Linux nixtrainer Challenge

Nirakar Suwal
Coventry ID: 13703716

BSc. (Hons) Computing, Softwarica College of IT and E-commerce
ST6005CEM Security

Arya Pokharel

Table of Contents

level0 –

```
level32@22203cf417e7:~$ su - level0
Password:
su: Authentication failure
level32@22203cf417e7:~$ su - level0
Password:
Congratulations,  You Escaped!!
Password for Level 1 is c341b271f5dba18dd4099435670a2c74

You will need to logout, and reconnect to continue
level0@22203cf417e7:~$
```

level1 –

The password was inside the manual

```
level0@22203cf417e7:~$ su - level1
Password:

Intructions for level1:

You will need to read the manpage for the level
man level1
level1@22203cf417e7:~$ man level1
level1@22203cf417e7:~$ su - level2
Password:
level2@22203cf417e7:~$
```

level2 –

followed the instruction of the man page and navigated to where the password is.

```
level4@22203cf417e7:~$ su - level2
Password:
level2@22203cf417e7:~$
```

level3 –

the password was in the manual. Searched for password using [“/password | n” to see the next mention of the word “password”]

```
level2@22203cf417e7:~$ man level2
level2@22203cf417e7:~$ su - level3
Password:
level3@22203cf417e7:~$
```

level4 –

again used the “/” to search for the mention of the word “password” to find the password

```
level3@22203cf417e7:~$ man level3
level3@22203cf417e7:~$ su - level4
Password:
level4@22203cf417e7:~$
```

level5 –

first used the ls -la command to show the files within the directory and used the cat command on the file “Password” to retrieve the password.

```
level5@22203cf417e7:~$ ls -la
total 20
drwxr-xr-x 1 level5 level5 4096 Apr 12 09:56 .
drwxr-xr-x 1 root   root   4096 Apr 23  2019 ..
-rw------- 1 level5 level5   77 Apr 12 09:58 .bash_history
-rwxr-xr-x 1 level5 level5   34 Apr 23  2019 Password
level5@22203cf417e7:~$ cat Password
e3f20995ffa525dd9f85966813bf1ef7

level5@22203cf417e7:~$
```

level6 –

This time the file name had spaces in between, so back slash “\” has been used to make the shell recognize the spaces and print out the file content which was the password for the next level.

Also, there is an alternative to using the back slash “\” which was encasing the filename within double quotes “” which also printed out the password.

```
level5@22203cf417e7:~$ su - level6
Password:
level6@22203cf417e7:~$ ls -la
total 20
drwxr-xr-x 1 level6 level6 4096 Apr 12 11:20 .
drwxr-xr-x 1 root   root   4096 Apr 23  2019 ..
-rw------- 1 level6 level6 1893 Apr 12 11:20 .bash_history
-rwxr-xr-x 1 level6 level6   33 Apr 23  2019 Spaces Have No Place In File
names.txt
level6@22203cf417e7:~$ cat Spaces\ Have\ No\ Place\ In\ Filenames.txt
a5c2b44a9f8c21d2e1bc8ef449ff49ad
level6@22203cf417e7:~$ cat "Spaces Have No Place In Filenames.txt"
a5c2b44a9f8c21d2e1bc8ef449ff49ad
level6@22203cf417e7:~$
```

level7 –

Here, double hyphen “—” is used to car the file content because the filename consists of a hyphen in the name which the shell would recognize as a flag which is not the case here so, double hyphen tells the shell that the following are not flags but positional arguments.

```
level7@22203cf417e7:~$ ls -la
total 20
-rwxr-xr-x 1 level7 level7   35 Apr 23  2019 -Another Silly -Name.txt
drwxr-xr-x 1 level7 level7 4096 Apr 12 11:35 .
drwxr-xr-x 1 root   root   4096 Apr 23  2019 ..
-rw------- 1 level7 level7  256 Apr 12 11:35 .bash_history
level7@22203cf417e7:~$ cat -- "-Another Silly -Name.txt"
78b6c29509af1e86b1abecf9f0ef126c


level7@22203cf417e7:~$
```

level8 –

Here, the man suggested to use “more “and “less “commands. Observing the workings of both the commands, “less” seemed to be cleaner and more preferred due to its opening of a different page to show the file content while “more” printed out the file content within the terminal cluttering the terminal.

```
level7@22203cf417e7:~$ su - level8
Password:
level8@22203cf417e7:~$ ls -la
total 24
drwxr-xr-x 1 level8 level8 4096 Apr 12 11:40 .
drwxr-xr-x 1 root   root   4096 Apr 23  2019 ..
-rw------- 1 level8 level8  122 Apr 12 11:40 .bash_history
-rwxr-xr-x 1 level8 level8 4673 Apr 23  2019 LargeFile.txt
level8@22203cf417e7:~$ man level8
level8@22203cf417e7:~$ less LargeFile.txt
level8@22203cf417e7:~$ more LargeFile.txt

This is a much larger file That contains the password for Level 8




Nice work using Head, But you need to display some more lines :)



Duis dolor eros, luctus at velit in, aliquet porttitor lacus.
Vivamus sapien mauris, congue ac ex ac, tempus lacinia nisi. Duis risus a
nte,
pulvinar quis nulla nec, egestas ullamcorper augue.

Vivamus pellentesque mi vitae imperdiet consequat. Duis congue, erat
sed laoreet accumsan, tellus sapien lacinia sem, eget ultrices purus
ipsum sit amet nisi. Praesent in diam nulla. Suspendisse porttitor
magna et purus bibendum, ac ornare ante consectetur. In vel ligula
neque. Quisque cursus feugiat lacus dictum feugiat. Aliquam erat
```

