# Wargames server 1.0 The quest for root

**By Spoofed Existence**

June 18, 2003

The astalavista.net wargames server came online. The moment I have been waiting for for several weeks. And the moment I noticed the wargames server was online, I went to the site and read the rules. Right after this, I started to explore the system. The services opened on the wargames server were listed on a page:
- SSHserver
- FTPserver
- Webserver
- PHP
- Telnet
- MySQL database 3.23.56-1
- phpMyAdmin

I used telnet to have a look at the banners of the ports (the responses of the open ports). I searched for exploits for those ports, but nothing: For none of the ports where exploits. And MySQL could not be managed from my IP. My guess was the only thing that could manage it was "localhost".
Though, there was one service I have never seen before. I didn't know anything of it: phpMyAdmin. What was this service? Not long after -- by searching arround on Google -- I found it out. It was some sort of MySQL control center: You could execute MySQL commands. Restricted to the rights of the user you logged in with, that is.

But first, before I continued, I decided to download the scans. The scan results of the wargames server -- of both Nessus and Shadow Security Scanner -- were uploaded. No real good vulnerabilities came out, except for two. But for both, you needed write access to the disk, to a specific filename. These files where possibly exploitable:
/cgi-bin/htsearch
/cgi-bin/sdbsearch.cgi

So I went back to phpMyAdmin. I tried some weak passwords for the root user like "root", "password", etcetera. None of them, as I expected, worked. So I tried a random username (I knew that often a none-existing username with an empty password would work). It worked: I got in! I could execute MySQL commands. Restricted under nobody rights.
Ok, this could be useful! I played arroud and created a database called "test". Then I executed the following commands on in:
CREATE TABLE test (conf VARCHAR(80))
INSERT INTO test VALUES('test')
SELECT * INTO OUTFILE '/tmp/file' FROM test

Just to test whether I could write. Unfortunately, I did not have write access: Not even to /tmp/! And the SQL version they used wasn't able to read files either. I tried some phpMyAdmin exploits... No success either.

I got stuck, once in a while I came back and had a look. After playing around, I found out that the wargames server had the following directories:
- cgi-bin
- icons
- images
- phpMyAdmin

All you had to do to find out whether a directory existed was go to http://IP/directory/, where IP is the wargamesserver IP and directory the directory you want to test. If it threw a file-not-found 404 error message, the directory didn't exist.

And the following users:

- root
- news
- mail

(thanks about this, Minky).
Finding out what users existed wasn't too hard (If you know how it can be done). You just had to go to http://IP/~username/, where you replaced IP with the wargamesserver IP and username with the username you want to know whether it exists. If it existed, it threw an "access denied" message. If it didn't exist, it threw a file-not-found 404 error.

But I didn't find anything more. I got stuck. My IP address didn't show up in the wargames server netstat list anymore, unless if I wanted to check whether it had been hacked yet.

But, probably, it became really silent arround the wargames server. I read a topic about Samba: It was installed to the wargames server. And from this point, the level of the wargames server went from Hard, straight to very low. I knew what was meant to be. I searched for an exploit for Samba, and I found this file: http://www.astalavista.net/data/sambal.c.
I copied the text into a file, and compiled it:
gcc -o sambal sambal.c
And ran it:
./sambal -b 0 -v IP
where IP was the wargames server IP.
Though, it didn't work. It displayed the message: Host is not running samba!

"Oh, isn't it?!", I thought. I opened the source code using my favorite editor and commented the lines that threw this message, and after this exited the exploit. I compiled it again, and after a while I had a root shell account.

Well, great! I had a shell! But I prefered to use SSH simply because you can do a lot more, so I typed the following commands:
echo "SpoofedEx:x:0:0:root:/root:/bin/bash" >> /etc/passwd
echo "SpoofedEx:!:12209:0:1000:::" >> /etc/shadow
Both lines I didn't exactly remember, so I did a cat /etc/passwd and cat /etc/shadow to have a look how the root user looked like, and copied those lines. The only thing I changed was the second column of /etc/shadow. I changed it to "!" so that it had an empty password. Those lines created a root-user called SpoofedEx.

I started putty and connected. Entered my username, SpoofedEx with an empty password. DAMN! Empty passwords aren't allowed.
So I changed the password by typing the command "passwd SpoofedEx".

And again I started putty and I logged in with success.

The next step was to add my name to it. First I had to find the index.php page, so I typed:
find / -name index.php
And it appeared to be, as expected, in the directory /srv/www/htdocs/. Editing was simple:
cd /srv/www/htdocs/
vi index.php
I made my edits in the html page and pressed Control + C, and then: ":wq":
"File is readonly! Use ! to overwrite".
And a simple ":wq!" saved the file, and wrote it over the old file, even with read-only option turned on.

Note: Another way would be to do chmod +w index.php, then edit, and then change it back with chmod -w index.php.

That was the way I got in the wargames server. First it was really hard, but it became very easy -- even for script-kiddies -- to enter the server. And till the day of today, I do not know how the first "version" of the wargamesserver was meant to be hacked. Was it meant for us to find our own exploit? Who knows... We might find out... One day...

Thanks everyone for the fun I had with the wargamesserver, Spoofed Existence