Módulo 5 - Aulas 3 e 4

Tarefas

No final deste módulo você deve submeter em um ÚNICO arquivo PDF os seguintes prints:

- Atividade 5.6: passo 18.
- Atividade 5.7: passo 9.
- Atividade 5.8: passo 7.
- Atividade 5.9: passo 9.
- Atividade 5.10: passo 5.

Regras para a elaboração do documento:

1. Antes de cada Print, adicione obrigatoriamente uma frase explicativa que sinalize do que se trata o print. A inserção de prints sem a devida frase explicativa será considerada como tentativa de atrapalhar a correção do instrutor e será penalizada a critério do instrutor. Exemplo:

Print da atividade 5.6: [Imagem com o Print]

2. Os Prints devem ser tirados da TELA CHEIA. Quando tirados da VM da AWS, devem ser capturados **obrigatoriamente** da tela cheia clicando no botão "Screenshot" → "Take screenshot" da barra de ferramentas do Hypervisor da AWS.
3. Insira **somente a quantidade de Prints solicitados por atividade** usando exclusivamente 1 página por print. **A página do documento onde você vai inserir o Print deve estar com a orientação no modo PAISAGEM** ´para termos melhor aproveitamento do espaço. Ou seja, seu documento deverá ter a mesma quantidade de páginas que a quantidade do total de Prints! A inserção de prints desnecessários será considerada como tentativa de atrapalhar a correção do instrutor e será penalizada com nota 0.

4. Apresente Prints legíveis e com tamanho correto para fácil leitura. O envio de prints com letras minúsculas poderá ser considerado como tentativa de atrapalhar a correção do instrutor e será penalizada a critério do instrutor.

Atividade 5.6 – Implementando o Controle de Acesso Discricionário (DAC) no Windows Server 2022 (cliente)

Nesta atividade, vamos implementar o Controle de Acesso Discricionário (DAC) no Windows Server 2022 (cliente) por meio de permissões de arquivos.

1. Vamos começar inicializando o Windows Server 2022 (cliente) via RDP ao IP: 192.168.98.30 (certifique-se que o nome de usuário é “ALUNO\nome1”), com usuário “nome1” e senha “S3nh@nom31”.
2. Clique onde está escrito “Type here to search” e escreva “Notepad”.
3. Clique no botão Notepad para abrir o Bloco de notas.
4. No Bloco de notas, escreva “Teste” e salve o arquivo com o nome “Arquivo1.txt” na pasta “Documents”. Feche o Bloco de notas.
5. Na barra de tarefas, clique em “File Explorer” para abrir o Explorador de Windows.
6. No campo esquerdo, clique em “Documents” e veja que o “Arquivo1” será mostrado no campo direito.
7. Clique com o botão direito na pasta “Documents” e selecione “Properties”.
8. Na janela nova, clique na aba “Security”.
9. Aqui você verá 3 “Group or user names”: SYSTEM, Nome1 ...; Administrators ....
10. Clique no botão “Edit...” para abrir a janela de permissões.
11. Clique em “Administrators” e veja que o administrador tem todas as permissões marcadas em “Allow” para permitir que o administrador conte com todas as permissões possíveis.
12. Agora, clique em “Remove”. Veja que uma mensagem é mostrada negando a remoção do Administrador. Clique em OK.

13. Agora, clique em “Nome1” e ative a caixa “Deny” para o Full control. Clique em “Apply”, em “Yes” e “Continue” em todos os avisos futuros até as janelas serem fechadas.
14. Volte ao “File Explorer” e veja que agora o arquivo “Arquivo1” sumiu e você não conta com acesso à pasta “Documents”.
15. No “File Explorer”, clique em outra pasta (por exemplo “Downloads”) e em “Documents” novamente. Uma mensagem de negação de permissão será apresentada, clique em “Continue”, insira as credenciais “Administrator” e senha “RnpEsr123@” (ou “RnpEsr123@2” caso a tenha atualizado). Na mensagem “You have been denied permission to access this folder”, clique em “Close”.
16. Clique com o botão direito na pasta “Documents”, selecione “Properties”.
17. Clique no usuário “Nome1” e desmarque todas as caixas “Deny” nas permissões. Clique em “Apply” → “Continue” até que o aviso desapareça.
18. Clique em outra pasta (por exemplo “Downloads”) e em “Documents”. Veja que agora você já conta novamente com acesso à pasta “Documents” (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**).
19. Feche as janelas e encerre a conexão RDP.