Also, the use of head was suggested in the man where “head” is used to print out the first few lines of the file. Here, we have specified the number of the first few lines to be displayed by “head -n <number of lines> filename”.

```
level8@22203cf417e7:~$ ls -al
total 24
drwxr-xr-x 1 level8 level8 4096 Apr 12 11:40 .
drwxr-xr-x 1 root   root   4096 Apr 23  2019 ..
-rw------- 1 level8 level8  122 Apr 12 11:40 .bash_history
-rwxr-xr-x 1 level8 level8 4673 Apr 23  2019 LargeFile.txt
level8@22203cf417e7:~$ man level8
level8@22203cf417e7:~$ head -n 40 LargeFile.txt
```

level9 –

Using “pwd” to check the current working directory. This time the password was the current working directory name.

```
level8@22203cf417e7:~$ su - level9
Password:
level9@22203cf417e7:~$ ls -la
total 16
drwxr-xr-x 1 level9 level9 4096 Apr 12 11:47 .
drwxr-xr-x 1 root   root   4096 Apr 23  2019 ..
-rw------- 1 level9 level9  149 Apr 12 11:47 .bash_history
level9@22203cf417e7:~$ man level9
level9@22203cf417e7:~$ pwd
/home/f3a643dd575af9baeb1ba1d032959358
level9@22203cf417e7:~$
```

level10 –

The password was within the password directory’s Level11.pass file upon which I used “cat” to retrieve the password.

```
level10@22203cf417e7:~$ ls -la
total 32
drwxr-xr-x 1 level10 level10 4096 Apr 23 13:25 .
drwxr-xr-x 1 root    root    4096 Apr 23  2019 ..
-rw------- 1 level10 level10  125 Apr 12 11:52 .bash_history
drwxr-xr-x 2 level10 level10 4096 Apr 23 13:25 .nano
drwxr-xr-x 1 level10 level10 4096 Apr 23 13:25 passwords
level10@22203cf417e7:~$ cd passwords
level10@22203cf417e7:~/passwords$ ls -la
total 20
drwxr-xr-x 1 level10 level10 4096 Apr 23 13:25 .
drwxr-xr-x 1 level10 level10 4096 Apr 23 13:25 ..
-rwxr-xr-x 1 level10 level10   34 Apr 23  2019 Level11.pass
level10@22203cf417e7:~/passwords$ cat Level11.pass
```

level11 –

Used this command to retrieve the password which was distributed among the three files in different directories. Used absolute path with cat to retrieve the passwords contained within each of the file and concatenated them to make one whole password to pass on to the next level.

```
level11@22203cf417e7:~$ cat /file11_1.txt ./file11_2.txt /opt/level11Stuf
f/Foo/file11_3.txt
```

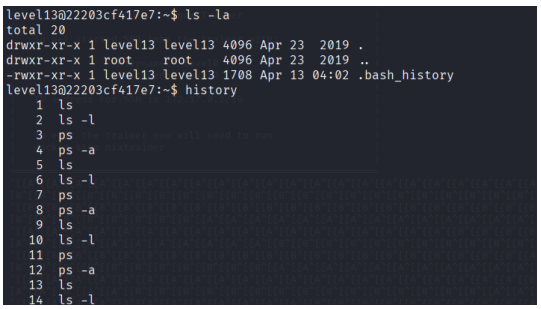
level12 –

Used the “history” command to see the commands executed as user level12 and among them was “cat /var/local/L12Pw.txt” which retrieved the password for the next level.

```
level12@22203cf417e7:~$ ls -la
total 20
drwxr-xr-x 1 level12 level12 4096 Apr 23  2019 .
drwxr-xr-x 1 root    root    4096 Apr 23  2019 ..
-rwxr-xr-x 1 level12 level12  191 Apr 12 12:24 .bash_history
level12@22203cf417e7:~$ man level12
level12@22203cf417e7:~$ history
    1  cd ~
    2  ps -a
    3  ls -la
    4  less /etc/passwd
    5  history
    6  nano /tmp/foo.txt
    7  ls
    8  cd /var/local
    9  cat /var/local/L12Pw.txt
   10  cd ~
   11  ls -a
   12  man level12
   13  man history
   14  man level12
   15  history
   16  cat /var/local/L12Pw.txt
   17  exit
   18  ls -la
   19  man level12
   20  history
level12@22203cf417e7:~$ cat /var/local/L12Pw.txt
```

level13

Here, the password was among the commands previously executed by the user level13.



