Módulo 04 - Aulas 1 e 2

Tarefas

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

- Atividade 4.1: passo 7.
- Atividade 4.2: passo 5.
- Atividade 4.3: passo 10.
- Atividade 4.4: passo 7.
- Atividade 4.5: passo 11.

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 4.1: [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 4.1 – Modificando os parâmetros de Controle de Autenticação no Kali Linux

Nesta atividade, vamos modificar a senha de usuário como parte do Controle de Autenticação no Kali Linux. Todo material apresentado aqui deve ser usado somente para fins acadêmicos.

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 para verificar os dados atuais de usuário:

```
┌──(aluno㉿kali)-[~]
└─$ whoami
aluno

┌──(aluno㉿kali)-[~]
└─$ pwd
/home/aluno
```

- O comando whoami é utilizado para imprimir o nome do usuário associado ao processo atual.
- O comando pwd (Print Working Directory) é utilizado para imprimir o diretório de trabalho atual. Ele fornece o caminho completo do diretório em que você está localizado no momento.

2. Veja agora o conteúdo do arquivo “passwd”:

```
┌──(aluno㉿kali)-[~]
└─$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/
nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
tcpdump:x:101:109::/nonexistent:/usr/sbin/nologin
sshd:x:102:65534::/run/sshd:/usr/sbin/nologin
polkitd:x:997:997:polkit:/nonexistent:/usr/sbin/nologin
_chrony:x:103:111:Chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin
kali:x:1000:1001:Kali Linux:/home/kali:/bin/zsh
aluno:x:1001:1002::/home/aluno:/bin/bash
rtkit:x:104:112:RealtimeKit,,,:/proc:/usr/sbin/nologin
usbmux:x:105:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
avahi:x:106:113:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/
nologin
lightdm:x:107:114:Light Display Manager:/var/lib/lightdm:/bin/false
pulse:x:108:115:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:109:118::/var/lib/saned:/usr/sbin/nologin
colord:x:110:119:colord colour management daemon,,,:/var/lib/colord:/
usr/sbin/nologin
xrdp:x:111:121::/run/xrdp:/usr/sbin/nologin
Debian-exim:x:112:122::/var/spool/exim4:/usr/sbin/nologin
logcheck:x:113:123:logcheck system account,,,:/var/lib/logcheck:/usr/
sbin/nologin
debian-tor:x:114:124::/var/lib/tor:/bin/false
clamav:x:115:125::/var/lib/clamav:/bin/false
geoclue:x:116:126::/var/lib/geoclue:/usr/sbin/nologin
postgres:x:117:130:PostgreSQL administrator,,,:/var/lib/postgresql:/
bin/bash
```

Cada linha possui sete campos separados por dois-pontos (:) e está na seguinte ordem (veja a linha que começa com “aluno”):

- **aluno**: Nome de usuário.
- **x**: Campo de senha, geralmente contendo uma letra "x", indicando que a senha está armazenada em outro local, como /etc/shadow.
- **1001**: ID de usuário (UID), um número único atribuído ao usuário no sistema.
- **1002**: ID de grupo primário (GID), o ID do grupo principal ao qual o usuário pertence. ****: Campo de comentário ou informações adicionais, geralmente vazio.
- **/home/aluno**: Diretório inicial do usuário, onde ele é direcionado após o login.
- **/bin/bash**: Caminho para o shell padrão do usuário, que é o Bash neste caso.

3. Em seguida, veja o conteúdo do arquivo “group”:

```
┌──(aluno㉿kali)-[~]
└─$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:kali,logcheck
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:kali
fax:x:21:
voice:x:22:
cdrom:x:24:kali
floppy:x:25:kali
tape:x:26:
sudo:x:27:kali,aluno
audio:x:29:kali,pulse
dip:x:30:kali
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
shadow:x:42:
utmp:x:43:
video:x:44:kali
sasl:x:45:
plugdev:x:46:kali
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:999:
systemd-network:x:998:
crontab:x:101:
input:x:102:
sgx:x:103:
kvm:x:104:
render:x:105:
netdev:x:106:kali
```

```
netdev:x:106:kali
messagebus:x:107:
_ssh:x:108:
tcpdump:x:109:
polkitd:x:997:
kali-trusted:x:110:
_chrony:x:111:
lxd:x:1000:kali
kali:x:1001:
aluno:x:1002:
rtkit:x:112:
avahi:x:113:
lightdm:x:114:
pulse:x:115:
pulse-access:x:116:
scanner:x:117:saned
saned:x:118:
colord:x:119:
ssl-cert:x:120:aluno,postgres
xrdp:x:121:
Debian-exim:x:122:
logcheck:x:123:
debian-tor:x:124:
clamav:x:125:
geoclue:x:126:
vboxusers:x:127:
docker:x:128:
_cvsadmin:x:129:
postgres:x:130:
```

O comando “cat /etc/group” exibe o conteúdo do arquivo “/etc/group”, que é um arquivo de banco de dados no formato de texto que armazena informações sobre grupos de usuários no sistema Linux:

- **aluno**: Nome do grupo.
- **x**: Campo de senha, que geralmente contém uma letra "x", indicando que a senha do grupo está armazenada em outro local, como /etc/gshadow.
- **1002**: ID do grupo (GID), um número único atribuído ao grupo no sistema.

