Pentesting-I: Recogida de información

Curso 2017-2018

1. Introducción: Recogida de información

La recogida de información es la primera fase en un proceso de Pentesting. En esta práctica vamos a probar algunas de las herramientas que ofrece la distribución Kali para tal propósito.

2. Preparando el entorno de trabajo

Para hacer las primeras pruebas necesitamos instalar una máquina virtual en la que tendremos alojada un sitio web para hacer pruebas. La máquina virtual es la denominada Metasploitable y como su nombre indica es una máquina diseñada para hacerle *perrerías*. Y la web se denomina Mutillidae, una web vulnerable que consta de distintos niveles de seguridad que podremos ir modificando y diversas funcionalidades que podremos ir atacando.

2.1. Instalando y Configurando Metasploitable

Sigue los sigueintes pasos:

1. Descarga la imagen de la máquina virtual del mismo Sourceforge. Se trata de un zip con la versión 2.0.0 de casi 900 Megas.
2. Crea en Virtualbox una máquina linux con los siguientes parámetros.
   - Tipo Linux / Otros Linux-64-bits
   - Memoria 512
   - Sistrema / Procesador / Enable PAE
   - Red / Modo Puente / Promiscuo / Permitir todo
3. Inicia la máquina autentícate tal y como te indica el banner (msfadmin/msfadmin). Para poner el teclado en español ejecuta el comando *sudo loadkeys es*
4. Configura el Mutillidae tal y como se explica *AQUÍ*

3. Secuestro de sesión: Autenticación mediante manipulación de Cookies.

Sigue los siguientes pasos.

1. Para manipular las Cookies tenemos que instalar un Add-on, para ello abrimos el navegador Firefox ESR y añadimos el Add-on *Cookie Manager +* en Menú/Add-ons/Extensions buscamos el Add-on y lo instalamos. Una vez instalado hay que reiniciar Firefox. Si queremos que aparezca el Add-on en la barra de herramientas podemos añadirlo con Menú/Customize y lo arrastramos a la barra de herramientas.

2. Entramos en Mutillidae, a través de la dirección ip de la máquina Metasploitable 2. Para que la autenticación mediante manipulación de Cookies funcione correctamente debemos asegurarnos que el nivel de seguridad es 0.

3. El objetivo principal de la práctica es conseguir recuperar un usuario con permisos de administración. Sabemos que cada usuario tiene un identificador (UID) pero no sabemos que UID corresponde al administrador. Vamos a crear los usuarios *pepe* y *paca* (con una password que no olvides, ya sabes) para ver como numera el sistema los identificadores.

4. Iniciamos sesión con el primero de los usuarios que hemos creado y utilizamos el Cookie Manager+ para ver que UID nos ha otorgado el sistema. Hacemos lo mismo con el segundo usuario que hemos creado. Ahora que sabemos como numera los identificadores el sistema podemos probar cambiando el UID en la propia cookie y actualizando la página para ver si nos podemos "convertir" en un usuario administrador. Podemos probar con UID's bajos, como 0 o 1.

5. Una vez que hemos descubierto el UID de administrador podemos probar a cambiar el nivel de seguridad de la web (Menú/Toggle Security) e intentarlo de nuevo. Para ello es conveniente resetear la BBDD de usuarios a través del botón del menú de la propia página.

4. Secuestro de sesión: Ataque con fuerza bruta usando la suite Burp

De nuevo sigue los pasos que se indican.

1. Configura te Firefox (Preferences/Advanced/Network/Settings) para que utilice un proxy en la dirección 127.0.0.1 y el puerto 8080.

2. Abrimos la suite Burp: Aplicaciones/Aplicaciones Web/burpsuite. No realizamos el update que nos sugiere. Elegimos Temporary Project – Use Burp defaults.

3. Lo primero que tenemos que hacer es configurar el Proxy. La idea es que Burp haga las funciones de Proxy, y por tanto con la posibilidad de interceptar el tráfico entre nuestro navegador que estará corriendo en nuestro Kali y el servidor de la página web que estará corriendo en la máquina Metasploitable:

   (a) Nos vamos a la pestaña de Proxy y en la pestaña de Options confirmamos que estamos escuchando sobre 127.0.0.1 (localhost) en el puerto 8080.

   (b) Para evitar interceptar todo el tráfico asociado al navegador, vamos restringir la escucha a la dirección objetivo: en la sección Intercept Client Request añadimos la regla „Is in the target scope„ como ya está creada basta con habilitarla con el checkbox correspondiente.

(c) Seguidamente nos vamos a Target/Scope y añadimos la dirección IP de Metasploitable2 seguido de la página mutillidae, es decir: "192.168.61.XXX".

(d) Desactivamos la intercepción para que no nos moleste: Proxy/Intercept/Intercept is on-off.