level14 –

The task was to list the files using “ls” so the password was in the obvious passwordfile.txt file upon which the “cat” command was used to retrieve the password.

```
level14@22203cf417e7:~$ ls -la
total 20
drwxr-xr-x 1 level14 level14 4096 Apr 13 04:05 .
drwxr-xr-x 1 root    root    4096 Apr 23  2019 ..
-rw------- 1 level14 level14   41 Apr 13 04:05 .bash_history
-rwxr-xr-x 1 level14 level14    0 Apr 23  2019 cruft.dat
-rwxr-xr-x 1 level14 level14    0 Apr 23  2019 cruft.txt
-rwxr-xr-x 1 level14 level14   64 Apr 23  2019 passwordfile.txt
level14@22203cf417e7:~$ man level14
level14@22203cf417e7:~$ cat passwordfile.txt
```

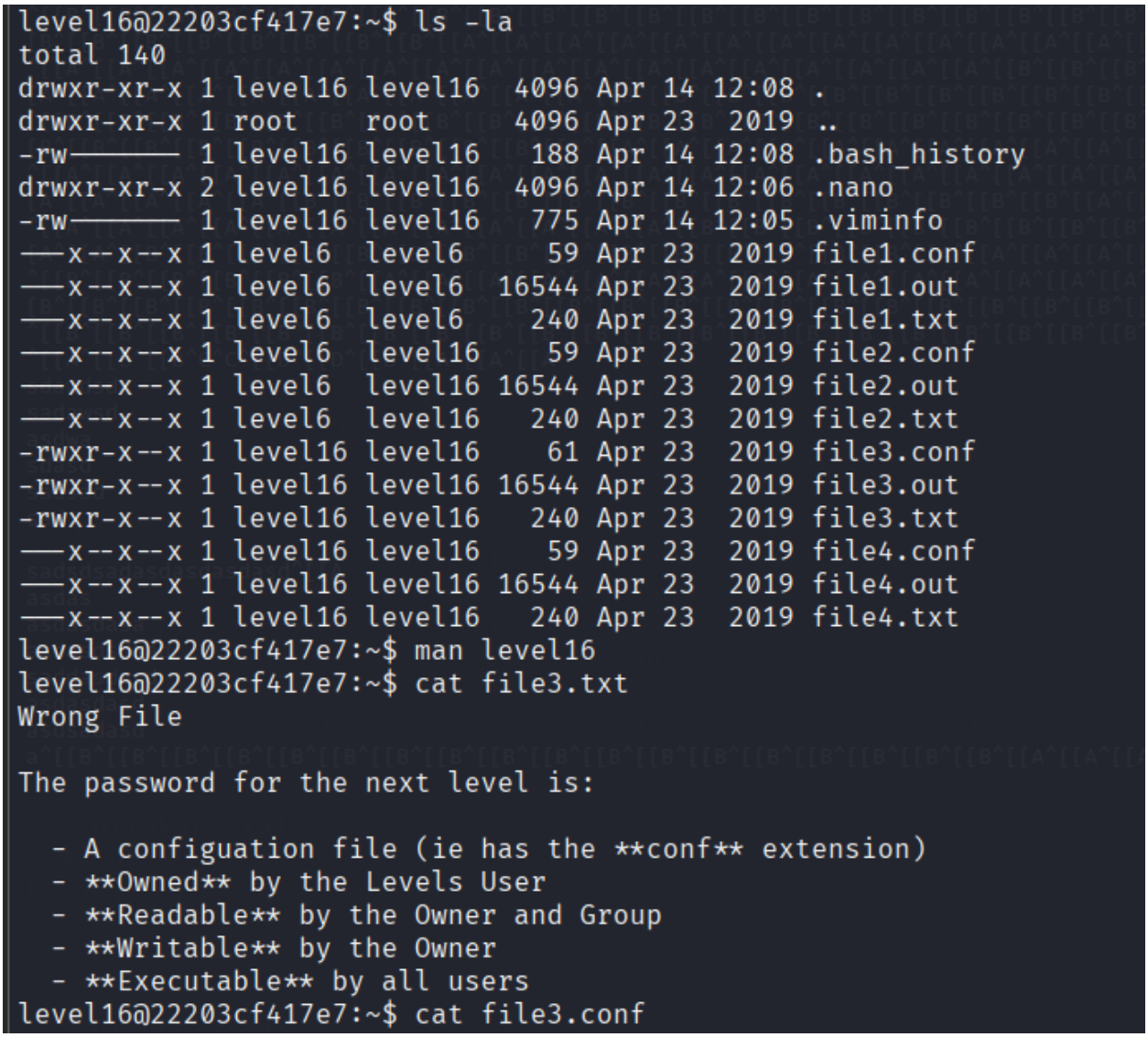
level15 –

Here, the password was inside a hidden file denoted by “.” In the front of the filename which was revealed using the command “-a” with “ls” i.e., listing the hidden files too.

```
level15@22203cf417e7:~$ ls -la
total 24
drwxr-xr-x 1 level15 level15 4096 Apr 13 04:17 .
drwxr-xr-x 1 root    root    4096 Apr 23  2019 ..
-rw------- 1 level15 level15  262 Apr 13 04:17 .bash_history
-rwxr-xr-x 1 level15 level15   64 Apr 23  2019 .hiddenpassword.txt
-rw------- 1 level15 level15  920 Apr 13 04:15 .viminfo
-rwxr-xr-x 1 level15 level15    0 Apr 23  2019 cruft.dat
-rwxr-xr-x 1 level15 level15    0 Apr 23  2019 cruft.txt
level15@22203cf417e7:~$ cat .hiddenpassword.txt
Password for the next level is 468c7152da29221bcac4a40df02ef387
level15@22203cf417e7:~$
```

