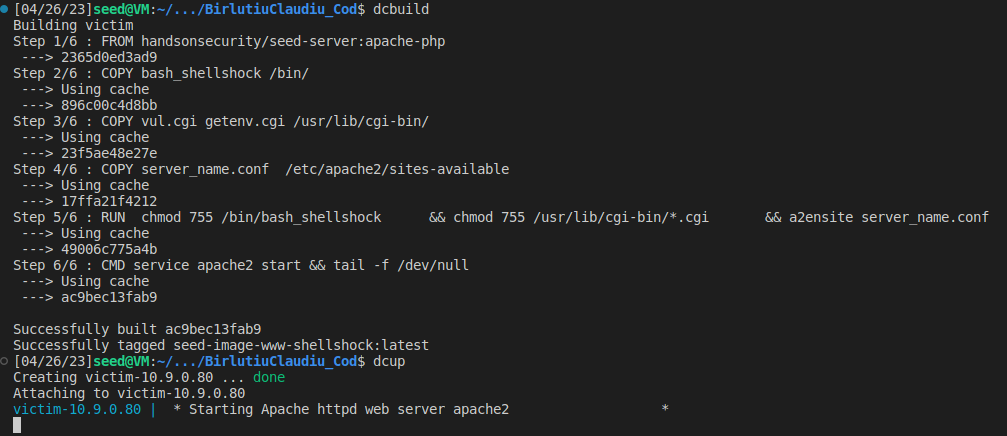
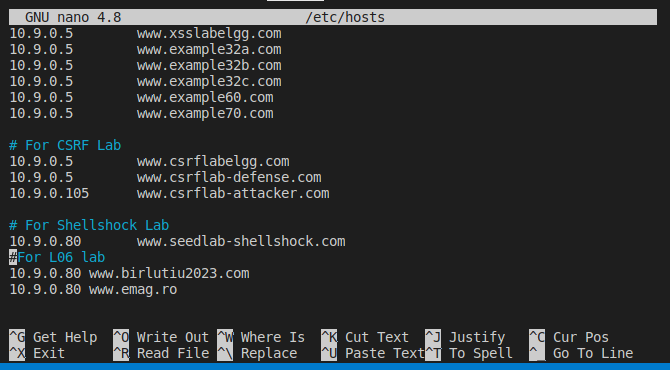
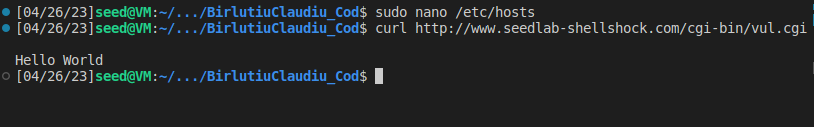
# Raport pentru lucrarea 7: Atacul Shellshock

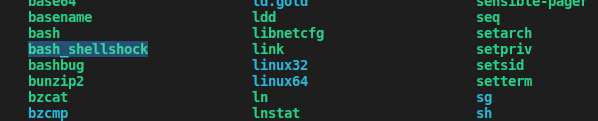
Autor: Birlutiu Clauidu-Andrei, gr 30643

## Sarcina 1: Experimente cu funcțiile Bash

* În prima faza mi-am creat environmentul de lucru prin construirea și pornitrea container-ului **victim-10.9.0.80**
* int et/hosts se va adauga intreare [www.seedlab-shelshock.com](http://www.seed-server.com/) pentru adresa 10.9.0.80 pentru simularea intrarii în DNS



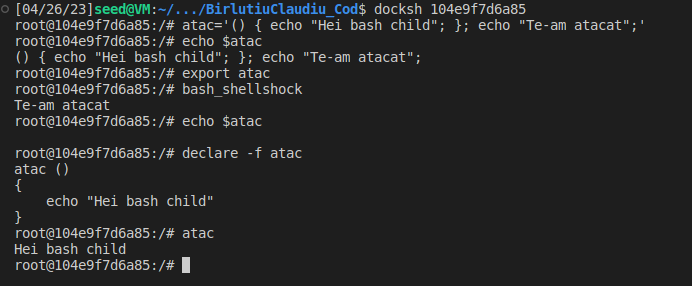
* am accesat programul CGI folosing progrmul curl din lina de comanda; astfel s-a rulat scriptul shell pe care l-a adaugat pentru afisarea unui mesaj de forma Hello World
* vizualizare versiune bash vulnerabila în directorul /bin de pe container



* vulnerbilitatea pe care o prezinta un bash (vulnerabil) este ca procesul părinte poate transmite o definiție de funcție altui proces copil folosind o variabila de mediu => datorita unei erori in procesul de parsare a functiei, bash poate sa execute o comanda/o parte din variabila de mediu cum ar fi un bash script; in cazul nostru, eu voi afisa un mesaj => “Te-am atacat” folosind un bash vulnerbaul de pe container

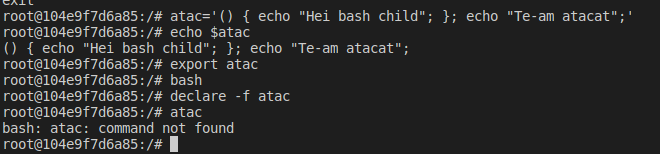
**CAZ BASH VULNERABIL**

* atac=' () { echo "Hei bash child"; }; echo "Te-am atacat";' - declaram într-o variabila definitia unei funcții urmata de un cod de atac la nivelul bash-ului parinte
* export atac
* bash\_shellshock -- se va rula bash-ul vulnerbail, iar la pasărea definitiei variabile atac, se va executa mai întâi codul de atac (cel subliniat)



**CAZ BASH NEVULNERABIL**

* executam aceeași pași și observam ca nu vom avea functia atac în procesul copil deschis cu un bash nevulnerabil



## Sarcina 2: Trimiterea de date spre Bash printr-o variabilă de mediu

### Sarcina 2.A. Folosirea browserului

### Sarcina 2.B. Utilizarea *curl*

## Sarcina 3: Lansarea atacului Shellshock

### Sarcina 3.A. Trimiterea fișierului /etc/passwd

### Sarcina 3.B. ID-ul de utilizator al procesului server

### Sarcina 3.C. Crearea unui fișier în /tmp

### Sarcina 3.D. Ștergerea fișierului din /tmp

## Sarcina 4: Obținerea unui shell conectat la atacator prin atacul Shellshock

## Sarcina 5: Utilizarea Bash corectat