Módulo 3.3

Redes y Seguridad
Gr. Ing. Informática
J.L. Vázquez Poletti

Objetivo

En este módulo aprenderemos a instalar y configurar dos *rootkits* sencillos, así como a usarlos para obtener información de la máquina objetivo. Por otro lado, emplearemos dos detectores de *rootkits* para localizarlos.

Además, será nuestra primera toma de contacto con la distribución **Backtrack**, instalada en la máquina desde la que nos conectaremos a la víctima, aunque si bien de momento usaremos muy poco su potencial.

ATENCIÓN: Este módulo está pensado para ser realizado en 2 sesiones.

Punto de partida

Volvemos a visitar ENCOM pero ahora como atacantes de incógnito. Nuestra intención es espiar la organización desde dentro, capturar valiosa información y tener desplegada una "cabeza de playa" que nos permita futuros ataques.

Nuestra máquina objetivo es una de las terminales del Centro de Proceso de Datos de ENCOM (**RyS-ENCOM**). Hemos podido acceder físicamente a la misma y hemos descubierto dos puntos débiles: una versión obsoleta del sistema operativo (Ubuntu 10.10) y la contraseña del usuario que puede ejecutar comandos como root.

Como atacante prevenido vale por dos, vamos a garantizar nuestro acceso instalando dos rootkits. De esta manera, si uno es descubierto, seguiremos teniendo acceso a través del otro, ya que aprovecha un componente distinto del sistema.

Escenario

Las máquinas tienen las siguientes direcciones IP en sus respectivos interfaces **eth** (0 ó 1 dependiendo de la máquina):

- **RyS-Backtrack:** 192.168.1.2.
- **RyS-ENCOM:** 192.168.1.3.

Para asignar la IP hay que ejecutar como usuario **root** el comando **ifconfig *<Interfaz>* *<IP>* up**.

KBeast: despliegue del rootkit

El primer rootkit escogido es **KBeast**, actúa a nivel de Kernel y tiene las siguientes características:

- Ocultación y protección anti-borrado de su módulo del Kernel.
- Ocultación y protección anti-borrado de sus ficheros y directorio.
- Ocultación y blindaje de su proceso (comandos **ps**, **pstree**, **top** y **lsof**).
- Ocultación de las conexiones (comandos **netstat**, **lsof**).
- Ocultación de su puerta de atrás a través del módulo de Kernel.

Máquinas Virtuales

- RyS-ENCOM (ubuntu:reverse)
- RyS-Backtrack (root:toor)

Más información

KBeast: http://core.ipsecs.com/rootkit/kernel-rootkit/

Jynx: http://www.blackhatlibrary.net/Jynx_Rootkit

Backtrack: http://www.backtrack-linux.org/

Netcat: http://netcat.sourceforge.net/

Rootkit Hunter: http://www.rootkit.nl/projects/rootkit_hunter.html

- Escalada de privilegios a través de su puerta trasera.
- Captura de pulsaciones de teclado.

1. El rootkit sólo puede instalarse como **root**.
2. El rootkit ha sido ya descargado en el directorio **/home/ubuntu/Flynn**. Hay que descomprimirlo y entrar en el nuevo directorio que se ha generado (**CONSEJO:** usar el comando **tar**).
3. Editar el fichero de configuración (**config.h**) y hacer los siguientes cambios:
    a. **Nombre del demonio:** tr0n
    b. **Valores con la cadena 'h4x':** tr0n
    c. **Directorio:** /usr/_tr0n_
    d. **Puerto de escucha:** 32123
    e. **Contraseña:** EndOfLine
4. Compilar e instalar el toolkit con el comando **./setup build**.
5. Comprobar que el despliegue ha sido exitoso:
    a. Aunque el demonio ya está corriendo con el PID que se indica, éste no aparece al listar los procesos.
    b. El directorio **/usr/_tr0n_** no aparece listado (ni siquiera como oculto) pero se puede entrar en él.

KBeast: consolidando la puerta trasera

Para garantizar que la puerta trasera siga abierta a pesar del reinicio de la máquina, hay que buscar un demonio del sistema que esté arrancado en el nivel de servicio que nos interesa (**3**).

1. Usar el comando **chkconfig** y el parámetro necesario.

PISTA: encadenar este comando con un **grep** nos puede ayudar bastante a filtrar información.

2. Escoger el demonio **sysstat**. Por tanto, editar su script (**/etc/init.d/sysstat**) de tal forma que a continuación de la sección de arranque añadamos las líneas enmarcadas (**es muy importante respetar el espaciado**):

```
case "$1" in

 start|restart|reload|force-reload)

     if [ "$ENABLED" = "true" ] ; then

          log_daemon_msg "Starting $DESC" "$NAME"

          start-stop-daemon --start --quiet --exec $DAEMON -- --
boot $SA1_OPTIONS || status=$?

          log_end_msg $status
```

fi

```
su - bin -c /usr/_tr0n_/_h4x_bd > /dev/null 2>&1

insmod /usr/_tr0n_/ipsecs-kbeast-v1.ko > /dev/null 2>&1
```

3. Reiniciar el sistema (**desde la propia máquina virtual**) para comprobar que la puerta trasera se abre de forma automática.
4. Comprobar la dirección IP de la máquina a través del comando **ifconfig** (interfaz **eth1**).

