INTRODUCCIÓN

Esta guía le guiará a través de la configuración de una máquina virtual "de evaluación" de Security Onion en Virtual Box.

REQUISITOS DEL SISTEMA

- CPU: mínimo 4x vCPUs
- RAM: mínimo 8GB
- Disco duro: mínimo 40GB

DESCARGAS

Descargue la ISO de Security Onion desde la siguiente ubicación:

https://github.com/Security-Onion-Solutions/security-onion/releases/tag/v16.04.5.5_20181212

CONFIGURACIÓN DE LA MÁQUINA VIRTUAL (VIRTUALBOX)

1. Crea una nueva VM utilizando el Modo Experto. Ponle el nombre que quieras. Configura el tipo a "Linux" y la versión a "Ubuntu (64-bit)".
2. Establece el tamaño de la memoria para la VM a un mínimo de 8GB, pero si es posible, dale a la VM tanta memoria como puedas.
3. Seleccione "Crear un nuevo disco duro virtual ahora" y haga clic en "Crear".
4. Aparecerá la pantalla de diálogo de creación del disco duro virtual. Especifique el tamaño del disco duro para la VM y haga clic en "Crear". El tamaño mínimo del disco debe ser de 40 GB.
5. Tipo de archivo (VDI) y Tipo de almacenamiento (Asignado dinámicamente) deben permanecer en sus valores por defecto.
6. La máquina virtual debería aparecer ahora en la lista de máquinas virtuales configuradas.
7. Haga clic con el botón derecho en la VM y seleccione "Configuración".
8. Haga clic en "Sistema" y luego en "Procesador". Establezca el número de vCPUs para la máquina virtual en un mínimo de cuatro, pero preferiblemente más.
9. Haga clic en "Almacenamiento" y haga clic en el icono de CD-ROM/DVD con "Vacío" al lado. El menú se actualizará y en "Atributos" aparecerá "Unidad óptica". Haga clic en el icono de CD-ROM/DVD de esa sección y seleccione "Elegir archivo de disco óptico virtual". Vaya a la ubicación donde guardó el archivo ISO y selecciónelo.
10. Haga clic en "Audio" y desactive las funciones de audio desmarcando "Activar audio".
11. Haz clic en "Red" y comprueba que el "Adaptador 1" está activado y conectado a NAT. Seleccione "Adaptador 2", actívelo y establezca la opción "Conectado a:" en "Adaptador sólo de host".
12. Si al seleccionar "Adaptador de sólo host" aparece el mensaje "Configuración no válida detectada", tendrás que crear primero un adaptador de sólo host:
13. En "Adaptador 2", desmarque "Habilitar adaptador de red" y haga clic en Aceptar.
14. Haga clic en Archivo -> Administrador de red host -> Crear -> Cerrar
15. Ahora debería poder volver al paso 10 y completar la configuración.
16. Haga clic en Aceptar.

CONFIGURACIÓN DE SECURITY ONION VM

1. Encienda la VM recién creada.
2. Cuando aparezca la pantalla del gestor de arranque de Security Onion, elija "Arrancar SecurityOnion 16.04.5.5" y pulse Intro.

