FACULDADE DE TECNOLOGIA SENAC GOIÁS
Tecnologia em Segurança da Informação

Aldo Filho
Jordan Hugs
Liniker Lettierre
Rony Carneiro

A INFLUÊNCIA DO SISTEMA OPERACIONAL NA SEGURANÇA DOS SERVIÇOS IPS

Lucília Gomes Ribeiro

GOIÂNIA,
2016

Aldo Filho
Jordan Hugs
Liniker Lettierre
Rony Carneiro

A INFLUÊNCIA DO SISTEMA OPERACIONAL NA SEGURANÇA DOS SERVIÇOS IPS

Relatório apresentado como requisito parcial para obtenção de aprovação na disciplina de Sistemas Operacionais, no Curso de Segurança da Informação, na Faculdade de Tecnologia Senac Goiás.

Lucília Gomes Ribeiro

GOIÂNIA,
2016

SUMÁRIO

1 INTRODUÇÃO

O sistema Operacional é um software que separa as aplicações do hardware que elas acessam e fornece serviços que permitem que cada aplicação seja executada com segurança e efetivamente, quando a memória RAM está cheia é o sistema operacional que decide quais processos devem sair da memória e quais processos devem entrar na memória e determina quais posições de memória ele pode usar, garantindo assim que os processos não alterem dados de outros processos. Quando dois processos querem usar o mesmo dispositivo serial que por natureza só permite o uso de um processo por vez é o sistema operacional que vai garantir que apenas um processo vai acessar este dispositivo serial por vez.

2 HARDENING

Hardening é um conjunto de processos realizado em cima de sistemas com a finalidade de mitigar as vulnerabilidades e corrigir falhas, o processo de hardening não pode ser estático, é um processo de constante mudança, cada cenário exige processos diferentes, um sistema hoje seguro não ficara para sempre seguro os dias surgem novas vulnerabilidades.

2.1 Política de senhas

Na computação as senhas fazem parte do processo de autenticação de um usuário para acessar serviços, a senha está em um dos pilares da segurança da informação a confidencialidade ela que diz que a pessoa que está usando a conta é de fato a pessoa autorizada, se um terceiro utiliza as credenciais do titular, o titular que vai arcar com as consequências pois senhas são intrasferível.

Uma boa senha não pode conter aspectos da vida pessoa, por exemplo: placa do carro, data de nascimento do filho, irmão (a), conjugue, pais, nome da rua, número do telefone, uma boa senha é constituível de Caracteres maiúsculos e minúsculos, números, caracteres especiais com no mínimo de 8 caracteres e que seja trocada periodicamente um intervalo razoável é a cada 3 meses

Vamos criar uma política de senha utilizando o PAM (Pluggable Authentication Modules). O PAM é uma parte muito importante na autenticação em um sistema Linux, praticamente todos os programas do Linux que realizam algum tipo de autenticação tem suporte para o PAM. Todos os arquivos de configuração do PAM se encontra em /etc/pam.d

Entre no arquivo “system-auth” e encontre a linha “password requisite”, substitua as opções por estas:

```
password requisite pam_cracklib.so retry=3 minlen=8 difok=5 ucredit=-1 lcredit=-2 dcredit=-1 ocredit=-1
```

retry=3: Após 3 tentativas de autenticação o usuário recebera uma mensagem de erro

minlen=8: Tamanho mínimo da senha é 8 caracteres

difok=5: A quantidade de caracteres que podem ser repetidos da última senha

ucredit=1: Pelo menos 1 carácter Maiúsculo

lcredit=1: Pelo menos um carácter Minusculo

dcredit=1: Pelo menos um digito

ocredit=: Pelo menos um simbolo especial

Garantindo as senhas não se repitam

password [success=1 default=ignore] pam_unix.so obscure sha512 remember=3

remember=3: Define que a nova senha não pode ser igual as últimas 3 senhas

Período de expiração das senhas

Para determinar o período de expiração das senhas entre no arquivo "/etc/pam.d"

Altere os valores para:

PASS_MAX_DAYS 90

PASS_MIN_DAYS 0

PASS_MIN_LEN 8

PASS_WARN_AGE 5

PASS_MAX_DAYS: O tempo máximo de duração da senha

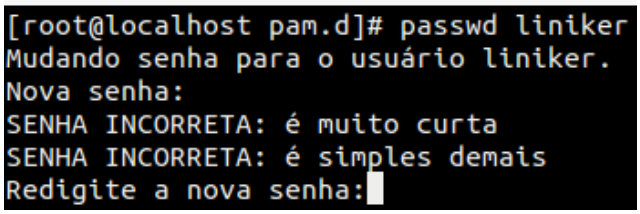
PASS_MIN_DAYS: O tempo mínimo para realizar alteração de senha