Parabéns! Agora você sabe que um arquivo criado por você pode ser gerenciado por você, limitando o acesso a todos (com exceção ao Administrador), inclusive a você mesmo!

Atividade 5.7 – Criando uma Organizational Unit (OU) no Windows Server 2022 (servidor)

Nesta atividade, vamos criar uma Organizational Unit (OU) contendo um usuário (com Common Name) no Windows Server 2022 (servidor). Esta atividade é a continuação das atividades do módulo anterior (aulas 5.1 a 5.5).

1. Vamos começar inicializando o Windows Server 2022 (servidor) via RDP ao IP: 192.168.98.20 (certifique-se que o nome de usuário é “WINSERVER\Administrator”), com usuário “administrator” e senha “RnpEsr123@”. Caso tenha mudado a senha, use a nova senha “RnpEsr123@2”
2. Na Barra de tarefas, clique no campo “Type here to search” e insira:

```
Active Directory Users and Computers
```

3. Clique em Active Directory Users and Computers.
4. Clique com o botão direito no domínio previamente criado “aluno.hacker.com” (coluna esquerda).
5. Selecione “New” → “Organizational Unit”.
6. Insira o nome “TI” e clique em “OK”.
7. No campo esquerdo, veja que foi criada a pasta “TI”. Clique com o botão direito nessa pasta e selecione: “New” → “User”.
8. No campo “First name” insira “Usuario”, no campo “Last name” insira “TI”.
9. No campo “User logon name”, insira “usuarioti” (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**). Esse será o Common Name.
10. Clique em Next. Insira a senha “usu@rioti1”, desmarque a opção “User must...” e marque a opção “Password never expires”.
11. Clique em “Next” e “Finish”. Veja que um novo usuário foi criado! Feche a conexão RDP.

Parabéns! Agora você sabe como podem ser usados os elementos de sistemas de gerenciamento de diretórios e usuários (Organizational Unit e Common Name) no AD do Windows Server 2022.

Atividade 5.8 - Implementando o Controle de Acesso Discricionário (DAC) no Kali Linux

Nesta atividade, vamos implementar o Controle de Acesso Discricionário (DAC) no Kali Linux por meio de permissões de arquivos.

Vamos começar inicializando nosso Kali Linux via RDP ao IP: 192.168.98.40, com usuário “aluno” e senha “rnpesr”.

1. Abra o Terminal e execute o seguinte comando (com senha “rnpesr”) para ser super usuário:

```
┌──(aluno㉿kali)-[~]
└─$ sudo -i
[sudo] senha para aluno:
```

2. Navegue até a pasta Documentos e crie um arquivo de texto chamado “texto.txt”:

```
┌──(root㉿kali)-[~]
└─# cd /home/aluno/Documentos/

┌──(root㉿kali)-[/home/aluno/Documentos]
└─# nano texto.txt
```

3. Insira o texto:

```
Teste1
```

Aperte “Ctrl+x” para sair, seguido de “s” para salvar e “Enter” para sair por completo.

4. Liste os arquivos contidos na pasta documentos.

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# ls
texto.txt
```

5. Liste as permissões do arquivo.

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# ls -l
total 4
-rw-r--r-- 1 root root 7 fev 10 18:10 texto.txt
```

A saída correspondente ao arquivo “texto.txt” conta com as seguintes propriedades:

- **total 4**: Indica o total de espaço ocupado por todos os arquivos listados no diretório. Neste caso, há apenas um arquivo listado.
- **-rw-r--r--**: Indica as permissões do arquivo. No Linux, as permissões são divididas em três conjuntos: permissões do proprietário, permissões do grupo e permissões para outros usuários. Neste caso, o arquivo é legível e gravável pelo proprietário (rw-), legível para o grupo (r--) e legível para outros usuários (r--).
- **1**: Indica o número de links (ou referências) para este arquivo. Como é 1, significa que este é o único nome de arquivo associado a este conjunto de dados.
- **root**: Indica o nome do proprietário do arquivo.
- **root**: Indica o grupo ao qual o arquivo pertence.
- **7**: Indica o tamanho do arquivo em bytes.
- **fev 10 18:10**: Indica a data e hora da última modificação do arquivo.
- **texto.txt**: Nome do arquivo.

