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)

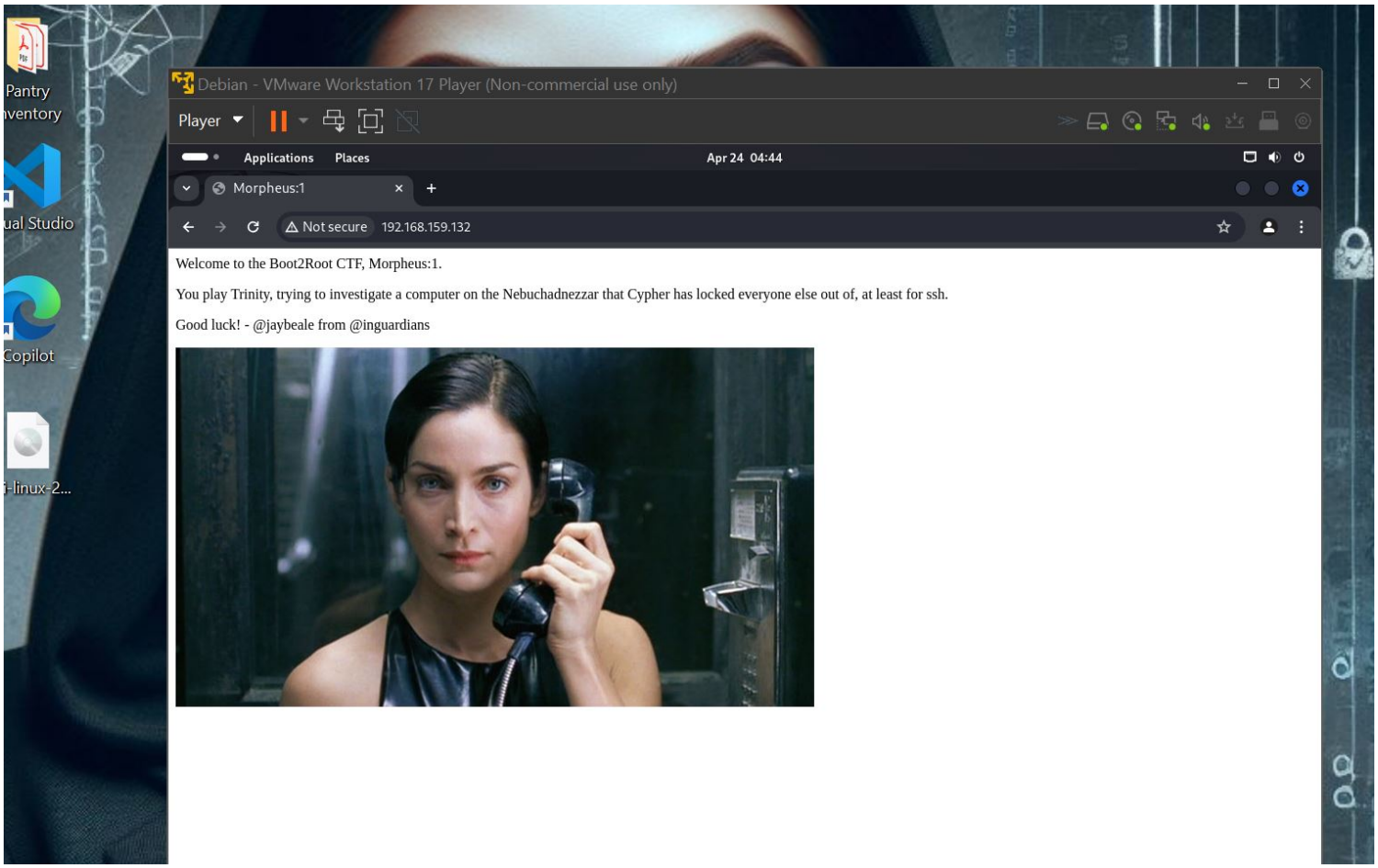
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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

