Wargames server 1.0 - A quick Deface

By Cra58cker

June 17, 2003

Introduction

Yo! Cra58cker fans (J\k) I have decided to write a quick WhitePaper on how I hacked the Astalavista wargame server.
Now, this whitepaper will be fairly short since, I didn't personally spend to my time in the actual server myself, I just wrote my name and that was partly it, I didn't have enough time to totally explore the system :-(Don't worry since other people such as Auzy and SpoofEx have written their own whitepapers and they proberly go into much more detail then I do, so If you want to quickly know how I done it then please, read on.......

The Astalavista Server

Ok, basically the server started off running the following services....

* SSHserver
* FTPserver
* Webserver
* PHP
* Telnet
* MySQL database 3.23.56-1
* phpMyAdmin

Basically the rules were simple, No DoS attacks, No Brute forcing, No modifying system files, Changing accounts and No port scanning.....
Now kindly the core members of Astalavista had given us the results from an output of a security scanner known as "Shadow Security Scanner" and also "Nessus". I said to myself "Ahh might as well have a look" so at the very moment I decided to download the results of the two security scanners :-)

The Results of the Scans

After analysing the results of the security scanners, I didn't really find anything that interesting and their wasn't really any "Major" vulnerabilities, the two I did noticed was...
/cgi-bin/htsearch
/cgi-bin/sdbsearch.cgi

but I then realised you had to have write access to use these, which I didn't I had no access :-(

Banner Grabbing and Default Hacker Techniques

I had to access to the server, so I decided to "Telnet" around, I basically telneted into all the major open ports and noted down the banners which told the exact version of the service running on the port :-) once I had collected that set of data I decided to try the odd default password on all the major ports, I tried things like........

User: root

Pass: Root -----------> Yeah! Like that was gonna work!

User: test
Pass: test

User: guest
Pass: guest

User: mail
Pass: mail

etc.........

You get the idea......
Anyhow, no such luck, which in a sense was actually quite good otherwise it would have been way to easy. Now remember at this point I wasn't using proxies or SOCKS because this was a wargame so I couldn't get in any trouble with the FEDS :P

After my default password bashing I decided to pay a vist to www.securityfocus.com and www.astalavista.net (The Exploit section) I then started looking for common popular exploits for the services running, I flicked through a few good ones, which I felt were compatiable with the wargame server but I never actually got around to trying them because the doorknocked and it was my mates, we went out for the rest of the night so I left it their.......

Fate

In the morning I payed a vist to www.astalavista.net and checked the forums, luckily the core members of astalavista had set-up and installed a new service on the wargame...... SAMBA!
This was now my big chance.......

The Hack

After refreshing my memory on samba.c I decided to copy it off of www.astalavista.net\data\samba.c, I put it in a text editor and read the comments on how to complie it (I would go into that now, but I am seriously trying to keep this short)ok, so I edited the code slightly and complied the script with the following syntax....

```
gcc samba.c -o samba
```

Then.....

```
./samba -b 0 -v IP Address of Wargame server
```

Now, I still had trouble running this partly because of careless editing in the code, I re-looked over the code and eventually got it working. I had a shell!
Now, the first thing I wanted to do was (And mainly the only thing)to edit the main index page with my name :-) Now I wasn't familiar with the Linux tool "Vi" so after talking to another Hacker "SpoofEX" he told me various commands while I was in the shell. Here is what I did....

1. Find the main webpage....... -------> find / -name index.php
2. Edit the main webpage....... -------> Vi index.php

3. Bingo! Up came the HTML source code for the main page! Now using VERY basic HTML skills I simply added my name and comment :-)
4. I now needed to save the changes which would lead to me writing to the file.......
I used the following command to save and write to the file -------> :wq! Enter

5. Closed

Done and thats how its done :-) Now, if you noticed I didn't bother downloading or "Catting" the main Passwd file, or I didn't install a backdoor, Sniffer or trojan or even creating myself a proper account, because I saw it as a bit of fun and I wanted other people to have a go ;-)

Britney Spears, Music and Michelle Trachtenberg!!!!!!!

Later that very day, alot of other Astalavista members worked out how it was done and all of a sudden, Pictures of Britney Spears, Michelle Trachtenberg and MIDI's were being uploaded to the main index page! It was a laugh! :-)

GreetZ and Thanks

I would like to take this oppurtunity to thank the whole of Astalavista for setting up a wargame :-) (Even though it was a bit too easy ;-)
and also, Shout outs to, my main Asta peole.......

Daremo, SpoofEX, Auzy, Fullpana, Rizzy, Minky and the rest of ya! :-)

Peace Cra58cker