level16 –

Here, the task was to check for permissions. The ones with the names “file3” had the permissions required for the user level16 to read, write, execute denoted by r, w, x respectively. Hence, following the output from file3.txt, running the file file3.conf gave out the password for the next level.



level17 –

The runme4 file has the SUID bit set (-rws--x--x), allowing it to run with the owner's privileges (elev17).
Although level17 can't read runme4, it can execute it as elev17.
This is why ./runme4 reveals the password while cat runme4 fails.
SUID is used here to safely grant temporary elevated access.

```
level17@22203cf417e7:~$ ls -la
total 144
drwxr-xr-x 1 level17 level17  4096 Apr 14 12:38 .
drwxr-xr-x 1 root    root     4096 Apr 23  2019 ..
-rw------- 1 level17 level17   697 Apr 14 12:38 .bash_history
drwxr-xr-x 2 level17 level17  4096 Apr 14 12:14 .nano
-rw-r--r-- 1 level17 level17 12288 Apr 14 12:38 .source.c.swp
-rw------- 1 level17 level17   943 Apr 14 12:38 .viminfo
-r-------- 1 elev17  elev17     64 Apr 23  2019 Pass.txt
---s--x--x 1 level17 level17 16624 Apr 23  2019 runme1
---x--x--x 1 elev17  elev17  16624 Apr 23  2019 runme2
---s--x--x 1 level17 elev17  16624 Apr 23  2019 runme3
---s--x--x 1 elev17  level17 16624 Apr 23  2019 runme4
---x--x--x 1 level16 level16 16624 Apr 23  2019 runme5
-rwxr--r-- 1 level17 level17   146 Apr 23  2019 source.c
level17@22203cf417e7:~$ man level17
level17@22203cf417e7:~$ cat runme4
cat: runme4: Permission denied
level17@22203cf417e7:~$ ./runme4
Attempting to access file:
```

level18 –

The SUID binary "runme" (owned by elev18) tries to run cat to access a file.
By creating a custom cat script in the current directory, the user hijacks this call.
The PATH variable is updated to prioritize the current directory (.) first.
Now, running "./runme" uses the custom cat, revealing the password or data.

```
level18@22203cf417e7:~$ ls -la
total 64
drwxr-xr-x 1 level18 level18  4096 Apr 17 13:29 .
drwxr-xr-x 1 root    root     4096 Apr 23  2019 ..
-rw------- 1 level18 level18   459 Apr 14 13:09 .bash_history
-rw------- 1 level18 level18   277 Apr 14 12:42 .lesshst
drwxr-xr-x 2 level18 level18  4096 Apr 14 12:43 .nano
-rw------- 1 level18 level18   706 Apr 14 12:53 .viminfo
-r-------- 1 elev18  elev18     36 Apr 23  2019 File.txt
-r-------- 1 elev18  elev18     64 Apr 23  2019 Pass.txt
-rwxr-xr-x 1 level18 level18    32 Apr 14 13:05 cat
---s--x--x 1 elev18  level18 16624 Apr 23  2019 runme
-rwxr--r-- 1 level18 level18   141 Apr 23  2019 source.c
level18@22203cf417e7:~$ nano cat
level18@22203cf417e7:~$ chmod +x cat
level18@22203cf417e7:~$ export PATH=.:PATH
level18@22203cf417e7:~$ ./runme
Attempting to access file:
```