4. Mude a senha do usuário atual para “rnpesr2”:

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

┌──(root㉿kali)-[~]
└─# passwd aluno
Nova senha:
Redigite a nova senha:
passwd: senha atualizada com sucesso
```

5. Clique com o botão direito (canto superior direito da tela do Kali Linux) no texto “aluno” → “Painel” → “Encerrar sessão” → “Encerrar sessão”.
6. De volta ao Linux Landing, inicialize o Kali Linux via RDP ao IP: 192.168.98.40, com usuário “aluno” e senha “rnpesr2”. Veja que foi autenticado com sucesso!
7. Repita o passo 4 (autentique-se com a senha “rnpesr2”) e efetue o procedimento para voltar a senha original “rnpesr” (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**).
8. Feche o Terminal.

Parabéns! Agora você sabe como modificar o Controle de Acesso de autenticação via senha no Kali Linux!

Atividade 4.2 – Explorando a ferramenta SELinux no Kali Linux

Nesta atividade, vamos explorar a ferramenta SELinux no Kali Linux. Todo material apresentado aqui deve ser usado somente para fins acadêmicos. O SELinux (Security-Enhanced Linux) é um conjunto de modificações no núcleo do sistema operacional Linux que implementa um sistema de controle de acesso obrigatório (MAC). Ele foi projetado para aprimorar a segurança do Linux, controlando de forma mais granular as permissões de acesso dos processos e usuários ao sistema. Ao contrário do modelo tradicional de controle de acesso no Linux, que é baseado em permissões de usuário e grupo, o SELinux adiciona políticas de segurança mais detalhadas, associando rótulos de segurança a arquivos, processos e recursos do sistema.

O SELinux possui 2 modos de operação:

- **Enforcing mode**: o SELinux implementa as políticas carregadas. O SELinux recusa o acesso com base nas regras da política SELinux e permite apenas as interações que são explicitamente autorizadas. O modo de imposição é o modo SELinux mais seguro.
- **Permissive mode**: o SELinux não implementa as políticas carregadas. O SELinux não nega o acesso, mas registra ações que violam as regras no log / var/log/audit/audit.log. O modo permissivo é o modo padrão durante a instalação. O modo permissivo também é útil em alguns casos específicos, por exemplo, durante a solução de problemas.

IMPORTANTE! NÃO ERRE OS PASSOS DESTE LABORATÓRIO! O ERRO PODE GERAR INDISPONIBILIDADE DE ACESSO FUTURO 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. Vamos ativar o SELinux. O SELinux é um conjunto de modificações no núcleo do sistema operacional Linux que implementa um sistema de controle de acesso obrigatório (MAC). Durante a ativação, o comando gera um novo arquivo de configuração do GRUB (GRand Unified Bootloader) para incorporar as alterações necessárias para o SELinux. O GRUB é configurado para carregar o kernel do SELinux, que inclui o suporte a políticas de segurança mais detalhadas:

