APPARMOR INSTALLATION

GITHUB with all the files:
https://github.com/D3SK3R/apparmor

first, download linux kernel

```
  https://wiki.archlinux.org/title/Kernel/Traditional_compilation
```

install the apparmor binary

```
  sudo pacman -S apparmor
```

add these lines to the kernel .config file:

```
  CONFIG_SECURITY_APPARMOR=y
  CONFIG_AUDIT=y
  CONFIG_LSM="landlock,lockdown,yama,integrity,apparmor,bpf"
```

compile the kernel then restart.

enable apparmor service

```
  sudo systemctl enable --now apparmor
```

check apparmor status

```
  aa-status
```

disable kernel rate limiting for logs:

```
  sysctl -w kernel.printk_ratelimit=0
```

---

now to setup the webserver
move the index.html and revshell.php from githubs's 'http' folder, to the httpd directory:

```
  /srv/http
```

edit the revshell.php, the line $ip
insert the host machine's IP Address

then start/restart httpd:

```
  systemctl start/restart httpd
```

get the machine's IP:

```
  ip a
```

and open the browser to that url

now, on the host machine, listen to connections:

```
  nc -tnlvp 2727
```

in the browser, run the revshell.php

```
  <arch machine IP>/revshell.php
```

it should pop up a shell on the attacker machine

now close that shell
copy the contents of the abstractions folder to /etc/apparmor.d/abstractions/

```
  cp abstractions/httpd-common /etc/apparmor.d/abstractions
```

copy the folder httpd.d and the rule usr.sbin.httpd to the apparmor directoy:

```
  cp -r httpd.d /etc/apparmor.d/
  cp usr.sbin.httpd /etc/apparmor.d/
```

now enforce/enable the httpd rule:

```
  aa-enforce /etc/apparmor.d/usr.sbin.httpd
```

and restart the httpd and apparmor services

```
  systemctl restart apparmor
  systemctl restart httpd
```

now on the host machine again, run a listener:

```
  nc -tnlvp 2727
```

and on the browser run that reverse shell

```
  <arch machine IP>/revshell.php
```

it shouldn’t work because apparmor won’t allow it to.

---

to disable/remove the rule:

disable:

```
  sudo aa-disable /etc/apparmor.d/usr.sbin.httpd
```

remove:

```
  rm /etc/apparmor.d/usr.sbin.httpd
  aa-remove-unknown
```