CyberOps Associates v1.0

Entorno de laboratorio de máquina virtual - Preguntas frecuentes.

Última actualización 21 diciembre 2020

¿Qué es Oracle VirtualBox? ¿Dónde lo consigo? ¿Y cuánto cuesta?

No puedo hacer que las máquinas virtuales funcionen correctamente en Oracle VirtualBox. ¿Que puedo hacer?

¿Qué son las máquinas virtuales CyberOps Workstation y Security Onion?

¿Qué es Mininet?

¿Por qué necesito toda esa memoria RAM?

¿Por qué mi mouse y teclado no funcionan fuera de la VM?

Las prácticas de laboratorio son demasiado extensas y no podemos terminarlas en una clase. ¿Qué debo hacer?

¿Cómo puedo eliminar las máquinas virtuales cuando finalice el curso?

¿Cómo reemplazo un archivo que se eliminó accidentalmente?

Hice un cambio en una máquina virtual y ya no funciona correctamente.

La pantalla de la VM está en negro, ¿qué hago ahora?

Copié el comando del PDF y lo pegué en el terminal ¿Por qué no funciona?

¿La supervisión de seguridad de red (NSM) no funciona en Security Onion? ¿Cómo lo reinicio?

El comando es realmente largo. ¿Qué puedo hacer para que sea más fácil?

He escrito mal un comando largo. ¿Tengo que volver a escribir para solucionarlo? ¿Qué es Oracle VirtualBox? ¿Dónde puedo conseguirlo? Además, ¿cuánto cuesta?

Oracle VirtualBox es un software gratuito multiplataforma de virtualización que se utiliza en este curso. Es de código abierto Se puede instalar en computadoras Windows, Linux, Mac OS X y Solaris x86. El software base del VirtualBox está licenciado bajo la versión 2 de la Licencia Pública General de GNU (GNU General Public License version 2) y el paquete de extensión está disponible bajo la Licencia de Uso y Evaluación Personal (Personal Use and Evaluation license). Si califica bajo los términos de esta licencia, VirtualBox está disponible sin costo alguno. VirtualBox puede ser descargado desde Oracle: http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html

Volver arriba

No logro que las máquinas virtuales funcionen correctamente en Oracle VirtualBox. ¿Qué puedo hacer?

Si actualmente tiene una versión de Oracle VirtualBox anterior a la versión 5.2.4, deberá actualizar a la versión 5.2.4 versión o superior para que las máquinas virtuales funcionen correctamente.

Back to Top

¿Qué son las máquinas virtuales CyberOps Workstation y Security Onion?

CyberOps Workstation es una Máquina virtual (VM) personalizada basada en Arch Linux. Esta VM se utiliza en la mayoría de las prácticas de laboratorio de este curso. La VM de la Cebolla de Seguridad (Security Onion VM) se utiliza en prácticas de laboratorio posteriores para revisar alertas autocompletadas y mensajes

de registro generados durante los ataques. La VM Security Onion se utiliza para monitoreo de seguridad de red, la detección de intrusiones y la gestión de registros.

Haga clic aquí para obtener más información sobre Security Onion.

Back to Top

¿Qué es Mininet?

Mininet está instalado en la VM CyberOps Workstation para servir de apoyo en las prácticas de laboratorio de este curso. Mininet es un *emulador de red* que crea una red de hosts virtuales, switches, controladores y enlaces.

Back to Top

¿Por qué necesito toda esa memoria RAM?

En este curso, se utilizan dos máquinas virtuales: CyberOps Workstation y Security Onion. El requisito mínimo de memoria RAM para ejecutar máquinas virtuales CyberOps Workstation es de 1 GB. Sin embargo, para la máquina virtual Security Onion, se recomienda 4 GB de RAM. Los requisitos de memoria RAM para Security Onion permiten que los servicios, tales como el monitoreo de seguridad de red (NSM) funcionen correctamente. Al trabajar con computadoras sin la memoria RAM requerida, es posible que parezca que las VM están funcionando correctamente; sin embargo, algunos de los servicios necesarios dejarán de funcionar sin previo aviso. Esto provoca la pérdida de datos capturados con las alertas y los mensajes de registro y la imposibilidad de realizar las prácticas de laboratorio en las que se utiliza Security Onion.