¿Qué usuario está lanzando el demonio cada vez que se arranca la máquina?

KBeast: Conexión y captura de información

Es el momento de pasar a la máquina desde la que conectarse. Una vez introducido el usuario y contraseña, se puede arrancar el entorno gráfico con el comando **startx** y de ahí, abril un terminal (segundo icono de abajo a la izquierda).

Para realizar la conexión, se empleará **Netcat**, una pequeña herramienta pero de gran potencia y con muchas funcionalidades. **Netcat** se invoca con el comando **nc**.

1. Conectarse a la víctima pasándole a **nc** la IP y el número puerto en el que se fijó la puerta de atrás.
2. Comprobar el usuario y grupo al que se pertenece.
3. A través del comando **w**, verificar los usuarios conectados a la máquina.
4. Ver el contenido de los archivos **acctlog.***.

¿A qué se corresponde el número que sirve como extensión de los archivos **acttlog**?

NOTA: para salir de la puerta trasera hay que pulsar **CTRL+C**.

Jynx: despliegue del rootkit

El segundo rootkit escogido es **Jynx** en su segunda versión, actúa por encima del Kernel y a las características de KBeast le suma:

- Autenticación multi-factor (definir puerto de origen en el cliente).
- Uso de SSL.

Aunque **Jynx** carece de una herramienta de captura de comandos de los usuarios.

1. El rootkit se encuentra también en el directorio **/home/ubuntu/Flynn** y nuevamente hay que ser **root** para configurarlo y desplegarlo.
2. Editar **config.h** con los siguientes cambios:
    a. **Valores con la cadena 'XxJynx':** Yori
    b. **Localización archivo reality.so:** /Yori/reality.so
    c. **Contraseña:** MCP
3. Ejecutar **make** y posteriormente **make install INSTALL=/Yori**.

4. Entrar en **/Yori** e intentar listar sus contenidos.

La diferencia principal de **Jynx** es que éste se engancha a un servicio del sistema que ya está corriendo (el servidor web).

5. Para hacer efectiva la puerta trasera, se deberá reiniciar el servidor con el siguiente comando: **/etc/init.d/apache2 restart**
6. Reiniciar el sistema (**desde la propia máquina virtual**) para comprobar que la puerta trasera se abre de forma automática.

¿Qué ventajas y desventajas tiene este *rootkit* respecto al anterior en su instalación?

Jynx: Conexión y captura de información

Se pasará nuevamente a la máquina desde la que conectarse.

1. Conectarse a la IP de la víctima a través del navegador web.
2. Conectarse a la víctima a través del comando **ncat** indicando que el puerto **80** (web). Introducir la contraseña indicada en la configuración del *rootkit*.
3. Añadir como dato de conexión el puerto local **42** (puerto desde donde se iniciará la conexión). Volver a introducir la contraseña (para salir, pulsar **CTR+C**).
4. Indicar como otro dato de conexión que se desea usar SSL. Volver a introducir la contraseña.
5. Navegar por los directorios.

¿Qué UID tiene nuestro usuario? ¿A quién pertenece?

El acceso será completo cuando se escalen privilegios. Esto se hace con el siguiente comando:

Yori=1 gpasswd /

Esto activa la escalada de privilegios empleando la variable de entorno definida en la configuración.

¿Qué usuario se es ahora?

Detección de los *rootkits*

Ahora se tomará el rol contrario, el del defensor.

En el sistema hay 2 detectores de *rootkits* instalados: **chrootkit** y **rkunter**. Por razones obvias, las siguientes operaciones se deben realizar como usuario **root**.

1. Ejecutar **chkrootkit**.

¿Se detecta algún indicio de *rootkit*?

2. Listar los tipos de pruebas que **rkhunter** puede realizar.

3. Listar los *rootkits* que **rkhunter** puede detectar.

¿Sirve la versión instalada de **rkhunter**?

Una versión más reciente de **rkhunter** se encuentra comprimida en el directorio **/home/ubuntu/CLU**.

1. Descomprimir el archivo
2. Dentro del nuevo directorio, ejecutar ./**installer.sh --install**.
3. El programa se invoca con el comando **rkhunter**.
4. Ejecutar **rkhunter** indicando que se quieren encontrar *rootkits*.

¿Qué *rootkits* se detectan?

Se realizará una nueva prueba para la cual será necesario **apagar la máquina virtual completamente (desde fuera de la misma) y volverla a arrancar**, a fin de recuperar el mismo estado del comienzo del módulo (sin *rootkits* instalados).

1. Volver a instalar **rkhunter**.
2. Volver a desplegar **KBeast** y **Jynx** pero **con las opciones por defecto**.
3. Volver a pasar **rkhunter**.

¿Qué *rootkits* se detectan? ¿Por qué?