**SEGURANÇA BÁSICA LINUX**

MODOS DE CONTROLE DE ACESSO

* Segurança envolve, acesso físico e lógico
* Modos de controle de acesso DAC, MAC e RBAC
* **DAC (Discretionary Access Control)** = É o modo de controle de acesso menos eficaz que o MAC e o RBAC, ele permite que o usuário dono do arquivo modifique as permissões sobre o arquivo, inclusive para outros. Além disso, ainda permite que um as permissões de um usuário seja usada por uma aplicação, por exemplo.
* **MAC(Mandatory Access Control)** = Mais seguro que o DAC, nele não são mais permitidos que o dono do arquivo altere as permissões para outro além dele próprio, também usuários de aplicação não herdarão mais as permissões do sujeito.
* **RBAC(Role Based Access Control)** = Um MAC melhorado , melhora no sentido de ser mais fácil o manuseio.

MÉTODOS BÁSICOS DE PROTEÇÃO

* **Usuário por conta** = Se um usuário for controlado por diversas pessoas, não há como ter certeza que uma ação foi realizada por um determinado sujeito.
* **Nenhum login para conta root** = Se os usuários puderem virar root, não há como afirmar quem de fato fez tal ação. Ao invés disso, é melhor adicionar o usuário ao arquivo /etc/sudoers. pois desta maneira a senha de root não precisa ser compartilhada, e ao usar o sudo , os logs são enviados para /var/log/secure. Um usuário precisa ter uma configuração semelhante a essa no arquivo sudoers:

**nina ALL=(ALL) ALL NOPASSWD: !/bin/su. /bin, /sbin/, /usr/bin/,**

**/usr/sbin/**

* **Configurar data de expiração das contas para usuários temporários** = Para evitar que o usuário de um consultor ou empregados temporários fiquem ativos sem a necessidade, é importante criar uma data de expiração para a conta. Para configurar uma conta com data de expiração digite: **usermod -e 2017-01-01 nina** .Para validar se a conta está com a data basta digitar **chage -l nina | grep Account**
* **Remover contas de usuários não utilizados** = Quanto menos usuários ativos , mais fácil o controle de acesso.
* **Proteger senhas** = As senhas devem conter letras maiúsculas, minúsculas, letras , números e caracteres especiais para se tornar forte. Não devendo ser usadas , datas de aniversários, nome, telefone, etc. O arquivo /etc/login.defs pode ser configurado parâmetros para trocas de senha. exemplo:

PASS\_MAX\_DAYS 99999

PASS\_MIN\_DAYS 0

PASS\_MIN\_LEN 5

PASS\_WARN\_AGE 7

* **Proteger o arquivo shadow** = Quando adicionamos uma senha a um usuário, automaticamente a senha é hasheada, ou seja, ela é criptografada e fica armazenada no arquivo /etc/shadow. Alguns hackers tentam desvendar os hashes e podemos achar na internet uma lista com possíveis significados das hashes, por isso é importante que o arquivo /etc/shadow não possua permissão para ninguém além dele mesmo, como abaixo:

ls -l /etc/shadow

---------- 1 root root 1431 Nov 5 12:29 /etc/shadow

* **Protegendo sistema de arquivos** = O arquivo /etc/fstab pode ser modificado para que possa impor bloqueio aos dispositivos. usando os parâmetros **nosuid**, **nodev**, **noexec**.

**nosuid** = Evita que programas executáveis com permissão de SUID e SGID sejam executados

**nodev** = Faz com que nenhum arquivo de dispositivo que for localizado seja reconhecido.

**noexec** = Faz com que nenhum programa executável seja executado.

Exemplo de bloqueio :

/dev/sdb1 /home ext4 nodev,noexec,nosuid 1 2

/dev/sdb2 /tmp ext4 nodev,noexec,nosuid 1 2

/dev/sdb3 /usr ext4 nodev 1 2

/dev/sdb4 /var ext4 nodev,noexec,nosuid 1 2

* **Detectando novas contas e privilégios falsificados** = Para monitorar a criação de um usuário ou até mesmo um privilégio atribuído, pode ser usado a ferramenta auditctl. Neste comando passaremos o -w nome-do-arquivo -p gatilho . Exemplo:

**auditctl -w /etc/passwd -p rwc** .

**r** = read , **w**= write, **a**=attribute, **x**=execute

Para visualizar os logs usando o analisador do auditctl, use o comando **ausearch -f /etc/passwd**

Se nenhum evento disparado o ausearch não retornará nada.

* **Detectar senhas ruins dos usuários** = Utilizando o programa John the Ripper é possível descobrir senhas fracas dos usuários, ou realizar testes de quebras de senha. Para instalar o pacote no Centos, digite yum install -y john . Depois de instalado use o comando unshadow para gravar o conteúdo de passwd e shadow em um terceiro arquivo qualquer , **unshadow /etc/passwd /etc/shadow > password.file,** claro que as credenciais de root devem ser removidas do arquivo ou demais usuários com alto privilégio antes de executar o teste com unshadow. Agora , basta executar **john password.file,** o consumo de CPU fica elevado ao usar esse comando.
* Instalar anti-virus e defensores de rootkits = rootkits são mais insidioso que o vírus, ele permanece escondido no sistema, consegue alterar comandos , manter privilégios administrativos. Para instalar uma ferramenta de remoção de rootkit, digite **yum install chkrootkit -y** e para instalação de antivírus, **yum install -y clamav .**
* [www.us-cert.gov](http://www.us-cert.gov)
* [www.sans.org/securoty-resources](http://www.sans.org/securoty-resources)
* [www.grc.com](http://www.grc.com)
* Acima são alguns sites que apontam vulnerabilidades encontradas.