Back to Top

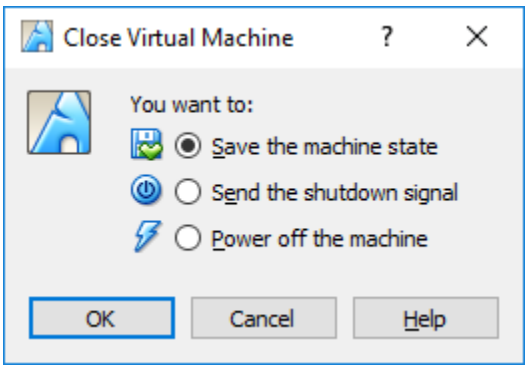
¿Por qué mi mouse y teclado no funcionan fuera de la VM?

Si su teclado o su mouse no funcionan fuera de la VM, presione la tecla CTRL que se encuentra en el lado derecho del teclado. Esta es llamada la tecla host de VirtualBox. La tecla host se muestra en la esquina inferior derecha de la ventana de la VM. Es posible que otros sistemas operativos de hosts utilicen otra tecla como tecla host.

Volver arriba

Las prácticas de laboratorio son demasiado extensas y no podemos terminarlas en una clase. ¿Qué debo hacer?

Si es posible, familiarícese con las prácticas de laboratorio antes de la clase. El estado de la VM puede guardarse, así puede continuar con las prácticas de laboratorio más tarde. Para guardar el estado de la VM, haga clic en la casilla **Guardar estado de la máquina** y haga clic en **Aceptar** cuando cierre la VM. La próxima vez que inicie la máquina virtual, podrá volver a trabajar en el sistema operativo a partir del estado que se guardó.



Cuando esté listo para reanudar las prácticas de laboratorio, seleccione la máquina virtual deseada y haga clic en **Iniciar**. La VM se iniciará en el mismo estado en el que se encontraba cuando se guardó.

Volver arriba

¿Cómo puedo eliminar las máquinas virtuales cuando finalice el curso?

1) Apague la VM
2) Haga clic derecho en la VM > **Eliminar** y seleccione **Eliminar todos los archivos**.

Volver arriba

¿Cómo puedo restaurar un archivo que fue borrado accidentalmente?

1) Apague la VM
2) Haga clic derecho en la VM > **Eliminar** y seleccione **Eliminar todos los archivos**.
3) Vuelva a importar la VM: **Archivos** > **Importar dispositivo**

Volver arriba

Hice un cambio en una VM y ya no funciona correctamente.

1) Apague la VM
2) Haga clic derecho en la VM > **Eliminar** y seleccione **Eliminar todos los archivos**.
3) Vuelva a importar la VM: **Archivos** > **Importar dispositivo**

Volver arriba

La pantalla de la máquina virtual está en negro, ¿qué debo hacer ahora?

Si la máquina virtual ha permanecido inactiva durante algún tiempo, es posible que la pantalla esté en negro. Haga clic en cualquier lugar dentro de la VM para mostrar la pantalla de inicio de sesión.

Volver arriba

Copié el comando desde el PDF y lo pegué en la ventana del terminal. ¿Por qué no funciona?

Al copiar y pegar comandos de documentos de prácticas de laboratorio, existe la posibilidad de que el formato y los caracteres del documento no sean compatibles con la línea de comandos. La solución es borrar y volver a escribir los caracteres que causan el problema. Luego, debería ejecutarse el comando.

Volver arriba

¿No está funcionando el monitoreo de seguridad de red (NSM) en Security Onion? ¿Cómo lo reinicio?

Los servicios NSM toman tiempo para iniciarse. Según los recursos del sistema del host, es posible que tomen un minuto o más. Si transcurrió ese periodo, y los servicios de NSM no se están ejecutando, abra la ventana del terminal e ingrese el comando **sudo so-restart.** Los servicios NSM comenzarán a reiniciarse.

Volver arriba

El comando es muy largo. ¿Qué puedo hacer para que sea más fácil ingresarlo?

Linux está diseñado para la interfaz de línea de comandos (CLI). Se incluyen varias funcionalidades para facilitar la entrada de comandos. Una de esas características es el autocompletado al presionar la tecla TAB. Al ingresar un comando o una ruta de directorio, utilice la tecla TAB para autocompletar. Linux mostrará las posibles terminaciones si la porción ingresada del comando o ruta no es única. Linux completará automáticamente el comando o la ruta si la porción ingresada es única.

Algunos comandos largos y complejos están documentados en un archivo de texto (***/home/analyst/lab.support.files/long_commands***) almacenado en la máquina virtual CyberOps Workstation.

Volver arriba

Ingresé de forma incorrecta un comando largo. ¿Tengo que volver a ingresarlo para corregirlo?

Puede utilizar la tecla flecha arriba para acceder a los comandos que se ejecutaron anteriormente en la misma ventana de terminal. Luego se puede editar el comando.

Volver arriba