PASS_MIN_LEN: Tamanho mínimo da senha

PASS_WARN_AGE: Tempo de aviso para alteração da senha

Testando as configurações:

Testando a senha: 1234



Testando a senha: 1234abcd

```
[root@localhost pam.d]# passwd liniker
Mudando senha para o usuário liniker.
Nova senha:
SENHA INCORRETA: é muito simples/sistemática
SENHA INCORRETA: é simples demais
Redigite a nova senha:
```

Testando a senha: Qpr$90An

```
[root@localhost pam.d]# passwd liniker
Mudando senha para o usuário liniker.
Nova senha:
Redigite a nova senha:
passwd: todos os tokens de autenticações foram atualizados com sucesso.
[root@localhost pam.d]#
```

2.2 NTP

Para uma boa auditoria é essencial que o horário do servidor esteja correto, para isto é preciso sincronizar hora correta com um servidor externo, preferencialmente do servidor de hora oficial do pais, para realizar estas configurações siga os comandos abaixo:

Instalando o ntpdate

```
# yum install ntp ntpdate
```

Configurando o servidor oficial brasileiro de NTP:

```
# ntpdate a.st1.ntp.br
```

Iniciando o serviço:

```
# service ntpd start
```

Configurando para que ele inicie junto com o sistema

```
# chkconfig ntpd on
```

A hora foi propositalmente editada para realizar o teste

```
[root@localhost CentOs]# date -s 10:10:10
Qui Jun 16 10:10:10 BRT 2016
```

Após a instalação do NTP:

```
[root@localhost CentOs]# date
Qui Jun 16 20:44:14 BRT 2016
```

2.3 PRE-LINKING BINARIES

Os pre-linking binaries melhorou o tempo de execução porem ele causa problemas na execução do AIDE (Falaremos dele adiante), por isto deve ser desativado

Entre no arquivo /etc/sysconfig/prelink

Encontre a linha:
Set PRELINKING = yes

Altere o valor de “yes” para “no”

Desabilite os prelink anteriores a nova configuração

```
# /usr/sbin/prelink -ua
```

2.4 AIDE

O AIDE (*Advanced Intrusion Detection Environment*) é uma ferramenta para auditoria, ele cria um banco de dados e utiliza ele para detectar alterações no sistema, como permissões UID, GID, hora da modificação, usuário, arquivos criados e excluídos e entre outros.

Para instalar o AIDE já previamente configurado utilize o seguinte comando:

```
#  yum install aide
```

Todas as opções do AIDE:

```
[root@localhost CentOs]# aide -help
Aide 0.14

Usage: aide [options] command

Commands:
  -i, --init            Initialize the database
  -C, --check           Check the database
  -u, --update          Check and update the database non-interactively
      --compare         Compare two databases

Miscellaneous:
  -D, --config-check    Test the configuration file
  -v, --version         Show version of AIDE and compilation options
  -h, --help            Show this help message

Options:
  -c [cfgfile]  --config=[cfgfile]      Get config options from [cfgfile]
  -B "OPTION"   --before="OPTION"       Before configuration file is read define OPTION
  -A "OPTION"   --after="OPTION"        After configuration file is read define OPTION
  -r [reporter] --report=[reporter]     Write report output to [reporter] url
  -V[level]     --verbose=[level]       Set debug message level to [level]
```

Após a instalação é preciso criar o banco de dados inicial:

```
[root@localhost CentOs]# aide --init

AIDE, version 0.14

### AIDE database at /var/lib/aide/aide.db.new.gz initialized.
```

Após a criação do primeiro banco de dados é necessário mudar seu nome

```
# mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

Execute a checagem do Banco de dados:

```
[root@localhost CentOs]# aide --check

AIDE, version 0.14

### All files match AIDE database. Looks okay!
```

Criando um arquivo para teste e realizando a checagem

```
[root@localhost CentOs]# touch  /usr/sbin/Auditoria_teste
[root@localhost CentOs]# aide --check
AIDE found differences between database and filesystem!!
Start timestamp: 2016-06-16 22:35:44

Summary:
  Total number of files:        71694
  Added files:                  1
  Removed files:                0
  Changed files:                1