4. El objetivo es secuestrar una sesión de usuario, pero el problema es que no sabemos qué usuarios tiene el sistema. Sin embargo, Mutillidae tiene una sección de blogs personales accesibles al público. En el menú de la izquierda navegamos a:
OWASP TOP 10 → A2- Cross Site Scripting(XSS) → "Via Input" (GET
POST) → View someone's blog. En el combobox podemos ver la lista de usuarios. Apuntamos 4 o 5 que queramos.

5. A continuación vamos a intentar sacar la contraseña de los usuarios seleccionados mediante fuerza bruta:

   (a) Vamos a la ventana de login de la página y activamos la intercepción en Burp (Proxy/Intercept/Intercept is off).

   (b) En la página de login podemos intentar logearnos con un nombre de usuario que queramos y probar con cualquier contraseña.

   (c) Volvemos a Burp y en Proxy/Intercept vemos que se ha interceptado el POST que el cliente hace al servidor. Podemos ver varios parámetros (en azul) y su valor (en rojo) entre los que se encuentra "username" y "password". Hacemos clic derecho en la interceción y clicamos en "Send to Intruder". Desactivamos la intercepción para que no nos moleste.

   (d) En Intruder verificamos que el Target es el correcto.

   (e) En Intruder/Positions vamos a definir el tipo de ataque y que parámetros son los que queremos atacar con fuerza bruta. El tipo de ataque será "Cluster bomb". En el panel de texto observamos el mensaje POST. En él los parámetros se encuentran entre dos símbolos §. Puesto que lo que nos interesa es modificar únicamente el username y la password, eliminamos el resto de símbolos § de los otros parámetros: login, showhints, PHPSESSID y login-php-submit-button.

   (f) En Intruder/Payloads deberán aparecer dos conjuntos de payloads: uno para el parámetro "username" (1) y otro para el parámetro "password" (2).

      I. En el primer payload set vamos a añadir los usuarios que hemos elegido anteriormente: Payload Options/Adds.

      II. En el segundo payload set vamos a añadir contraseñas que pensemos que se puedan utilizar frecuentemente como por ejemplo: password, password1, 123456, letmein,... En este punto también se pueden añadir diccionarios de contraseñas.

   (g) En Intruder/Options podemos ver las opciones de configuración de las cabeceras que usa Intruder durante los ataques. Las dejamos tal cual están por defecto y le damos a "Start Attack".

6. A continuación, veremos como se realizan diversas peticiones al servidor probando todas las configuraciones posibles de usuario/contraseña. Una vez terminado el ataque, en la ventana de abajo podemos ver en cada uno de los ataques la petición y la respuesta (incluso renderizada) del servidor y si hemos podido entrar con ese usuario y esa contraseña.

7. Prueba a hacer el ataque usando un diccionario (recuerda que en el segundo payload puedes especificar un fichero). Puedes utilizar el diccionario que usa John de Ripper: /usr/share/john/password.lst.

5. Banner Grabbing: husmeando con Netcat

Netcat, la navaja suiza de los hackers, es una utilidad que permite entre otras muchas cosas recoger información de la red. A continuación tienes algunos comandos que puedes ejecutar en tu Kali y observar los resultados. Netcat también se puede utilizar para poner dos máquinas en comunicación y a partir de ahí se abre un sin fin de posibilidades para los hackers. En este enlace puedes echar un vistazo para hacerte una idea de qué cosas se pueden hacer comunicando máquinas y consultado el estado de puertos. *Netcat* En este otro puedes ver cómo poner a la escucha una shell remota.

Otro poco de Netcat

Desde el punto de vista del husmeador ejecuta estas órdenes.

```
$ echo '' | nc -v -n -w1  69.89.31.180 21-30
$ echo '' | nc -v -n -w1  69.89.31.180 80
$ echo `' | ncat --ssl 156.35.160.2 443
```

Ahora ejecuta la orden `$ nc -l -p 1234`, con ella creamos un sevidor en el puerto 1234 de nuestro localhost. Ahora abre un navegador (cliente) y escribe en la URL 'localhost:1234/loquesea' y mira lo que recibe el servidor.

6. Banner Grabbing: husmeando con Nmap

Nmap es otra de las grandes del Pentesting. Se trata de una herramienta potentísima que nos daría para un curso entero de prácticas. En nuestro caso solo vamos a realizar un par de pruebas. Para ello utilizaremos Zenmap, la versión gráfica del Nmap que viene con Kali.

Arranca la aplicación y escanea, con Quick scan alguna que te interese. Seguidamente incluye algún parámetro para intentar identificar, por ejemplo el sistema operativo de la máquina. En este enlace *Nmap-briefoptions* tienes resumidas algunas de las opciones que puedes utilizar.