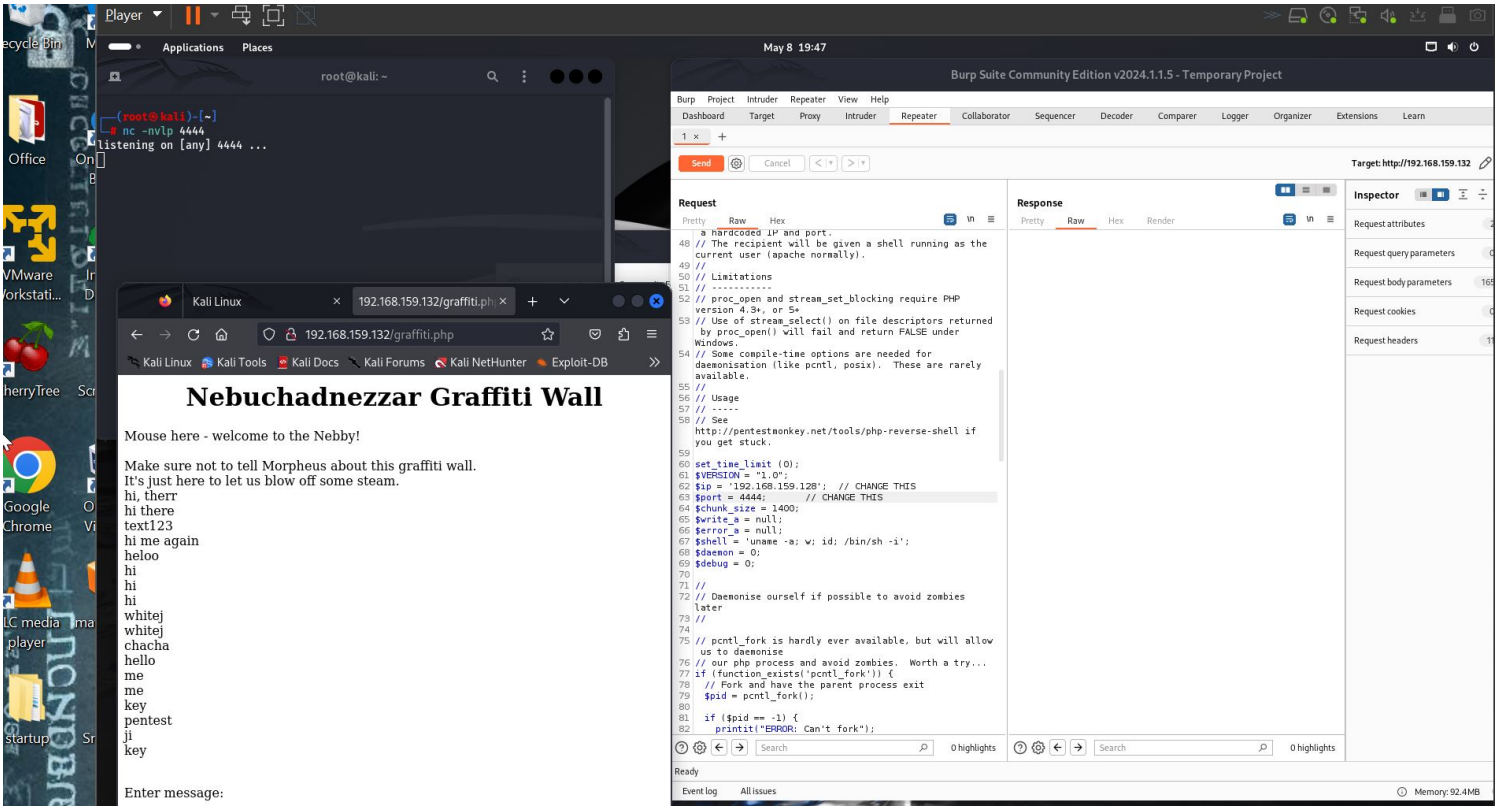
gobuster -u http://192.168.159.132 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt

We found some interesting files and pages
http://192.168.159.132/javascript

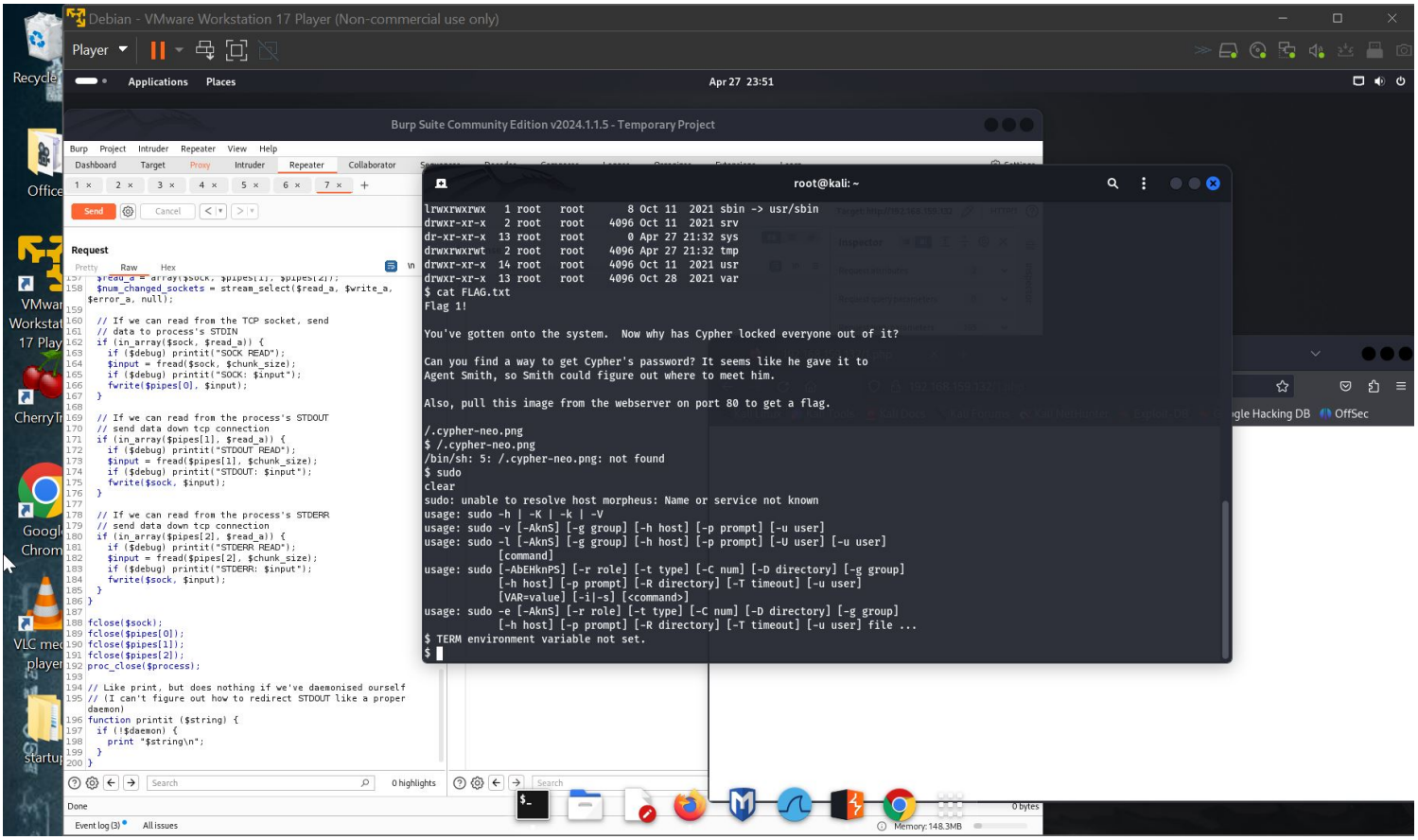
http://192.168.159.132/robot.txt
http://192.168.159.132/graffiti.php
http://192.168.159.132/graffiti.txt

