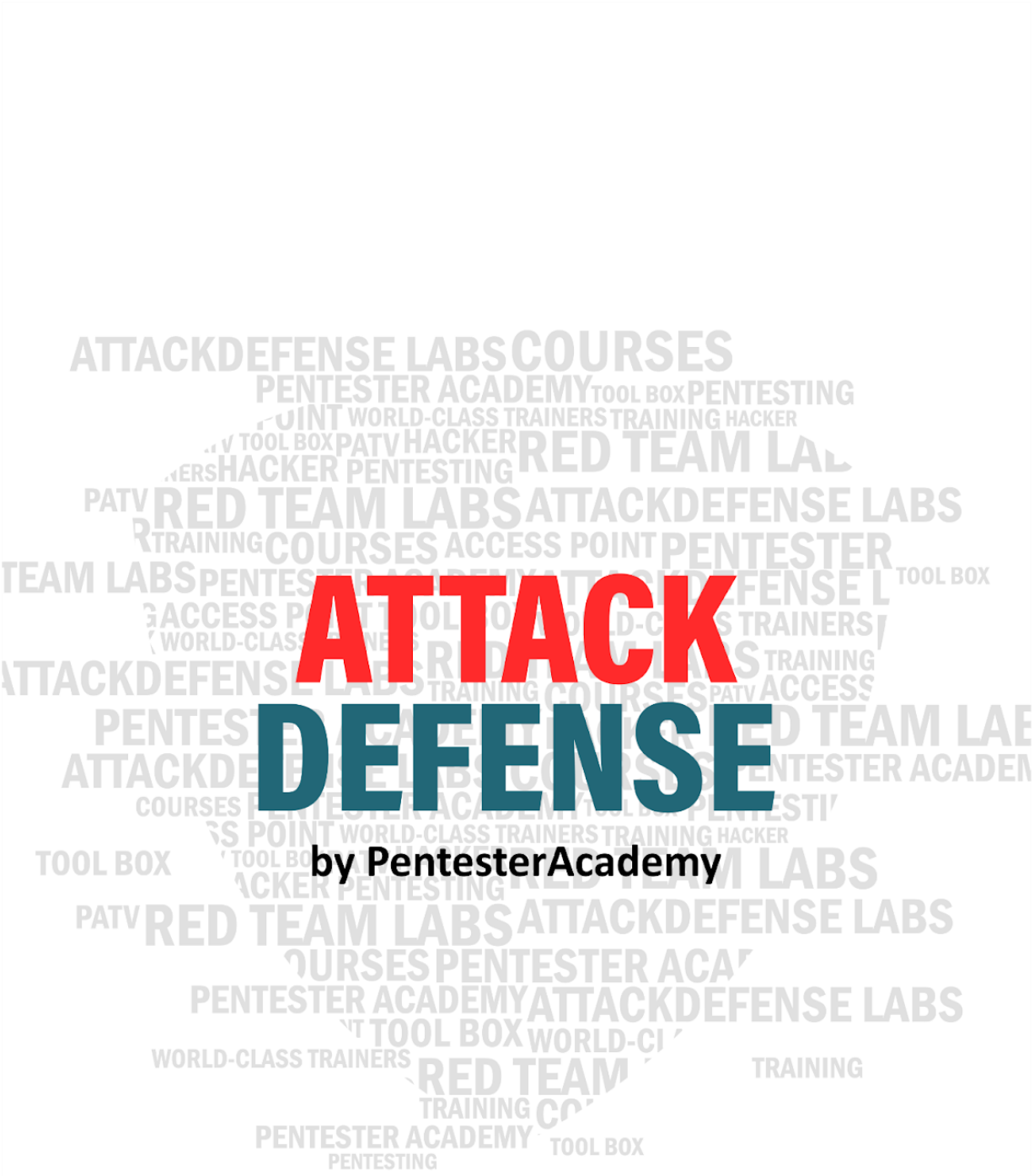
ATTACK
DEFENSE
by PentesterAcademy

| Name | Confining Services with AppArmor |
|---|---|
| URL | https://attackdefense.com/challengedetails?cid=1833 |
| Type | Privilege Escalation : AppArmor |

**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.

A PHP based web shell is hosted on the webserver running on the machine. The index page accepts the “cmd” argument. However, it allows a remote user to run all commands (allowed to www-data user) and list files of the system root directory (/).

**Objective:** Create AppArmor profiles to confine the setup so it can only provide the following functionality to a remote user:

1. Run date, id commands
2. List the contents of the webroot directory (i.e. /var/www/html)
3. Not be able to list the contents of the system root directory (i.e. /)

**Solution:**

**Step 1:** Check the listening sockets opened on the machine and alongwith the process names.

**Command:** sudo netstat -lnp

```
student@localhost:~$ sudo netstat -lnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      387/nginx: master p
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      376/sshd
tcp6       0      0 :::80                   :::*                    LISTEN      387/nginx: master p
tcp6       0      0 :::22                   :::*                    LISTEN      376/sshd
raw6       0      0 :::58                   :::*                    7           224/systemd-network
```

```
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     STREAM     LISTENING     15794    424/systemd          /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     15798    424/systemd          /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     15068    424/systemd          /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     15069    424/systemd          /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     15070    424/systemd          /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     15071    424/systemd          /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     10160    1/init               /run/systemd/private
unix  2      [ ACC ]     SEQPACKET  LISTENING     10905    1/init               /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     10907    1/init               /run/systemd/journal/stdout
unix  2      [ ACC ]     STREAM     LISTENING     12200    1/init               /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     15445    358/php-fpm: master  /run/php/php7.2-fpm.sock
student@localhost:~$
```

Nginx is listening on port 80.

