

[illegible]

<b>Name</b>	Lesser Known Hacks
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=1816">https://attackdefense.com/challengedetails?cid=1816</a>
<b>Type</b>	Beginner Skills : Linux For Pentesters

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

**Objective: Try the following less known hacks.**

1. Use python to start a webserver in the present working directory. Open another terminal and do a curl request to it.
2. View bash command history.
3. Fire a command and make sure it is not captured in the bash command history.
4. List all lines of a file in reverse order (i.e. last line first).
5. Delete all content of a file with one line command .
6. Write output of a command (say ps -ef) to three files at the same time.
7. Generate MD5 or SHA1 hash of a file
8. Find previous fired commands from bash history using reverse search.
9. Check information of a file.
10. Use screen to preserve the console output and running tasks in case of connection break (mostly useful while working on remote machines).

**Solution:**

**Q 1. Use python to start a webserver in the present working directory. Open another terminal and do a curl request to it.**

Create a dummy index.html and start the Python webserver

**Commands:**

echo "hi" > index.html  
python -m SimpleHTTPServer 80

```
root@attackdefense:~# echo "hi" > index.html
root@attackdefense:~#
root@attackdefense:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Open another terminal. Check the opened socket using netstat.

**Command:** netstat -tln

```
root@attackdefense:~# netstat -tln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.11:37045        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8000           0.0.0.0:*               LISTEN      81/ttyd
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN      90/python
root@attackdefense:~#
```

Fetch the index.html using curl.

**Command:** curl http://127.0.0.1

```
root@attackdefense:~# curl http://127.0.0.1
hi
root@attackdefense:~#
```

## Q 2. View bash command history.

View bash command history

**Command:** history

```
root@attackdefense:~# history
 1 netstat -tln
 2 curl http://127.0.0.1
 3 history
root@attackdefense:~#
```

**Q 3. Fire a command and make sure it is not captured in the bash command history.**

If a <space> is typed before the command, the bash history won't log it.

**Command:** <space>date

```
root@attackdefense:~# history
 1 netstat -tln
 2 curl http://127.0.0.1
 3 history
root@attackdefense:~#
root@attackdefense:~# date
Thu Apr  9 01:25:51 UTC 2020
root@attackdefense:~#
root@attackdefense:~# history
 1 netstat -tln
 2 curl http://127.0.0.1
 3 history
root@attackdefense:~#
```

**Q 4. List all lines of a file in reverse order (i.e. last line first).**

The cat utility is used to print the contents of a file

**Command:** cat /etc/passwd

```
root@attackdefense:~# 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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
student:x:999:999:student:/home/student:/bin/sh
teacher:x:998:997:teacher:/home/teacher:/bin/sh
root@attackdefense:~#
```

The tac utility can be used to print the file in reverse order.

**Command:** tac /etc/passwd

```
root@attackdefense:~# tac /etc/passwd
teacher:x:998:997:teacher:/home/teacher:/bin/sh
student:x:999:999:student:/home/student:/bin/sh
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
games:x:5:60:games:/usr/games:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
sys:x:3:3:sys:/dev:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
root:x:0:0:root:/root:/bin/bash
root@attackdefense:~#
```

### Q 5. Delete all content of a file with one line command .

A simple blank input redirection can blank the file. Copy a text file and remove its content.

#### Commands:

```
cp -a /etc/passwd test
```

```
> test
```

```
cat test
```

```
root@attackdefense:~# cp -a /etc/passwd test
root@attackdefense:~#
root@attackdefense:~# > test
root@attackdefense:~#
root@attackdefense:~# cat test
root@attackdefense:~#
```

### Q 6. Write output of a command (say ps -ef) to three files at the same time.

The tee utility can be used for this purpose

**Command:** ps -ef | tee file1 file2 file3

```
root@attackdefense:~# ps -ef | tee file1 file2 file3
UID      PID  PPID  C  STIME TTY          TIME CMD
root         1      0  0  01:18 ?                00:00:00 /bin/bash /startup.sh
root        81      1  0  01:19 ?                00:00:00 /usr/local/bin/ttyd -p 8000 bash
root        82     81  0  01:19 pts/0          00:00:00 bash
root        91     81  0  01:20 pts/1          00:00:00 bash
root       106     91  0  01:29 pts/1          00:00:00 ps -ef
root       107     91  0  01:29 pts/1          00:00:00 tee file1 file2 file3
root@attackdefense:~#
```

The content will be written to all three files.

**Command:** cat file1



