Práctica Nikto

23 de febrero de 2017

José David Manzanarez Velázquez A01337545
david.manzanarez.v@gmail.com

Objetivo

Aprender a utilizar una herramienta de escaneo de vulnerabilidades de un servidor remoto.

Metodología

1. Una vez que hayas ingresado a Kali, inicia una nueva terminal.
2. En la primera línea escribe *nikto* para verificar que tu versión de Kali tenga la aplicación instalada.
3. Después, escribe ***nikto -list-plugins*** y verifica que las siguientes líneas sean desplegadas:

   Plugin: ssl

   SSL and cert checks - Perform checks on SSL/Certificates

   a. Si no es así, escribe ***nikto -update***
4. Si las líneas anteriores fueron desplegadas, para iniciar el escaneo del servidor remoto escribe: ***nikto -h www.google.com*** (en caso de ser requerido para no atraer atención innecesaria al Tec utilizar ***nikto -h www.google.com -useproxy 201.16.147.193***. Si esto arroja un error, revisar la página http://proxylist.hidemyass.com/ y escribir en lugar de ***201.16.147.193*** la dirección IP de uno de los proxies listados siempre y cuando tenga una barra verde en *Connection Time* y *High+KA* en la columna *Anon.*
5. Luego, ingresar en la terminal las siguientes líneas:
   a. ***nikto -host www.google.com -maxtime 10 -findonly***
   b. ***nikto -host www.narsatrev.com -maxtime 10 -findonly***
   c. ***nikto -host www.reddit.com -maxtime 10 -findonly***
   d. ***nikto -host www.bloomberg.com -maxtime 10 -findonly***

   ¿Cómo varían los resultados de cada uno de los comandos ejecutados?
6. Vuelve a la terminal y escribe:
   a. ***nikto -D v -host www.narsatrev.com***

   ¿Cómo varían los headers mientras avanza la operación? ¿Qué clase códigos de estatus envía el servidor en función del archivo probado? ¿Cómo varían los plugins utilizados?

b. Prueba ahora con los dominios www.facebook.com y www.sandersweb.com

¿Cómo cambia la información que provee un servidor y otro

7. Ahora escribe en la terminal lo siguiente:

   nikto -D v -Tuning 1 -host www.sandersweb.com -maxtime 10

   Cuando acabe, escribe:

   nikto -D v -Tuning 2 -host www.sandersweb.com -maxtime 10

   Y finalmente:

   nikto -D v -Tuning 9 -host www.sandersweb.com -maxtime 10

   ¿Qué archivos revisa cada uno de los dos comandos?

8. Para guardar los resultados del escaneo escribe:

   nikto -Display v -o resultados.html -Format html -host www.google.com

   Una vez que acabe el escaneo (aproximadamente 2 minutos), ve al explorador de archivos y abre resultados.html con el browser default de Kali.

9. Busca en todos los archivos probados por el escaner un valor diferente a OSDVB-0 en todos los bloques (e.g. debe haber un OSDVB-5737 casi hasta el final)

10. Abre una nueva pestaña y busca OSDVB-Número, ingresa en el link de CVE que muestre este resultado.

    ¿Qué clase de vulnerabilidad detectó nikto en el reporte?