**Step 2:** Check the processes running unconfined on the system.

**Command:** sudo aa-unconfined --paranoid

```
student@localhost:~$ sudo aa-unconfined --paranoid
1 /lib/systemd/systemd (/sbin/init) not confined
193 /lib/systemd/systemd-journald not confined
201 /lib/systemd/systemd-udevd not confined
224 /lib/systemd/systemd-networkd not confined
240 /sbin/auditd not confined
354 /usr/bin/python3.6 (/usr/bin/python3) not confined
355 /usr/sbin/rsyslogd not confined
356 /lib/systemd/systemd-logind not confined
358 /usr/sbin/php-fpm7.2 (php-fpm: master process (/etc/php/7.2/fpm/php-fpm.conf)) not confined
361 /usr/bin/dbus-daemon not confined
376 /usr/sbin/sshd not confined
379 /sbin/agetty not confined
382 /usr/sbin/php-fpm7.2 not confined
383 /usr/sbin/php-fpm7.2 not confined
387 /usr/sbin/nginx (nginx: master process /usr/sbin/nginx -g daemon on; master_process on;) not confined
388 /usr/sbin/nginx not confined
389 /usr/sbin/nginx not confined
421 /usr/sbin/sshd not confined
424 /lib/systemd/systemd not confined
425 /lib/systemd/systemd not confined
451 /usr/sbin/sshd (sshd: student@pts/0) not confined
452 /bin/bash (bash -c clear;/bin/bash) not confined
454 /bin/bash (/bin/bash) not confined
462 /usr/bin/sudo not confined
463 /usr/bin/python3.6 (/usr/bin/python3) not confined
student@localhost:~$
```

**Step 3:** Check the apparmor status.

**Command:** sudo aa-status

```
student@localhost:~$ sudo aa-status
apparmor module is loaded.
53 profiles are loaded.
16 profiles are in enforce mode.
   /sbin/dhclient
   /usr/bin/lxc-start
   /usr/bin/man
   /usr/lib/NetworkManager/nm-dhcp-client.action
   /usr/lib/NetworkManager/nm-dhcp-helper
   /usr/lib/chromium-browser/chromium-browser//browser_java
   /usr/lib/chromium-browser/chromium-browser//browser_openjdk
   /usr/lib/chromium-browser/chromium-browser//sanitized_helper
   /usr/lib/connman/scripts/dhclient-script
   /usr/sbin/haveged
37 profiles are in complain mode.
   /usr/lib/chromium-browser/chromium-browser
   /usr/lib/chromium-browser/chromium-browser//chromium_browser_sandbox
   /usr/lib/chromium-browser/chromium-browser//lsb_release
   /usr/lib/chromium-browser/chromium-browser//xdgsettings
   /usr/lib/dovecot/anvil
   /usr/lib/dovecot/auth
   /usr/lib/dovecot/config
   /usr/lib/dovecot/deliver
   /usr/lib/dovecot/dict
0 processes have profiles defined.
0 processes are in enforce mode.
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
student@localhost:~$
```

**Step 4:** Open another terminal T2. Run id, date and file listing command using curl.

**Commands:**
curl http://localhost?cmd=id
curl "http://localhost?cmd=date"
curl "http://localhost?cmd=ls -l ."

```
student@localhost:~$ curl http://localhost?cmd=id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

student@localhost:~$ curl "http://localhost?cmd=date"
Fri Apr 24 02:48:23 UTC 2020

student@localhost:~$ curl "http://localhost?cmd=ls -l ."
total 20
-rw-r--r-- 1 root root 10918 Oct 24  2019 index.html
-rw-r--r-- 1 root root   612 Apr 24 01:39 index.nginx-debian.html
-rw-r--r-- 1 root root    61 Apr 24 01:37 index.php
```

**Step 5:** However, the listing of the system root directory also works.

**Command:** curl "http://localhost?cmd=ls -l /"

```
student@localhost:~$ curl "http://localhost?cmd=ls -l /"
total 76
drwxr-xr-x   2 root root  4096 Apr 24 01:39 bin
drwxr-xr-x   2 root root  4096 Aug 18  2019 boot
drwxr-xr-x  16 root root  3900 Apr 24 02:34 dev
drwxr-xr-x  90 root root  4096 Apr 24 01:40 etc
drwxr-xr-x   3 root root  4096 Oct 23  2019 home
drwxr-xr-x  15 root root  4096 Apr 24 01:39 lib
drwxr-xr-x   2 root root  4096 Aug 18  2019 lib64
drwx------   2 root root 16384 Aug 18  2019 lost+found
drwxr-xr-x   2 root root  4096 Aug 18  2019 media
drwxr-xr-x   2 root root  4096 Aug 18  2019 mnt
drwxr-xr-x   3 root root  4096 Aug 18  2019 opt
dr-xr-xr-x 100 root root     0 Apr 24 02:33 proc
drwx------   5 root root  4096 Apr 24 02:34 root
drwxr-xr-x  16 root root   500 Apr 24 02:35 run
```

**Step 6:** Switch to terminal T1, change to apparmor profile directory and run aa-autodep to generate a new blank profile.

