CyberOps Associates v1.0

Ambiente de Laboratório de Máquinas Virtuais - Perguntas Frequentes

Última atualização 20 outubro aa

O que é Oracle VirtualBox? Onde é que o consigo? e quanto custa?

O Oracle VirtualBox é um software de virtualização multiplataforma gratuito, de código aberto, usado neste curso. Ele pode ser instalado em computadores Windows, Linux, Mac OS X e Solaris x86. O software básico VirtualBox é licenciado sob a GNU General Public License versão 2 e o pacote de extensão está disponível sob a licença de Uso Pessoal e Avaliação. Se você se qualificar sob os termos desta licença, o VirtualBox estará disponível gratuitamente. O VirtualBox pode ser baixado da Oracle: http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html

Voltar ao início

Não consigo fazer com que as máquinas virtuais funcionem corretamente no Oracle VirtualBox. O que devo fazer?

Se você tiver atualmente uma versão do Oracle VirtualBox anterior à versão 5.2.4, será necessário atualizar para a versão 5.2.4 ou superior para que as máquinas virtuais funcionem corretamente.

Back to Top

O que são as máquinas virtuais CyberOps Workstation e Security Onion?

A CyberOps Workstation é uma VM personalizada baseada no Arch Linux. Esta VM é usada na maioria dos laboratórios deste curso. A VM Security Onion é usada em laboratórios posteriores para revisar alertas pré-

preenchidos e mensagens de registro geradas durante as explorações. A VM Security Onion é usada para monitoramento de segurança de rede, detecção de intrusões e gerenciamento de logs.

Clique aqui para saber mais sobre o Security Onion.

Back to Top

O que é Mininet?

A Mininet é instalada na CyberOps Workstation VM para dar suporte aos laboratórios neste curso. Mininet é um *emulador de rede* que cria uma rede de hosts virtuais, switches, controladores e links.

Back to Top

Por que preciso de toda essa memória RAM?

Neste curso, duas máquinas virtuais são usadas: CyberOps Workstation e Security Onion. O requisito mínimo de memória RAM para executar máquinas virtuais CyberOps Workstation é de 1 GB. No entanto, para a máquina virtual Security Onion, recomenda-se 4 GB de RAM. A recomendação de memória RAM na VM Security Onion permite que os serviços, como o monitoramento de segurança de rede (NSM), funcionem corretamente. Ao trabalhar com computadores sem a memória RAM mínima, a VM pode parecer estar funcionando corretamente; no entanto, alguns dos serviços necessários deixarão de funcionar sem aviso prévio. Isso resultará na perda de dados capturados com alertas e mensagens de log e na incapacidade de executar os laboratórios que usam a VM Security Onion.

Back to Top

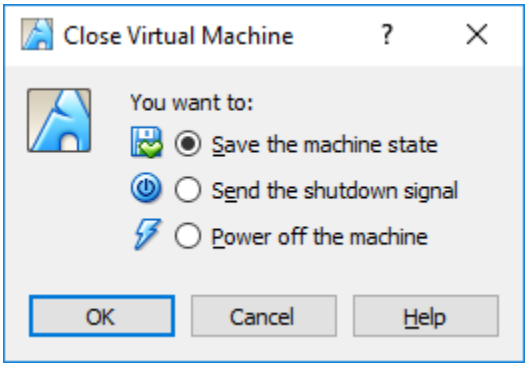
Por que meu mouse e teclado não estão funcionando fora da VM?

Se o teclado ou mouse não funcionar fora da VM, pressione a tecla CTRL que está no lado direito do teclado. Isso é chamado de chave de host VirtualBox. A chave do host é mostrada no canto inferior direito da janela da VM. Outros sistemas operacionais de host podem usar outra chave como a chave de host.

Voltar ao início

Os exames são muito longos, e não podemos terminar em um período de aula. O que devo fazer?

Familiarize-se com os laboratórios antes da aula, se possível. O estado da VM pode ser salvo para que você possa continuar os laboratórios posteriormente. Para salvar o estado da VM, clique no botão de opção **Salvar o estado da máquina** e clique em **OK** ao fechar a VM. Na próxima vez que você iniciar a máquina virtual, poderá retomar o trabalho no sistema operacional a partir do estado salvo.



Quando estiver pronto para retomar os laboratórios, selecione a VM desejada e clique em **Iniciar**. A VM iniciará no mesmo estado de quando foi salva.

Voltar ao início

Como faço para remover as máquinas virtuais quando terminar o curso?

1) Desligue a VM
2) Clique com o botão direito na VM > **Remover**, selecione **Excluir todos os arquivos**

Voltar ao início

Como substituo um arquivo que foi excluído acidentalmente?

1) Desligue a VM
2) Clique com o botão direito em VM> **Remover,** selecione **Excluir todos os arquivos**
3) Importar novamente a VM: **Arquivo** > **Importar Equipamento**

Voltar ao início

Eu fiz uma alteração em uma VM, e ela não está mais funcionando corretamente.

1) Desligue a VM
2) Clique com o botão direito em VM> **Remover,** selecione **Excluir todos os arquivos**
3) Reimporte a VM: **Arquivo**> **Importar appliance**

Voltar ao início

A tela da VM é preta, o que faço agora?

Quando a VM está ociosa há algum tempo, a tela pode estar preta. Clique em qualquer lugar da VM para exibir a tela de login.

Voltar ao início

Copiei o comando do PDF e colei no terminal. Por que não está funcionando?

Ao copiar e colar comandos de documentos de laboratório, existe a possibilidade de que a formatação e os caracteres do documento podem não ser compatíveis com a linha de comando. A solução é excluir e digitar novamente os caracteres ofensivos. O comando deve então ser executado.

Voltar ao início

O monitoramento de segurança de rede (NSM) não está funcionando no Security Onion? Como faço para reiniciá-lo?

Os serviços do NSM levam tempo para inicializar. Dependendo dos recursos do sistema host, eles podem levar um minuto ou mais. Se esse período tiver passado e os serviços NSM não estiverem em execução, abra um terminal e digite o comando **sudo so-restart**. Os serviços NSM começarão a reinicializar.

Voltar ao início

O comando é muito longo. O que posso fazer para facilitar?

O Linux foi projetado para a interface de linha de comando. Vários recursos estão incluídos para facilitar a entrada de comandos. Um desses recursos é o preenchimento automático da chave TAB. Ao digitar um comando ou um caminho de diretório, use a tecla TAB para concluí-lo. O Linux exibirá as conclusões possíveis se a parte digitada não for exclusiva. O Linux completará automaticamente o comando ou caminho assim que a parte digitada for exclusiva.

Alguns dos comandos longos e complexos são documentados em um arquivo de texto (**/home/analyst/lab.support.files/long_commands***)* armazenado na máquina virtual CyberOps Workstation.

Voltar ao início

Eu digitei errado um longo comando. Tenho que digitar novamente para consertá-lo?

Você pode usar a seta para cima para acessar os comandos que foram executados anteriormente na mesma janela de terminal. O comando pode então ser editado.

Voltar ao início