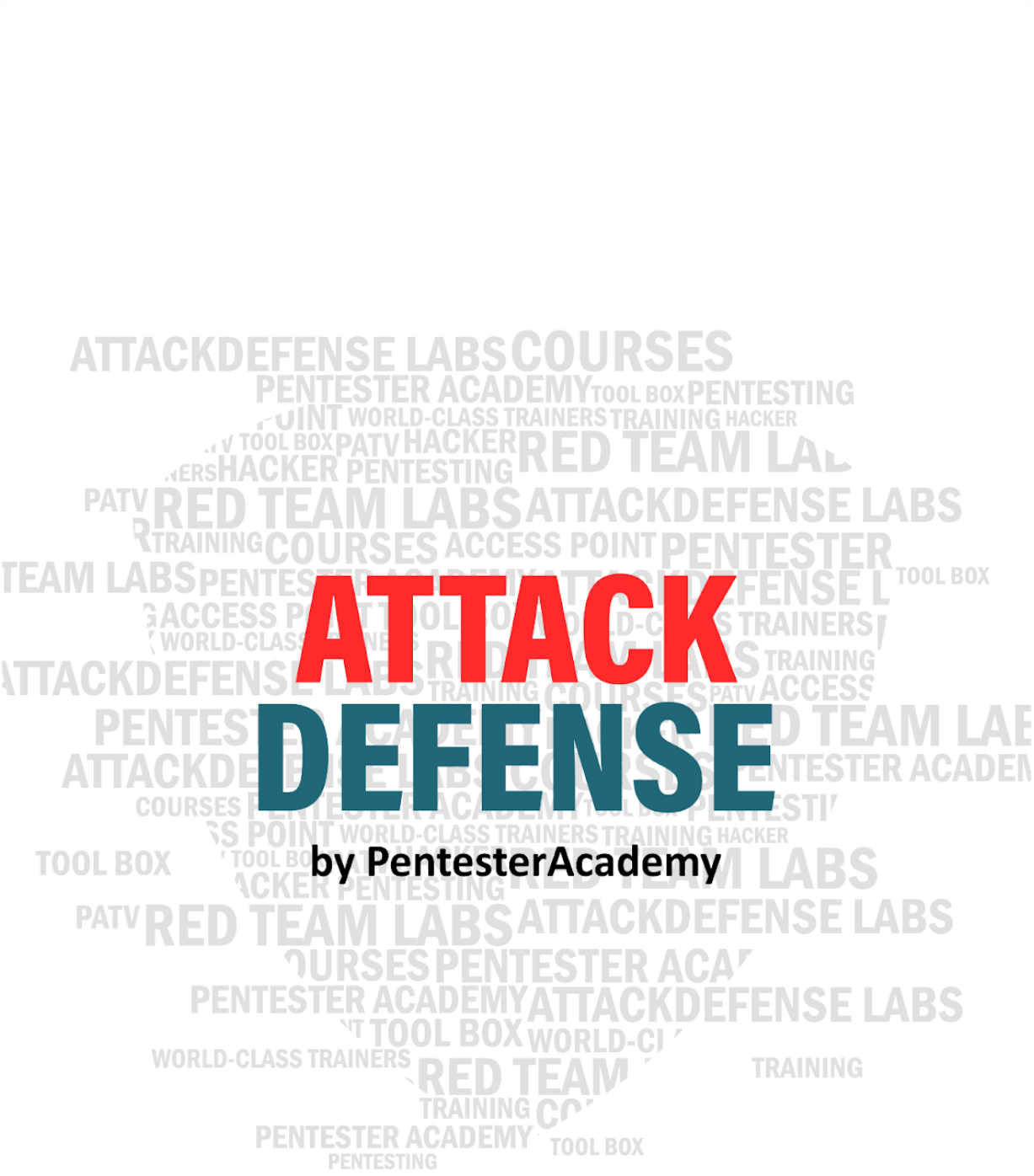
ATTACK
DEFENSE
by PentesterAcademy

Name	Confining Services with AppArmor II
URL	https://attackdefense.com/challengedetails?cid=1834
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 backdoored FTP server (vsftpd 2.3.4) is running on the local machine. The backdoor is publicly known and provides the attacker a shell on the machine.