```
┌──(root㉿kali)-[~]
└─# selinux-activate
Activating SE Linux
Generating grub configuration file ...
Found background image: /usr/share/images/desktop-base/desktop-grub.png
Found linux image: /boot/vmlinuz-6.5.0-kali3-cloud-amd64
Found initrd image: /boot/initrd.img-6.5.0-kali3-cloud-amd64
Found linux image: /boot/vmlinuz-6.1.0-kali7-cloud-amd64
Found initrd image: /boot/initrd.img-6.1.0-kali7-cloud-amd64
Found linux image: /boot/vmlinuz-6.1.0-kali5-cloud-amd64
Found initrd image: /boot/initrd.img-6.1.0-kali5-cloud-amd64
done
SE Linux is activated.  You may need to reboot now.
```

O comando apresenta as seguintes saídas:

- **Activating SE Linux**: Mensagem indicando a ativação do SELinux.
- **Generating grub configuration file ...**: Indica que está sendo gerado o arquivo de configuração do GRUB, um gerenciador de inicialização comumente usado em sistemas Linux.
- **Found background image: /usr/share/images/desktop-base/desktop-grub.png**: Informa que foi encontrado uma imagem de plano de fundo para o GRUB, localizada em /usr/share/images/desktop-base/desktop-grub.png.
- **Found linux image: /boot/vmlinuz-6.5.0-kali3-cloud-amd64**: Esta linha indica que foi encontrado um kernel Linux com a versão 6.5.0-kali3-cloud-amd64 localizado em /boot/vmlinuz-6.5.0-kali3-cloud-amd64.
- **Found initrd image: /boot/initrd.img-6.5.0-kali3-cloud-amd64**: Informa que foi encontrado um arquivo de imagem initrd correspondente ao kernel Linux encontrado na linha anterior.
- **Found linux image: /boot/vmlinuz-6.1.0-kali7-cloud-amd64**: Indica que foi encontrado outro kernel Linux com a versão 6.1.0-kali7-cloud-amd64 localizado em /boot/vmlinuz-6.1.0-kali7-cloud-amd64.
- **Found initrd image: /boot/initrd.img-6.1.0-kali7-cloud-amd64**: Informa que foi encontrado outro arquivo de imagem initrd correspondente ao segundo kernel Linux encontrado.
- **Found linux image: /boot/vmlinuz-6.1.0-kali5-cloud-amd64**: Indica a descoberta de um terceiro kernel Linux com a versão 6.1.0-kali5-cloud-amd64 localizado em /boot/vmlinuz-6.1.0-kali5-cloud-amd64.

- **Found initrd image: /boot/initrd.img-6.1.0-kali5-cloud-amd64**: Informa que foi encontrado outro arquivo de imagem initrd correspondente ao terceiro kernel Linux encontrado.
- **done**: Indica que a geração do arquivo de configuração do GRUB foi concluída com sucesso.
- **SE Linux is activated. You may need to reboot now.**: Esta linha indica que o SELinux foi ativado com sucesso e que talvez seja necessário reiniciar o sistema para que as alterações tenham efeito.

3. Reinicie a máquina virtual:

```
┌──(root㉿kali)-[~]
└─# reboot
```

Ao reiniciar, a tela apresenta uma mensagem similar à seguinte que você **não poderá visualizar** pelo fato de estar numa VM que perde a conexão ao reiniciar:

```
*** Warning -- SELinux default policy relabel is requires.
*** Relabeling could take a very long time, dependeing on file
*** system size and speed of hard drives.
libsemanage.add_user: user sddm not in password file
Warning: Skipping the following R/O filesystems:
/run/credentials/systemd-sysctl.service
/run/credentials/systemd-sysusers.service
/run/credentials/systemd-tmpfiles-setup-dev.service
/run/credentials/systemd-tmpfiles-setup.service
Relabeling /
75.5%
```

A mensagem mostrada acima representa:

- **Warning -- SELinux default policy relabel is requires**: Aviso indicando que é necessário relabelar a política padrão do SELinux.
- **Relabeling could take a very long time, depending on file system size and speed of hard drives**: Aviso sobre o possível tempo prolongado de relabeling, que depende do tamanho do sistema de arquivos e da velocidade dos discos rígidos.

- **libsemanage.add_user: user sddm not in password file**: Mensagem indicando que o usuário "sddm" não está no arquivo de senhas.
- **Warning: Skipping the following R/O filesystems**: Aviso sobre a omissão dos seguintes sistemas de arquivos somente leitura. a. /run/credentials/systemd-sysctl.service b. /run/credentials/systemd-sysusers.service c. /run/credentials/systemd-tmpfiles-setup-dev.service d. /run/credentials/systemd-tmpfiles-setup.service
- **Relabeling / 75.5%**: Indicação de que o relabeling está em andamento e está 75.5% concluído, referindo-se ao diretório raiz ("/").

4. **Aguarde 12 minutos**. No Linux Landing, inicialize o Kali Linux via RDP ao IP: 192.168.98.40, com usuário “aluno” e senha “rnpesr”.
5. Veja o status do SELinux (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

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

┌──(root㉿kali)-[~]
└─# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             default
Current mode:                   permissive
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

O status atual é:

- **SELinux status**: Indica que o SELinux está habilitado no sistema.
- **SELinuxfs mount**: Mostra o ponto de montagem do sistema de arquivos SELinux, que é /sys/fs/selinux.
- **SELinux root directory**: Indica o diretório raiz do SELinux, que é /etc/selinux.
- **Loaded policy name**: Apresenta o nome da política SELinux carregada, que é "default".

- **Current mode**: Indica o modo SELinux atual, que está definido como "permissive" (permissivo). No modo permissivo, o SELinux não nega o acesso, mas registra violações de política no log.
- **Mode from config file**: Mostra o modo SELinux configurado no arquivo de configuração, que também é "permissive".
- **Policy MLS status**: Indica que o Modelo de Nível de Segurança (MLS) da política está habilitado.
- **Policy deny_unknown status**: Permite a política negar acessos a recursos não reconhecidos.
- **Memory protection checking**: Indica que a verificação de proteção de memória está configurada como "actual" e é considerada segura.
- **Max kernel policy version**: Mostra a versão máxima da política do kernel, que é 33.

6. Veja a lista dos usuários SELinux no sistema, juntamente com informações sobre suas configurações de rotulagem, níveis MLS (Multi-Level Security) e papéis SELinux:

```
┌──(root㉿kali)-[~]
└─# semanage user -l

                Rótulo     MLS/       MLS/
Usuário do SELinux Prefixo    Nível MCS  Intervalo MCS
Funções do SELinux

guest_u         user       s0         s0
guest_r
root            sysadm     s0         s0-s0:c0.c1023
staff_r sysadm_r system_r
staff_u         staff      s0         s0-s0:c0.c1023
staff_r sysadm_r
sysadm_u        sysadm     s0         s0-s0:c0.c1023
sysadm_r
system_u        user       s0         s0-s0:c0.c1023
system_r
unconfined_u    unconfined s0         s0-s0:c0.c1023
system_r unconfined_r
user_u          user       s0         s0
user_r
xdm             user       s0         s0
system_r xdm_r
xguest_u        user       s0         s0
xguest_r
```

- **Rótulo**: Esta coluna lista os nomes de usuário do SELinux.
- **MLS/Prefixo**: O MLS (Multilevel Security) é uma extensão do SELinux que fornece controle de acesso baseado em níveis de segurança. O "Prefixo" indica o prefixo de segurança associado ao usuário. Neste caso, todos os usuários têm o mesmo prefixo "s0", o que significa que estão todos no mesmo nível de segurança.
- **Nível MCS**: Este campo indica o nível de segurança do usuário em termos de Categorias de Segurança Mínimas (MCS). Neste caso, todos os usuários têm o mesmo nível de segurança "s0".
- **Intervalo MCS**: Indica o intervalo permitido para o usuário em termos de Categorias de Segurança Mínimas. Aqui, todos os usuários têm o mesmo intervalo "s0-s0:c0.c1023".
- **Funções do SELinux**: Esta coluna lista as funções do SELinux associadas a cada usuário. Por exemplo:

- **guest_r**: Essa função (role) permite ao usuário acessar recursos designados para a função de convidado. Geralmente usada para usuários convidados com privilégios mínimos e acesso altamente restrito ao sistema.
- staff_r: Essa função permite ao usuário acessar recursos designados para a função de staff.
- sysadm_r: Essa função permite ao usuário acessar recursos designados para a função de sysadm.
- system_r: Essa função permite ao usuário acessar recursos designados para a função de sistema.
- unconfined_r: Essa função permite ao usuário acesso não restrito aos recursos.
- user_r: Essa função permite ao usuário acessar recursos designados para a função de usuário.
- xdm_r: Essa função permite ao usuário acessar recursos designados para o gerenciador de exibição X.
- **xguest_r**: Essa função permite acesso limitado e isolado para usuários convidados em ambientes gráficos. Projetada para segurança, restringe a escrita apenas em diretórios temporários e evita alterações permanentes no sistema.

7. Observe a lista de configurações de políticas SELinux associadas a usuários de login no sistema:

```
┌──(root㉿kali)-[~]
└─# semanage login -l

Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *
root                 unconfined_u         s0-s0:c0.c1023       *
sddm                 xdm                  s0-s0                *
```

- **Login Name**: O nome do usuário de login no sistema.
- **SELinux User**: O usuário SELinux associado a esse usuário de login.
- **MLS/MCS Range**: A faixa de níveis MLS/MCS permitida para esse usuário SELinux.
- **Service**: O serviço associado a esse usuário de login.

Na saída fornecida:

- **default**: Refere-se às configurações padrão para usuários não especificados. O usuário SELinux associado é "unconfined_u" com a faixa de MLS s0-s0:c0.c1023. O serviço associado é "*", o que significa que se aplica a todos os serviços não especificados.
- **root**: Para o usuário de login "root", o usuário SELinux associado é "unconfined_u" com a faixa de MLS s0-s0:c0.c1023. O serviço associado é "*", aplicando-se a todos os serviços não especificados.
- **sddm**: Para o usuário de login "sddm", o usuário SELinux associado é "xdm" com a faixa de MLS s0-s0. O serviço associado é "*", aplicando-se a todos os serviços não especificados.

8. Em seguida, verifique a lista de variáveis booleanas do SELinux com seus estados atuais e valores padrão:

```
┌──(root㉿kali)-[~]
└─# semanage boolean -l
SELinux boolean                State  Default Description

aide_mmap_files                (off  ,  off)  Control if AIDE can mmap
files. AIDE can be compiled with the option 'with-mmap' in which case
it will attempt to mmap files while running.
allow_cvs_read_shadow          (off  ,  off)  Determine whether cvs can
read shadow password files.
allow_execheap                 (off  ,  off)  Allow unconfined
executables to make their heap memory executable.  Doing this is a
really bad idea. Probably indicates a badly coded executable, but could
indicate an attack. This executable should be reported in bugzilla
allow_execmem                  (off  ,  off)  Allow unconfined
executables to map a memory region as both executable and writable,
this is dangerous and the executable should be reported in bugzilla")

…

xguest_use_bluetooth           (off  ,  off)  Determine whether xguest
can use blue tooth devices.
xscreensaver_read_generic_user_content (on   ,   on)  Grant the
xscreensaver domains read access to generic user content
xserver_allow_dri              (off  ,  off)  Allow DRI access
xserver_can_network            (off  ,  off)  Allows the X server to
use TCP/IP networking functionality (insecure).
xserver_client_writes_xserver_tmpfs (off  ,  off)  Allows clients to
write to the X server tmpfs files.
xserver_gnome_xdm              (off  ,  off)  Use gnome-shell in gdm
mode as the X Display Manager (XDM)
xserver_object_manager         (off  ,  off)  Support X userspace
object manager
xserver_xdm_can_network        (off  ,  off)  Allows the X display
manager to use TCP/IP networking functionality (insecure).
zabbix_can_network             (off  ,  off)  Determine whether zabbix
can connect to all TCP ports
```

Os parâmetros de cada aplicação são:

- **SELinux boolean**: O nome da variável booleana do SELinux.
- **State**: O estado atual da variável booleana (ligado ou desligado).
- **Default**: O valor padrão da variável booleana (ligado ou desligado).
- **Description**: Uma descrição da função ou controle que a variável booleana representa

9. Liste as definições de portas no SELinux, incluindo os tipos de porta, protocolos e números de porta associados:

```
┌──(root㉿kali)-[~]
└─# semanage port -l
SELinux Port Type              Proto    Port Number

afs3_callback_port_t           tcp      7001
afs3_callback_port_t           udp      7001
afs_bos_port_t                 udp      7007

...

zookeeper_client_port_t        tcp      2181
zookeeper_election_port_t      tcp      3888
zookeeper_leader_port_t        tcp      2888
zope_port_t                    tcp      8021
```

A saída lista:

- **SELinux Port Type**: O tipo SELinux associado à porta.
- **Proto**: O protocolo associado à porta (TCP ou UDP).
- **Port Number**: O número da porta associado ao tipo SELinux e ao protocolo.

10. Opcional **Não execute este passo nas VMs do ambiente Hacker do Bem, execute somente em uma VM local no seu computador**. Caso queira modificar o modo de funcionamento do SELinux, siga o passo 2.3 de:

```
https://access.redhat.com/documentation/en-us/
red_hat_enterprise_linux/8/html/using_selinux/changing-selinux-states-
and-modes_using-selinux
```

11. Desabilite o SELinux. Para isso, acesse o arquivo de configuração:

```
┌──(root㉿kali)-[~]
└─# nano /etc/selinux/config
```

12. Mude a linha:

```
SELINUX=permissive
```

Para:

```
SELINUX=disabled
```

Aperte “Ctrl + x”, “s” e “ENTER” para sair e salvar.

13. Reinicie a máquina virtual:

```
┌──(root㉿kali)-[~]
└─# reboot
```

14. De volta ao Linux Landing, **aguarde 3 minutos** e inicialize o Kali Linux via RDP ao IP: 192.168.98.40, com usuário “aluno” e senha “rnpesr”. Após logar, veja o status do SELinux no Terminal:

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

┌──(root㉿kali)-[~]
└─# sestatus
SELinux status:                 disabled
```

Parabéns! Você conhece os comandos de verificação de funcionamento do SELinux!

Atividade 4.3 – Criando um cofre de senhas com o KeePassXC no Kali Linux

Nesta atividade, vamos explorar a cofre de senhas KeePassXC no Kali Linux. O KeePassXC é um gerenciador de senhas de código aberto, multiplataforma e altamente seguro. Projetado para armazenar senhas de forma criptografada, o KeePassXC oferece uma interface gráfica intuitiva e recursos avançados para gerenciamento de credenciais. Sua principal característica é a capacidade de criar e armazenar senhas complexas de forma segura, gerando combinações únicas para cada conta. Além disso, o KeePassXC suporta recursos como categorização, tags, pesquisa avançada e a capacidade de armazenar informações adicionais associadas às contas. Todo material apresentado aqui deve ser usado somente para fins acadêmicos.

