addr (linux)
    - *The ip range is important to note*
    - *Can you ping the host?*

Start the pwn

- Scan ip of machine
  - Using nmap
    - Port Scanner
    - Network Mapper
    - nmap -sVC -O -T4 [HOST IP]
      - NMAP Cheat Sheet
      - Assuming target is up

Resources

- Awesome Pentest Resource list
- Awesome Hacking Resource list
- Pentest Monkey
- Vulnerable Virtual Machines