Objective: Create AppArmor profiles to confine the FTP service while meeting the following conditions:

1. The "student" user should be able to login to his FTP account.
2. No one should be able to get a shell using the backdoor.

Solution:

Step 1: 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
```

```
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
   /usr/lib/dovecot/dovecot-auth
```

```
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:~$
```

Check the Running FTP service

Step 2: List the opened listening network sockets on the machine.

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 0.0.0.0:21              0.0.0.0:*               LISTEN      382/vsftpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      384/sshd
tcp6       0      0 :::22                   :::*                    LISTEN      384/sshd
raw6       0      0 :::58                   :::*                    7           229/systemd-network
```

Vsftpd service is listening on port 21.

Step 3: Connect to FTP service using ftp client.

Command: ftp localhost

Credentials:
Username: student
Password: student

Run pwd command on successful login.

Command: pwd

```
student@localhost:~$ ftp localhost
ftp: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
220 (vsFTPd 2.3.4)
Name (localhost:student):
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/student"
ftp> quit
221 Goodbye.
student@localhost:~$
```

So, FTP service is working fine.

Step 4: Open the backdoor shell.

Command: ftp localhost

Credentials:
Username: a:)
Password: <blank> // This means NO password, directly press enter

```
student@localhost:~$ ftp localhost
ftp: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
220 (vsFTPd 2.3.4)
Name (localhost:student): a:)
331 Please specify the password.
Password:
```

On passing these credentials, the backdoor opens a listen shell session on port 6200.

Step 5: Open another terminal T2 and check the list of listening sockets to verify the newly opened backdoor socket.

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 0.0.0.0:21              0.0.0.0:*               LISTEN      382/vsftpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      384/sshd
tcp        0      0 0.0.0.0:6200            0.0.0.0:*               LISTEN      463/vsftpd
tcp6       0      0 :::22                   :::*                    LISTEN      384/sshd
raw6       0      0 :::58                   :::*                    7           229/systemd-network
```

Step 6: Use netcat to connect to the opened port and run whoami command to check the user (privilege level).

Commands:
nc localhost 6200
whoami

```
student@localhost:~$ nc localhost 6200
whoami
root
```

Step 7: Restart the service to restore the initial state of the machine.

Command: sudo /etc/init.d/vsftpd restart

```
student@localhost:~$ sudo /etc/init.d/vsftpd restart
Stopping FTP server: vsftpd.
Starting FTP server: vsftpd.
student@localhost:~$
```

The service is restarted.

Generating profile for vsftpd

Step 8: To confine the vsftpd using the apparmor, a profile is needed. Change to apparmor profile directory and create a blank profile for it.

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

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

Step 9: Check the generated profile.

Command: sudo cat usr.local.sbin.vsftpd

```
student@localhost:/etc/apparmor.d$ sudo cat usr.local.sbin.vsftpd
# Last Modified: Sat Apr 25 10:00:18 2020
#include <tunables/global>

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

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

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

Step 10: Move the profile to “complain” mode and restart the service.

Command: sudo aa-complain usr.local.sbin.vsftpd

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

```
student@localhost:/etc/apparmor.d$ sudo /etc/init.d/vsftpd restart
Stopping FTP server: vsftpd.
Starting FTP server: vsftpd.
student@localhost:/etc/apparmor.d$
```

Step 11: Check the AppArmor status.

Command: sudo aa-status

```
1 processes have profiles defined.
0 processes are in enforce mode.
1 processes are in complain mode.
   /usr/local/sbin/vsftpd (639)
0 processes are unconfined but have a profile defined.
student@localhost:/etc/apparmor.d$
```

The process vsftpd is in the “complain” mode.

Step 12: Login to FTP service again using the previously used “student” credentials.

Command: ftp localhost

```
student@localhost:~$ ftp localhost
ftp: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
220 (vsFTPd 2.3.4)
Name (localhost:student):
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/student"
ftp> quit
221 Goodbye.
student@localhost:~$
```

Step 13: Run logprof to update the profile according to the use case.