```

root@attackdefense:~# cat file1
UID      PID  PPID  C  STIME TTY      TIME CMD
root      1    0    0  01:18 ?        00:00:00 /bin/bash /startup.sh
root     81    1    0  01:19 ?        00:00:00 /usr/local/bin/ttyd -p 8000 bash
root     82   81    0  01:19 pts/0    00:00:00 bash
root     91   81    0  01:20 pts/1    00:00:00 bash
root    106   91    0  01:29 pts/1    00:00:00 ps -ef
root    107   91    0  01:29 pts/1    00:00:00 tee file1 file2 file3
root@attackdefense:~#

```

**Command:** cat file2

```

root@attackdefense:~# cat file2
UID      PID  PPID  C  STIME TTY      TIME CMD
root      1    0    0  01:18 ?        00:00:00 /bin/bash /startup.sh
root     81    1    0  01:19 ?        00:00:00 /usr/local/bin/ttyd -p 8000 bash
root     82   81    0  01:19 pts/0    00:00:00 bash
root     91   81    0  01:20 pts/1    00:00:00 bash
root    106   91    0  01:29 pts/1    00:00:00 ps -ef
root    107   91    0  01:29 pts/1    00:00:00 tee file1 file2 file3
root@attackdefense:~#

```

Similarly, the same content is in file3.

## Q 7. Generate MD5 or SHA1 hash of a file

### Commands:

md5sum /bin/bash

sha1sum /bin/bash

```

root@attackdefense:~#
root@attackdefense:~# md5sum /bin/bash
97f18607b616eb5d1bdf312ae09715c8 /bin/bash
root@attackdefense:~#
root@attackdefense:~# sha1sum /bin/bash
127fefa36c6e7e35cdb4396110cb944382dae914 /bin/bash
root@attackdefense:~#

```

### Q 8. Find previous fired commands from bash history using reverse search.

Recursive search on the bash history enables. On Pressing Ctrl+R, the prompt enters into reverse search mode

```
root@attackdefense:~#  
(reverse-i-search)`':
```

Typing any character makes the search to suggest commands from the history.

```
root@attackdefense:~#  
(reverse-i-search)`ps': ps -ef | tee file1 file2 file3
```

The user needs to press ENTER once the desired command is found.

### Q 9. Check the information of a file.

The file command can be used.

#### Commands:

file test

file /etc/passwd

file /bin/bash

```
root@attackdefense:~# file test  
test: empty  
root@attackdefense:~#  
root@attackdefense:~# file /etc/passwd  
/etc/passwd: ASCII text  
root@attackdefense:~#  
root@attackdefense:~# file /bin/bash  
/bin/bash: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter  
88017e1b386d955ce384f28b0bc642d5f6a38d, for GNU/Linux 3.2.0, stripped  
root@attackdefense:~#
```

### Q 10. Use screen to preserve the console output and running tasks in case of connection break (mostly useful while working on remote machines).



Run screen command

**Command:** screen

It will open an informational page. Press space or Enter to close that

```
GNU Screen version 4.06.02 (GNU) 23-Oct-17

Copyright (c) 2015-2017 Juergen Weigert, Alexander Naumov, Amadeusz Slawinski
Copyright (c) 2010-2014 Juergen Weigert, Sadrul Habib Chowdhury
Copyright (c) 2008-2009 Juergen Weigert, Michael Schroeder, Micah Cowan, Sadrul Habib Chowdhury
Copyright (c) 1993-2007 Juergen Weigert, Michael Schroeder
Copyright (c) 1987 Oliver Laumann

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the
Free Software Foundation; either version 3, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY
or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program (see the file COPYING); if not, see
http://www.gnu.org/licenses/, or contact Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02111-1301 USA.

Send bugreports, fixes, enhancements, t-shirts, money, beer & pizza to screen-devel@gnu.org

Capabilities:
+copy +remote-detach +power-detach +multi-attach +multi-user +font +color-256 +utf8 +rxvt +builtin-telnet

[Press Space or Return to end.]
```

Open vim in edit mode. (vim will create the file if it doesn't exist)

```
This is a temporary work
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

While in the middle of editing, simulate a connection break by refreshing your terminal tab. The terminal will load but the vim command view will go away.

List the running screen sessions

**Command:** screen -list

```
root@attackdefense:~# screen -list
There is a screen on:
      159.pts-2.attackdefense (04/09/20 01:40:41)      (Detached)
1 Socket in /run/screen/S-root.
root@attackdefense:~#
```

Attach to the screen

**Command:** screen -r

```
root@attackdefense:~# screen -r
```

Only one screen is running so this will work. In case of multiple screens the name has to be specified.

And, this will bring back the vim command view

```
This is a temporary work
```

```
~
~
~
~
~
~
~
~
~
~
~
```