3. Aparecerá el escritorio de Security Onion. En esta pantalla, haz doble clic en el icono "Instalar SecurityOnion 16.04".
4. Seleccione el idioma que desea utilizar y pulse "Continuar".
5. En la pantalla "Preparando la instalación de SecurityOnion", marque la opción "Descargar actualizaciones mientras se instala SecurityOnion" y pulse "Continuar".
6. En "Tipo de instalación", seleccione "Borrar disco e instalar SecurityOnion". Haga clic en "Instalar ahora".
7. Aparecerá una pantalla de confirmación titulada "¿Escribir los cambios en los discos?". Haga clic en "Continuar".
8. En la pantalla "¿Dónde estás?", selecciona "Nueva York" para la zona horaria del Este. Haga clic en "Continuar".
9. En la pantalla "Disposición del teclado", selecciona la disposición del teclado y el idioma que prefieras. Haz clic en "Continuar".
10. Rellene la pantalla "¿Quién es usted?" con sus datos y contraseña. Nota: no puedes utilizar el nombre de usuario "root". Toma nota de este nombre de usuario y contraseña, ya que los necesitarás de nuevo. Haga clic en "Continuar" cuando haya rellenado todos los campos obligatorios.
11. Aparecerá la ventana "Instalar" se instalará Security Onion. Espere a que se complete este proceso.
12. Cuando aparezca el mensaje "Instalación completada", haga clic en "Reiniciar ahora". La máquina virtual se apagará. Cuando se le solicite, pulse "Intro".
13. El sistema se reiniciará. Deje que el contador del gestor de arranque se complete y arranque automáticamente.
14. Inicie sesión con la cuenta que configuró en el paso 10.
15. Haga doble clic en el icono "Setup" del Escritorio. Se le pedirá la contraseña para tareas administrativas. Esta es la contraseña que utilizó para iniciar sesión en Security Onion.
16. En la pantalla "Configuración de Security Onion...", haga clic en "Sí, continuar".
17. Cuando se le pregunte si "¿Desea configurar /etc/network/interfaces ahora?", haga clic en la opción "Sí".
18. Seleccione la primera interfaz de la lista para que sea la "interfaz de gestión" y haga clic en "Aceptar".
19. Cuando se le pregunte si desea utilizar "DHCP o direcciones estáticas", seleccione "DHCP" y haga clic en "Aceptar".
20. Cuando se le pregunte si desea "configurar interfaces de sniffing (monitorización)", haga clic en la opción "Sí".
21. Seleccione la interfaz restante de la lista para que sea la interfaz de "sniffing" y haga clic en "Aceptar".
22. Haga clic en la opción "Sí, realizar cambios" cuando se le solicite.
23. Haz clic en la opción "Sí, reiniciar" cuando se te solicite.
24. El sistema se reiniciará. Deje que el sistema vuelva automáticamente a la pantalla de inicio de sesión.
25. Inicie sesión de nuevo.
26. Vuelva a hacer doble clic en el icono "Configuración" del Escritorio. Se le pedirá la contraseña para tareas administrativas. Esta es la contraseña que utilizó para acceder a Security Onion.
27. En la pantalla "Configuración de Security Onion...", vuelva a hacer clic en "Sí, continuar".
28. Cuando se le pregunte si "¿Desea omitir la configuración de red?", haga clic en la opción "Sí".
29. Cuando se le pregunte si desea utilizar "Modo de evaluación o Modo de producción", seleccione "Modo de evaluación" y haga clic en "Aceptar".
30. Cuando se le pregunte "¿Qué interfaz de red debería monitorizar?", asegúrese de que la segunda interfaz (que seleccionó en el paso 21) sigue seleccionada. Haz clic en "Aceptar".

31. En "Vamos a crear nuestra primera cuenta de usuario", introduce un nombre de usuario. Anótalo. Se utilizará para iniciar sesión en las aplicaciones de Security Onion y es independiente de la contraseña utilizada para iniciar sesión en el sistema operativo. Haga clic en "Aceptar".
32. A continuación se le pedirá una contraseña para la cuenta creada en el paso 31. Introduzca una contraseña y anótela. Introduzca una contraseña y anótela. Haga clic en "Aceptar". Confirme la contraseña y haga clic en "Aceptar".
33. Aparecerá un mensaje con una lista de todos los cambios que la configuración realizará en el sistema. Haga clic en la opción "Sí, proceder con los cambios".
34. Se iniciará el proceso de instalación. Deje que el proceso se ejecute hasta que finalice.
35. En la pantalla “Security Onion Setup is now complete!", haga clic en "OK". Lea cada una de las pantallas que aparecen a continuación. Recomiendo tomar nota de los comandos ya que es útil conocerlos.
36. sudo sostat - información detallada sobre el estado del servicio
37. sudo sostat-quick - visita guiada de la salida de sostat
38. sudo sostat-redacted - información redactada, segura para compartir públicamente
39. sudo so-allow - permite conexiones a puertos distintos de TCP 22
40. Una vez que haya hecho clic a través de todas las indicaciones, abra una ventana de terminal yendo a "Aplicaciones", "Herramientas del sistema" y luego "Terminal Xfce".
41. En el símbolo del sistema, introduzca el siguiente comando "sudo ufw allow 443" y, si se le pide una contraseña, introduzca la misma contraseña utilizada para iniciar sesión en Security Onion. También ejecute el comando "sudo ufw allow 7443"; de nuevo, si se le pide una contraseña, utilice la contraseña utilizada para iniciar sesión en Security Onion.
42. En este punto, puede apagar Security Onion haciendo clic en el icono de la esquina superior derecha de la pantalla de la VM, luego en el icono del botón de encendido y finalmente en "Power Off".

(Opcional) Puede hacer un Clon o Instantánea de la VM si desea tener una copia a la que volver después de probar el sistema.

