Segurança em Ambiente Linux

Uma visão geral das tecnologias, ferramentas e abordagens utilizadas na área de segurança do Sistema Operacional Linux

Parte III:
Introdução ao SELinux (Secure Enhanced Linux)

Ademar de Souza Reis Jr.
<ademar@conectiva.com.br>
http://www.ademar.org

XII Congresso C. Computação Bolívia
Tarija – Bolívia – Outubro 2005

última versão atualizada disponível em
http://www.ademar.org/

Conteúdo

- Histórico e motivação
- Comparação SELinux vs Linux
- Conceitos
- Explorando um sistema em funcionamento
- Dicas e recomendações
- Estágio atual e futuro

Linux padrão: política discreta de acesso

Discretionary Access Control (DAC)

- Permissões padrão Unix (rwx)
- Usuários e grupos padrão Unix
- Programas e serviços executando com privilégios de um determinado usuário
- Root: super-usuário

SELinux: Política de acesso mandatória

Mandatory Access Control (MAC)

- Programas são executados dentro de um conjunto de regras de interação com o sistema (política)
- *Type Enforcement*(R): tipos de processos, arquivos e recursos do sistema
- *Role-based access control:* controle de usuários
- Políticas aplicáveis a programas e usuários
- Não existe (necessariamente) super-usuário

SELinux: histórico e motivação

- Projeto de pesquisa da NSA (National Security Agency) (USA)
- Objetivo: aplicar a tecnologia (já em desenvolvimento acadêmico) em um SO de uso geral/amplo
- LSM (Linux Security Modules)
- Oficialmente suportado a partir do kernel 2.6.X (Nov. 2000)
- Por quê a NSA escolheu o Linux?

SELinux: funcionamento

- **Kernel + programas de usuário + regras**
- **Permissões atuais são respeitadas**
- **Atributos extendidos (xattr)**
- **Definições**
  - role
  - domain
  - security context
  - policy

SELinux: funcionamento (cont)

- **Modos de execução:** permissive vs enforcement
- **Políticas:** strict vs targeted
- `/selinux`
- `/etc/selinux`
- **Perda de performance**

SELinux: demonstração

```
[root@optimus64 ~]# ls /etc/fstab --context
-rw-r--r--  root     root     system_u:object_r:etc_t          /etc/fstab

[root@optimus64 ~]# ls --context
-rw-------  root     root     root:object_r:user_home_t        anaconda-ks.cfg
drwxr-xr-x  root     root     root:object_r:user_home_t        Desktop
drwx------  root     root     root:object_r:user_home_t        Mail

[root@optimus64 ~]# ls --context /home/ademar/
drwxr-xr-x  ademar   ademar   user_u:object_r:user_home_t      Desktop
drwxr-xr-x  ademar   ademar   user_u:object_r:user_home_t      linux-2.0.40
drwxr-xr-x  ademar   ademar   user_u:object_r:user_home_t      linux-2.2.26
drwxr-xr-x  ademar   ademar   user_u:object_r:user_home_t      linux-2.6.13.1
```

```
[root@optimus64 ~]# ps aux -Z | grep gnome
root:system_r:unconfined_t      root      2957  0.0  0.8  21660  8808 ?        Ss   19:47   0:00 gnome-session
root:system_r:unconfined_t      root      3123  0.3  1.2  37732 12664 ?        Sl   19:47   0:00 gnome-terminal

[root@optimus64 ~]# ps aux -Z | grep httpd
root:system_r:httpd_t           root      3195  0.8  1.0  21204 10856 ?        Ss   19:50   0:00 /usr/sbin/httpd
root:system_r:httpd_t           apache    3197  0.0  1.0  21204 10868 ?        S    19:50   0:00 /usr/sbin/httpd
root:system_r:httpd_t           apache    3198  0.0  1.0  21204 10868 ?        S    19:50   0:00 /usr/sbin/httpd
```

Dicas e recomendações

- SELinux é apenas uma tecnologia que adiciona um nível a mais de proteção a um sistema
- SELinux não é a solução para todos os problemas de segurança
- Utilize o modo “permissive” até certificar-se de que tudo está OK
- Cuidado com arquivos criados com SELinux desligado
- Política “targeted” é ideal para sistemas desktop

Estágio atual e perspectivas de futuro

- Tecnologia estável e madura, mas ainda difícil de ser utilizada
- Performance está sendo melhorada
- Fedora e RHEL suportam SELinux nativamente
- Debian, Gentoo, SuSE e outros: pacotes externos
- Empresas e órgãos atuantes no desenvolvimento: NSA, Red Hat, Tresys Technologies, IBM

Para saber mais...

- NSA SELinux official site: http://www.nsa.gov/selinux/
- NSA SELinux FAQ: http://www.nsa.gov/selinux/info/faq.cfm
- SELinux community page: http://selinux.sourceforge.net
- UnOfficial FAQ: http://www.crypt.gen.nz/selinux/faq.html
- Writing SE Linux policy HOWTO: https://sourceforge.net/docman/display_doc.php?docid=21959&group_id=21266
- Getting Started with SE Linux HOWTO: the new SE Linux (Debian) https://sourceforge.net/docman/display_doc.php?docid=20372&group_id=21266
- IRC: irc.freenode.net, #selinux