GAINING ROOT

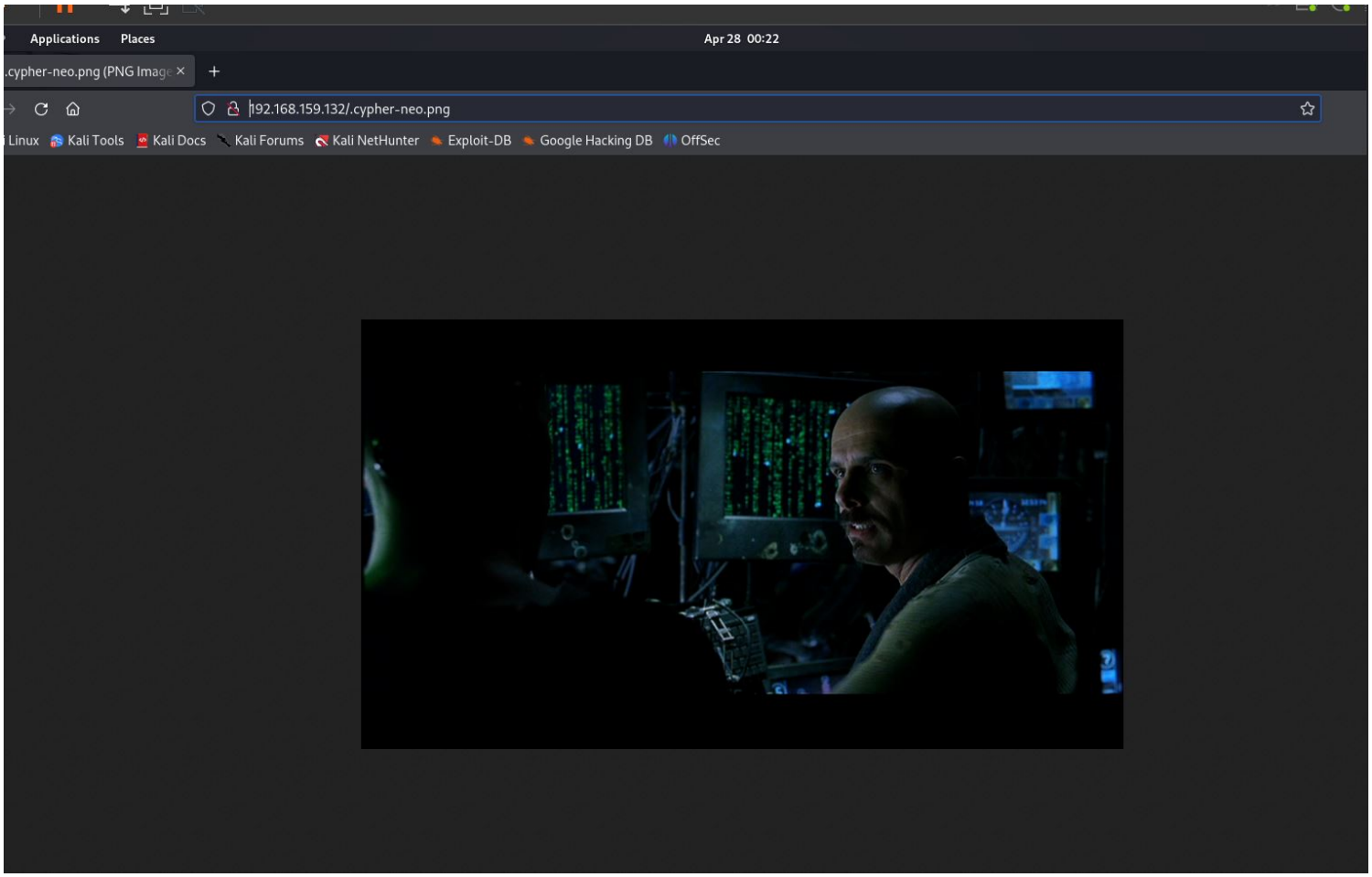
We are going to gain root/ shell by intercepting the Http POST and GET method uisng Burp