DESCARGAS

Los siguientes archivos deben descargarse en su Security Onion:

https://github.com/wave-length/Presentations/raw/master/MAR19-DC919-SecurityOnion/Files/Ex1-honeynet.org-Scan19.tar.gz
https://s3.amazonaws.com/tcpreplay-pcap-files/bigFlows.pcap

EJERCICIO 1 - INTRODUCCIÓN A SQUIL

1. Una vez que haya iniciado sesión en su VM, abra una ventana de terminal haciendo clic en "Aplicaciones", luego en "Utilidades" y desplácese hacia abajo y haga clic en "Terminal". Cambia el directorio al lugar donde has almacenado los pcaps del Ejercicio descargados. Si has utilizado el navegador web Chromium, esos archivos están almacenados en el directorio "Descargas".
2. Extrae los archivos contenidos en Ex1-honeynet.org-Scan19.tar.gz utilizando el siguiente comando:

```
mkdir ./Ejercicio1/ && tar fvxz Ex1-honeynet.org-Scan19.tar.gz --directory ./Ejercicio1
```

3. Cambia de directorio al directorio "Ejercicio1".

4. Minimiza la ventana del terminal y haz doble clic en el icono "Squil" del escritorio. Inicia sesión en Squil utilizando las credenciales que configuraste cuando construiste la Security Onion VM; ten en cuenta que no son las mismas credenciales que utilizas para iniciar sesión en el sistema. Aparecerá una nueva ventana preguntando qué redes monitorizar. Debería haber dos opciones - seconion-ossec y seconion-enxxxx. Ignora la interfaz etiquetada como "ossec"; fíjate en lo que sigue al guión en la interfaz que empieza por "en". Debería ser algo parecido a enp#s#, donde los signos # son números. Este es el nombre de la interfaz Ethernet de captura utilizada para la monitorización y será necesaria más adelante. Haga clic en "Seleccionar todo" una vez que haya anotado el nombre de la interfaz Ethernet y luego en "Iniciar SGUIL". Debería aparecer la interfaz sguil. Asegúrese de que la pestaña "Eventos en Tiempo Real" está seleccionada y que la caja bajo la pestaña está libre de eventos. Si hay eventos en la lista, haga clic en uno y pulse F8 para borrarlo. Si hay más de uno, siga pulsando F8 hasta que se borren todos.
5. Vuelva a poner el terminal en primer plano. En la línea de comandos, introduzca el siguiente comando:

```
sudo sleep 15s && sudo tcpreplay -i <nombre de la interfaz Ethernet> -M 100 newdat3.log
```

6. Por ejemplo, si el nombre de su interfaz Ethernet de captura es "enp0s8", el comando sería el siguiente

```
sudo sleep 15s && sudo tcpreplay -i enp0s8 -M 100 newdat3.log
```

7. Cuando pulse enter, se le pedirá la contraseña sudo; utilice la contraseña utilizada para iniciar sesión en la VM. A continuación, vuelve a la pantalla sguil y espera.
8. En unos quince segundos, tiempo suficiente para volver a squil, tcpreplay reproducirá el archivo pcap newdat3.log y los eventos aparecerán en squil. Debería haber aproximadamente 15 eventos. Echemos un vistazo a algunos de ellos.
9. Haga click en el evento con el Mensaje de Evento "GPL TELNET Bad Login". Los campos de la parte inferior de la ventana deberían aparecer. Si no lo hacen, asegúrese de que las casillas junto a "DNS Inverso", "Habilitar DNS Externo", "Mostrar Datos de Paquetes" y "Mostrar Regla" estén todas marcadas.
10. Averigüemos el posible origen de este intento fallido de inicio de sesión... Al lado de "Whois Query" hay tres botones de radio; selecciona "Src IP" y espera a que se llene el campo que hay debajo. Desplácese hacia abajo en ese campo hasta que vea "country:". ¿Qué código de país de dos letras aparece? Puede utilizar Google para determinar de qué país se trata o, si se desplaza hacia abajo hasta los campos "address:", puede encontrarlo allí. ¿Qué país es el posible origen de este ataque?
11. Ahora que hemos determinado dónde se encuentra probablemente la IP del ataque, concluimos que se trata de un intento de acceso no autorizado, ya que no conocemos a nadie en ese país que pudiera acceder a este sistema. Squil le permite clasificar eventos basándose en los resultados de una investigación. Para clasificar este suceso, haga clic con el botón derecho del ratón en el "RT" situado a la izquierda de la fila correspondiente a este suceso. En el menú emergente, vaya a "Actualizar estado del suceso" y elija "CAT III - Intento de acceso no autorizado (F3)". También puede seleccionar el suceso y pulsar F3. El suceso no desaparecerá del campo "Sucesos en tiempo real".
12. La vista "Eventos en Tiempo Real" le permite ver los eventos a medida que son generados por el IDS. Como analista SOC que monitoriza un IDS, esta es la cola de eventos de la que usted escogería e investigaría los eventos. Ahora, digamos que quiere ver todos los eventos que han sido clasificados como "Intento de Acceso No Autorizado". Para ello, seleccione "Consulta" en la barra de menú squil, elija "Consulta por categoría" y, a continuación, la consulta "CAT III: Intento de acceso no autorizado". Se abrirá una pantalla de creación de consultas. Con la función de

