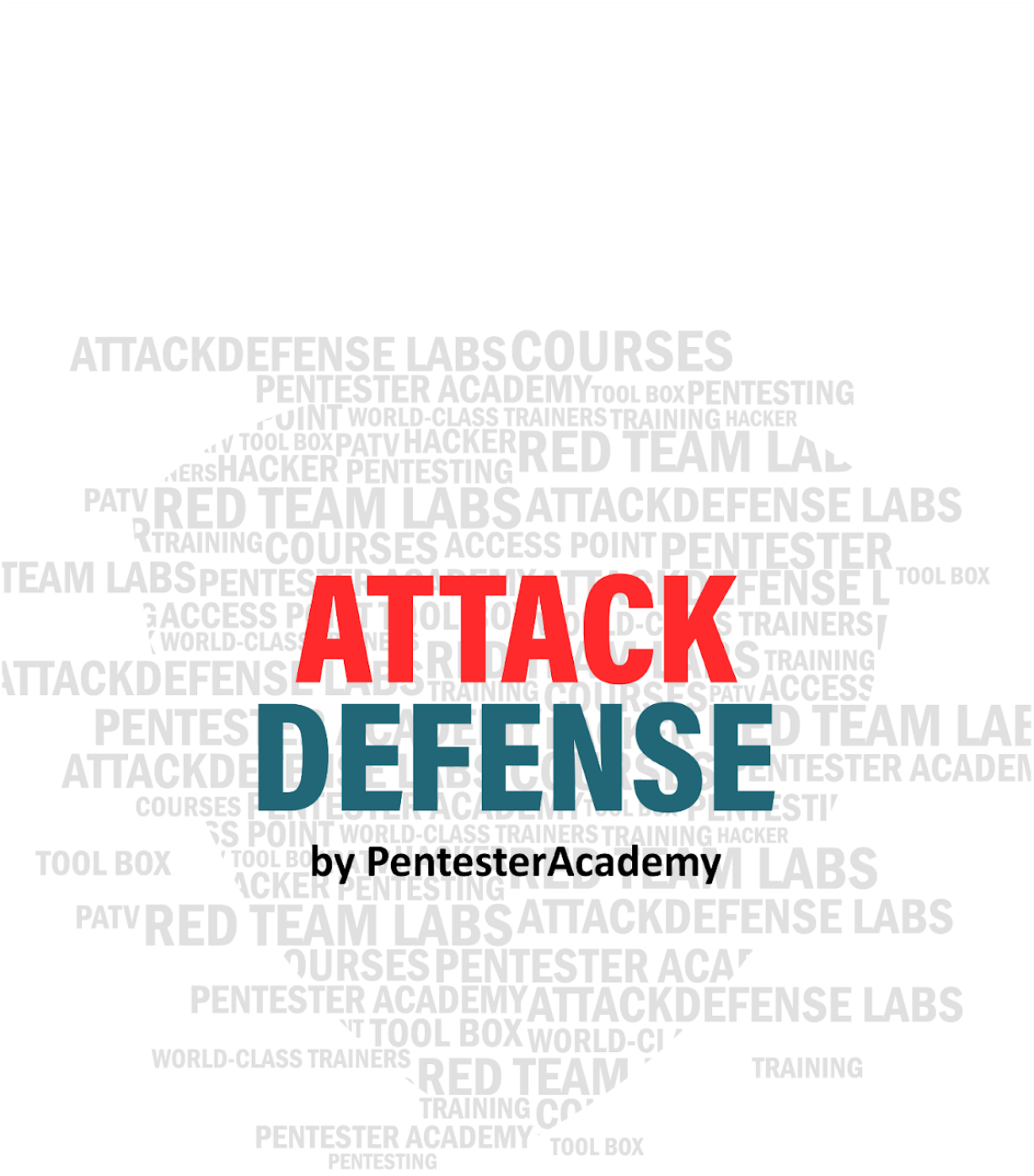
ATTACK
DEFENSE
by PentesterAcademy

Name	AppArmor Profile II
URL	https://attackdefense.com/challengedetails?cid=1832
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.