Command: sudo aa-logprof

The logprof utility will read the audit.log file for the logs generated by vsftpd 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/local/sbin/vsftpd
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
```

Move the pointer to point 4. Similarly, for all such prompts, the cursor needs to be moved to the point of interest before pressing the key.

This entry is for net_bind_service capability.

Key pressed: a (allow)

```
Profile:    /usr/local/sbin/vsftpd
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 sys_admin capability.

Key pressed: d (deny)

```
Profile:    /usr/local/sbin/vsftpd
Capability: sys_admin
Severity:   10

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

This entry is for setgid capability.

Key pressed: a (allow)

```
Profile:    /usr/local/sbin/vsftpd
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 sys_chroot capability.

Key pressed: a (allow)

```
Profile:    /usr/local/sbin/vsftpd
Capability: sys_chroot
Severity:   10

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

This entry is for setuid capability.

Key pressed: a (allow)

```
Profile:    /usr/local/sbin/vsftpd
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 owner/read access to vsftpd.conf configuration file.

Key pressed: a (allow)

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

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /etc/vsftpd.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 write/lock access to vsftpd.log file.

Key pressed: a (allow)

```
Profile:  /usr/local/sbin/vsftpd
Path:     /var/log/vsftpd.log
New Mode: wk
Severity: 8

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - /var/log/vsftpd.log wk,]
(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 owner/read access to nsswitch.conf configuration file.

Key pressed: a (allow)

```
Profile:  /usr/local/sbin/vsftpd
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 owner/read access to the passwd file.

Key pressed: a (allow)

```
Profile:  /usr/local/sbin/vsftpd
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 owner/read access to shells file.

Key pressed: a (allow)

```
Profile:  /usr/local/sbin/vsftpd
Path:     /etc/shells
New Mode: owner r
Severity: 1

  1 - #include <abstractions/lxc/container-base>
  2 - #include <abstractions/lxc/start-container>
 [3 - owner /etc/shells 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/read access to the shadow file.

Key pressed: a (allow)

```
Profile:  /usr/local/sbin/vsftpd
Path:     /etc/shadow
New Mode: owner r
Severity: 5

  1 - #include <abstractions/authentication>
  2 - #include <abstractions/lxc/container-base>
  3 - #include <abstractions/lxc/start-container>
 [4 - owner /etc/shadow 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/read access to the group file.

Key pressed: a (allow)

```
Profile:  /usr/local/sbin/vsftpd
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 using inet stream socket.

Key pressed: a (allow)

```
Profile:        /usr/local/sbin/vsftpd
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
```

Save the profile changes.

Key pressed: s (save)

```
= Changed Local Profiles =

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

 [1 - /usr/local/sbin/vsftpd]
(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/local/sbin/vsftpd.
student@localhost:/etc/apparmor.d$
```

Step 14: Check the modified profile.

Command: sudo cat /etc/apparmor.d/usr.local.sbin.vsftpd

```
student@localhost:~$ sudo cat /etc/apparmor.d/usr.local.sbin.vsftpd
# Last Modified: Sat Apr 25 11:03:17 2020
#include <tunables/global>

/usr/local/sbin/vsftpd {
  #include <abstractions/base>

  capability setgid,
  capability setuid,
  deny capability sys_admin,
  capability sys_chroot,

  capability net_bind_service,

  network inet stream,

  /lib/x86_64-linux-gnu/ld-*.so mr,
  /usr/local/sbin/vsftpd mr,
  /var/log/vsftpd.log wk,
  owner /etc/group r,
  owner /etc/nsswitch.conf r,
  owner /etc/passwd r,
  owner /etc/shadow r,
  owner /etc/shells r,
  owner /etc/vsftpd.conf r,

}
```

Step 15: Move this profile to “enforce” mode.

Command: sudo aa-enforce usr.local.sbin.vsftpd

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

Step 16: Check the apparmor status to verify the change,

Command: sudo aa-status

```
3 processes have profiles defined.
3 processes are in enforce mode.
   /usr/local/sbin/vsftpd (628)
   /usr/local/sbin/vsftpd (629)
   /usr/local/sbin/vsftpd (739)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
student@localhost:/etc/apparmor.d$
```

All vsftpd processes are in “enforce” mode.

