Working with AppArmor



Andrew Mallett
Linux Author and Trainer

@theurbanpenguin www.theurbanpenguin.com



Module Overview



Understanding AppArmor and application security

Installing utilities

Installing profiles

Protecting services

Creating profiles

Protecting your own applications



AppArmor



AppArmor is a MAC, Mandatory Access Control, application security system promoted by SUSE



Works with the Linux Kernel LSM (Linux Security Module)



Protects even where process are running as root

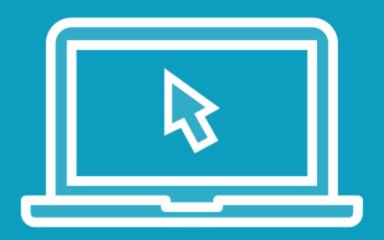


```
# zypper in -y apparmor-utils
# aa-status
# zypper in -y apparmor-profiles
```

Installing Tools and Profiles

Adding the tools will enable AppArmor on your system but without profiles. Adding profiles add targets to secure





Up and running with AppArmor

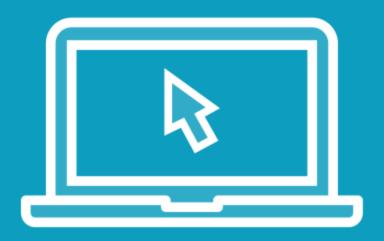
- Install utils
- Install profiles
- use aa-status

AppArmor Profiles

AppArmor profiles are a set of rules that are applied to services and executables protecting your applications:

- 1. Enforcing: Rules are enforced and violations logged
- 2. Complain: No rule enforcement, violations logged
- Rules: These are just rules and not the service or application, if we start a service managed by a profile we will see the profile become active





Reading profile information

- with aa-status
- start service
- /etc/apparmor.d

```
# vim test.py
#!/usr/bin/python3
FILE = 'mytextfile'
try:
   open(FILE, 'a').close()
   print(f'Created file: {FILE}')
except:
   print(f'Failed to create file {FILE}')
   exit(1)
```

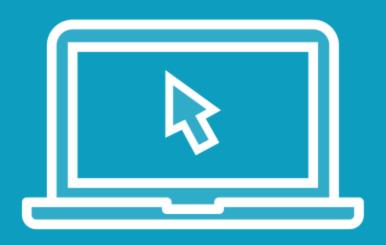
Simple Python Script

We can create a very simple script to test AppArmor. Don't forget to make the script executable. Without a profile it can run unconfined; however, we can also create a profile to ensure only the correct file name is accessed



Create and test Python Script





Creating the profile



Updating the profile



Summary



In this module we have introduced AppArmor

- apparmor-utils apparmor-profiles
- rcapparmor start
- aa-status
- aa-genprof (genprof)
- aa-logprof (logprof)
- /var/log/messages



