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.

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