Verify the Profile

Step 17: Connect to FTP service using ftp client using “student” credentials.

Command: ftp localhost

Run pwd command on successful login.

Command: pwd

```
student@localhost:~$ ftp localhost
ftp: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
220 (vsFTPd 2.3.4)
Name (localhost:student):
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/student"
ftp> quit
221 Goodbye.
student@localhost:~$
```

So, FTP service is working fine.

Step 18: Open the backdoor shell.

Command: ftp localhost

Credentials:
Username: a:)
Password: <blank> // This means NO password, directly press enter

```
student@localhost:~$ ftp localhost
ftp: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
220 (vsFTPd 2.3.4)
Name (localhost:student): a:)
331 Please specify the password.
Password:
```

On passing these credentials, the backdoor opens a listen shell session on port 6200.

Step 19: On checking the list of listening sockets, 6200 is opened by the vsfptd. And, this is because the process has the capabilities to open the listening sockets and if those capabilities are blocked, the FTP server won't be able to function.

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 0.0.0.0:21              0.0.0.0:*               LISTEN      382/vsftpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      384/sshd
tcp        0      0 0.0.0.0:6200            0.0.0.0:*               LISTEN      463/vsftpd
tcp6       0      0 :::22                   :::*                    LISTEN      384/sshd
raw6       0      0 :::58                   :::*                    7           229/systemd-network
```

Step 20: However, when netcat is connected to the opened port and whoami command is run, it won't work.

Commands:
nc localhost 6200
whoami
date

```
student@localhost:~$ nc localhost 6200
whoami
date
^C
student@localhost:~$
```

This is because the vsftpd doesn't have the ability to open a shell anymore. The same can be verified by checking the denial logs in audit.log file.

Command: sudo vim /var/log/audit/audit.log

```
student@localhost:~$ sudo vim /var/log/audit/audit.log
student@localhost:~$
```

```
type=AVC msg=audit(1587813291.680:1089): apparmor="AUDIT" operation="accept" profile="/usr/local/sbin/vsftpd" pid=628 comm="vsftpd" lport=6200 f
amily="inet" sock_type="stream" protocol=6 requested_mask="accept"
type=AVC msg=audit(1587813292.680:1090): apparmor="DENIED" operation="exec" profile="/usr/local/sbin/vsftpd" name="/bin/dash" pid=628 comm="vsft
pd" requested_mask="x" denied_mask="x" fsuid=0 ouid=0
type=AVC msg=audit(1587813292.680:1091): apparmor="AUDIT" operation="accept" profile="/usr/local/sbin/vsftpd" pid=628 comm="vsftpd" lport=6200 f
amily="inet" sock_type="stream" protocol=6 requested_mask="accept"
type=AVC msg=audit(1587813293.680:1092): apparmor="DENIED" operation="exec" profile="/usr/local/sbin/vsftpd" name="/bin/dash" pid=628 comm="vsft
pd" requested_mask="x" denied_mask="x" fsuid=0 ouid=0
type=AVC msg=audit(1587813293.680:1093): apparmor="AUDIT" operation="accept" profile="/usr/local/sbin/vsftpd" pid=628 comm="vsftpd" lport=6200 f
amily="inet" sock_type="stream" protocol=6 requested_mask="accept"
type=AVC msg=audit(1587813294.680:1094): apparmor="DENIED" operation="exec" profile="/usr/local/sbin/vsftpd" name="/bin/dash" pid=628 comm="vsft
pd" requested_mask="x" denied_mask="x" fsuid=0 ouid=0
```

These denial logs (highlighted in yellow) clearly show that vsftpd was stopped from opening the dash shell.

Learning:

- AppArmor can help us to confine a service to specific functions.
- Even a vulnerable/backdoored software can't do much harm when confined properly with apparmor.

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)
- Beginning AppArmor profile development (https://ubuntu.com/tutorials/beginning-apparmor-profile-development)