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

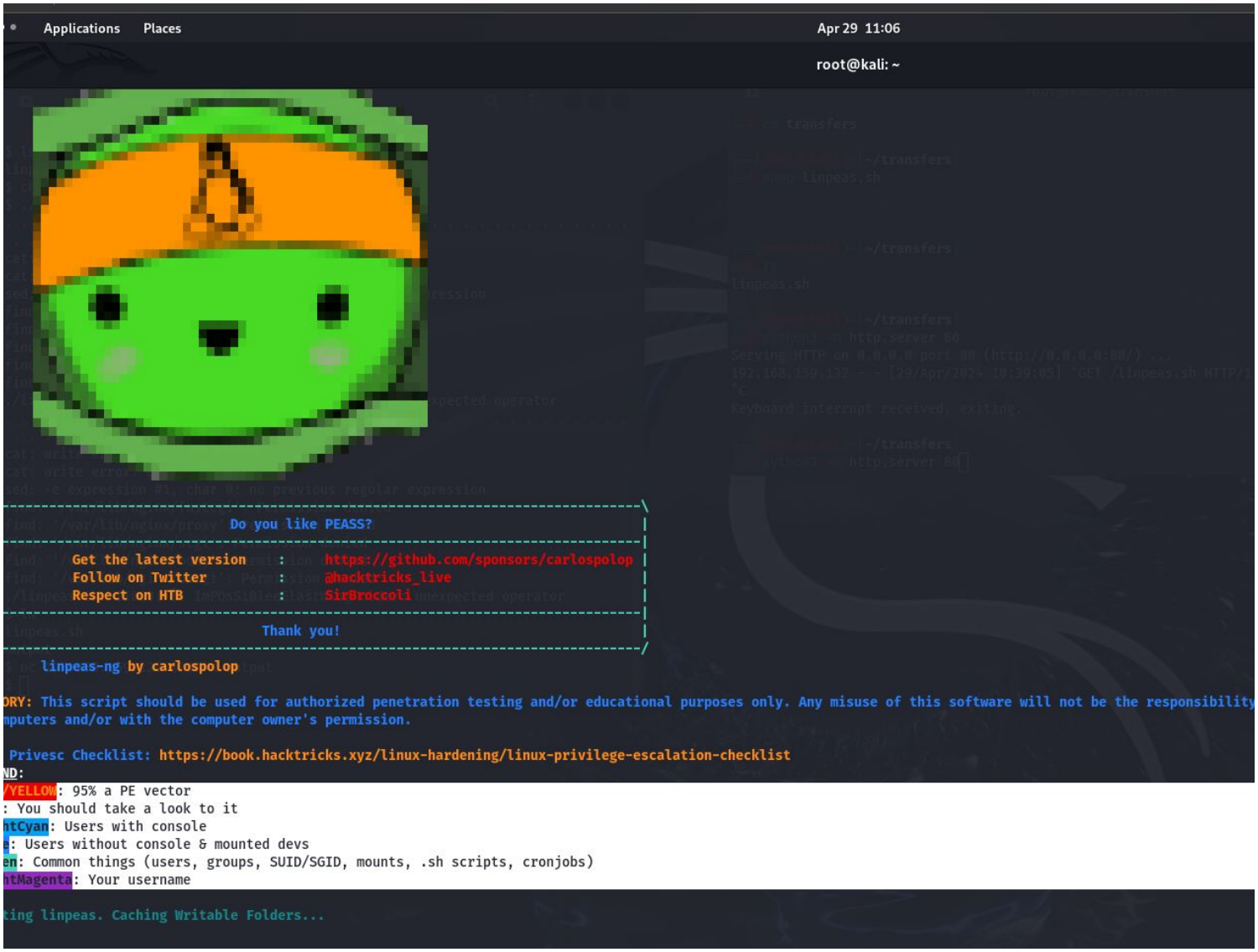


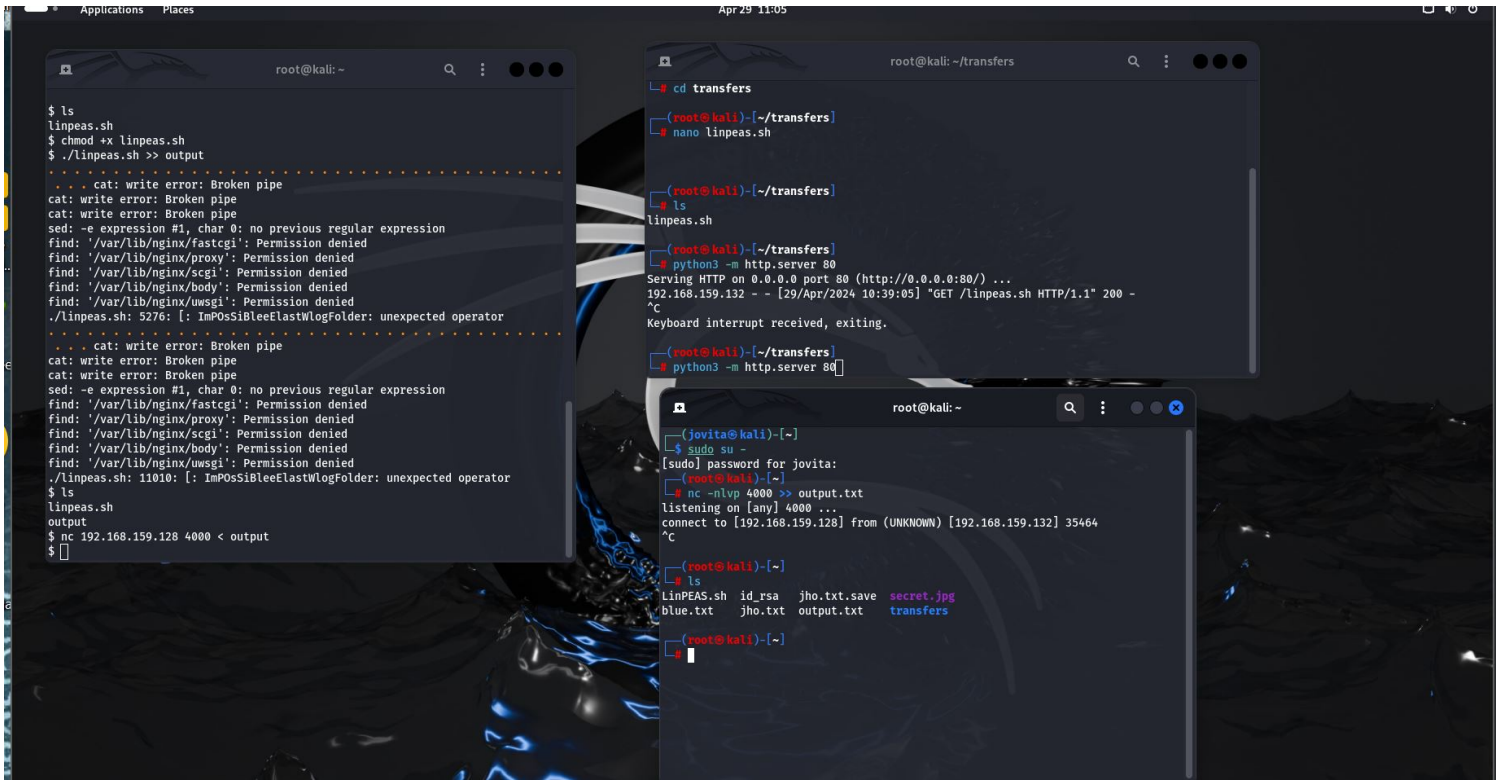
We have gained shell but not as root