creación de consultas, puede consultar los eventos catalogados por Security Onion. Para este ejercicio, haga clic en el botón "Enviar". Aparecerá una nueva pestaña con los resultados de la consulta y debería aparecer el evento que clasificó en el paso 9. Cuando esté listo para continuar, cierre esta pestaña con el botón "Cerrar" situado en la esquina superior izquierda.

13. Squil también le permite realizar análisis de paquetes en la misma interfaz. Seleccione el evento denominado "ET ATTACK_RESPONSE Possible /etc/passwd via SMTP (linux style)". Los campos de la parte inferior deberían rellenarse; si no lo hacen, asegúrate de que las casillas de verificación a las que se hace referencia en el Paso 7 están marcadas. Utilizando los campos codificados en color azul en la parte inferior derecha de la pantalla, podemos ver la información de la cabecera y la carga útil del paquete, incluyendo la IP y el puerto de origen y destino. El campo "DATA" es donde queremos buscar información sobre este ataque. Según la descripción del evento
14. ¿Cuál es la dirección de correo electrónico del destinatario (TO:)?

EJERCICIO 2 - INTRODUCCIÓN A SQUERT

1. Minimice la interfaz squil y abra la interfaz squert utilizando el icono del escritorio. El login es el mismo nombre de usuario y contraseña que en squil. Una vez conectado, borra todas las alertas de la interfaz squert. Para ello, haga clic en el cuadrado rojo situado junto a un evento y, a continuación, haga clic en la opción "No Action Req'd" (No es necesaria ninguna acción) situada en la parte izquierda de la ventana, debajo de "Classification" (Clasificación). La sección de clasificación de la interfaz es similar a la sección Clasificar de squert. Probaremos esta funcionalidad en breve.
2. Vuelve a tu terminal una vez que todos los eventos se hayan borrado en squert. Cambia el directorio a '/opt/examples' escribiendo 'cd /opt/examples'. Ejecuta tcpreplay, como se muestra en el Ejercicio 1, e importa bredolab-sample.pcap.
3. sudo tcpreplay -i <nombre de la interfaz Ethernet> -M 100 bredolab.pcap
4. Probablemente se le pedirá su contraseña sudo, como en el Ejercicio 1; de nuevo, esta es la misma contraseña que utilizó para iniciar sesión en la VM.
5. Una vez que tcpreplay finalice, en squert, haz clic en el botón de actualización de la interfaz en la parte superior de la pantalla. Serán dos flechas formando un círculo y puede estar marcado con un signo de exclamación rojo. Después de hacer clic en este icono, deberían aparecer al menos seis alertas en la interfaz de squert; si no es así, espera y vuelve a hacer clic en el botón de actualización.
6. Haga clic en la alerta marcada como "ET Trojan Tibs/Harnig Downloaded Activity". Observe la información que aparece: la firma IDPS, incluidos algunos enlaces a información e información específica del evento, como la hora, el host de origen y el host de destino.
7. En "Categorizar 4 evento(s)", haga clic en el cuadrado rojo con el número cuatro dentro. El número indica el número de veces que algo, en este caso paquetes, activó esta alerta. Aparecerán filas adicionales para cada uno de los paquetes capturados y sus horas de captura. Haga clic en el ID de evento de cualquiera de los paquetes. ¡Esto iniciará un pivote desde squert a la interfaz de capME! Aquí podrá examinar el contenido del paquete capturado y, si lo desea, descargar un PCAP del sistema de análisis offline.
8. Utilizando la información presentada en la interfaz capME!, ¿cuál fue el dominio desde el que se descargó este troyano? Pista: Fíjate en las líneas marcadas como "SRC".
9. Usando la información presentada en la interfaz de capME!, parece que el servidor web envió algo de vuelta - ¿qué? Pista: Mira las líneas marcadas "DST".
10. Parece que esto podría ser malicioso. Tenemos la capacidad de clasificar eventos en squert, igual que squil. Cierra la pestaña capME! y vuelve a la interfaz squert. El evento para "ET Trojan Tibs/Harnig Downloaded Activity" debería seguir seleccionado. Asegúrate de que "Categorizar 4

Evento(s)" sigue apareciendo en el evento y luego haz clic en el enlace de la izquierda etiquetado como "malicioso" en "Clasificación". Si en lugar de "Categorizar 4 evento(s)" aparece "Categorizar 0 evento(s)" u otro número, haz clic en la casilla situada bajo el cuadrado rojo con cuatro dentro hasta que aparezca "Categorizar 4 evento(s)" y haz clic en el enlace de la categoría "malicioso".