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 para inicializar o KeePassXC (**execute com o usuário ALUNO e NÃO como root**):

```
┌──(aluno㉿kali)-[~]
└─$ keepassxc
```

2. Perceba que uma interface gráfica chamada “KeePassXC” foi aberta. Clique em “+ Criar Banco de Dados”.
3. Vamos supor que a base de dados armazenará contas e senhas pessoais. Insira o nome “Pessoal” no campo “Nome do banco de dados” e clique em “Continuar”.
4. Na aba “Definições de cifra”, clique em “Avançado”.
5. Veja que o algoritmo de criptografia usado é o “AES 256-bit”, que é o melhor possível a ser usado atualmente. Clique em “Continuar”.
6. Insira a senha “rnpesr” nos campos “Insira senha” e “Confirmar senha”. Clique em “Concluído”. Clique em “Continuar com senha fraca” no aviso de Senha fraca.
7. Na janela aberta para salvar um arquivo, acesse a pasta “Documentos” e clique em “Salvar” para salvar o arquivo “Senhas.kdbx”.
8. Agora, uma interface gráfica é aberta. Nela você gerenciará as suas contas com credenciais. Adicione uma credencial clicando no botão “+”.
9. Insira os seguintes dados:

- Título: Netflix
- Nome de usuário: meuemail@gmail.com
- Senha: minhasenhanetflix
- URL: https://www.netflix.com

Clique em “OK”.

10. Veja que os dados da sua conta “Netflix” foram armazenados (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**).
11. Caso queira, adicione mais contas.
12. Selecione a conta “Netflix” e clique no botão com o símbolo de Lixeira para apagar essa linha. Veja que os dados da sua conta “Netflix” foram eliminados. Feche o KeePassXC.
13. Para mais detalhes, veja o site oficial:

```
https://keepassxc.org/docs/KeePassXC_GettingStarted
```

14. Acesse a pasta Documentos, apague o arquivo “Senhas.kdbx” e feche o Terminal:

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

┌──(aluno㉿kali)-[~/Documentos]
└─$ ls
Senhas.kdbx

┌──(aluno㉿kali)-[~/Documentos]
└─$ rm Senhas.kdbx
```

Parabéns! Você conhece como usar a senha de cofres “KeePassXC”!

Atividade 4.4 – Ataque de Dicionário Off-line contra credenciais no Kali Linux

Nesta atividade, vamos explorar a ferramenta John the Ripper no Kali Linux para descobrir a senha de um usuário desse sistema operacional usando o ataque de dicionário. John the Ripper, muitas vezes abreviado como John, é uma poderosa ferramenta de quebra de senha utilizada em testes de segurança e auditorias de senhas. Integrada no Kali Linux, o John é projetado para realizar ataques de força bruta e ataques de dicionário em senhas criptografadas. Ele suporta uma variedade de algoritmos de hash e é capaz de identificar padrões em senhas fracas. Todo material apresentado aqui deve ser usado somente para fins acadêmicos.

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 usuários do Kali Linux e o Hash correspondente a cada senha:

```
┌──(root㉿kali)-[~]
└─# cat /etc/shadow
root:$y$j9T$O3sufKDNguuCDtodqFh/
L0$m.k5WMUA2.hVPGRRGkOwSIb18G4dcYK6vq2YhxMsYQB:19740:0:99999:7:::
daemon:*:19426:0:99999:7:::
bin:*:19426:0:99999:7:::
sys:*:19426:0:99999:7:::
sync:*:19426:0:99999:7:::
games:*:19426:0:99999:7:::
man:*:19426:0:99999:7:::
lp:*:19426:0:99999:7:::
mail:*:19426:0:99999:7:::
news:*:19426:0:99999:7:::
uucp:*:19426:0:99999:7:::
proxy:*:19426:0:99999:7:::
www-data:*:19426:0:99999:7:::
backup:*:19426:0:99999:7:::
list:*:19426:0:99999:7:::
irc:*:19426:0:99999:7:::
_apt:*:19426:0:99999:7:::
nobody:*:19426:0:99999:7:::
systemd-network:!*:19426::::::
messagebus:!:19426::::::
tcpdump:!:19426::::::
sshd:!:19426::::::
polkitd:!*:19426::::::
_chrony:!:19426::::::
kali:!:19464:0:99999:7:::
aluno:$y$j9T$KNkC7Yio6rYK1A2Esp4Qq.
$FL1BfzLd78LQJnXnbXHL7krDSSJBvHSvaYrpsX5V.c0:19762:0:99999:7:::
rtkit:!:19740::::::
usbmux:!:19740::::::
avahi:!:19740::::::
lightdm:!:19740::::::
pulse:!:19740::::::
saned:!:19740::::::
colord:!:19740::::::
xrdp:!:19740::::::
Debian-exim:!:19740::::::
logcheck:!:19740::::::
debian-tor:!:19740::::::
clamav:!:19740::::::
geoclue:!:19740::::::
postgres:!:19761::::::
```

O arquivo /etc/shadow armazena informações criptografadas sobre as senhas dos usuários do sistema. Ele inclui hashes de senha e dados relacionados à conta do usuário, como a data da última alteração de senha, prazo de validade da senha, entre outros. O acesso a esse arquivo é restrito, permitido apenas para usuários privilegiados, normalmente o usuário root.

3. Adicione um, usuário novo “teste1” e coloque a senha “abcd123”:

```
┌──(root㉿kali)-[~]
└─# useradd -p $(openssl passwd -1 abcd123) teste1
```

O comando possui os seguintes parâmetros:

- **useradd**: Comando para adicionar um novo usuário ao sistema.
- **-p $(openssl passwd -1 abcd123)**: Define a senha do novo usuário. O comando openssl passwd -1 abcd123 gera a senha criptografada para "abcd123", que é então atribuída ao usuário.
- **teste1**: É o nome do usuário que está sendo adicionado ao sistema.

4. Repita o passo 2 e visualize a criação do novo usuário “teste 1” na última linha com a senha cifrada:

```
┌──(root㉿kali)-[~]
└─# cat /etc/shadow
root:
$y$j9T$Kbjz04D5OinDiwjgh6t6X0$MQFAgKOIDXHHNhVeb3G.yhOCSny7P1iwozrEHEZaE
UB:19789:0:99999:7:::
daemon:*:19426:0:99999:7:::
bin:*:19426:0:99999:7:::
sys:*:19426:0:99999:7:::
sync:*:19426:0:99999:7:::
games:*:19426:0:99999:7:::
man:*:19426:0:99999:7:::
lp:*:19426:0:99999:7:::
mail:*:19426:0:99999:7:::
news:*:19426:0:99999:7:::
uucp:*:19426:0:99999:7:::
proxy:*:19426:0:99999:7:::
www-data:*:19426:0:99999:7:::
backup:*:19426:0:99999:7:::
list:*:19426:0:99999:7:::
irc:*:19426:0:99999:7:::
_apt:*:19426:0:99999:7:::
nobody:*:19426:0:99999:7:::
systemd-network:!*:19426::::::
messagebus:!:19426::::::
tcpdump:!:19426::::::
sshd:!:19426::::::
polkitd:!*:19426::::::
_chrony:!:19426::::::
kali:!:19464:0:99999:7:::
aluno:$y$j9T$Y8os5JtEbwp4QefI6xWZO/
$wRJTfaItKlJVfxbDUiyKa9MOtto9BORqIZv7fdIC1m9:19789:0:99999:7:::
rtkit:!:19807::::::
usbmux:!:19807::::::
avahi:!:19807::::::
lightdm:!:19807::::::
pulse:!:19807::::::
saned:!:19807::::::
colord:!:19807::::::
tss:!:19807::::::
strongswan:!:19807::::::
dnsmasq:!:19807::::::
speech-dispatcher:!:19807::::::
nm-openvpn:!:19807::::::
nm-openconnect:!:19807::::::
xrdp:!:19807::::::
postgres:!:19807::::::
Debian-exim:!:19807::::::
```

```
logcheck:!:19807::::::
debian-tor:!:19807::::::
freerad:!:19807::::::
clamav:!:19807::::::
geoclue:!:19807::::::
teste1:$1$H6qvteqS$dZ84C5VJ0rWJ9YWoVAUNP1:19838:0:99999:7:::
```

5. Com o mouse, clique direito, selecione e copie os dados relacionados ao usuário criado (os dados cifrados após “teste1:1” podem ser diferentes):

```
teste1:$1$H6qvteqS$dZ84C5VJ0rWJ9YWoVAUNP1:19838:0:99999:7:::
```

6. Acesse a pasta Documentos e crie um arquivo txt e cole o texto do passo anterior:

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

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

Após colar o texto do passo 5, saia apertando “Ctrl+x” seguido de “S” e “ENTER”.

7. Finalmente, descubra a senha associada ao usuário “teste1” com John the Ripper, demora ao redor de 1 minuto (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**):