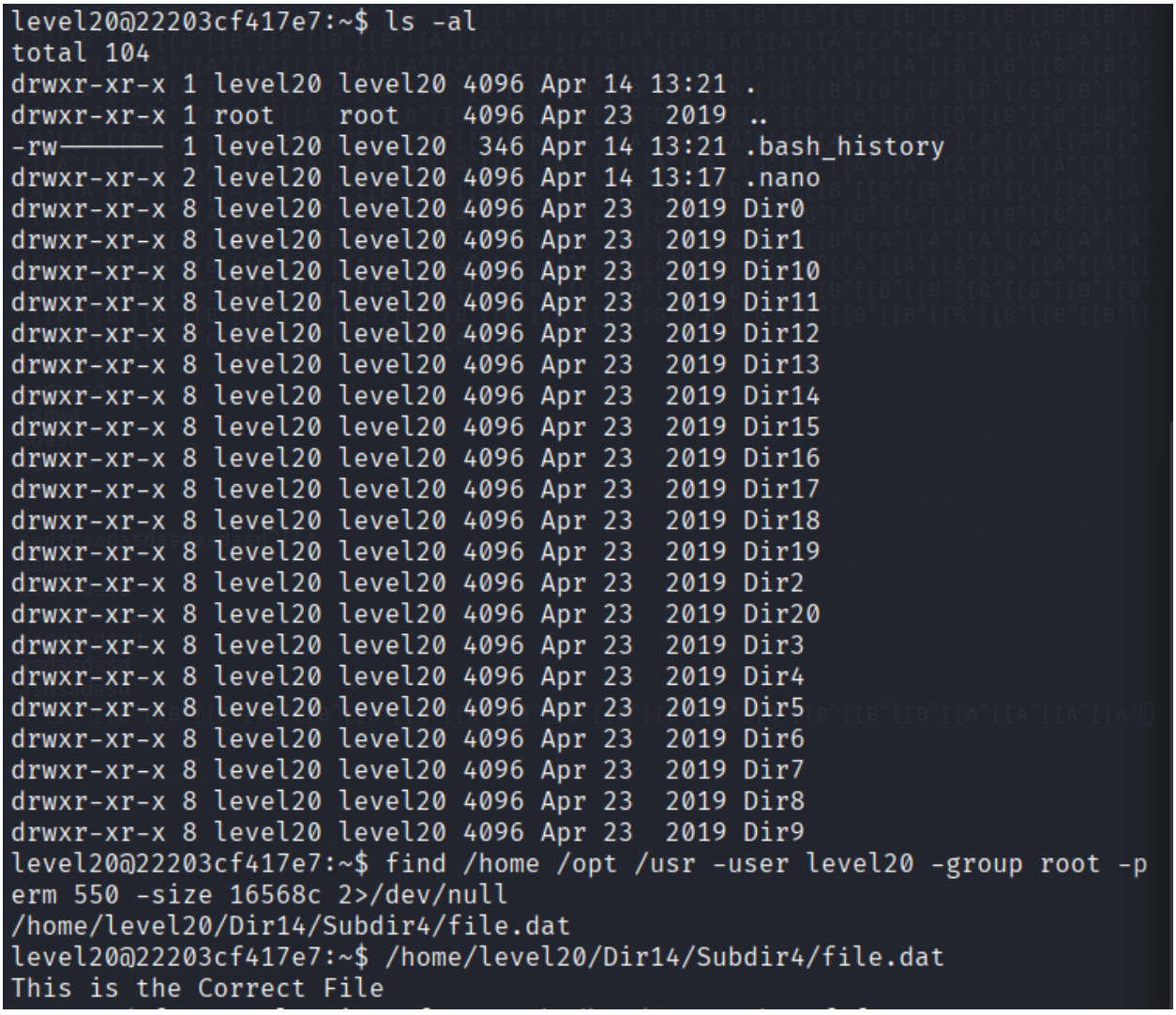
level19-

The task was to find a file named good.txt hidden in a nested directory structure. I used the find command to locate it under /home/level19/Dir12/Sub8/. At first, I tried to run the file as a command, which failed. Then, using cat, I correctly read its contents and found the password. This level emphasized using find efficiently and understanding the difference between executing and reading files.

```
level19@22203cf417e7:~$ ls -la
total 100
drwxr-xr-x  1 level19 level19 4096 Apr 14 13:12 .
drwxr-xr-x  1 root    root    4096 Apr 23  2019 ..
-rw-------  1 level19 level19   95 Apr 14 13:12 .bash_history
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir0
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir1
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir10
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir11
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir12
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir13
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir14
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir15
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir16
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir17
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir18
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir19
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir2
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir20
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir3
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir4
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir5
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir6
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir7
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir8
drwxr-xr-x 13 level19 level19 4096 Apr 23  2019 Dir9
level19@22203cf417e7:~$ man level19
level19@22203cf417e7:~$ find /home -name good.txt
/home/level19/Dir12/Sub8/good.txt
level19@22203cf417e7:~$ /home/level19/Dir12/Sub8/good.txt
/home/level19/Dir12/Sub8/good.txt: line 1: Password: command not found
level19@22203cf417e7:~$ cat /home/level19/Dir12/Sub8/good.txt
```

level20 –

This level required finding a specific file using detailed search criteria. I used the find command to locate a file owned by level20, in the root group, with 550 permissions, and an exact size of 16568 bytes. The correct file was found in Dir14/Subdir4. Executing it revealed the password. This task helped me practice precise file searches using advanced find options.



