Laboratório - Configurar recursos de segurança no Windows e Linux

# Objetivos

Parte 1: Atualizar o Windows e o Linux

Part 2: Política de Segurança Local do Windows

Parte 3: Configurar regras de firewall

Parte 4: Instalar e executar aplicativos

# Recursos necessários

=   1 PC com Windows 10.

=   Esta máquina virtual CSE-LABVM

=   Acesso à Internet

# Histórico/Cenário

Neste laboratório, você atualizará os sistemas Windows e Linux. Você vai configurar a política de segurança local e as regras de firewall no Windows. No Linux, você instalará dois aplicativos: chkrootkit e lynis.

# Instruções

## Parte 1: Atualização do Windows e Linux

As novas vulnerabilidades e métodos de ataque são descobertos o tempo todo. É uma boa ideia manter seu PC atualizado para mitigar a exploração das vulnerabilidades conhecidas.

### Etapa 1: Verificar a conectividade entre o CSE-LABVM e o computador host do Windows.

Nesta etapa, você verificará a conectividade com a Internet para baixar as atualizações. Além disso, você verificará a conectividade entre **CSE-LABVM** e Windows PC para poder executar tarefas posteriormente neste laboratório.

a.     Antes de iniciar o **CSE-LABVM**, selecione-o e escolha **Configurações** > **Rede**. Para o **Adaptador 1**, altere a opção **Conectado a:** para **Adaptador em Ponte**. Em seguida, você pode escolher o adaptador. Muitos computadores têm dois adaptadores: um para redes sem fio e outro para redes com fio. Escolha o que o computador está usando para se conectar à Internet.

b.     Inicie o CSE-LABVM e aguarde até que ele seja inicializado.

c.     No CSE-LABVM, abra um terminal e digite **ip address** para determinar o Endereço IP.

d.     No computador host do Windows, abra um prompt de comando e digite **ipconfig** para determinar o Endereço IP.

#### Pergunta:

Registre o endereço IP para CSE-LABVM e Windows PC.

CSE-LABVM:

Digite suas respostas aqui.

PC com Windows

Digite suas respostas aqui.

e.     Nos respectivos prompts de comando, faça ping em um site de sua escolha para verificar se o host do Windows e o **CSE-LABVM** podem acessar a Internet.

f.      Verifique se o host do Windows pode executar ping no **CSE-LABVM**.

g.     No **CSE-LABVM**, tente fazer ping no host do Windows. O **CSE-LABVM** pode não ser capaz de executar ping no host do Windows devido às configurações de firewall padrão no Windows. Você modificará a regra de firewall posteriormente neste laboratório para permitir pings pelo Firewall do Windows. Pressione **CTRL-C** para interromper os pings, se necessário.

### Etapa 2: Verificação de Atualizações no Windows

a.     No **Menu Iniciar do Windows**, pesquise por **checar por atualizações**.

b.     Na janela do **Windows Update**, é possível revisar as atualizações opcionais e o histórico de atualizações. Explore todas as opções disponíveis relacionadas ao Windows Update e responda às seguintes perguntas.

#### Perguntas:

Quando foi a última vez que o sistema procurou por atualizações?

Digite suas respostas aqui.

Quais são as horas ativas atuais? O que o Windows fará fora do horário de trabalho?

Digite suas respostas aqui.

### Etapa 3: Update e Upgrade do Linux

a.     No **CSE-LABVM**, digite o comando **apt-get** para ver a lista de comandos disponíveis. O **comando apt-get update** sempre deve ser feito antes de uma atualização.

b.     Insira o comando **sudo apt-get update** para ressincronizar os arquivos de índice do pacote de suas fontes. Digite a senha **password** quando solicitado.

cisco@labvm:~$ **sudo apt-get update**

[sudo]senha para cisco:

c.     No terminal, digite o comando **sudo apt-get upgrade** para recuperar e atualizar os pacotes atualmente instalados com novas versões disponíveis. Este comando não removerá os pacotes atualmente instalados. Se a versão mais recente não puder ser atualizada, nenhuma alteração será feita nos pacotes.

Digite a senha **password** quando solicitado. Responda **y** quando for perguntado se você deseja continuar. Este processo pode levar de 10 a 20 minutos.

cisco@labvm:~$ **sudo apt-get upgrade**

[sudo]senha para cisco:

Lendo listas de pacotes ... Concluído

Criando uma árvore de dependência

Lendo informações de estado ... Concluído

Calculando a atualização ... Concluído

<output omitted>

É necessário obter 479 MB de arquivos.

Após essa operação, 53,7 MB de espaço em disco adicional serão usados.

