

Forum:[Hack Forums](#)

Thread: [\[TUT\]\[HackThisSite\]\[2\] Basic Missions 7-9 \(Linux Commands, SSI, Directory Traversal\)](#)

LGhost - May 10, 2015, 9:56 am

Ok, continuing our last episode of this "Road To Hacker". We have learned how to inspect and modify HTML code and how to inject javascript. If you didn't see the last tutorial [it is here](#).

In this one we will learn more things. Things like SSI (Server Side Includes), Directory Traversal and some linux commands. Let's get started!

Note: For those who don't know, this tutorial is inspired on www.hackthissite.org. All this basic missions can be found there.

Basic 7

For this mission you'll need to know some basic linux commands.

Obs: Linux is a cool opensource OS and for hacking and pentesting is even better ([Kali](#) is a distribution focusing pentest)... You will not need to have Linux for doing this Basic 7.

Here's a list of the most common commands:

Code ls - shows the content of the folder in witch it runs

uname - shows useful information about the machine (like it's name, operating system and kernel)

history - shows the list of commands used in the terminal

sudo - allows a permitted user to execute commands as the superuser or another user

mkdir - creates a new directory

cal - displays calendar of the present month or any other month of any other year.

date - displays the current date and time (and can set it too)

cp - copies one file from one location to another location.

pwd - shows the full path for the current working directory

cd - changes the working directory to another

I know this is not all but it's some of the most common.

Back to the mission it says that "Sam has set up a script that returns the output from the UNIX cal command.". This means that when we enter a date is executing the "cal" command to show us the date. But the "password in an obscurely named file saved in this very directory". So... what is the command to list the files on a directory? Yeah, it's the "ls" command. But... How do we run it? ... Well, the semicolon (";") is able to do just that. It ends a command. Can you figure what we have to do to inject the "ls" command? ... We have to put "; ls" on the year field and click "view" ;) Then we will get all the files in that directory on the bottom of the page.

[img]http://snag.gy/Y4wHv.jpg[/img]

So... The the only "obscurely named file" I see is the "k1kh31b1n55h.php"... Go to that page and you'll get the password (:

Basic 8

This time Sam's daughter wrote a PHP program that saves files, let's test it... Write something in the input box and submit... You see that it creates a file a gives a link to that file. If you click:

[img]http://snag.gy/lxZij.jpg[/img]

If look to the link you'll see that the extension is ".shtml" witch is an HTML file that includes SSI (Server Side Includes). For this Basic we'll need to make an SSI Injection, to know more about SSI and how to perform some SSI Injections follow this [amazing tutorial by Zixem](#) and after you read all let's begin our work (: ... We know that the file is in "/var/www/hackthissite.org/html/missions/basic/8/"... so we want again to run the "ls" command. To do this we are interested in the "exec" function to execute a shell command (in this case "ls"). What we are looking for is:

Code `[b]<!--[/b]#exec cmd="ls"-->`

Type that in the name field and submit. Click on the file generated and you'll get a list of the files on the directory:

[img]http://snag.gy/GUCGJ.jpg[/img]

Now that files are the ones on the "tmp" directory. We want to see the files on the "https://www.hackthissite.org/missions/basic/8/" directory, so we need to go one directory up... That means we need to combine SSI Injection with Directory Traversals. Read [this tutorial](#) to know the basics of Directory Traversals.

So "." means it's a directory up. Let's update our "ls" command:

Code `[b]<!--[/b]#exec cmd="ls .."-->`

Submitting you'll have the files in the "basic/8/" directory:

[img]http://snag.gy/RcfsP.jpg[/img]

And there it is our "obscured password file" :D

Basic 9

If you read the instructions you'll see that he says "in my attempt to limit people to using server side includes to display the directory listing to level 8 only, I have mistakenly screwed up somewhere.. there is a way to get the obscured level 9 password"... he says that there is a vuln in level 8 that can get you level 9 password let's go back to 8 and try to use the same SSI + Directory Traversal technique to get the file with the password of level 9.

The link that runs the PHP script in level 8 is:

Code `https://www.hackthissite.org/missions/basic/8/tmp/`

And the link of level 9 is:

Code `https://www.hackthissite.org/missions/basic/9/`

So we want to go up 2 directories (to "/basic/") and get to level 9 ("/9/"). For that we do this "../..9/" on the "ls" command. The SSI command needed is:

Code `[b]<!--[/b]#exec cmd="ls ../../9/"-->`

And after submitting that on level 8 the result is:

[img]http://snag.gy/Roxav.jpg[/img]

Go to that page on level 9 and there you have the password :D

That's all for now! Next tutorial will be about missions 10 and 11 and we will learn some things like Cookie Modification and Web Servers. See you there ;)

Next tutorial is available:

[\[TUT\]\[HackThisSite\]\[3\] Basic Missions 10-11 \(Cookie Modification, Web Servers\)](#)