6. Agora, vamos atribuir o controle de acesso DAC para o arquivo “texto.txt”:

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# chmod u+rwx texto.txt
```

A saída anterior conta com as seguintes propriedades:

- **chmod**: Este é o comando para alterar as permissões de um arquivo ou diretório no Linux.
- **u**: Isso indica o usuário proprietário do arquivo. No comando, "u" representa o proprietário.
- **+rwx**: Essa parte indica as permissões que estão sendo adicionadas ao usuário proprietário. "rwx" significa permissão de leitura (r), gravação (w) e execução (x). Portanto, com essa parte do comando, estão sendo concedidas permissões de leitura, gravação e execução ao proprietário do arquivo.
- **texto.txt**: Este é o nome do arquivo ao qual você está aplicando as permissões.

7. Finalmente, veja como mudaram as permissões do arquivo “texto.txt” (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# ls -l
total 4
-rwxr--r-- 1 root root 7 fev 10 18:10 texto.txt
```

A saída anterior conta com as seguintes propriedades:

- **-rwxr--r--**: Essa parte indica as permissões do arquivo. No Linux, as permissões são divididas em três partes: permissões do proprietário, permissões do grupo e permissões de outros. Cada parte é composta por três caracteres:
- O primeiro caractere "-" indica que é um arquivo regular (não um diretório ou outro tipo de arquivo).
- "rwx" indica que o proprietário do arquivo (no caso, o usuário "root") tem permissões de leitura, gravação e execução.
- "r--" indica que o grupo ao qual o arquivo pertence tem permissão de leitura, mas não de gravação ou execução.
- "r--" também indica que outros usuários têm permissão apenas de leitura.
- **1**: O número "1" após as permissões indica a quantidade de links (ou referências) para o arquivo. Neste caso, existe apenas uma referência para o arquivo.
- **root**: O primeiro "root" representa o nome do proprietário do arquivo, que é "root" neste caso. O proprietário é o usuário que possui o controle total sobre o arquivo e suas permissões.
- **root**: O segundo "root" representa o grupo ao qual o arquivo pertence. Neste caso, o grupo também é "root". Os usuários pertencentes a esse grupo podem ter permissões específicas para o arquivo.
- **7**: O "7" indica o tamanho do arquivo em bytes. Neste exemplo, o arquivo "texto.txt" tem um tamanho de 7 bytes.
- ** fev 10 18:10**: Essa parte mostra a data e a hora da última modificação do arquivo.
- **texto.txt**: Por fim, "texto.txt" é o nome do arquivo.

8. Feche o Terminal e **não apague** o arquivo "texto.txt".

Parabéns! Agora você sabe como implementar o controle de acesso DAC em arquivos do Kali Linux!

Atividade 5.9 - Implementando o Acesso Baseado em Função (RBAC) no Kali Linux

Nesta atividade, vamos implementar o Acesso Baseado em Função (RBAC) no Kali Linux por meio de permissões de arquivos.

Vamos começar inicializando nosso Kali Linux via RDP ao IP: 192.168.98.40, com usuário “aluno” e senha “rnpesr”.

1. Abra o Terminal e execute o seguinte comando (com senha “rnpesr”) para ser super usuário:

```
┌──(aluno㉿kali)-[~]
└─$ sudo -i
[sudo] senha para aluno:
```

2. Liste os arquivos contidos na pasta documentos.

```
┌──(root㉿kali)-[~]
└─# cd /home/aluno/Documentos/

┌──(root㉿kali)-[/home/aluno/Documentos]
└─# ls
texto.txt
```