11. El evento que estábamos viendo ahora desaparecerá de la cola. Para volver a verlo, haz clic en el número cuatro junto a malicioso en la sección "Clasificación". Para volver a ver la cola después de intentar esto, haga clic en "SÍ" junto a "Filtrado por objeto" en la parte superior derecha de la interfaz. Al hacerlo, se mostrarán todos los eventos del sistema, incluidos los categorizados. Haga clic en "OFF" junto a "sólo cola" y luego en el botón "actualizar" para restaurar la cola.

EJERCICIO 3 - INTRODUCCIÓN A KIBANA

1. Este ejercicio requerirá muchos datos, así que usaremos el bigFlows.pcap proporcionado por el autor de tcpreplay. Carga este pcap de la misma forma que hemos cargado los pcaps en los Ejercicios 1 y 2:

```
sudo tcpreplay -i <nombre de la interfaz Ethernet> -M 100 bigFlows.pcap
```

2. Este pcap tardará uno o dos minutos en cargarse en Security Onion y ser analizado. Mientras esto sucede, puedes minimizar la ventana de terminal y abrir Kibana usando el enlace en tu escritorio de Security Onion. Si se le pide que inicie sesión, son las mismas credenciales utilizadas para squil y squert.
3. Comprueba que el pcap ha completado la carga comprobando en la ventana de terminal las estadísticas que indican que el número de paquetes "Intentados" y "Exitosos" son 791.615. Si los números reales son diferentes, eso significa que Kibana no está cargando. Si los números reales son diferentes, eso está bien.
4. Vuelva a la interfaz de Kibana y haga clic en el elemento "Dashboard" en el menú de la izquierda. Aparecerá la pantalla Dashboard en el panel de contenido que te proporcionará información sobre los tipos de tráfico y eventos procesados por Security Onion. Haga clic en la opción "HTTP" del menú "Bro Hunting" en el panel de contenido gris. Una vez que el panel se actualice, desplácese por el contenido que se presenta. Podrá ver información como los países con los que se comunican los hosts, los tipos de contenido que se cargan, los dominios con los que se contacta y las cadenas de agente de usuario. Esta información es generada por el motor Bro(Zeek) que se ejecuta en el sistema Security Onion.
5. Probemos otra vista de datos. Vuelva a la parte superior del panel de contenido y haga clic en "NIDS" en "Datos de alerta". Cuando el panel se actualice, eche un vistazo. Podrá ver información como el tipo de alerta, las IP de origen y destino, los puertos de origen y destino, los países contactados y los datos de frecuencia.
6. Haz clic en "Avisos de Bro" en "Datos de alerta". Debería haber algunas alertas de certificados SSL caducados. Esto ilustra el poder de Bro. Tiene la capacidad no sólo de inspeccionar los certificados SSL, sino también otras cabeceras e información del cliente, como las cadenas de agente de usuario, para obtener información sobre el entorno.
7. Ahora echemos un vistazo a las capacidades de visualización de datos de Kibana. Haga clic en el elemento "Visualizar" en el menú de la izquierda. En la lista de visualizaciones, seleccione "Bro - Conexiones - Servicio por país de destino". El panel de contenido se actualizará con un gráfico visual de los países contactados y gráficos que muestran con qué frecuencia se contactó con los puertos de destino.
8. Vuelva a hacer clic en la opción "Visualizar" del menú de la izquierda. En el campo de búsqueda del panel de contenido, escriba "Mapa" y, en los resultados, seleccione "Conexiones - Destino - Suma de Bytes Totales (Mapa de Mosaicos)". El panel de contenido se actualizará y mostrará un mapa con círculos en varias ubicaciones. Los círculos se colocan en las ubicaciones estimadas

para los hosts que fueron el destino de los paquetes transmitidos en la red. El tamaño y el color de los círculos se determinan en función de la cantidad de datos enviados a esos hosts.

9. Kibana, su lenguaje de consulta y capacidades abarcan un cuerpo tan grande de información que hay libros enteros y clases sobre ello. Siéntase libre de hurgar y probar las diferentes visualizaciones o algunas consultas. Kibana es de sólo lectura por lo que no hay riesgo de corrupción o eliminación de datos experimentando con él.