**Commands:**
cd /etc/apparmor.d
sudo aa-autodep nginx

```
student@localhost:/etc/apparmor.d$ sudo aa-autodep nginx
Writing updated profile for /usr/sbin/nginx.
student@localhost:/etc/apparmor.d$
```

**Step 7:** Check the contents of the newly created profile.

**Command:** sudo cat usr.sbin.nginx

```
student@localhost:/etc/apparmor.d$ sudo cat usr.sbin.nginx
# Last Modified: Fri Apr 24 02:50:12 2020
#include <tunables/global>

/usr/sbin/nginx flags=(complain) {
  #include <abstractions/base>

  /lib/x86_64-linux-gnu/ld-*.so mr,
  /usr/sbin/nginx mr,

}
student@localhost:/etc/apparmor.d$
```

**Step 8:** Check the apparmor status.

**Command:** sudo aa-status

```
3 processes have profiles defined.
0 processes are in enforce mode.
0 processes are in complain mode.
3 processes are unconfined but have a profile defined.
   /usr/sbin/nginx (387)
   /usr/sbin/nginx (388)
   /usr/sbin/nginx (389)
student@localhost:/etc/apparmor.d$
```

The nginx is now showing up under the “undefined but have a profile” category because of the newly created profile.

**Step 9:** Move the nginx profile to complain mode.

**Command:** sudo aa-complain usr.sbin.nginx

```
student@localhost:/etc/apparmor.d$ sudo aa-complain usr.sbin.nginx
Setting /etc/apparmor.d/usr.sbin.nginx to complain mode.
student@localhost:/etc/apparmor.d$
```

**Step 10:** Restart the process so it can be started under the profile restrictions.

**Command:** sudo /etc/init.d/nginx restart

```
student@localhost:/etc/apparmor.d$ sudo /etc/init.d/nginx restart
[ ok ] Restarting nginx (via systemctl): nginx.service.
student@localhost:/etc/apparmor.d$
```

**Step 11:** Check the apparmor status.

**Command:** sudo aa-status

```
3 processes have profiles defined.
0 processes are in enforce mode.
3 processes are in complain mode.
   /usr/sbin/nginx (734)
   /usr/sbin/nginx (735)
   /usr/sbin/nginx (736)
0 processes are unconfined but have a profile defined.
student@localhost:/etc/apparmor.d$
```

The nginx process is moved to “complain” mode.

**Step 12:** Currently the profile has no effect. Adjust the profile according to the nginx.

**Command:** sudo aa-logprof

The logprof utility will read the audit.log file for the logs generated by nginx service and prompt the user to classify the action.

```
student@localhost:/etc/apparmor.d$ sudo aa-logprof
Reading log entries from /var/log/audit/audit.log.
Updating AppArmor profiles in /etc/apparmor.d.
Complain-mode changes:

Profile:    /usr/sbin/nginx
Capability: dac_override
Severity:   9

 [1 - #include <abstractions/lxc/container-base>]
  2 - #include <abstractions/lxc/start-container>
  3 - capability dac_override,
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

Move the pointer to point 3. Similarly, for all such prompts, the cursor needs to be moved to the point of interest before pressing the key.

This entry is for dac_override capability.

**Key pressed:** a (to allow the capability)

```
Profile:    /usr/sbin/nginx
Capability: dac_override
Severity:   9

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - capability dac_override,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

This entry is for net_bind_service capability.

**Key pressed:** a (to allow the capability)

```
Profile:    /usr/sbin/nginx
Capability: net_bind_service
Severity:   8

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/nis>
 [4 - capability net_bind_service,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

This entry is for setgid capability.

**Key pressed:** a (to allow the capability)

```
Profile:    /usr/sbin/nginx
Capability: setgid
Severity:   9

  1 - #include <abstractions/dovecot-common>
  2 - #include <abstractions/lxc/container-base>
  3 - #include <abstractions/lxc/start-container>
  4 - #include <abstractions/postfix-common>
 [5 - capability setgid,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

This entry is for setuid capability.

**Key pressed:** a (to allow the capability)

```
Profile:    /usr/sbin/nginx
Capability: setuid
Severity:   9

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/postfix-common>
 [4 - capability setuid,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

This entry is to allow write access to the error.log file. But to make sure that it can access all other files with .log extension in this directory (i.e. /var/log/nginx) like access.log, one can use the “Glob with the Extension” option.

**Key pressed:** e (Glob with Extension)

```
Profile:  /usr/sbin/nginx
Path:     /var/log/nginx/error.log
New Mode: w
Severity: 8

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - /var/log/nginx/error.log w,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
```

Allow the newly added entry with the Glob.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /var/log/nginx/error.log
New Mode: w
Severity: 8

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - /var/log/nginx/error.log w,
 [4 - /var/log/nginx/*.log w,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
```

This entry is to allow read access to the openssl configuration.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /etc/ssl/openssl.cnf
New Mode: owner r
Severity: 2

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/openssl>
  4 - #include <abstractions/ssl_keys>
 [5 - owner /etc/ssl/openssl.cnf r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read access to the nginx configuration. Add a Glob with Extension for this.

