

Forum:[Hack Forums](#)

Thread: [Scheduled cron jobs](#)

happywilli - March 8, 2018, 5:55 am

Hello,

I've been using SQLMAP to inject a webserver on our Test lab and I was able to access it by SQL inject it.

I found a Scheduled cron job that is writeable that I can modify and it runs with root access.

Got any tips on what Code I can run to get ex root access?

//W

[BLANK] - March 8, 2018, 8:15 am

There are a lot of choices, pretty much anything that you can do in bash you could do in the cron job. You could setup a reverse tunnel which will be running as root. You could add a new user. You could download and execute a shell script etc.

happywilli - March 8, 2018, 8:18 am

(Mar 8, 2018 09:15 AM)EasyGhost Wrote: [\[CITE\]](#) There are a lot of choices, pretty much anything that you can do in bash you could do in the cron job. You could setup a reverse tunnel which will be running as root. You could add a new user. You could download and execute a shell script etc.

Thanks for replying.

I've got access to OS-Shell on the webserver.

but I do not have root access. What is your recommendation?

[BLANK] - March 8, 2018, 8:23 am

Before going into details, is this a test box of some sort? Are you on a local network with the target host? Or is this a live webserver that you are hacking?

happywilli - March 8, 2018, 8:32 am

(Mar 8, 2018 09:23 AM)EasyGhost Wrote: [\[CITE\]](#) Before going into details, is this a test box of some sort? Are you on a local network with the target host? Or is this a live webserver that you are hacking?

this is a test lab, through VPN.

webserver is unix machine, PHP.

[BLANK] - March 8, 2018, 8:35 am

<http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

Use one of the reverse shells listed above to create a connection to your local host. Because the cron job is running as root, the reverse shell should also be root. At that point you can do whatever you want with root privileges.

happywilli - March 8, 2018, 9:09 am

Use one of the reverse shells listed above to create a connection to your local host. Because the cron job is running as root, the reverse shell should also be root. At that point you can do whatever

you want with root privileges.

[/quote]

I downloaded the php shell; php-reverse-shell

I uploaded it and tried to run it and listen to the port assigned but I get error message:

WARNING: Failed to daemonise. This is quite common and not fatal. Successfully opened reverse shell to IP port 443 ERROR: Shell connection terminated

[BLANK] - *March 8, 2018, 10:13 am*

What is the exact php code you are using? Also, does it appear that the target host is terminating shell, or your local host?