

Bash Scripting, Dirty Pipe & more!

Network Security Emphasis

Ian Cook March 15th, 2022

Quick Intro: What is Bash? Why does it matter?

“**Bash** (AKA **B**ourne **A**gain **S**hell) is a **type of interpreter** that processes shell commands. A **shell interpreter** takes commands in plain text format and calls **Operating System services** to do something. For example, `ls` command lists the files and folders in a directory. Bash is the improved version of **Sh** (*Bourne Shell*). A **shell scripting** is writing a program for the shell to execute and a **shell script** is a file or program that shell will execute.”



Diving into it: TryHackMe free room!!! (today's theme)

For today: <https://tryhackme.com/room/bashscripting>

For tomorrow (or another day): <https://tryhackme.com/room/catregex>

<https://tryhackme.com/room/linuxstrengthtraining>

<https://www.shellscript.sh/>

<https://www.codecademy.com/learn/bash-scripting>



Quick Intro: What the heck is Dirty Pipe?

CVE-2022-0847

On Monday 7th March, a vulnerability in the Linux Kernel was disclosed publicly which could allow an attacker to escalate privileges

The vulnerability resides in the pipe tool, which is used for unidirectional communication between processes, so the researcher called it “Dirty Pipe”.



```
Kali Linux (Ubuntu 20.04 LTS) [Kali Linux] - 7:21 PM
Kali Linux (Ubuntu 20.04 LTS) [Kali Linux] - 7:21 PM
File Machine View Host Devices Help
1. root@pentest:~$
File Edit View Help
root@pentest:~$ whoami
root
root@pentest:~$ sudo -l
[sudo] password for root:
Sorry, user root may not run sudo on pentest.
root@pentest:~$
```

Confirming whether user has root permissions

Diving into it: Again on TryHackMe (sorry not sorry)

For today: <https://tryhackme.com/room/dirtypipe>

For tomorrow:

(Log4j room <https://tryhackme.com/room/solar>)

(Vulnerabilities101 <https://tryhackme.com/room/vulnerabilities101>)

(Apache Path Traversal <https://tryhackme.com/room/cve202141773>)



Resources:

<https://linuxconfig.org/bash-scripting-tutorial>

<https://ryanstutorials.net/bash-scripting-tutorial/>

<https://www.redhat.com/sysadmin/learn-bash-scripting>

https://www.tutorialspoint.com/unix/shell_scripting.htm

<https://www.educative.io/courses/master-the-bash-shell/3j8399P3M6M>

<https://www.techtarget.com/searchdatacenter/definition/bash-Bourne-Again-Shell>

<https://medium.com/sysf/bash-scripting-everything-you-need-to-know-about-bash-shell-programming-cd08595f2fba>



Resources:

<https://thehackernews.com/2022/03/dirty-pipe-linux-flaw-affects-wide.html>

<https://securelist.com/cve-2022-0847-aka-dirty-pipe-vulnerability-in-linux-kernel/106088/>

<https://redhuntlabs.com/blog/the-dirty-pipe-vulnerability.html>

https://twitter.com/Fire30_/status/1503422980612923404?s=20&t=t90ZPQtmVg3TTeOyY6i6VA

<https://dirtypipe.cm4all.com/>