---------------------------------------------------
Added files:
---------------------------------------------------

added: /usr/sbin/Auditoria_teste

---------------------------------------------------
Changed files:
---------------------------------------------------

changed: /usr/sbin

---------------------------------------------------
Detailed information about changes:
---------------------------------------------------


Directory: /usr/sbin
  Mtime    : 2016-06-16 21:27:57              , 2016-06-16 22:35:40
  Ctime    : 2016-06-16 21:27:57              , 2016-06-16 22:35:40
```

Para não relatar as mesmas alterações é preciso atualizar o banco de dados

```
# aide --update
```

Este comando ele checa novamente os arquivos e gera um novo banco de dados

```
[root@localhost CentOs]# aide --update
AIDE found differences between database and filesystem!!
Start timestamp: 2016-06-16 22:53:48

Summary:
  Total number of files:        71694
  Added files:                  1
  Removed files:                0
  Changed files:                1


---------------------------------------------------
Added files:
---------------------------------------------------

added: /usr/sbin/Auditoria_teste

---------------------------------------------------
Changed files:
---------------------------------------------------

changed: /usr/sbin

---------------------------------------------------
Detailed information about changes:
---------------------------------------------------


Directory: /usr/sbin
  Mtime    : 2016-06-16 21:27:57              , 2016-06-16 22:35:40
  Ctime    : 2016-06-16 21:27:57              , 2016-06-16 22:35:40
```

O arquivo: aide.db.new.gz e o novo banco de dados gerado

```
[root@localhost CentOs]# ls -lt /var/lib/aide
total 9808
-rw-------. 1 root root 5020052 Jun 16 23:00 aide.db.new.gz
-rw-------. 1 root root 5019937 Jun 16 21:42 aide.db.gz
```

Para ter controle das alterações altere o nome do banco de dados para um que o identifique. Mude o nome do novo banco de dados para o nome padrão “aide.db.gz”

```
[root@localhost aide]# pwd
/var/lib/aide
[root@localhost aide]# ls
aide.db.gz  aide.db.new.gz
[root@localhost aide]# mv aide.db.gz aide.db.gz-17.06.2016-18:30
[root@localhost aide]# mv aide.db.new.gz aide.db.gz
[root@localhost aide]# ls
aide.db.gz  aide.db.gz-17.06.2016-18:30
[root@localhost aide]#
```

Novo banco de dados preparado para analisar novas modificações

```
[root@localhost aide]# aide --check

AIDE, version 0.14

### All files match AIDE database. Looks okay!
```

2.5 Analise de pacotes instalados

Analisar os pacotes instalados na procura de pacotes desnecessários e suspeitos, uma dica é redirecionar a saída do comando para um arquivo de texto, por padrão o sistema operacional vem com dezenas de pacotes instalados, utilize o comando abaixo:

```
# rpm -qa >PacotesInstalados.txt
```

Este arquivo pode ser visualizado por praticamente todos os editores de texto

3 CONCLUSÃO

Diversas medidas são tomadas para proteger as aplicações de um servido, por exemplo: criptografia do trafego de rede, senhas fortes nas aplicações, AntiSpam. Mas muitos administradores esquecem a parte principal o Sistema Operacional, se o SO está vulnerável todas as aplicações estão em risco mesmo sendo tomadas diversas medias para proteger determinada aplicação, um hacker pode invadir o servidor pelo SO e obter todos os arquivos dos serviços ignorando a segurança feita nas aplicações.

4 REFERÊNCIAS BIBLIOGRÁFICAS

Hardening - Artigo Revista Infra Magazine 1

http://www.devmedia.com.br/hardening-artigo-revista-infra-magazine-1/20818

Acesso em 12 de junho de 2016

NTP Oficial Brasil

http://ntp.br/

Acesso em 16 de junho de 2016

Security Harden CentOS

https://highon.coffee/blog/security-harden-centos-7/

Acesso em 16 de junho de 2016

How to Install AIDE on CentOS 7

http://linoxide.com/monitoring-2/install-aide-centos-7/

Acesso em 16 de junho de 2016

A Importância de uma senha segura

http://www.uenp.edu.br/index.php/graduacao-uenp/246-administrativo-e-tecnico/nucleo-tecnologia-da-informacao2/seguranca-info/426-a-importancia-de-uma-senha-segura

Acesso em 16 de junho de 2016

Saiba como aumentar a segurança dos sistemas Linux configurando políticas de senhas

http://www.linuxdescomplicado.com.br/2014/01/saiba-como-aumentar-seguranca-dos.html

Acesso em 16 de junho de 2016