level21 –

In this level, I needed to find a file owned by level20 and grouped under level21. I used the find command with user and group filters. The correct file, le21.txt, was located in the manual pages directory. Reading it revealed the password for the next level. This reinforced using find for ownership-based file searches.

```
level21@22203cf417e7:/$ find ./ -user level20 -group level21  2>/dev/null
./usr/share/man/man6/le21.txt
level21@22203cf417e7:/$ cat ./usr/share/man/man6/le21.txt
```

level22 –

In this level, I found a password file owned by elev22 and not directly accessible. Using find, I located a binary /bin/reader also owned by elev22. Running it with the restricted file as input successfully printed the password for Level 23. This task illustrated privilege escalation via SUID binaries.

```
level22@22203cf417e7:~$ find / -user elev22 -group elev22  2>/dev/null
/home/level22/Level23.pw
/bin/reader
level22@22203cf417e7:~$ /bin/reader /home/level22/Level23.pw
```

level23 –

In this task, a large data.txt file was provided. I used grep to search for the pattern "PW24:" inside the file. This revealed the password for Level 24 directly within the output. The goal was to efficiently extract specific data from a large file using text-processing commands.

```
level23@22203cf417e7:~$ ls -la
total 172
drwxr-xr-x 1 level23 level23   4096 Apr 23  2019 .
drwxr-xr-x 1 root    root      4096 Apr 23  2019 ..
-rwxr-xr-x 1 level23 level23 162000 Apr 23  2019 data.txt
level23@22203cf417e7:~$ grep "PW24:" data.txt
```

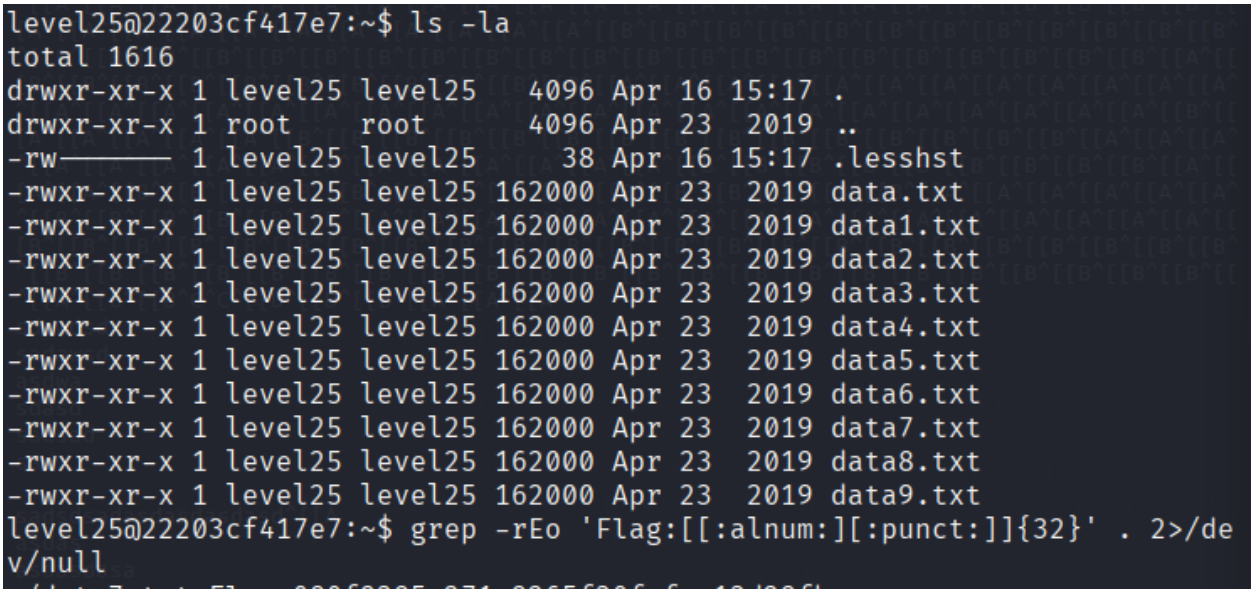
level24 –

The task required extracting a password matching a specific pattern from data.txt. I used grep with a regular expression to match a string that fits the format: 5 lowercase letters, 2 digits, 5 uppercase letters, 2 special characters, and 2 digits. This revealed the correct password.

```
level24@22203cf417e7:~$ ls -la
total 172
drwxr-xr-x 1 level24 level24   4096 Apr 23  2019 .
drwxr-xr-x 1 root    root      4096 Apr 23  2019 ..
-rwxr-xr-x 1 level24 level24 162000 Apr 23  2019 data.txt
level24@22203cf417e7:~$ grep -oE '[a-z]{5}[0-9]{2}[A-Z]{5}[^a-zA-Z0-9]{2}
[0-9]{2}' data.txt
```