3. Liste todos os usuários que existem no Kali Linux:

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# getent passwd | cut -d: -f1
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
_apt
nobody
systemd-network
messagebus
tcpdump
sshd
polkitd
_chrony
kali
systemd-timesync
aluno
rtkit
xrdp
usbmux
avahi
pulse
saned
lightdm
colord
tss
dnsmasq
strongswan
speech-dispatcher
nm-openvpn
nm-openconnect
postgres
Debian-exim
logcheck
debian-tor
freerad
```

```
fleetlau
clamav
geoclue
_rpc
pipewire
statd
teste1
```

4. Liste todos os grupos que existem no Kali Linux:

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# getent group | cut -d: -f1
root
daemon
bin
sys
adm
tty
disk
lp
mail
news
uucp
man
proxy
kmem
dialout
fax
voice
cdrom
floppy
tape
sudo
audio
dip
www-data
backup
operator
list
irc
src
shadow
utmp
video
sasl
plugdev
staff
games
users
nogroup
systemd-journal
systemd-network
crontab
input
sgx
kvm
render
netdev
```

```
netdev
messagebus
tcpdump
_ssh
polkitd
kali-trusted
_chrony
lxd
kali
systemd-timesync
aluno
rtkit
ssl-cert
xrdp
avahi
pulse
pulse-access
scanner
saned
lightdm
colord
tss
bluetooth
plocate
nm-openvpn
pipewire
nm-openconnect
postgres
wireshark
Debian-exim
logcheck
debian-tor
freerad
clamav
geoclue
docker
_cvsadmin
vboxusers
clock
teste1
```

5. Vamos criar grupos que representam funções específicas. Crie o grupo contabilidade:

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# groupadd contabilidade
```

6. Repita o passo 4 e veja que agora aparece o grupo “contabilidade” no final da lista:

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# getent group | cut -d: -f1
root
daemon
bin
sys
adm
tty
disk
lp
mail
news
uucp
man
proxy
kmem
dialout
fax
voice
cdrom
floppy
tape
sudo
audio
dip
www-data
backup
operator
list
irc
src
shadow
utmp
video
sasl
plugdev
staff
games
users
nogroup
systemd-journal
systemd-network
crontab
input
sgx
kvm
render
netdev
```

```
netdev
messagebus
tcpdump
_ssh
polkitd
kali-trusted
_chrony
lxd
kali
systemd-timesync
aluno
rtkit
ssl-cert
xrdp
avahi
pulse
pulse-access
scanner
saned
lightdm
colord
tss
bluetooth
plocate
nm-openvpn
pipewire
nm-openconnect
postgres
wireshark
Debian-exim
logcheck
debian-tor
freerad
clamav
geoclue
docker
_cvsadmin
vboxusers
clock
teste1
contabilidade
```

7. Agora, vamos atribuir o usuário “teste1” ao grupo “contabilidade”:

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# usermod -aG contabilidade teste1
```

8. Em seguida, vamos atribuir a propriedade do arquivo “texto.txt” ao grupo “contabilidade”

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# chown :contabilidade texto.txt
```

9. Finalmente, vamos atribuir permissões de leitura, gravação e execução ao proprietário/grupo do arquivo (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# chmod 770 texto.txt
```

O comando acima conta com os seguintes parâmetros:

- **chmod**: Este é o comando para alterar as permissões.
- **770**: Esses são os argumentos que especificam as permissões que você deseja atribuir ao arquivo "meuarquivo.txt". As permissões são representadas por três dígitos, cada um correspondendo a um conjunto de permissões:
- O primeiro dígito (7) representa as permissões para o proprietário do arquivo.
- O segundo dígito (7) representa as permissões para o grupo do arquivo.
- O terceiro dígito (0) representa as permissões para outros usuários (ou seja, usuários que não são o proprietário nem fazem parte do grupo do arquivo).

10. Apague o arquivo “texto.txt” e feche o terminal:

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# rm texto.txt
```

Parabéns! Agora você sabe como implementar o Acesso Baseado em Função (RBAC) no Kali Linux.

Atividade 5.10 - Implementando a Rotação de Senha no Kali Linux

Nesta atividade, vamos implementar as políticas de rotação de senhas para um usuário no Kali Linux.

Vamos começar inicializando nosso Kali Linux via RDP ao IP: 192.168.98.40, com usuário “aluno” e senha “rnpesr”.