Deseja continuar? [Y/n] **Y**

## Parte 2: Política de segurança local do Windows (opcional)

A política de segurança local do Windows de um sistema é um conjunto de informações sobre a segurança do seu computador. Nesta parte, você definirá a política de senha local, as configurações de bloqueio de conta e a política de auditoria.

**Observação**: a política de segurança local vem apenas com as edições do Windows Pro ou Enterprise. Se você tiver a edição Home, poderá pesquisar na Internet por tutoriais sobre "Como habilitar a política de segurança local (secpol.msc)." Por exemplo, o site majorgeeks.com tem um excelente tutorial. Se você não tem permissão ou prefere não alterar a Política de segurança local no host do Windows, leia esta parte e siga para a próxima parte.

### Etapa 1: Configurar a política de senha local no Windows

Você determinou que a política de segurança para senha é a seguinte:

=   Um usuário deve usar uma senha exclusiva por, no mínimo, duas alterações de senha.

=   As senhas precisam ter pelo menos oito caracteres.

=   As senhas devem ser alteradas a cada 90 dias.

=   Só pode alterar a senha uma vez por dia.

=   Uma senha deve consistir em três destes quatro elementos:

=   Pelo menos um caractere alfabético em letras minúsculas.

=   Pelo menos um caractere alfabético em letras maiúsculas.

=   Pelo menos um caractere numérico.

=   Pelo menos um caractere de símbolo.

a.     Navegue até a **Política de Segurança Local** pesquisando e abrindo o **Painel de Controle**.

b.     Clique em **Ferramentas Administrativas** > Pesquise por **Política de Segurança Local**

c.     Abra a **Política de Segurança Local**.

#### Pergunta:

Liste algumas configurações de política de segurança:

Digite suas respostas aqui.

d.     Expanda **Políticas de Conta** e clique em **Política de Senha**. Seis políticas serão exibidas no painel direito com as configurações de segurança padrão associadas.

e.     A primeira política, **Aplicar histórico de senhas**, é usada para definir o número de senhas exclusivas que o usuário deve inserir antes de poder reutilizar uma senha. Clique duas vezes em **Aplicar histórico de senhas** para abrir a janela **Propriedades de Aplicar histórico de senhas**. Defina o valor como **2**.

f.      Preencha os valores que você deve definir na **Política de Segurança Local** para as configurações de segurança restantes da **Política de Senha**.

| Política | Configuração de Segurança |
| --- | --- |
| Aplicar histórico de senhas |  |
| Tempo de vida máximo da senha |  |
| Tempo de vida mínimo da senha |  |
| Comprimento mínimo da senha |  |
| A senha deve atender a requisitos de complexidade |  |
| Armazenar senhas usando criptografia reversível |  |

Linha em branco, sem informações adicionais

Linha em branco, sem informações adicionais

**Observação**: a configuração de segurança **Armazenar senhas usando criptografia reversível** sempre deve ser desativada. Armazenar senhas que usam criptografia reversível é basicamente o mesmo que armazenar versões de texto simples das senhas. Por esse motivo, esta política nunca deve ser ativada, a menos que os requisitos de aplicativos superem a necessidade de proteger as informações de senha.

g.     Clique duas vezes em cada uma das políticas e defina os valores de acordo com as entradas da tabela acima.

### Etapa 2: Testar as configurações de segurança da diretiva de senhas.

Tente mudar a senha para testar as configurações de segurança da diretiva de senhas. Experimente uma nova senha que não atenda aos requisitos de tamanho ou complexidade.

a.     No menu Iniciar, pesquise **Alterar sua senha**.

b.     Clique em **Senha**. Clique em **Alterar**

c.     Digite sua senha atual. Clique em **Avançar** para continuar.

d.     Digite sua nova senha duas vezes e forneça uma dica de senha. Verifique se a nova senha não atende aos requisitos de comprimento ou complexidade configurados na etapa anterior. Clique em **Avançar** para continuar.

**e.** Clique em **Concluir.** Você deve receber uma mensagem informando que sua nova senha não atende aos requisitos da política de senha. clique em **Fechar**para continuar.

### Etapa 3: Configurar as opções de segurança da Política de Bloqueio de Conta.

a.     Volte para a janela Política de segurança local.

b.     Expanda as **Políticas de Conta** e clique em **Política de Bloqueio de Conta**. Três políticas são exibidas no painel direito com suas configurações de segurança padrão associadas.

c.     Altere as configurações padrão para o seguinte:

o    Um usuário deve esperar 10 minutos para o contador de bloqueio ser reiniciado.

o    O acesso dos usuários ao computador é bloqueado após 5 tentativas de inserir a senha correta.

#### Perguntas:

Quanto tempo o usuário tem que aguardar antes de tentar fazer login novamente?

Digite suas respostas aqui.

Quantas vezes um usuário pode tentar fazer login antes que a conta seja bloqueada?

Digite suas respostas aqui.