**Key pressed:** e (Glob with Extension)

```
Profile:  /usr/sbin/nginx
Path:     /etc/nginx/nginx.conf
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /etc/nginx/nginx.conf r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

Allow the newly added entry with the Glob.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /etc/nginx/nginx.conf
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - owner /etc/nginx/nginx.conf r,
 [4 - owner /etc/nginx/*.conf r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read access to the nsswitch configuration.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /etc/nsswitch.conf
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/nameservice>
 [4 - owner /etc/nsswitch.conf r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read access to the passwd file.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /etc/passwd
New Mode: owner r
Severity: 4

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/nameservice>
 [4 - owner /etc/passwd r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read access to the group file.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /etc/group
New Mode: owner r
Severity: 4

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/nameservice>
 [4 - owner /etc/group r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read access to the modules-enabled directory.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /etc/nginx/modules-enabled/
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /etc/nginx/modules-enabled/ r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read access to the mod-http-geoip configuration file.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /usr/share/nginx/modules-available/mod-http-geoip.conf
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /usr/share/nginx/modules-available/mod-http-geoip.conf r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read access to the mod-http-image-filter configuration file.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /usr/share/nginx/modules-available/mod-http-image-filter.conf
New Mode: owner r
Severity: unknown

 [1 - #include <abstractions/lxc/container-base>]
  2 - #include <abstractions/lxc/start-container>
  3 - owner /usr/share/nginx/modules-available/mod-http-image-filter.conf r,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read access to the mod-mail configuration file. But as there are a lot of modules for nginx, it makes sense to use Glob with Extension.

**Key pressed:** e (Glob with Extension)

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /usr/share/nginx/modules-available/mod-mail.conf
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - owner /usr/share/nginx/modules-available/mod-mail.conf r,
 [4 - owner /usr/share/nginx/modules-available/*.conf r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read access to the mime.types file.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /etc/nginx/mime.types
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /etc/nginx/mime.types r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read access to the conf.d directory.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /etc/nginx/conf.d/
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /etc/nginx/conf.d/ r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read access to the sites-enabled directory.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /etc/nginx/sites-enabled/
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /etc/nginx/sites-enabled/ r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read access to the default configuration file.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /etc/nginx/sites-available/default
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /etc/nginx/sites-available/default r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read access to the fastcgi-php.conf configuration file.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /etc/nginx/snippets/fastcgi-php.conf
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /etc/nginx/snippets/fastcgi-php.conf r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow read/write access to the nginx.pid file.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /run/nginx.pid
New Mode: owner rw
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /run/nginx.pid rw,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is to allow usage of inet v4 stream socket.

**Key pressed:** a (to allow the capability)

```
Profile:        /usr/sbin/nginx
Network Family: inet
Socket Type:    stream

  1 - #include <abstractions/apache2-common>
  2 - #include <abstractions/lxc/container-base>
  3 - #include <abstractions/lxc/start-container>
  4 - #include <abstractions/nameservice>
 [5 - network inet stream,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

This entry is to allow usage of inet v6 stream socket.

**Key pressed:** a (to allow the capability)

```
Profile:        /usr/sbin/nginx
Network Family: inet6
Socket Type:    stream

  1 - #include <abstractions/apache2-common>
  2 - #include <abstractions/lxc/container-base>
  3 - #include <abstractions/lxc/start-container>
  4 - #include <abstractions/nameservice>
 [5 - network inet6 stream,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

Once all the entries are done, save the profile.

**Key pressed:** s (to save the profile)

```
Adding network inet6 stream, to profile.

= Changed Local Profiles =

The following local profiles were changed. Would you like to save them?

 [1 - /usr/sbin/nginx]
(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean profiles / Abo(r)t
Writing updated profile for /usr/sbin/nginx.
student@localhost:/etc/apparmor.d$
```

**Step 13:** Check the updated nginx profile.

**Command:** sudo cat usr.sbin.nginx

```
student@localhost:/etc/apparmor.d$ sudo cat usr.sbin.nginx
# Last Modified: Fri Apr 24 03:12:08 2020
#include <tunables/global>

/usr/sbin/nginx flags=(complain) {
  #include <abstractions/base>

  capability dac_override,
  capability net_bind_service,
  capability setgid,
  capability setuid,

  network inet stream,
  network inet6 stream,
```

```
  /var/log/nginx/*.log w,
  owner /etc/group r,
  owner /etc/nginx/*.conf r,
  owner /etc/nginx/conf.d/ r,
  owner /etc/nginx/mime.types r,
  owner /etc/nginx/modules-enabled/ r,
  owner /etc/nginx/sites-available/default r,
  owner /etc/nginx/sites-enabled/ r,
  owner /etc/nginx/snippets/fastcgi-php.conf r,
  owner /etc/nsswitch.conf r,
  owner /etc/passwd r,
  owner /etc/ssl/openssl.cf r,
  owner /run/nginx.pid rw,
  owner /usr/share/nginx/modules-available/*.conf r,
  owner /{usr/,}lib{,32,64}/** mr,

}
```

**Step 14:** Move the profile to enforce mode.

**Command:** sudo aa-enforce usr.sbin.nginx

```
student@localhost:/etc/apparmor.d$ sudo aa-enforce usr.sbin.nginx
Setting /etc/apparmor.d/usr.sbin.nginx to enforce mode.
student@localhost:/etc/apparmor.d$
```

**Step 15:** Check the apparmor status.

**Command:** sudo aa-status

```
3 processes have profiles defined.
3 processes are in enforce mode.
   /usr/sbin/nginx (796)
   /usr/sbin/nginx (797)
   /usr/sbin/nginx (798)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
student@localhost:/etc/apparmor.d$
```

**Step 16:** Switch to terminal T2. Run id, date and file listing command using the curl command.

**Commands:**
curl http://localhost?cmd=id
curl "http://localhost?cmd=date"
curl "http://localhost?cmd=ls -l ."

```
student@localhost:~$ curl "http://localhost?cmd=id"
<html>
<head><title>502 Bad Gateway</title></head>
<body bgcolor="white">
<center><h1>502 Bad Gateway</h1></center>
<hr><center>nginx/1.14.0 (Ubuntu)</center>
</body>
</html>
student@localhost:~$
student@localhost:~$ curl "http://localhost?cmd=date"
<html>
<head><title>502 Bad Gateway</title></head>
<body bgcolor="white">
<center><h1>502 Bad Gateway</h1></center>
<hr><center>nginx/1.14.0 (Ubuntu)</center>
</body>
</html>
student@localhost:~$ curl "http://localhost?cmd=ls -l"
<html>
<head><title>502 Bad Gateway</title></head>
<body bgcolor="white">
<center><h1>502 Bad Gateway</h1></center>
<hr><center>nginx/1.14.0 (Ubuntu)</center>
</body>
</html>
student@localhost:~$
```

These commands are not working as the nginx is not able to access the php-fpm UNIX socket.

**Step 17:** Adjust the profile accordingly to allow the read/write permission on this socket.

**Command:** sudo aa-logprof

The logprof utility will read the audit.log file for the logs generated by nginx service and prompt the user to classify the action.

