SELINUX
&
FIREWALL

Selinux is stands for security enhanced linux.

There are some problems in discretionary access control (DAC) is that you cant control everything that a user does. File permission and ACL cant save you from everything .because the process that they are using that can change the file permission too and that can give them elevated privileges . So if the software is compromised it can be used to gain access .for example if someone compromise the ssh process it might harm other system

Selinux is is designed by the NSA in amarica

so they with the DAC(discretionary access controll) they add another thing call MAC(mandatory access controll)

its built in the linux kernel in 2.6 it is used in redhat centos and also the debian version now

Selinux Breakdown:

1) selinux is deny by defaut.So by default it will not give access unless it is changed

2)SElinux log everyting.every change every allow and who has do what

3) it allow exceptions one at a time

SELINUX modes:

1) Enforcing : that actually applies the MAC policy in the system

2) Permissive : Selinux is enabled but does not enforce. But the logging can continue,its good for troubleshooting

3) Disabled : Selinux is disabled.never use this

There are four different types of enforcement

1) Type enforcement: Primary control that use the targeted policy

2) Roll based access control : Enforcement based on the users role

3) Multi-level Security
4) Multi Targeted security

Benefits:

1) policies are separated then the Selinux
2) great logging
3) great controll over system like files ,network,process and execution

problem:
1) it takes time to implement
2) Selinux takes time to perform
3) everything is logged so its hard to find the main problem

users:
1) Web servers
2) File server

its a very powerfull tools.but it is very complex

how linux may be compromised??

→ software vulnerabilities
→ configuration error
→ Social engineering
→ Rootkits,Viruses,Trojans

Software vulnerabilities:
1) buffer overflow is the number 1 of vulnerabilities. this is exploits in memory leak

2) Software may not be patched .if you compile linux code and install you cant patch the software .thats why it is necessary to use the package manager

configuration error:
1) we can configure the server with wrong is permission and suppose not disable port and dont configure firewall It can be a problem

Social engineering: users are the weakest part of the system. If the user leaks the password the attacker can get into the system
user can accidentally delete necessary file

1)chrootkit
2) RK hunter
3) ClamAV

are the tools for mitigating the rotkit in linux