### Etapa 4: Configurar as opções de segurança da Política de Auditoria.

a.     Expanda o menu **Políticas Locais** e clique em **Política de Auditoria**.

b.     Clique duas vezes para abrir as propriedades da **Auditoria de eventos de logon de conta**.

c.     Na guia **Configuração de Segurança Local**, observe as caixas de seleção para **Sucesso** e **Falha**.

d.     Clique na guia **Explicar** para saber mais sobre esta configuração de segurança. Clique em **OK** para fechar a janela **Propriedades**.

e.     Continue a analisar cada configuração de segurança. Clique na guia **Explicar** de cada uma delas e leia o que ela faz.

## Parte 3: Configurar regras de firewall

O tráfego viaja dentro e fora dos dispositivos usando portas. O firewall controla o fluxo do tráfego. Pense no firewall como um agente de segurança que controla o tráfego de entrada e de saída com base nas regras de firewall.

Nesta parte, você configurará o Windows Defender Firewall em um Windows.

### Etapa 1: Investigar o Windows Defender Firewall

a.     No menu Iniciar, pesquise e abra o **Windows Defender Firewall**. O estado normal para o Firewall do Windows é Ativado.

**Observação**: se você estiver usando um PC com Windows administrado por uma empresa, poderá aparecer a mensagem, **Para sua segurança, algumas configurações são gerenciadas pelo administrador do sistema.**

#### Pergunta:

Quais são os benefícios do Firewall do Windows?

Digite suas respostas aqui.

b.     No painel esquerdo da janela, clique **em Permitir um aplicativo ou recurso pelo Windows Defender Firewall**. Os **Programas e Serviços** que o Firewall do Windows não estiver bloqueando, serão listados com uma marca de seleção.

**Nota**: você pode adicionar aplicativos à lista. Esse recurso poderá ser necessário caso você tenha um aplicativo que exija comunicações externas, mas por algum motivo, o Firewall do Windows não consegue executar a configuração automaticamente.

A criação de muitas exceções no arquivo Programas e Serviços pode gerar consequências negativas.

#### Pergunta:

Descreva uma consequência negativa de ter muitas exceções.

Digite suas respostas aqui.

c.     Clique em **Cancelar** para sair da janela Permitir aplicativos.

### Etapa 2: Configurar os recursos de Segurança Avançada no Firewall do Windows

**Observação**: essa etapa pode não ser permitida pela política de segurança da sua empresa.

Nesta etapa, você criará uma regra de entrada que permitirá pacotes de solicitação de eco pelo firewall.

a.     No painel esquerdo da janela Firewall do Windows, clique em **Configurações avançadas**.

b.     No **Firewall do Windows Defender com Segurança Avançada no Computador Local**, você pode configurar Regras de Entrada, Regras de Saída ou Regras de Segurança de Conexão. Você também pode clicar em **Monitoramento** para exibir o status das regras configuradas.

c.     Clique em **Regras de Entrada** e, no painel **Ações**, clique em **Nova Regra**.

d.     No **Assistente de Nova Regra de Entrada**, selecione **Personalizar** e clique em **Avançar** duas vezes. Você deve estar na etapa **Protocolo e Portas**.

e.     Para **Tipo de Protocolo**, selecione **ICMPv4** e clique em **Personalizar**.

f.      Na janela **Personalizar configurações de ICMP** , selecione **Tipos específicos de ICMP**, selecione **Echo Request**e clique **em OK**.

g.     Clique em **Próximo** três vezes. Você deve estar na etapa **Perfil**.

h.     Desmarque **Pública** para que o PC com Windows não responda a uma solicitação de eco em um local de rede pública, como um cibercafé. Clique em **Avançar** para continuar.

i.      Forneça um nome para a nova regra de entrada que ofereça uma boa descrição da regra e clique em **Concluir**. Agora você deve ver sua regra no topo da lista de **Regras de Entrada** na janela de diálogo do **Firewall do Windows Defender com Segurança Avançada**.

j.      Agora, a regra foi criada e ativada. Verifique se o **CSE-LABVM** pode executar ping no host do Windows e receber respostas.

## Parte 4: Instalar e Executar aplicativos

Nesta parte, você instalará duas novas aplicações no **CSE-LABVM**: **chkrootkit** e **lynis**. O aplicativo **chkrootkit** será baixado de um repositório de software. No entanto, adicionaremos um novo repositório para que possamos instalar o **lynis**, fornecido pelo CISOfy.