```
student@localhost:/etc/apparmor.d$ sudo aa-logprof
Reading log entries from /var/log/audit/audit.log.
Updating AppArmor profiles in /etc/apparmor.d.
Complain-mode changes:
Enforce-mode changes:

Profile:  /usr/sbin/nginx
Path:     /run/php/php7.2-fpm.sock
New Mode: owner rw
Severity: unknown

 [1 - #include <abstractions/lxc/container-base>]
  2 - #include <abstractions/lxc/start-container>
  3 - owner /run/php/php7.2-fpm.sock rw,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

Move the pointer to point 3.

This entry is for read/write access on php7.2-fpm UNIX socket.

**Key pressed:** a (to allow the capability)

```
Profile:  /usr/sbin/nginx
Path:     /run/php/php7.2-fpm.sock
New Mode: owner rw
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /run/php/php7.2-fpm.sock rw,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

Save the profile.

**Key pressed:** s (save the changes)

```
= Changed Local Profiles =

The following local profiles were changed. Would you like to save them?

 [1 - /usr/sbin/nginx]
(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean profiles / Abo(r)t
Writing updated profile for /usr/sbin/nginx.
student@localhost:/etc/apparmor.d$
```

**Step 18:** Switch to terminal T2. Run id, date and file listing command using the curl command.

**Commands:**
curl http://localhost?cmd=id
curl "http://localhost?cmd=date"
curl "http://localhost?cmd=ls -l ."

```
student@localhost:~$ curl "http://localhost?cmd=id"
uid=33(www-data) gid=33(www-data) groups=33(www-data)

student@localhost:~$ curl "http://localhost?cmd=date"
Fri Apr 24 03:19:05 UTC 2020

student@localhost:~$ curl "http://localhost?cmd=ls -l ."
total 20
-rw-r--r-- 1 root root 10918 Oct 24  2019 index.html
-rw-r--r-- 1 root root   612 Apr 24 01:39 index.nginx-debian.html
-rw-r--r-- 1 root root    61 Apr 24 01:37 index.php

student@localhost:~$
```

This time all the commands worked. However, the file listing of the system root directory is also possible.

**Command:** curl "http://localhost?cmd=ls -l ."

```
student@localhost:~$ curl "http://localhost?cmd=ls -l /"
total 76
drwxr-xr-x  2 root root  4096 Apr 24 01:39 bin
drwxr-xr-x  2 root root  4096 Aug 18  2019 boot
drwxr-xr-x 16 root root  3900 Apr 24 02:34 dev
drwxr-xr-x 90 root root  4096 Apr 24 01:40 etc
drwxr-xr-x  3 root root  4096 Oct 23  2019 home
drwxr-xr-x 15 root root  4096 Apr 24 01:39 lib
drwxr-xr-x  2 root root  4096 Aug 18  2019 lib64
drwx------  2 root root 16384 Aug 18  2019 lost+found
drwxr-xr-x  2 root root  4096 Aug 18  2019 media
```

This is happening because the command is being executed by php-fpm service and not nginx. Hence, the php-fpm also has to be confined.

**Step 19:** Create a blank profile for php-fpm.

**Commands:** sudo aa-autodep php-fpm7.2

```
student@localhost:/etc/apparmor.d$ sudo aa-autodep php-fpm7.2
Writing updated profile for /usr/sbin/php-fpm7.2.
student@localhost:/etc/apparmor.d$
```

**Step 20:** Check the generated profile.

**Commands:** sudo cat usr.sbin.php-fpm7.2

```
student@localhost:/etc/apparmor.d$ sudo cat usr.sbin.php-fpm7.2
# Last Modified: Fri Apr 24 03:21:02 2020
#include <tunables/global>

/usr/sbin/php-fpm7.2 flags=(complain) {
  #include <abstractions/base>

  /lib/x86_64-linux-gnu/ld-*.so mr,
  /usr/sbin/php-fpm7.2 mr,

}
student@localhost:/etc/apparmor.d$
```

**Step 21:** Check the apparmor status.

**Command:** sudo aa-status

```
6 processes have profiles defined.
3 processes are in enforce mode.
   /usr/sbin/nginx (796)
   /usr/sbin/nginx (797)
   /usr/sbin/nginx (798)
0 processes are in complain mode.
3 processes are unconfined but have a profile defined.
   /usr/sbin/php-fpm7.2 (358)
   /usr/sbin/php-fpm7.2 (382)
   /usr/sbin/php-fpm7.2 (383)
student@localhost:/etc/apparmor.d$
```

As the profile is created, now the php-fpm will be listed under the “unconfined but have profile” category.

**Step 22:** Move this policy to complain mode and restart the service.

**Commands:**
sudo aa-complain usr.sbin.php-fpm7.2
sudo /etc/init.d/php7.2-fpm restart