PRIVILEDGE ESCALATION

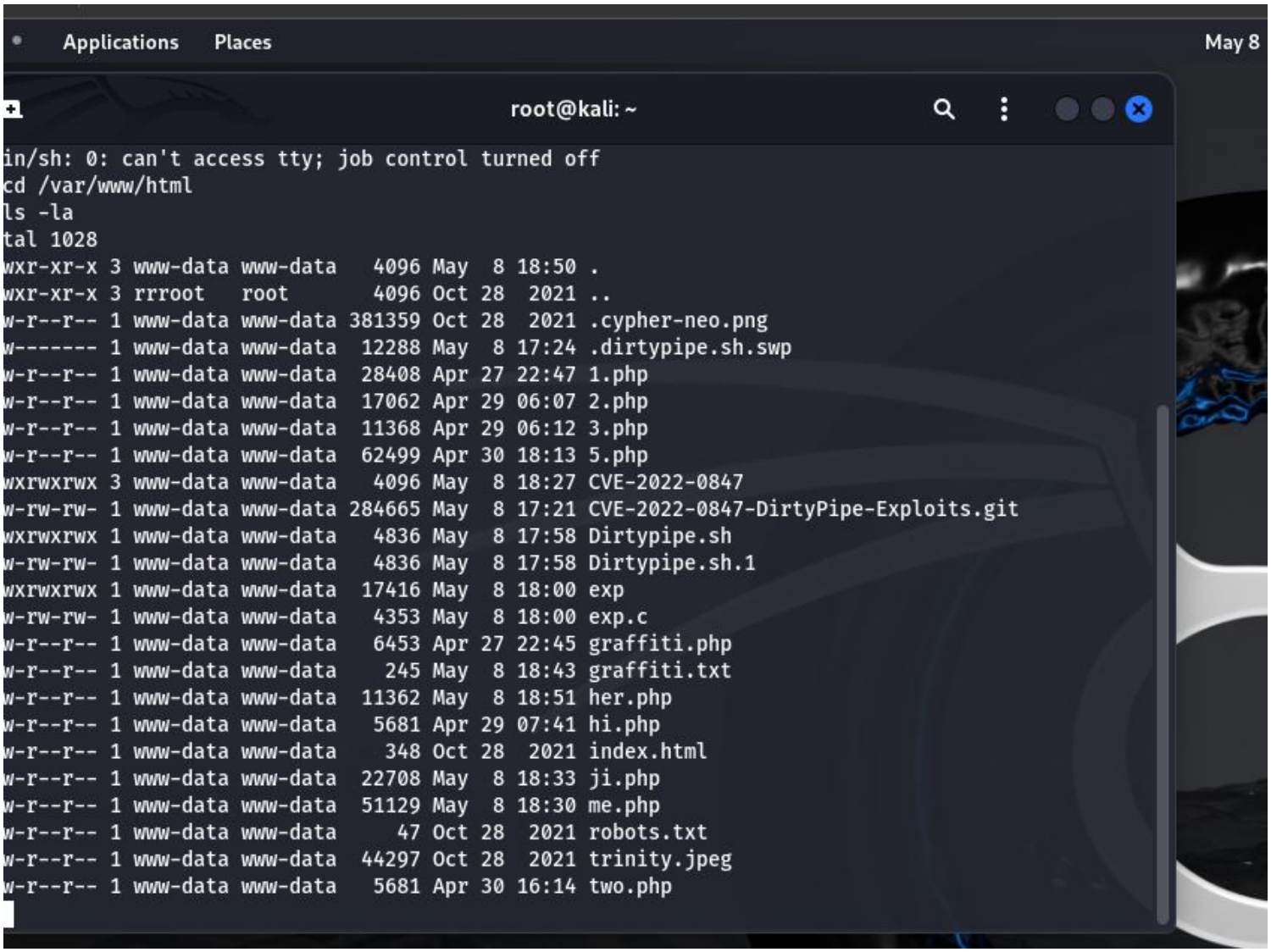
We are going to elevate our priviledges by first running Linpeas and check the vunerablility



