SELinux

1. Introdução

O que é o SELinux?

O SELinux (Security-Enhanced Linux) é um sistema de segurança desenvolvido pela NSA (Agência de Segurança Nacional dos EUA) que adiciona uma camada adicional de segurança ao sistema operacional Linux. Ele controla o acesso de processos e usuários a recursos do sistema, como arquivos, diretórios e portas de rede, com base em políticas de segurança definidas. O SELinux é projetado para proteger contra ataques de exploração de vulnerabilidades de software e para limitar o impacto de um ataque bem-sucedido. Ele é usado em muitas distribuições Linux, incluindo Red Hat, CentOS e Fedora.

DAC (Discretionary Access Control) vs MAC (Mandatory Access Control)

O DAC é o sistema padrão do LINUX. É o sistema de controle de acesso baseado em permissões de arquivos (leitura, escrita, execução Ex: -rw-r--r--). É o que se vê do lado esquerdo dos arquivos quando executamos o comando ls -l.

```
$ ls -l
-rw-r--r-- 1 root root 0 Jan 1 00:00 file1
-rwx------ 1 root root 0 Jan 1 00:00 file2
-r-x------ 1 root root 0 Jan 1 00:00 file3
```

O MAC é um sistema de controle de acesso baseado em rótulos. É o que se vê do lado direito dos arquivos quando executamos o comando ls -Z. Isso adiciona um rótulo de segurança a cada arquivo, que é usado para determinar se um usuário/serviço pode acessar um arquivo ou não, conforme definido pelas políticas de segurança.

```
$ ls -Z
-rw-r--r--. root root system_u:object_r:unlabeled_t:s0 file1
-rwx------. root root system_u:object_r:unlabeled_t:s0 file2
-r-x------. root root system_u:object_r:unlabeled_t:s0 file3
```

2. Instalação

Nos sistemas baseados em Red Hat, o SELinux é instalado por padrão. Para verificar se o SELinux está instalado, execute o comando abaixo:

```
sestatus
```

Poderá adicionar funcionalidades adicionais ao SELinux, como o SELinux para Apache (entre muitos outros), instalando o pacote policycoreutils-python. Para instalar o pacote, execute o comando abaixo:

```
yum install policycoreutils-python
```

Existem ainda outros pacotes que poderão ser instalados dependendo das necessidades. Na documentação oficial do Red Hat, encontramos a seguinte lista de pacotes:

```
- policies: selinux-policy-targeted, selinux-policy-mls
- tools: policycoreutils, policycoreutils-gui, libselinux-utils, policycoreutils-
python-utils, setools-console, checkpolicy
```

3. Configuração

O ficheiro principal de configuração do SELinux é o /etc/selinux/config. Este ficheiro contém as seguintes opções:

```
- SELINUX: define o modo de execução do SELinux
  - SELINUX=disabled: desativa o SELinux durante o arranque
  - SELINUX=permissive: coloca o SELinux em modo permissivo, imprimindo apenas
mensagens de aviso
  - SELINUX=enforcing: coloca o SELinux em modo de execução
- SELINUXTYPE: define o tipo de política SELinux a ser usada
  - SELINUXTYPE=targeted: define a política SELinux como targeted
  - SELINUXTYPE=minimum: define a política SELinux como minimum, apenas processos
selecionados são protegidos
  - SELINUXTYPE=mls: define a política SELinux como multi level security (MLS)
```

Na mesma pasta, existe ainda o ficheiro /etc/selinux/semanage.conf. Este ficheiro **"/etc/selinux/semanage.conf"**, é um ficheiro de configuração para a ferramenta de gestão SELinux "semanage". Ele contém definições para a localização padrão do armazenamento de políticas, a localização padrão do armazenamento de módulos de políticas e o caminho padrão dos módulos de políticas. Estas definições são usadas pelo "semanage" para gerir as políticas e módulos SELinux no sistema. O ficheiro pode ser editado para alterar as definições padrão do "semanage".