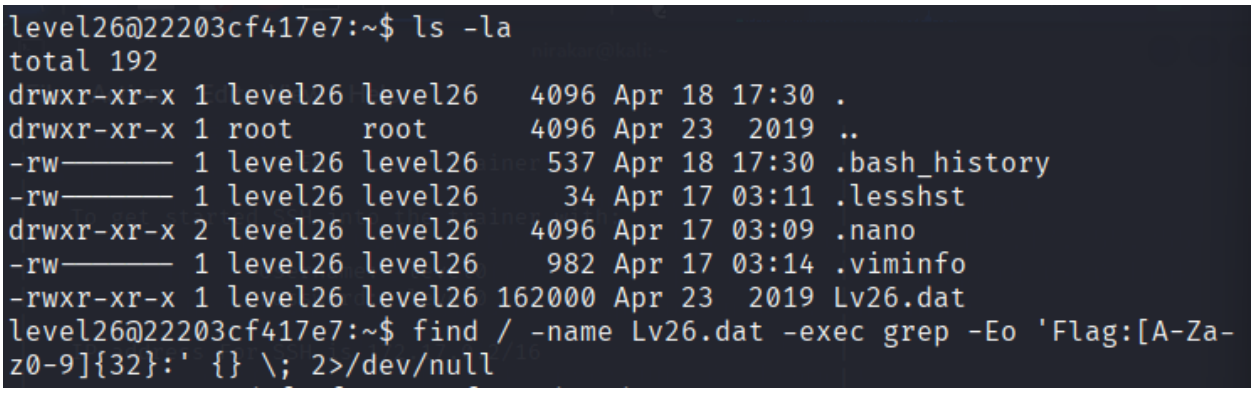
level25 –

This level involved searching multiple files for the flag. I used a recursive grep command with a regex to match the pattern Flag:<32-char string>. The search revealed the correct flag in data7.txt.



level26 –

I used the find command to locate the file Lv26.dat, and then executed grep with a regex to extract the flag. The correct flag was found in the same-named file using -exec with grep.



level27 –

Compared two files using the diff command to identify any differences. The output showed a single differing line between file1.txt and file2.txt. The correct password was found in file2.txt at that line.

```
level27@22203cf417e7:~$ ls -la
total 336
drwxr-xr-x 1 level27 level27   4096 Apr 18 17:29 .
drwxr-xr-x 1 root    root      4096 Apr 23  2019 ..
-rw------- 1 level27 level27     77 Apr 18 17:29 .bash_history
-rwxr-xr-x 1 level27 level27 162000 Apr 23  2019 file1.txt
-rwxr-xr-x 1 level27 level27 161952 Apr 23  2019 file2.txt
level27@22203cf417e7:~$ diff file1.txt file2.txt
879c879
< ouQWQsCruMyXgBTEkAqHAqdahNRlwvwzEhNAgbqtrIOodqtkRtbBAxlSeBJCoAOWWZzoqka
etqpahyHK
---
```

level28 –

Used md5sum on all .txt files to compare file contents via hash values. Most files had identical checksums except one. The file with a different hash was the correct one and contained the password in the filename.

```
level28@22203cf417e7:~$ ls -la
total 1776
drwxr-xr-x 1 level28 level28   4096 Apr 18 17:29 .
drwxr-xr-x 1 root    root      4096 Apr 23  2019 ..
-rw------- 1 level28 level28   2290 Apr 18 17:29 .bash_history
-rwxr-xr-x 1 level28 level28 162000 Apr 23  2019 0ad360e45e0ab518ed1c01dc
5bfdde20.txt
-rwxr-xr-x 1 level28 level28 162000 Apr 23  2019 0fc1d6918da0bacc7d8b3dcb
f25853ad.txt
-rwxr-xr-x 1 level28 level28 162000 Apr 23  2019 4112b747ff854154ff38e271
ee6ecdcb.txt
-rwxr-xr-x 1 level28 level28 162000 Apr 23  2019 468c7152da29221bcac4a40d
f02ef387.txt
-rwxr-xr-x 1 level28 level28 162000 Apr 23  2019 4a3a11a46d26a7814d89e6ef
e0c0fd2a.txt
-rwxr-xr-x 1 level28 level28 162000 Apr 23  2019 697508bad63a602679c94257
78ac0faf.txt
-rw-r--r-- 1 level28 level28      0 Apr 18 08:08 TZAIBcxgahdetJpZMeyEqdCW
OWYzQqWXYXAeXUAyYRtEEdRmNtvKXrIufiUxphnImrygoHwlumkBzncb
-rwxr-xr-x 1 level28 level28 162000 Apr 23  2019 a6e10027186a4a360c3ca27e
58d75968.txt
-rwxr-xr-x 1 level28 level28 162000 Apr 23  2019 bf07d664ee94c60247486886
9e31e5a4.txt
-rwxr-xr-x 1 level28 level28 162000 Apr 23  2019 e3cb9dac40a829e5d0194b8f
adc5ea0b.txt
-rwxr-xr-x 1 level28 level28 162000 Apr 23  2019 f3a643dd575af9baeb1ba1d0
32959358.txt
-rwxr-xr-x 1 level28 level28 162000 Apr 23  2019 fa0d9a03c23ceeedc7ced507
d5c37d9f.txt
level28@22203cf417e7:~$ for file in *.txt; do
>   md5sum "$file"
> done | sort
0d3eedffcfed00b5586766a7c1f1a92c  0ad360e45e0ab518ed1c01dc5bfdde20.txt
0d3eedffcfed00b5586766a7c1f1a92c  0fc1d6918da0bacc7d8b3dcbf25853ad.txt
0d3eedffcfed00b5586766a7c1f1a92c  4112b747ff854154ff38e271ee6ecdcb.txt
0d3eedffcfed00b5586766a7c1f1a92c  468c7152da29221bcac4a40df02ef387.txt
0d3eedffcfed00b5586766a7c1f1a92c  697508bad63a602679c9425778ac0faf.txt
0d3eedffcfed00b5586766a7c1f1a92c  a6e10027186a4a360c3ca27e58d75968.txt
0d3eedffcfed00b5586766a7c1f1a92c  bf07d664ee94c602474868869e31e5a4.txt
0d3eedffcfed00b5586766a7c1f1a92c  e3cb9dac40a829e5d0194b8fadc5ea0b.txt
0d3eedffcfed00b5586766a7c1f1a92c  f3a643dd575af9baeb1ba1d032959358.txt
0d3eedffcfed00b5586766a7c1f1a92c  fa0d9a03c23ceeedc7ced507d5c37d9f.txt
bdb76d110b1ae4bc775e842ecb2f85aa  4a3a11a46d26a7814d89e6efe0c0fd2a.txt
```

