RF's Guide to Dumping Your PS2 Bios over LAN

Below you will find my guide on how to dump your PS2's BIOS over LAN. There isnt any tutorials around, and it took me a good while to write this.

First of all I know there are other ways of doing this, but this is the way it worked best for me Please leave any comments or questions you may have, as I will do my best to make anything you dont understand more clear or re-word steps etc.

Also, most of this can be found through google. However lots of sites have links to modchips/warez etc so please no links. I would like to thank all the great ps2 dev's and the ps2 community for providing lots of info.

A downloadable copy of this guide is attached to the first post, all files included in the first post are freeware and freely distributable.

Dumping Your BIOS over LAN

What You Will Need

1. An 8mb memory card (An official Sony memory card is preferred with atleast 1mb free)
2. A Ethernet Adapter (The adapter with both Ethernet and Dialup ports is preferred)
3. A router setup to use static IP’s
4. A CD-Writer + one CD-R
5. A Retail Playstation (NOT A PS2) game.

What This Guide Will NOT Cover

1. Modchips and how you will boot your custom code onto your ps2.
2. How to setup your LAN with static ip’s

Table of Contents

1. General Overview

Much of the information is easy to find if you just do a Google search for the big stuff such as the memory card exploit (aka Independence Exploit), however I am unable to post these sites as they often do contain links to things such as modchips etc that we do not support here on NGEmu. Before starting you will need a way such as a modchip or swapdiscs to boot custom code on your ps2. We will be burning a custom disc to cd-r in this tutorial so if you have no way to boot it on your ps2, then all your work will be in vain.

---

2. Memory card Exploit

What this will allow you to do is upload custom executables (.ELF) files to your ps2 and execute them.

A) First look at your psx disc and note the disc ID. The disc ID will be in the format SLUS-01473, and will be on both the case and the cd itself.

B) Now create a folder on your hard drive to keep all the exploit files in. For this example we will use C:\PS2Exploit. After that is downloaded, grab the MemcardExploit.rar below and extract it to your folder.

C) After extracting you should see CDGenPS2.exe, titleman.exe, TITLE.DB, and the Exploit folder. Open a command prompt and switch to that directory.

Code:

```
Opening a command prompt.
        Start > Run > cmd > OK
Changing To the Directory
cd \
cd PS2Exploit
```

D) In the prompt type “titleman –a XXXX-XXX.XX” without quotes, and instead of X’s use your disc ID. For example I used Rainbow Six: Lone Wolf as my playstation game so I typed in SLUS_014.73. If you did it correctly it will say it is done.

Note: Sometimes depending on your psx game you will have to use a dash instead an underscore in your disc ID. If you aren’t sure, it dosent hurt to repeat step D with another disc ID.

E) Close the cmd prompt and copy your TITLE.DB to the Exploit folder. You should now have in the Exploit folder the Files folder, EXPINST.ELF, CDVD.IRX, and a SYSTEM file (SYSTEM.CNF, but Microsoft hides the CNF extension).

Note: To check if your TITLE.DB is correct, open it within wordpad or notepad and take a look. However, don’t edit this file as simply editing it in rich text will break it (I think).

F) Now go into the Files folder. BOOT.ELF is the execuatable that is booted each time the exploit is run. For now this is set to ps2menu, but you can use whatever file management app you would like. I just happen to use ps2menu myself.

Now open CONFIG.DAT with notepad or wordpad. You will see three IP addresses that you will need to customize to your own lan. The first is the IP address you want the PS2 to have. The second is the subnet of your lan. The third is the gateway or your routers ip.

G) Now go back to the main folder and locate CDGenPS2.exe and execute it. Now drag and drop the exploit files in the “Exploit” folder (Not the Exploit folder itself) into the right pane of CDGenPS2 (See screenshot below). This must be done in the following order:

1. SYSTEM.CNF
2. EXPINST.ELF
3. CDVD.IRX
4. TITLE.DB
5. FILES (Drag the whole folder)

Now on the left press the IMG button (the top one with a CD over it) and save your img somewhere to burn. Now use Alcohol120% to burn this image in **Mode2 Form1** and the writing method as **DAO/SAO**.

H) Now all that is left is to throw in your burned disc and boot it using any method you see fit. Make sure your memory card is in slot one and it should automatically install once it is booted. After it is complete it will say Finished! Now shut down your ps2 with the switch on the back, then turn it back on and eject your exploit cd.

I) Now put in your psx disc, after a few seconds you should see ps2menu! Read the top left corner so you can learn how to use ps2menu etc.

Note: Yes it was a lot of work, but its worth it. Now you have a way of browsing all the files you have on your ps2, backup game saves, transfer new or updated executables with execftps, and executing custom executables without having to burn more discs. All your elfs and files should stay in the BADATA-SYSTEM folder.

Update: Instead of PS2Menu you might want to give LaunchELF (Unofficial) a try. The latest version as of July 26, 2006 is v3.80 (Note: There are two versions of LaunchELF. The original LaunchELF was discontinued a long time ago, but was picked up by other authors and is now known as the "Unofficial LaunchELF").

---

3. Dumping the bios

For dumping your bios, everything you need can be found here: http://ps2dev.org/ps2/Loaders. Grab PS2Link 1.22 and XLink Beta 1.

A. Power on your ps2 and use ps2menu to browse to your BADATA-SYSTEM directory on your memory card.

B. Find EXECFTPS.ELF and hit X to execute it. If all goes well it should come up saying “FTP Server initialized on port 21…!”

C. Now open up your favorite FTP Application and ftp into your ps2. Any username/password combo will work. You should be presented with a mc folder. Double click into the mc folder and you will see a 0 folder. When you are inside your memory card, locate the BADATA-SYSTEM folder and create a new folder called ps2link.

D. Now use winrar to extract the ps2link_122.tar.gz archive you downloaded from ps2dev. Delete the licenses folder, and the README file to save the most space on your memory card.

E. Open the IPCONFIG.DAT from the ps2link_122.tar.gz with notepad. Just like before, fill out the ip information like we did above for the memory card exploit.

F. FTP all the files from the ps2link archive into the ps2link folder you created on your ps2 memory card. After the transfer is complete, turn the ps2 off with the switch at the back. Then boot back into ps2menu.

G. Once back into ps2menu, browse to the BADATA-SYSTEM folder and go into your newly created ps2link folder. Find and highlight the ps2link.elf and press X to execute it.

H. Once the ps2link server is started, unpack the xlink_win32_beta1.zip archive you downloaded from ps2dev.

I. When you open XLink it prompts for the ps2 ip information. Fill that in and press save. Next go to www.pcsx2.net and grab the dumpbios archive.

J. In XLink, make sure it says Connected at the top, then press Run. Locate your DUMPBIOS.ELF and set any options you would like (such as shutting down the ps2 after your file has been run).

K. Congratulations, after a few minutes you should have dumped your ps2’s bios! You also have setup your ps2 to run pretty much anything you throw at it.

Note: I take no responsibility for you breaking your ps2, burning bad cd’s etc.
