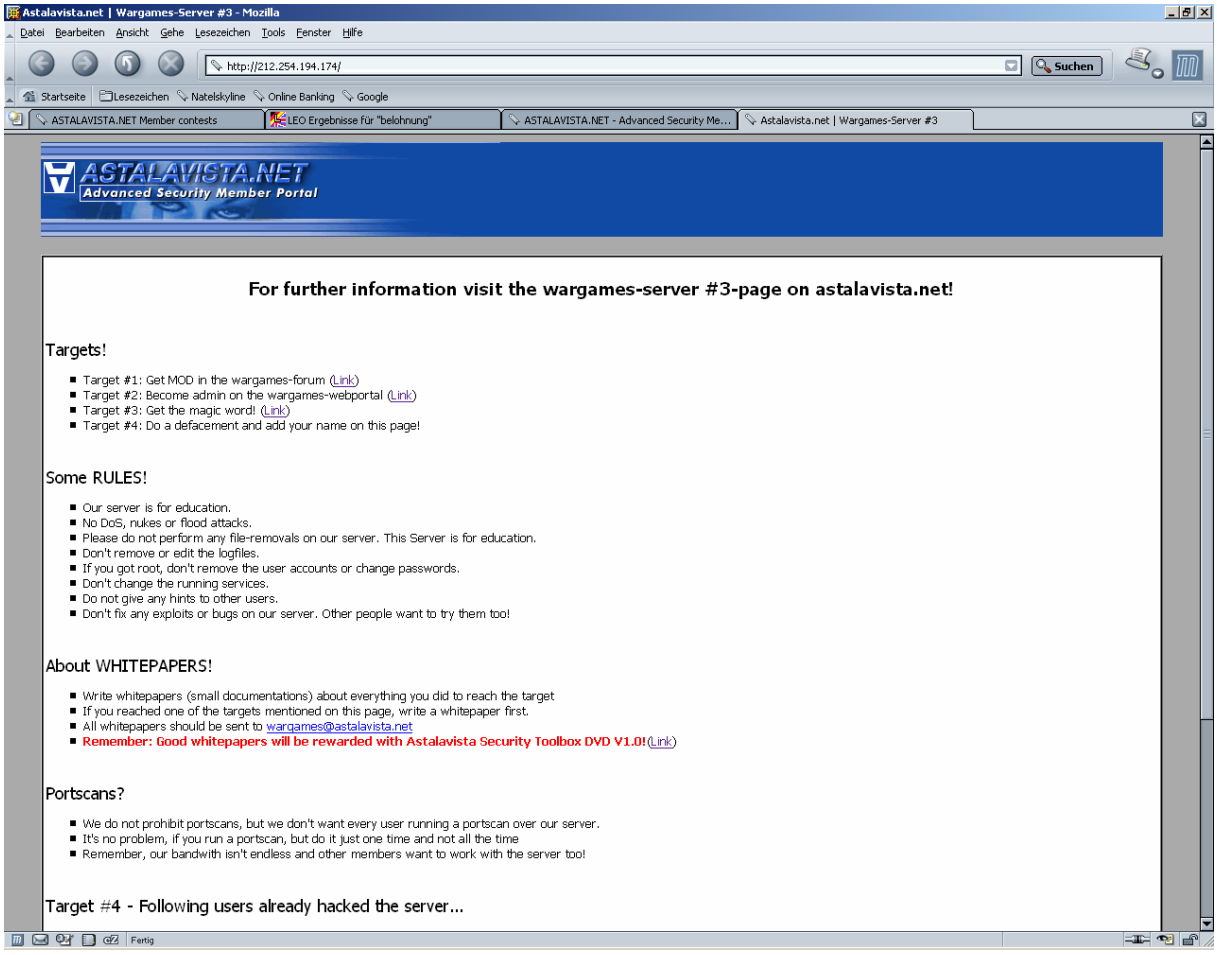
How to set up a wargames-server? v0.1



Written by Gwanun
thomas.kaelin@astalavista.net

Date: 2004-04-30

1. Introduction

Hi all! First of all: thanks for reading this file. It gives me the affirmation, that my time wasn't wasted. :) I didn't have in mind to write a paper about this topic, but after being asked for several times if I couldn't write, I decided to do it anyway.

Ermh, yeah, what else..?! Oh, yeah: SORRY for all the mistakes in this paper. English isn't my mother-tongue, but I'm giving my best to write as clearly as possible! But there are still a huge amount of errors…

If you have some question useful suggestions for this file, do not hesitate to send me an email to thomas.kaelin@astalavista.net. Okay, but now enough fort he introduction, I hope you will like my file!

Enjoy and greetings
Gwanun

2. Basics about wargames-servers

This part is written for all the people out there who don't know what a wargames-server exactly is. If you already know this, you can skip this part unworried.

A wargames-server is a computer which is placed in the internet. On this computer, a server-operating (Linux, Windows, Solaris...) is running offering several services (ftp, mySQL, apache…). But what's the difference to a normal server?

On the wargames-server, you are invited by the administrator to hack the box. You will not be harassed by any department (fbi, police, whatever...). You are all the time on the legal side! So a WGS (wargames-server) is an awesome possibility to improve you hacking skills and your knowledge about servers.

Usually, the administrator of the WGS gives you some targets you should reach, for example: Doing defacement, copying a file from a protected folder or even getting root as the highest quest!