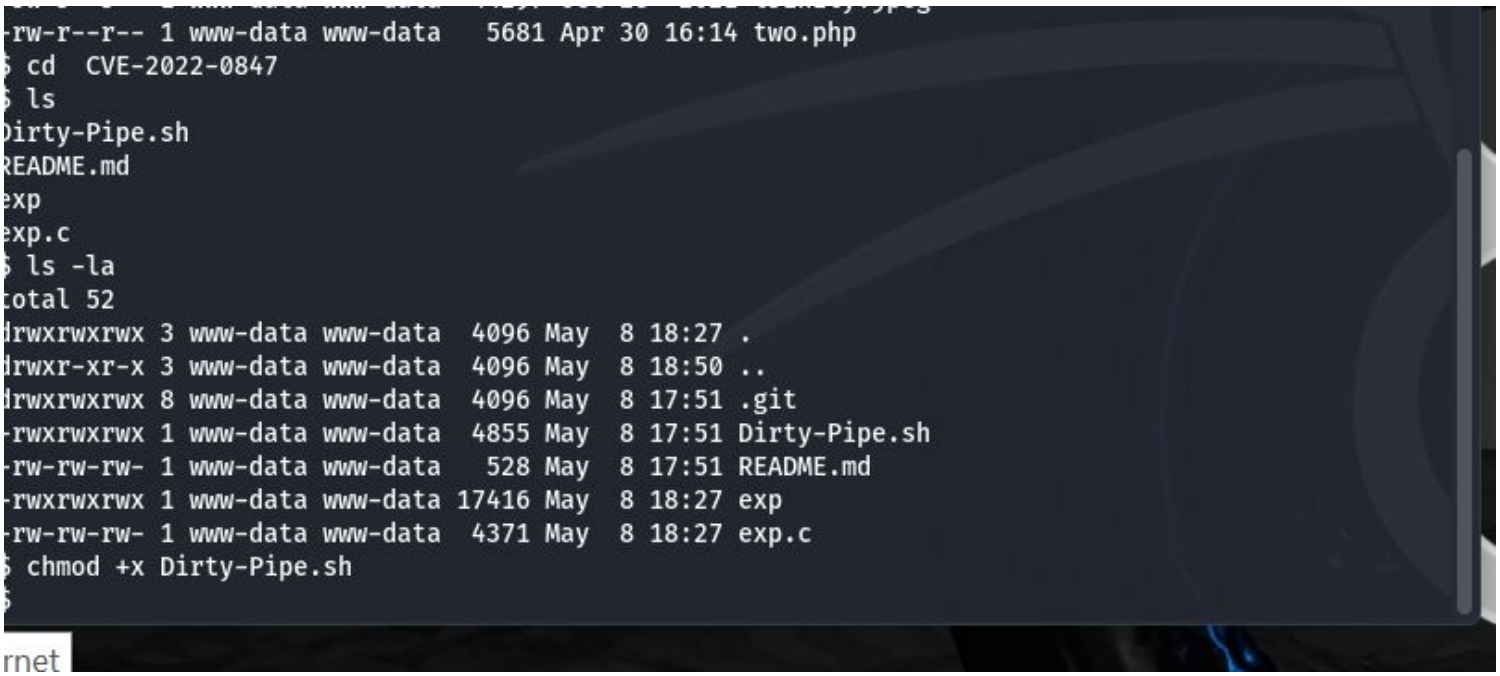


From the output we find out our system is vunerable to CVE-2022-0847 DirtyPipe

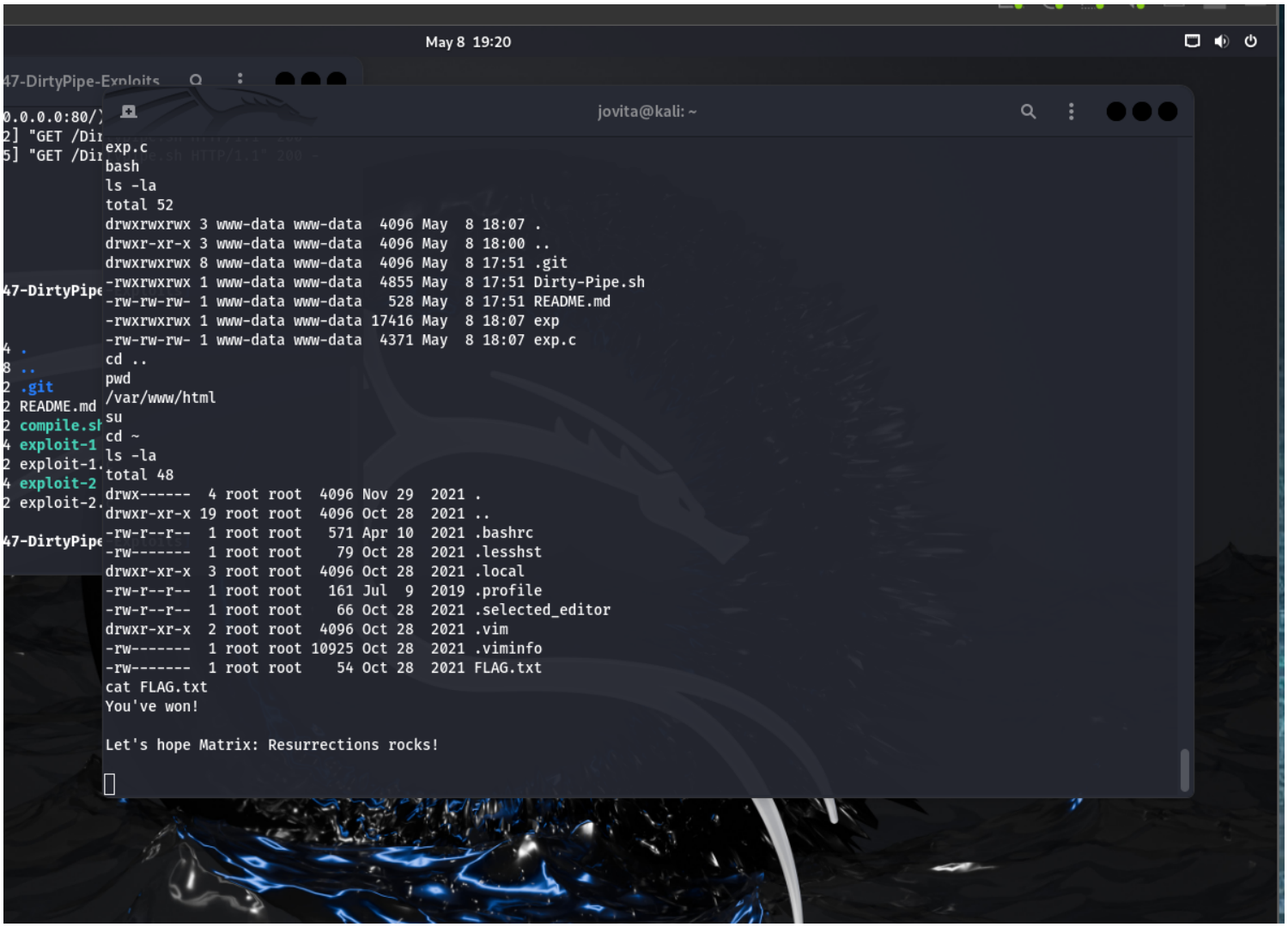
we find the exploit of DirtyPipe, use wget to download it to our remoote server



we change the mode to make the file executable



we execute it
bash Dirty-Pipe.sh



Viola!!!
we are root of this machine