```
┌──(root㉿kali)-[/home/aluno/Documentos]
└─# john -format=crypt credencial.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt
5:sha256crypt 6:sha512crypt]) is 2 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if
any.
Proceeding with wordlist:/usr/share/john/password.lst
abcd123          (teste1)
1g 0:00:00:00 DONE 2/3 (2024-04-25 18:54) 1.960g/s 8364p/s 8364c/s
8364C/s Alexis..bigred
Use the "--show" option to display all of the cracked passwords
reliably
Session completed.
```

O comando executa uma tentativa de quebra de senha usando o John the Ripper com o formato de hash definido como "crypt" para as senhas contidas no arquivo "credencial.txt":

- **Loaded 1 password hash (crypt, generic crypt(3) [?/64])**: Indica que foi carregado um único hash de senha no formato "crypt". A mensagem "[?/64]" sugere que o formato específico do hash não foi identificado, mas que o programa pode tentar várias formas de quebra até encontrar o correto.
- **Cost 1...Cost 2**: Indica informações sobre o custo computacional associado à quebra de senha para diferentes algoritmos de criptografia.
- **Will run 2 OpenMP threads**: Informa que o programa utilizará 2 threads OpenMP para processar a quebra de senha, o que pode acelerar o processo em sistemas com múltiplos núcleos de CPU.
- **Proceeding with single, rules:Single**: Indica que o programa está seguindo o modo "single", que é o padrão de execução sem regras adicionais de quebra de senha.
- **Almost done: Processing the remaining buffered candidate passwords, if any**: Sinaliza que a quebra de senha está quase concluída e que o programa está processando as senhas candidatas restantes, se houver.

- **Proceeding with wordlist:/usr/share/john/password.lst**: Indica que o programa está usando uma lista de palavras-chave localizada em "/usr/share/john/password.lst" para tentar quebrar a senha.
- **abcd123 (teste1)**: Indica que a senha "abcd123" foi encontrada para o usuário "teste1".
- **1g 0:00:00:00 DONE...Alexis..bigred**: Informações sobre o progresso da quebra de senha, incluindo o tempo decorrido, a velocidade de quebra e algumas informações sobre as tentativas feitas.
- **Use the "--show" option to display all of the cracked passwords reliably**: Sugere o uso da opção "--show" para exibir todas as senhas que foram quebradas de forma confiável.
- **Session completed**: Indica que a sessão de quebra de senha foi concluída com sucesso.

8. Apague o arquivo "credencial.txt", feche o terminal e encerre a conexão RDP com o Kali Linux.:

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

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

Parabéns! Agoira, você sabe como usar o John the Ripper para descobrir senhas de usuários no Linux!

Atividade 4.5 – Gerenciando credenciais no Windows Server 2022

Nesta atividade, vamos explorar a ferramenta Credential Manager do Windows Server 2022. Todo material apresentado aqui deve ser usado somente para fins acadêmicos.

Vamos começar inicializando o Windows Server 2022 (cliente) via RDP ao IP: 192.168.98.30, com usuário “administrator” e senha “RnpEsr123@” (use a senha “RnpEsr123@2” caso o SO peça para atualizar a senha).

1. Na Barra de tarefas, clique no campo “Type here to search” e escreva:

```
Credential Manager
```

2. Clique na aplicação “Credential Manager”.
3. A janela do “Credential Manager” será aberta. No campo “Manage your credentials”, clique em “Web Credentials”.
4. Visualize as senhas de sites armazenadas no Windows Server 2022 no campo “Web Passwords” (pode ser que esteja em branco).
5. Clique em “Windows Credentials” e visualize as opções de credenciais “Windows Credentials”, “Certificate-based Credentials” e “Generic Credentials”.
6. Clique em “Back up Credentials” para poder efetuar um backup das credenciais existentes no Windows Server 2022.
7. Clique em “Browse...” e selecione a pasta “Desktop”.
8. Forneça o nome “backup” no campo “File Name” e clique em “Save”.
9. Clique em “Next”. Acione o “CTRL + ALT + DELETE” clicando no símbolo de ajustes (ícone da chave de boca) na barra esquerda da VM e em “Send Ctrl+Alt+Delete”, para efetuar o Backup.
10. Insira a senha “RnpEsr123” nos 2 campos de “Password” e aperte “Next”. Visualize que a mensagem “The backup was successful” foi apresentada. Clique em “Finish”.
11. Finalmente, veja que o arquivo “backup.cdr” foi criado no Desktop do Windows Server 2022 (**NÃO SE ESQUEÇA DE PRINTAR ESTE PASSO!**).
12. Apague o arquivo “backup.crd” (Shift + Delete), feche as janelas abertas e encerre a conexão RDP com o Windows Server (cliente).

Parabéns! Você sabe como gerenciar as credenciais no Windows Server 2022.