### Etapa 1: Instalar e Executar o chkrootkit

A ferramenta **chkrootkit** é usada para verificar sinais de rootkit em um sistema local. O Rootkit é um tipo de malware que pode permanecer oculto no computador e pode ser usado para causar danos significativos ao dispositivo por hackers.

a.     Em um terminal, digite o comando **sudo apt install chkrootkit** Digite a senha **password** quando solicitado.

cisco@labvm:~$ **sudo apt install chkrootkit**

[sudo]senha para cisco:

b.     Insira o comando **sudo chkrootkit** para executar uma verificação do rootkit.

cisco@labvm:~$ **sudo chkrootkit**

c.     A saída pode ser filtrada para procurar por sequências de caracteres interessadas, como o worm. O comando **chkrootkit** pode ser executado junto com o comando **grep** com a opção **–i** para ignorar a distinção entre maiúsculas e minúsculas (case distinction) nas cadeias de caracteres de interesse.

cisco@labvm:~$ **sudo chkrootkit | grep -i worm**

Searching for LPD Worm files and dirs...                    nothing found

Searching for Ramen Worm files and dirs...                  nothing found

Searching for Adore Worm...                                 nothing found

Searching for ShitC Worm...                                 nothing found

Searching for Omega Worm...                                 nothing found

Searching for Sadmind/IIS Worm...                           nothing found

Searching for TC2 Worm default files and dirs...            nothing found

! cisco       32822 pts/0  grep --color=auto -i worm

### Etapa 2: Instalar o Lynis

O **lynis** é uma ferramenta de segurança para sistemas que executam sistemas operacionais baseados em Unix, como Linux e macOS. O **lynis** será usado posteriormente em outra atividade para proteger um sistema Linux. A aplicação **Lynis**é mantida pelo [CISOfy](https://cisofy.com/lynis/). Nesta etapa, adicionaremos o repositório de software e instalaremos o Lynis.

a.     Copie e cole o seguinte comando em um terminal para importar a chave do servidor de chaves CISOfy. Essa chave é necessária para verificar a integridade do download ao baixar o **lynis**:

cisco@labvm:~$ **sudo apt-key adv --keyserver keyserver.ubuntu.com --recv-keys 013baa07180c50a7101097ef9de922f1c2fde6c4**

Executing: /tmp/apt-key-gpghome.8C6X477onz/gpg.1.sh --keyserver keyserver.ubuntu.com --recv-keys 013baa07180c50a7101097ef9de922f1c2fde6c4

gpg: key FEBB7D1812576482: public key "CISOfy software signing <software@cisofy.com>" imported

gpg: Total number processed: 1

gpg:               imported: 1

b.     Copie e cole o seguinte comando em um terminal para adicionar o repositório **lynis** mantido pelo CISOfy.

cisco@labvm:~$ **echo "deb https://packages.cisofy.com/community/lynis/deb/ stable main" | sudo tee /etc/apt/sources.list.d/cisofy-lynis.list**

deb https://packages.cisofy.com/community/lynis/deb/ stable main

c.     Faça uma atualização depois de adicionar um novo repositório. No prompt, digite **sudo apt-get update**.

d.    Use o comando **apt install** para instalar o Lynis.

cisco@labvm:~$ **sudo apt install lynis**

Reading package lists... Concluído

Building dependency tree

Reading state information... Concluído

The following NEW packages will be installed:

  lynis

0 upgraded, 1 newly installed, 0 to remove and 17 not upgraded.

Need to get 0 B/262 kB of archives.

After this operation, 1,681 kB of additional disk space will be used.

Selecting previously unselected package lynis.

(Reading database ... 205787 files and directories currently installed.)

Preparing to unpack .../lynis\_3.0.6-100\_all.deb ...

Unpacking lynis (3.0.6-100) ...

Setting up lynis (3.0.6-100) ...

Processing triggers for man-db (2.9.1-1) ...

#### Pergunta:

Na saída, qual é a versão instalada do Lynis?

Digite suas respostas aqui.

e.     Para verificar a versão instalada, digite o comando **lynis show version** no terminal.

cisco@labvm:~$ **lynis show version**

3.0.6

f.      Se você quiser determinar a versão mais recente fornecida pelo CISOfy, digite o seguinte comando no terminal.

cisco@labvm:~$ **sudo apt-cache policy lynis**

lynis:

  Installed: 3.0.6-100

  Candidate: 3.0.6-100

  Version table:

 \*\*\* 3.0.6-100 500

        500 https://packages.cisofy.com/community/lynis/deb stable/main amd64 Packages

        500 https://packages.cisofy.com/community/lynis/deb stable/main i386 Packages

        100 /var/lib/dpkg/status

     2.6.2-1 500

        500 http://archive.ubuntu.com/ubuntu focal/universe amd64 Packages

        500 http://archive.ubuntu.com/ubuntu focal/universe i386 Packages

g.     Você pode executar **sudo apt-get update** e **sudo apt-get upgrade** novamente para garantir que você tenha todas as atualizações mais recentes do CISOfy.

Fim do documento