Objective: Create an AppArmor profile for a copy of the cat utility. Use Easyprof to generate the default template and then modify the profile so it can only read passwd file.

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
   /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
```

```
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
```

```
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:~$
```

Making a copy of system utility

Step 2: Create a copy of the cat binary. Name it as per your liking. Here, it is named “rcat” (stands for restricted cat).

Command: sudo cp /bin/cat /bin/rcat

```
student@localhost:~$ sudo cp /bin/cat /bin/rcat
student@localhost:~$
```

Step 3: Check the file permissions on the rcat binary.

Command: ls -l /bin/rcat

```
student@localhost:~$ ls -l /bin/rcat
-rwxr-xr-x 1 root root 35064 Apr 23 07:09 /bin/rcat
student@localhost:~$
```

Step 4: Print the contents of /etc/passwd using rcat command. The /etc/passwd file is readable to all users, so rcat will succeed.

Command: rcat /etc/passwd

```
student@localhost:~$ rcat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

Generating a template profile for rcat

Step 5: To confine the rcat using the apparmor, a profile is needed. In the Apparmor profile I challenge, the profile was generated using aa-genprof command. In this challenge, aa-easyprof utility will be used.

Command: sudo aa-easyprof /bin/rcat

```
student@localhost:~$ sudo aa-easyprof /bin/rcat
# vim:syntax=apparmor
# AppArmor policy for rcat
# ###AUTHOR###
# ###COPYRIGHT###
# ###COMMENT###

#include <tunables/global>

# No template variables specified
```

```
"/bin/rcat" {
  #include <abstractions/base>

  # No abstractions specified

  # No policy groups specified

  # No read paths specified

  # No write paths specified
}
```

This command generates a default template for the rcat binary and by default everything is Disabled.

Step 6: Write this template into a file, move the file to the location of other apparmor files and load it into the kernel.

Commands:
sudo aa-easyprof /bin/rcat > bin.rcat
sudo mv bin.rcat /etc/apparmor.d/
sudo apparmor_parser -a /etc/apparmor.d/bin.rcat

```
student@localhost:~$ sudo aa-easyprof /bin/rcat > bin.rcat
student@localhost:~$
student@localhost:~$ sudo mv bin.rcat /etc/apparmor.d/
```

```
student@localhost:~$ sudo apparmor_parser -a /etc/apparmor.d/bin.rcat
student@localhost:~$
```

Step 7: Check the AppArmor status.

Command: sudo aa-status

```
student@localhost:~$ sudo aa-status
apparmor module is loaded.
54 profiles are loaded.
17 profiles are in enforce mode.
   /bin/rcat
   /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
```

The profile for rcat is included in the enforce mode.

Step 8: Open another terminal (T2) and start tail on the audit.log

Command: sudo tail -f /var/log/audit/audit.log | grep apparmor

```
student@localhost:~$ sudo tail -f /var/log/audit/audit.log | grep apparmor
```

Step 9: Switch back to terminal T1 and try to print the contents of the /etc/passwd file.

Command: rcat /etc/passwd

```
student@localhost:~$ rcat /etc/passwd
rcat: /etc/passwd: Permission denied
student@localhost:~$
```