```
student@localhost:/etc/apparmor.d$ sudo aa-complain usr.sbin.php-fpm7.2
Setting /etc/apparmor.d/usr.sbin.php-fpm7.2 to complain mode.
student@localhost:/etc/apparmor.d$
student@localhost:/etc/apparmor.d$ sudo /etc/init.d/php7.2-fpm restart
[ ok ] Restarting php7.2-fpm (via systemctl): php7.2-fpm.service.
student@localhost:/etc/apparmor.d$
```

**Step 23:** Check the apparmor status.

**Command:** sudo aa-status

```
6 processes have profiles defined.
3 processes are in enforce mode.
   /usr/sbin/nginx (796)
   /usr/sbin/nginx (797)
   /usr/sbin/nginx (798)
3 processes are in complain mode.
   /usr/sbin/php-fpm7.2 (1296)
   /usr/sbin/php-fpm7.2 (1298)
   /usr/sbin/php-fpm7.2 (1299)
0 processes are unconfined but have a profile defined.
student@localhost:/etc/apparmor.d$
```

The php-fpm process is in complain mode now.

**Step 24:** Switch to terminal T2. Run id, date and file listing command using the curl command.

**Commands:**
curl http://localhost?cmd=id
curl "http://localhost?cmd=date"
curl "http://localhost?cmd=ls -l ."

```
student@localhost:~$ curl "http://localhost?cmd=ls -l ."
total 20
-rw-r--r-- 1 root root 10918 Oct 24  2019 index.html
-rw-r--r-- 1 root root   612 Apr 24 01:39 index.nginx-debian.html
-rw-r--r-- 1 root root    61 Apr 24 01:37 index.php

student@localhost:~$ curl "http://localhost?cmd=id"
uid=33(www-data) gid=33(www-data) groups=33(www-data)

student@localhost:~$ curl "http://localhost?cmd=date"
Fri Apr 24 03:23:44 UTC 2020

student@localhost:~$
```

**Step 25:** Adjust the profile accordingly to allow these binaries and dependencies.

**Command:** sudo aa-logprof

The first entry is to access the dash shell.

**Key pressed:** i (inherit)

```
student@localhost:/etc/apparmor.d$ sudo aa-logprof
Reading log entries from /var/log/audit/audit.log.
Updating AppArmor profiles in /etc/apparmor.d.

Profile:  /usr/sbin/php-fpm7.2
Execute:  /bin/dash
Severity: unknown

(I)nherit / (C)hild / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t / (F)inish
```

This entry is for dac_override capability.

**Key pressed:** d (deny)

```
Profile:    /usr/sbin/php-fpm7.2
Capability: dac_override
Severity:   9

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - capability dac_override,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

This entry is for chown capability.

**Key pressed:** d (deny)

```
Profile:    /usr/sbin/php-fpm7.2
Capability: chown
Severity:   9

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - capability chown,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

This entry is for net_admin capability.

**Key pressed:** a (allow)

```
Profile:    /usr/sbin/php-fpm7.2
Capability: net_admin
Severity:   8

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - capability net_admin,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

This entry is for setgid capability.

**Key pressed:** d (deny)

```
Profile:    /usr/sbin/php-fpm7.2
Capability: setgid
Severity:   9

  1 - #include <abstractions/dovecot-common>
  2 - #include <abstractions/lxc/container-base>
  3 - #include <abstractions/lxc/start-container>
  4 - #include <abstractions/postfix-common>
 [5 - capability setgid,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

This entry is for setuid capability.

**Key pressed:** d (deny)

```
Profile:    /usr/sbin/php-fpm7.2
Capability: setuid
Severity:   9

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/postfix-common>
 [4 - capability setuid,]
(A)llow / [(D)eny] / (I)gnore / Audi(t) / Abo(r)t / (F)inish
```

This entry is for read access on php.ini file. However, it is better to add a Glob (without extension here).

**Key pressed:** g (glob)

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/php/7.2/fpm/php.ini
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/php>
 [4 - owner /etc/php/7.2/fpm/php.ini r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish

Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/php/7.2/fpm/php.ini
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/php>
  4 - owner /etc/php/7.2/fpm/php.ini r,
 [5 - owner /etc/php/7.2/fpm/*.ini r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for read/owner access on conf.d directory. However, it is better to add a Glob (without extension here).

**Key pressed:** g (glob)

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/php/7.2/fpm/conf.d/
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/php>
 [4 - owner /etc/php/7.2/fpm/conf.d/ r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish

Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/php/7.2/fpm/conf.d/
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/php>
  4 - owner /etc/php/7.2/fpm/conf.d/ r,
 [5 - owner /etc/php/7.2/fpm/*/ r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for read/owner access on opcache.ini file. However, it is better to add a Glob (without extension here).

**Key pressed:** g (glob)

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/php/7.2/mods-available/opcache.ini
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/php>
 [4 - owner /etc/php/7.2/mods-available/opcache.ini r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish

Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/php/7.2/mods-available/opcache.ini
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/php>
  4 - owner /etc/php/7.2/mods-available/opcache.ini r,
 [5 - owner /etc/php/7.2/mods-available/* r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for accessing /usr and /lib directories.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /usr/lib/php/20170718/opcache.so
Old Mode: r
New Mode: owner mr
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/php>
  4 - #include <abstractions/ubuntu-browsers.d/plugins-common>
 [5 - owner /{usr/,}lib{,32,64}/** mr,]
  6 - owner /usr/lib/php/20170718/opcache.so mr,
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for owner/read access of openssl.cnf configuration file.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/ssl/openssl.cnf
New Mode: owner r
Severity: 2

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/openssl>
  4 - #include <abstractions/ssl_keys>
 [5 - owner /etc/ssl/openssl.cnf r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for owner/write/lock access to a file in /tmp directory.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /tmp/.ZendSem.FyQo3Z
New Mode: owner rwk
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/php>
  4 - #include <abstractions/user-tmp>
 [5 - owner /tmp/.ZendSem.FyQo3Z rwk,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for read/owner access to php-fpm.conf file. However, it is better to add a Glob (without extension here).

**Key pressed:** g (glob)

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/php/7.2/fpm/php-fpm.conf
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /etc/php/7.2/fpm/php-fpm.conf r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish

Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/php/7.2/fpm/php-fpm.conf
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - owner /etc/php/7.2/fpm/php-fpm.conf r,
 [4 - owner /etc/php/7.2/fpm/* r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for read/owner access to www.conf file. However, it is better to add a Glob (without extension here).

**Key pressed:** g (glob)

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/php/7.2/fpm/pool.d/www.conf
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /etc/php/7.2/fpm/pool.d/www.conf r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish

Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/php/7.2/fpm/pool.d/www.conf
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - owner /etc/php/7.2/fpm/pool.d/www.conf r,
 [4 - owner /etc/php/7.2/fpm/pool.d/* r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for write/owner access to php7.2-fpm.log file.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /var/log/php7.2-fpm.log
New Mode: owner w
Severity: 8

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /var/log/php7.2-fpm.log w,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for read access to nsswitch.conf file.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/nsswitch.conf
New Mode: owner r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/nameservice>
 [4 - owner /etc/nsswitch.conf r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for read access to passwd file.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/passwd
New Mode: owner r
Severity: 4

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/nameservice>
 [4 - owner /etc/passwd r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for read access to group file.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/group
New Mode: owner r
Severity: 4

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/nameservice>
 [4 - owner /etc/group r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for owner/write/read access on php7.2-fpm.sock UNIX socket.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /run/php/php7.2-fpm.sock
New Mode: owner rw
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /run/php/php7.2-fpm.sock rw,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for owner/write access to php7.2-fpm.pid file.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /run/php/php7.2-fpm.pid
New Mode: owner w
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /run/php/php7.2-fpm.pid w,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for owner/write access to notify file.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /run/systemd/notify
New Mode: owner w
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /run/systemd/notify w,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / (O)wner permissions off / Abo(r)t / (F)inish
```

