metasploit

Metasploit

Metasploit http://www.metasploit.com/ es un software para hacer pruebas de penetración. Dispone de un conjunto de herramientas que permite realizar todas las fases de un test de intrusión.

Una vez instalado, o si hemos usando una distribución de seguridad como Kali Linux, lo primero que tenemos que hacer es arrancar los servicios necesarios para el correcto funcionamiento del Metasploit Framework.

En especial debemos arrancar las bases de de datos (msdb y postgresql)

```
systemctml start postgresql
msfdb init
```

iniciamos el metasploit

```
msfconsole
```

con el comando **db_status** para comprobar que se ha conectado correctamente a las bases de datos

Conceptos

Exploit

Un exploit es una vulnerabilidad. Para ver los exploits

```
show exploits
```

Payload

Los payloads son cargas útiles de código las cuales ejecutan en la vulnerabilidad algun tipo de acción, ya sea la obtención de una Shell y tomar el control del sistema afectado o provocar un desbordamiento o saturación del sistem Para ver los payloads

```
show payloads
```

Si las base de datos conectadas no veríamos ningun exploit o payload

Diferentes tipos de payloads:

- Meterpreter es un payload avanzado y multifacético que opera mediante inyección dll. Reside completamente en la memoria del host remoto y no deja rastros en el disco duro, por lo que es

muy difícil de detectar
- PassiveX, es un payload que puede ayudar a eludir los firewalls de salida restrictivos. Lo hace mediante el uso de un control ActiveX para crear una instancia oculta de Internet Explorer. Usando el nuevo control ActiveX, se comunica con el atacante a través de

solicitudes y respuestas HTTP.

- IPV6 Diseñados para funcionar en redes que usen el protocolo IPv6.

Encoder

Los **encoder** cifran nuestros payloads o exploits Para ver los encoders

```
search encoder
```

Para ver el número total de cada uno

```
banner
```

Cargar módulos manualmente en Metasploit

A veces necesitamos cargar un módulo manualmente que no se ha descargado automáticamente. Por ejemplo, vamos a si algún equipo de nuestra red es vulnerable al ransomware wannacry y para ello vamos a descargar el módulo correspondiente.

Para ello primeros buscamos si existe dicho módulo, en este caso particular se encuentra en https://www.rapid7.com/db/modules/auxiliary/scanner/smb/smb_ms17_010.

En la página podemos ver el nombre del módulo y donde debe de ir ubicado→**auxiliary/scanner/smb/smb_ms17_010 .**

Bajamos hasta el enlace al **Source Code** que nos llevará a la página https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb

Pulsamos en el botón para verlo el código en formato **raw** y copiamos la url de la página resultante.

Ahora vamos a nuestra consola de la máquina donde tenemos instalado metasploit y nos situamos en el directorio **cd /usr/share/metasploit-framework/modules/auxiliary/scanner/smb**

una vez en dicho directorio ejecutamos wget y pegamos la url anterior

```
wget
https://raw.githubusercontent.com/rapid7/metasploit-framework/master/modules
/auxiliary/scanner/smb/smb_ms17_010.rb
```

Ahora ejecutamos msfconsole y cargamos nuestro módulo

```
use auxiliary/scanner/smb/smb_ms17_010
```

```
set RHOSTS 192.168.1.1
run
```

y nos indicará si el host indicado es vulnerable

Referencias

- http://calebbucker.blogspot.com.es/2013/02/auditando-servidores-web-joomla-con.html
- http://www.hackplayers.com/2013/07/introduccion-karmetasploit.html
- http://www.hackplayers.com/2017/05/como-detectar-pcs-vulnerables-a-wannacry.html