3. How to start?

The first thing and maybe the most important: Choose a corresponding operating system. You are free to use every operating system you like. But you should consider some points:
Take an operating system which you know more or less. Because something is wrong on the box, it's up to you, to fix it! So you should have a fundamental knowledge about your system!
Never take the newest version, because mostly they are quite difficult to hack. They don't have as many exploit as the older have.

Take a more or less well known system. Anybody is interested in hacking a "BIADIX"-Box. (This operating system really exists, if you don't believe or became curious watch out here: http://www.distrowatch.com/table.php?distribution=biadix)

If you have evaluated the right OS for your needs, you should check if is hackable. Means: go to Google and search for exploits. You should make sure, that it is possible to hack the box! Otherwise it's very, very boring for the attackers! If you can't find any useful exploits change the operating system.

Okay, you have found the one you like? I took for my server "Slackware 8.1". It's fast, I worked quite often with it and I know that it has some exploits if I don't patch them!

Than hurry on to the next part!

4. The Hardware & Internet-Connection

The hardware is not very important at all. For my server I took the following components:

- Pentium III 600 MHz
- 256 MB RAM
- 12 GB hard disk

This is enough, because you don't have to give the people out there a high-end server. This configuration is enough for our purpose.

More important is a good, stable connection to the internet! You have to own a fixed ip and at least an upload of 512kbit/s.

5. Choosing the right services & defining targets

Now you should decide which services you want to offer on your WGS and what targets the attackers should reach. Take a piece of paper and write all your ideas on a paper. What would you embrace on other servers? What's interesting for other users? How difficult should the targets be? Note everything on your paper!

Here are some examples:

- Getting root and doing a defacement
- Receiving mod-rights on a web board
- Copying a file out of the file system
- Decrypting a file
- Getting access to a protected folder

You could do everything! But now follows the more difficult part: You have to find a version of the service which includes exploits. Basic rule: as older the version, as more exploits and bugs are there, and as easier is it to hack the service. So find a good middle way, make some easy targets for beginners and some harder for intermediate visitors.

You should also choose some services with no security-holes in. This makes the whole work for the attackers a little bit more difficult, because if they know that there is an exploit for each service running on the WGS it is easy to find one for it. But if they don't know, which services are exploitable, they have to search more carefully.

Download and collect all you files you will need later.

6. Simulating the server

Before you start on the real server, I recommend you to set up the whole server in a VMWare box. This is not necessary, but it is a good possibility to check if everything works you have planned. So you are sure, that on the real box it is going to work like you want! You also can easily check, if all the exploits you find are really working. But if you are sure, that it will work, you certainly can skip this.

7. Setting up the box

Okay, now set up the box with the operating system you evaluated before and configure all your desired services. And check once again, if it is really possible, to reach all the targets. It's not very funny for the attackers to experience after two months of hard work that is just impossible to finish one or more targets!

8. Making a backup

Finally everything works like you want? All services are configured? So make a ghost image of the server! Because there are always stupid monkeys out there who like it to destroy your configuration. And than you will be happy about your image... just copy it back and the WGS is back again! I also recommend storing the ghost-image externally (on another computer, not the WGS itself).

9. Defining rules

Nothing works without rules.. As more exact there are, as better the server is going to run. It copied the rules for the Astalavista WGS#3 as an example:

- No outgoing activity will be allowed from any box within our wargames suite. We do not want anyone launching attacks from our platforms. We are not liable for any activities going on upon the server, as we do not have control over it. With this, we will aid the authorities if anything unlawful does occur.
- Do not remove any files or others data.
- Do not tamper with log files or the logging features in place.
- We will not tolerate any form of nukes, floods or DoS Attacks. We do not want to find any unethical or immoral actions being performed upon our servers. The war games are here for you and your peers to have fun learn and expand your knowledge of "hacking" legally. Please do not turn this into something illegal.
- If you do get root PLEASE DO NOT pull a rm -rf / or any form of file removal that you have not created. Please remember the servers are here for all of us to learn from.
- If a gap in security is found, please do NOT try to remove it: other people also want to try out this security gap.
- If root-rights should be reached, please do not make any alterations in the system configuration (bug fixes, etc).
- Do not install any rootkits on the server
- Don't give any hints to other users, how to reach the targets. Everyone should reach them himself! This means: No topics about exploits in the forum!

And watch out that the attackers consider these rules! If not, take the server down for a day.. two days.. a week! Remember: You are doing this because you want to offer something, but you don't get paid for it, so if they don't want to accept the rules…

10. Maintaining the server

You should check the configuration about 2-3 times a week. If you notice that something is wrong with your machine, you have to fix it. Remove all service which weren't installed by you! Otherwise somebody could use your box as a proxy, IRC-server …

11. Whitepapers

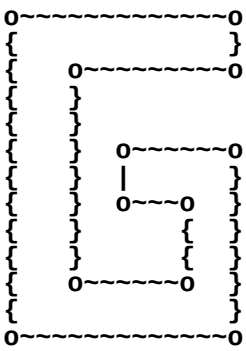
Of course you want to benefit from the WGS. So let the attackers write whitepapers. Whitepapers are documents, in which all the steps are mentioned, the attackers needed to reach one of the targets. Maybe give them an award for the whitepapers, because anyone wants to spend hours and hours just for free!

12. Last Words

Thanks for reading again! :D

Greetings to:

- The whole Astalavista-Team: http://www.astalavista.ch/index.php?page=222
- All members of astalavista.net reading this whitepaper
- All fans of the real music: Trance! :)
- All fans of "the lord of the rings"



wanun