This entry is for owner/write/read access to index.php file

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /var/www/html/index.php
New Mode: r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/web-data>
 [4 - /var/www/html/index.php r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
```

Save the changes to the profile.

**Key pressed:** s (save changes)

```
= Changed Local Profiles =

The following local profiles were changed. Would you like to save them?

 [1 - /usr/sbin/php-fpm7.2]
(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean profiles / Abo(r)t
Writing updated profile for /usr/sbin/php-fpm7.2.
student@localhost:/etc/apparmor.d$
```

**Step 26:** Check the modified profile file.

**Command:** sudo cat usr.sbin.php-fpm7.2

```
student@localhost:/etc/apparmor.d$ sudo cat usr.sbin.php-fpm7.2
# Last Modified: Fri Apr 24 03:29:02 2020
#include <tunables/global>

/usr/sbin/php-fpm7.2 flags=(complain) {
  #include <abstractions/base>

  deny capability chown,
  deny capability dac_override,
  deny capability setgid,
  deny capability setuid,

  capability net_admin,
```

```
  /bin/dash mrix,
  /lib/x86_64-linux-gnu/ld-*.so mr,
  /usr/sbin/php-fpm7.2 mr,
  /var/www/html/index.php r,
  owner /etc/group r,
  owner /etc/nsswitch.conf r,
  owner /etc/passwd r,
  owner /etc/php/7.2/fpm/* r,
  owner /etc/php/7.2/fpm/*.ini r,
  owner /etc/php/7.2/fpm/*/ r,
  owner /etc/php/7.2/fpm/pool.d/* r,
  owner /etc/php/7.2/mods-available/* r,
  owner /etc/ssl/openssl.cnf r,
  owner /run/php/php7.2-fpm.pid w,
  owner /run/php/php7.2-fpm.sock rw,
  owner /run/systemd/notify w,
  owner /tmp/.ZendSem.FyQo3Z rwk,
  owner /var/log/php7.2-fpm.log w,
  owner /{usr/,}lib{,32,64}/** mr,

}
```

**Step 27:** Move the profile to enforce mode.

**Command:** sudo aa-enforce usr.sbin.php-fpm7.2

```
student@localhost:/etc/apparmor.d$ sudo aa-enforce usr.sbin.php-fpm7.2
Setting /etc/apparmor.d/usr.sbin.php-fpm7.2 to enforce mode.
student@localhost:/etc/apparmor.d$
```

**Step 28:** Check the apparmor status.

**Command:** sudo aa-status

```
6 processes have profiles defined.
6 processes are in enforce mode.
   /usr/sbin/nginx (796)
   /usr/sbin/nginx (797)
   /usr/sbin/nginx (798)
   /usr/sbin/php-fpm7.2 (1296)
   /usr/sbin/php-fpm7.2 (1298)
   /usr/sbin/php-fpm7.2 (1299)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
student@localhost:/etc/apparmor.d$
```

Both nginx and php-fpm are in enforce mode.

**Step 29:** Switch to terminal T2. Run id, date and file listing command using the curl command.

**Commands:**
curl http://localhost?cmd=id
curl "http://localhost?cmd=date"
curl "http://localhost?cmd=ls -l ."