1. Abra o Terminal e execute o seguinte comando (com senha “rnpesr”) para ser super usuário:

```
┌──(aluno㉿kali)-[~]
└─$ sudo -i
[sudo] senha para aluno:
```

2. Verifique os parâmetros atuais da senha do usuário "root" (a data pode estar diferente no seu laboratório):

```
┌──(root㉿kali)-[~]
└─# passwd -S
root P 2024-07-02 0 99999 7 -1
```

Os parâmetros do comando mostrado acima são:

- **root**: Indica que as informações exibidas se referem ao usuário "root", que é o superusuário ou administrador do sistema.
- **P**: O status da senha. Aqui, "P" indica que a senha está definida e é válida.
- **2024-07-02**: Indica a data em que a senha foi modificada pela última vez. Neste caso, a senha foi modificada em 02 de julho de 2024.
- **0**: Representa o número mínimo de dias que devem passar após a alteração da senha antes que ela possa ser alterada novamente. Um valor de "0" significa que a senha pode ser alterada a qualquer momento.
- **99999**: Esse é o número máximo de dias em que a senha é válida antes de expirar. Neste exemplo, a senha é válida por um período muito longo, quase 100 mil dias.
- **7**: Este é o número de dias antes do vencimento da senha em que o usuário receberá um aviso para alterar a senha. No exemplo, o usuário "root" será avisado 7 dias antes do vencimento da senha.

- **-1**: Este é o número de dias após o vencimento da senha em que a conta será desativada. Um valor de "-1" indica que a conta nunca será desativada com base no vencimento da senha.

3. Verifique os parâmetros atuais da senha do usuário "aluno" (a data pode estar diferente no seu laboratório):

```
┌──(root㉿kali)-[~]
└─# exit

┌──(aluno㉿kali)-[~]
└─$ passwd -S
aluno P 2025-09-06 0 99999 7 -1
```

Os parâmetros do comando mostrado acima são:

- **aluno**: As informações se referem ao usuário "aluno". Este é o nome de usuário em questão.
- **P**: O "P" na segunda coluna indica o status da senha. Neste caso, "P" significa que a senha do usuário "aluno" está disponível e pode ser usada para fazer login.
- **2025-09-06**: Indica a data em que a senha foi modificada pela última vez. Neste caso, a senha foi modificada em 6 de setembro de 2025.
- **0**: Representa o número mínimo de dias que devem passar após a alteração da senha antes que ela possa ser alterada novamente. Um valor de "0" significa que a senha pode ser alterada a qualquer momento.
- **99999**: Esse é o número máximo de dias em que a senha é válida antes de expirar. Neste exemplo, a senha é válida por um período muito longo, quase 100 mil dias.
- **7**: Este é o número de dias antes do vencimento da senha em que o usuário "aluno" receberá um aviso para alterar a senha. No exemplo, o usuário "aluno" será avisado 7 dias antes do vencimento da senha.
- **-1**: Este é o número de dias após o vencimento da senha em que a conta será desativada. Um valor de "-1" indica que a conta nunca será desativada com base no vencimento da senha.

4. Agora, vamos mudar os parâmetros de senha:

```
┌──(aluno㉿kali)-[~]
└─$ sudo nano /etc/login.defs
```

5. No arquivo de configuração, edite e deixe o texto com as seguintes modificações. De:

```
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
```

Para (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
PASS_MAX_DAYS   270
PASS_MIN_DAYS   90
PASS_WARN_AGE   10
```

As mudanças nos parâmetros mostrados acima significam:

- **PASS_MAX_DAYS**: Define o número máximo de dias em que uma senha é válida antes de expirar.
- **PASS_MIN_DAYS**: Define o número mínimo de dias que uma senha deve estar em uso antes de poder ser alterada.
- **PASS_WARN_AGE**: Define o número de dias antes do vencimento da senha em que o usuário deve ser avisado para alterar sua senha.

6. Aperte “Ctrl+x” para sair, seguido de “s” para salvar e “Enter” para sair por completo. Feche o Terminal.

Parabéns! Agora você sabe implementar as configurações básicas da Rotação de senhas em função da idade dela!