level29 –

Found a binary checker and a password list pwlist.txt. Redirected the file into the program using input redirection (<). The program automatically scanned and identified the correct password.

```
level29@22203cf417e7:~$ ls -la
total 64
drwxr-xr-x 1 level29 level29  4096 Apr 20 13:10 .
drwxr-xr-x 1 root    root     4096 Apr 23  2019 ..
drwxr-xr-x 2 level29 level29  4096 Apr 20 13:10 .nano
-rwxr-xr-x 1 level29 level29 16832 Apr 23  2019 checker
-rwxr-xr-x 1 level29 level29 22000 Apr 23  2019 pwlist.txt
level29@22203cf417e7:~$ nano pwlist.txt
level29@22203cf417e7:~$ ./checker < pwlist.txt
Password Check:
Enter data -1 to exit>
Password found MNdytAUKxv
```

level30 –

Used a similar method as the previous level with the checker binary and pwlist.txt. Input redirection fed the password list into the checker. The program output the correct password.

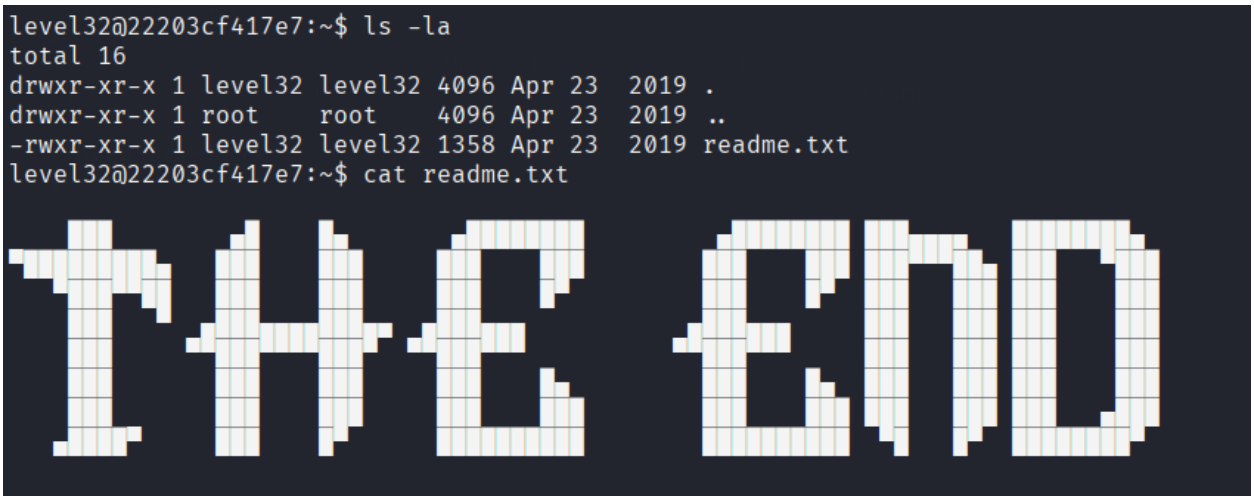
```
level30@22203cf417e7:~$ ls -la
total 56
drwxr-xr-x 1 level30 level30  4096 Apr 23  2019 .
drwxr-xr-x 1 root    root     4096 Apr 23  2019 ..
-rwxr-xr-x 1 level30 level30 16904 Apr 23  2019 checker
-rwxr-xr-x 1 level30 level30 22000 Apr 23  2019 pwlist.txt
level30@22203cf417e7:~$ ./checker < pwlist.txt 2>/dev/null
Password Check:
Enter data -1 to exit>
```

level31 –

Used a while loop to read passwords from pwlist.txt and pass each into ./checker. The outputs were saved to passwords.txt. On inspecting the file, the correct password was revealed.

```
level31@22203cf417e7:~$ cat pwlist.txt | while read pass; do echo "$pass"
 | ./checker; done >> passwords.txt 2>/dev/null
level31@22203cf417e7:~$ less passwords.txt
```

level32 –


level32@22203cf417e7:~$ ls -la
total 16
drwxr-xr-x 1 level32 level32 4096 Apr 23 2019 .
drwxr-xr-x 1 root   root   4096 Apr 23 2019 ..
-rwxr-xr-x 1 level32 level32 1358 Apr 23 2019 readme.txt
level32@22203cf417e7:~$ cat readme.txt
THE END