MSF Into The Worm Hole Outline

#MSFIntoTheWormHole Outline

1. MSF Into The Worm Hole
    a. Intro
    b. History of MSF

i. NetPen

1. ii. WebPen
    c. MSF Parts
    i. Exploits
    ii. Payload
    iii. Shellcode
    iv. Modules
    v. Listeners
    vi. Auxiliary Modules
    vii. Plugins
    1. WMap
    2. SET
        a. Web Attacks
    viii. Utilities

1. MSFpayload
        a. **Mini Lab**
2. MSFencode
        a. **Mini Lab**
    d. Information Gathering
    i. Scanning with NMap

1. LAB

    ii. Port Scanning With MSF
    iii. Targeted Scans

1. SMB scanning
2. SQL scanning
3. SSH scanning
4. FTP scanning
5. SNMP scanning
6. **LAB**
    e. Vuln Scanning With WMap
    i. **LAB**

    f. Auxiliaries and Me
    i. Current HTTP or Web related Auxiliaries
    ii. How to build
    iii. Write custom aux scanner
    iv. **LAB**

1. Understanding the structure

a. How do we leverage the MSF api?
b. Requirements

i. msf/core
ii. define module types and add options
iii. define options/auxiliary functions

2. Where do we store our custom auxiliary?
   a. How do we load?
3. Run
   a. Run against target ***.***.***.*** port 31337
   g. Client-Side Attacks
   h. Browser Exploits
   1. What happens in a Browser exploit?
      a. NOPs
   2. Debugging a Browser NOP slide
   3. How this works in the real world
      a. Aurora Exploit
   4. Building a Browser exploit
      a. "LAB"
   i. I will be doing the live walkthrough, class will not actively be doing the same

3. h. XSSF (Cross-site Scripting Framework)
   i. What is it?
   ii. How to install on Kali 1.0 and Install
   iii. How do we use it

1. Create Custom Java Applet exploit
2. Create XSSF page
      a. Launch custom java while page is still active
   iv. **"LAB"**
   j. SQLMap and Metasploit
   i. What is SQLMap?
   ii. How do I use it?
   iii. **"LAB"**

1. sqlmap --os-pwn
   k. What did we learn?
   l. Closing
2. Open lab for anyone that wants to play