Semanage

O "semanage" é uma ferramenta de gestão SELinux que permite gerir as políticas e módulos SELinux no sistema. O "semanage" pode ser usado para gerir as políticas SELinux, módulos SELinux, mapeamentos de usuários e mapeamentos de rótulos. O "semanage" pode ser usado para gerir as políticas SELinux, módulos SELinux, mapeamentos de usuários e mapeamentos de rótulos.

Será talvez a ferramenta mais importante para gerir o SELinux.

Semanage - fcontext

O "semanage fcontext" é usado para gerir os contextos de arquivos e pastas. Permite informar o SELinux de que um dado ficheiro pertence a um determinado tipo de ficheiro. Por exemplo, se tivermos um ficheiro html para ser lido por um servidor web, poderemos informar o SELinux de que este ficheiro pertence ao tipo de ficheiro httpd_sys_content_t. Para isso, executamos o comando abaixo:

```
# Adicionar um ficheiro html ao tipo de ficheiro httpd_sys_content_t
semanage fcontext -a -t httpd_sys_content_t /var/www/html/index.html
# Aplicar as alterações
restorecon -v /var/www/html/index.html
# Verificar se o ficheiro foi adicionado ao tipo de ficheiro httpd_sys_content_t
semanage fcontext -l | grep index.html # ou
ls -Z /var/www/html/index.html
    # -rw-r--r--. root root system_u:object_r:httpd_sys_content_t:s0
/var/www/html/index.html
```

De referir que o semanage entende regex, pelo que poderá adicionar-se todos os ficheiros de uma dada pasta, por exemplo:

```
# Adicionar todos os ficheiros existentes dentro da pasta /var/www/html/ ao tipo
de ficheiro httpd_sys_content_t
semanage fcontext -a -t httpd_sys_content_t '/var/www/html(/.*)?'
restorecon -R -v /var/www/html  # -R para aplicar recursivamente
```

Para remover um ficheiro de um tipo de ficheiro, execute o comando abaixo:

```
semanage fcontext -d -t httpd_sys_content_t /var/www/html/index.html
restorecon -v /var/www/html/index.html
ls -Z /var/www/html/index.html
    # -rw-r--r--. root root system_u:object_r:unlabeled_t:s0
/var/www/html/index.html
```

Existem dezenas de tipos de ficheiros, e poderá consultar a lista completa das políticas existentes executando o comando abaixo:

```
semanage fcontext -l
```

Semanage - port

O **"semanage port"** é usado para gerir os contextos de portas. Permite informar o SELinux de que uma determinada porta pertence a um determinado tipo de porta. Por exemplo, se tivermos um serviço web rodando na porta 80, poderemos informar o SELinux de que esta porta pertence ao tipo de porta http_port_t. Para isso, executamos o comando abaixo:

```
# Adicionar a porta 80 ao tipo de porta http_port_t
semanage port -a -t http_port_t -p tcp 80
# Verificar se a porta foi adicionada ao tipo de porta http_port_t
semanage port -l | grep 80 # ou
semanage port -l | grep http_port_t

# Remover a porta 80 do tipo de porta http_port_t
semanage port -d -t http_port_t -p tcp 80
```

O semanage port não subtitui uma firewall, mas pode ser usado para limitar muito o acesso externo ao computador. Se por algum motivo, o firewall estiver bem configurado e mesmo assim não lhe for possível aceder a um serviço, poderá estar a faltar configurar o **semanage port**.

Troubleshooting

Após modificar algo no sistema e não funcionar como deveria, poderá ser necessário verificar o log do SELinux para ver se há alguma mensagem de erro. Para isso, execute o comando abaixo:

```
sealert -a /var/log/audit/audit.log
```

Este comando é uma maravilha! Indica os erros e dá sugestões de como corrigir, e tudo isso de forma bem clara e bem detalhada. No entanto, as soluções são quase sempre para alterar os módulos SELinux, e não para alterar as políticas SELinux. Normalmente, as soluções passam pelo comando **semanage**. Mas com a mensagem de erro, poderá pesquisar online e encontrar a solução correspondente via **semanage**.

Referências

site:Red Hat - SELinux

troubleshooting - site:Red Hat - SELinux

troubleshooting - site:segurança informática