The attempt failed (as everything is blocked for this binary by the default profile template) and corresponding logs will appear in T2.

```
type=AVC msg=audit(1587636470.956:153): apparmor="AUDIT" operation="open" profile="/bin/rcat" name="/etc/ld.so.cache" pid=496 comm="rcat" reques
ted_mask="r" fsuid=1000 ouid=0
type=AVC msg=audit(1587636470.956:154): apparmor="AUDIT" operation="getattr" profile="/bin/rcat" name="/etc/ld.so.cache" pid=496 comm="rcat" req
uested_mask="r" fsuid=1000 ouid=0
type=AVC msg=audit(1587636470.972:155): apparmor="AUDIT" operation="open" profile="/bin/rcat" name="/lib/x86_64-linux-gnu/libc-2.27.so" pid=496
comm="rcat" requested_mask="r" fsuid=1000 ouid=0
type=AVC msg=audit(1587636470.972:156): apparmor="AUDIT" operation="getattr" profile="/bin/rcat" name="/lib/x86_64-linux-gnu/libc-2.27.so" pid=4
96 comm="rcat" requested_mask="r" fsuid=1000 ouid=0
type=AVC msg=audit(1587636470.976:157): apparmor="AUDIT" operation="file_mmap" profile="/bin/rcat" name="/lib/x86_64-linux-gnu/libc-2.27.so" pid
=496 comm="rcat" requested_mask="r" fsuid=1000 ouid=0
type=AVC msg=audit(1587636470.992:158): apparmor="AUDIT" operation="getattr" profile="/bin/rcat" name="/dev/pts/0" pid=496 comm="rcat" requested
_mask="r" fsuid=1000 ouid=1000
type=AVC msg=audit(1587636470.992:159): apparmor="DENIED" operation="open" profile="/bin/rcat" name="/etc/passwd" pid=496 comm="rcat" requested_
mask="r" denied_mask="r" fsuid=1000 ouid=0
```

Step 10: The denials can also be checked by using aa-notify utility.

Key pressed: sudo aa-notify -s 1 -v

```
student@localhost:~$ sudo aa-notify -s 1 -v
Profile: /bin/rcat
Operation: open
Name: /etc/passwd
Denied: r
Logfile: /var/log/audit/audit.log
(3 found, most recent from 'Thu Apr 23 10:07:50 2020')

AppArmor denials: 3 (since Wed Apr 22 10:08:05 2020)
For more information, please see: https://wiki.ubuntu.com/DebuggingApparmor
student@localhost:~$
```

This command is showing that the attempt to read the /etc/passwd by rcat binary was denied 3 times (we executed rcat /etc/passwd 2 more times to get multiple attempts) in the last 1 day.

Modifying the rcat profile

Step 11: The read permission for /etc/passwd needs to be added. Run logprof utility to update the profile.

Command: sudo aa-logprof

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

Profile:  /bin/rcat
Path:     /etc/passwd
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
```

One can observe the various entries shown by this command. The 4th entry is of interest.

Step 12: Move the cursor to entry 4 and select allow by pressing ‘a’ key.

Key pressed: a

```
Profile:  /bin/rcat
Path:     /etc/passwd
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
```

To save the changes, finish the process by pressing the “s” button.

```
Adding /etc/passwd r, to profile.

= Changed Local Profiles =

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

 [1 - /bin/rcat]
(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 /bin/rcat.
```

And the corresponding log will be printed on T2

```
type=AVC msg=audit(1587636576.868:168): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/bin/rcat" pid=504 comm="apparm
or_parser"
```

Step 13: Check the modified profile file.

Key pressed: sudo cat /etc/apparmor.d/bin.rcat

```
student@localhost:~$ sudo cat /etc/apparmor.d/bin.rcat
# Last Modified: Thu Apr 23 10:09:36 2020
#include <tunables/global>

# vim:syntax=apparmor
# AppArmor policy for rcat
# ###AUTHOR###
# ###COPYRIGHT###
# ###COMMENT###
# No template variables specified


/bin/rcat {
  #include <abstractions/base>

  /etc/passwd r,

}
```

Step 14: Try to print the contents of the /etc/passwd file.

Command: rcat /etc/passwd

```
student@localhost:~$ rcat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
```

The attempt succeeded as the read access on /etc/passwd file is granted to rcat binary. Please remember that this binary can't perform any other task except from this one.

Step 15: Try to read a normal file (for e.g. .bashrc)

Command: rcat .bashrc

```
student@localhost:~$ rcat .bashrc
rcat: .bashrc: Permission denied
student@localhost:~$
```

The rcat binary will fail because it doesn't have permission to read anything other than /etc/passwd.

Hacks Learned:

- AppArmor can help us to confine a binary only to one task (i.e. read a specific file).
- Similarly, by extrapolating the same, such task specific binaries/scripts/processes can be created for the low-privilege user.

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)