```
student@localhost:~$ curl "http://localhost?cmd=ls -l ."

student@localhost:~$ curl "http://localhost?cmd=date"

student@localhost:~$ curl "http://localhost?cmd=id"

student@localhost:~$
```

None of the commands are running properly.

**Step 30:** Adjust the profile accordingly to allow these binaries and dependencies.

**Command:** sudo aa-logprof

The first entry to access the ls command.

**Key pressed:** i (inherit)

```
student@localhost:/etc/apparmor.d$ sudo aa-logprof
Reading log entries from /var/log/audit/audit.log.
Updating AppArmor profiles in /etc/apparmor.d.

Profile:  /usr/sbin/php-fpm7.2
Execute:  /bin/ls
Severity: unknown

(I)nherit / (C)hild / (N)amed / (X) ix On / (D)eny / Abo(r)t / (F)inish
```

This entry is to access the date command.

**Key pressed:** i (inherit)

```
Profile:  /usr/sbin/php-fpm7.2
Execute:  /bin/date
Severity: unknown

(I)nherit / (C)hild / (P)rofile / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t / (F)inish
```

This entry is to access the id command.

**Key pressed:** i (inherit)

```
Profile:  /usr/sbin/php-fpm7.2
Execute:  /usr/bin/id
Severity: unknown

(I)nherit / (C)hild / (P)rofile / (N)amed / (U)nconfined / (X) ix On / (D)eny / Abo(r)t / (F)inish
```

This entry is to access the ls command.

**Key pressed:** s (save profile)

```
= Changed Local Profiles =

The following local profiles were changed. Would you like to save them?

 [1 - /usr/sbin/php-fpm7.2]
(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean profiles / Abo(r)t
Writing updated profile for /usr/sbin/php-fpm7.2.
student@localhost:/etc/apparmor.d$
```

**Step 31:** Switch to terminal T2. Run id, date and file listing command using the curl command.

**Commands:**
curl http://localhost?cmd=id
curl "http://localhost?cmd=date"
curl "http://localhost?cmd=ls -l ."

```
student@localhost:~$ curl "http://localhost?cmd=ls -l ."

student@localhost:~$ curl "http://localhost?cmd=id"
uid=33 gid=33 groups=33

student@localhost:~$ curl "http://localhost?cmd=date"
Fri Apr 24 03:37:59 UTC 2020
```

Two of the commands are able to execute i.e. id and date. However, the listing of webroot is not working.

**Step 32:** Adjust the profile accordingly to allow the listing.

**Command:** sudo aa-logprof

```
student@localhost:/etc/apparmor.d$ sudo aa-logprof
Reading log entries from /var/log/audit/audit.log.
Updating AppArmor profiles in /etc/apparmor.d.
```

The first entry is for read access to nsswitch file.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/nsswitch.conf
Old Mode: owner r
New Mode: r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/nameservice>
 [4 - /etc/nsswitch.conf r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
```

This entry is for read access to passwd file.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/passwd
Old Mode: owner r
New Mode: r
Severity: 4

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/nameservice>
 [4 - /etc/passwd r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
```

This entry is for read access to group file.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /etc/group
Old Mode: owner r
New Mode: r
Severity: 4

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/nameservice>
 [4 - /etc/group r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
```

The first entry is for read access on /var/www/html directory.

**Key pressed:** a (allow)

```
Profile:  /usr/sbin/php-fpm7.2
Path:     /var/www/html/
New Mode: r
Severity: unknown

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
  3 - #include <abstractions/web-data>
 [4 - /var/www/html/ r,]
(A)llow / [(D)eny] / (I)gnore / (G)lob / Glob with (E)xtension / (N)ew / Audi(t) / Abo(r)t / (F)inish
```

Save the profile.

**Key pressed:** s (save profile)

```
= Changed Local Profiles =

The following local profiles were changed. Would you like to save them?

 [1 - /usr/sbin/php-fpm7.2]
(S)ave Changes / Save Selec(t)ed Profile / [(V)iew Changes] / View Changes b/w (C)lean profiles / Abo(r)t
Writing updated profile for /usr/sbin/php-fpm7.2.
student@localhost:/etc/apparmor.d$
```

**Step 33:** Try to list the files of the webroot.

**Command:** curl "http://localhost?cmd=ls -l ."

```
student@localhost:~$ curl "http://localhost?cmd=ls -l ."
total 20
-rw-r--r-- 1 root root 10918 Oct 24  2019 index.html
-rw-r--r-- 1 root root   612 Apr 24 01:39 index.nginx-debian.html
-rw-r--r-- 1 root root    61 Apr 24 01:37 index.php

student@localhost:~$
```

And, the listing works now.

**Step 34:** Try to list the files of the system root.

**Command:** curl "http://localhost?cmd=ls -l /"

```
student@localhost:~$ curl "http://localhost?cmd=ls -l /"

student@localhost:~$
```

This command is not working so the objective is complete.

**Step 35:** One  can check the change in file access permissions section of the php-fpm profile to find the newly added permission.

**Command:** sudo cat usr.sbin.php-fpm7.2

```
  /bin/dash mrix,
  /bin/date mrix,
  /bin/ls mrix,
  /etc/group r,
  /etc/nsswitch.conf r,
  /etc/passwd r,
  /lib/x86_64-linux-gnu/ld-*.so mr,
  /usr/bin/id mrix,
  /usr/sbin/php-fpm7.2 mr,
  /var/www/html/ r,
  /var/www/html/index.php r,
```

**Learning:**

- Creating policy for running exposed processes.
- Adjusting the policy to enable required functionality while blocking the unwanted activities.
- Even if an attacker can get a RCE or CI on a webapp, he can't go further.

**References:**

- AppArmor man page (http://manpages.ubuntu.com/manpages/bionic/man7/apparmor.7.html) (http://manpages.ubuntu.com/manpages/bionic/man5/apparmor.d.5.html)