# Nessus - Sección de Scanners

Submitted by freed0m on Mon, 11/04/2005 - 11:36.Aplicaciones

La herramienta de auditoria de vulnerabilidades Nessus, permite configurar distintos tipos de scanner de puertos con distintos plugins, todos ellos se encuentran agrupados en la familia de Port Scanners y son los siguientes:

**Netstat 'scanner'**: mediante este plugin podremos ejecutar el comando netstat para identificar puertos abiertos en el sistema. Este plugin es para comprobaciones locales, y se identifica con el número 14272.

**Nmap (NASL wrapper)**: este plugin no necesita mayor aclaración, es un port de Nmap al formato NASL (Nessus Attack Scripting Language). Este plugin tiene el número 14259.

**Exclude toplevel domain wildcard host**: la función de este scanner es verificar que no estamos lanzando Nessus contra un dominio de primer nivel, o contra un rango de direcciones IP asignadas a Nessus, es curioso que se introduzcan estas configuraciones en los plugins, quizás para recordar que aunque Nessus es una herramienta de hacking automático, tanto con Nessus como con otras herramientas de esta índole es importante conocer con mayor detalle que y como hace lo que hace, en lugar de emplearla de forma indiscriminada. El número de plugin que identifica este scanner es el 11840.

**SYN Scan**: al activar este plugin realizaremos un análisis SYN "rápido" de las direcciones IP destino. Las consideraciones en cuanto a "rápido", se deben a que en este análisis se tiene en cuenta el RTT (Round Trip Time), que es el tiempo total de ida y vuelta, de los paquetes entre el host que lanza Nessus y el host destino.
Entre las recomendaciones de uso de este plugin hay que considerar que si tenemos activado el plugin de Nmap, estaremos analizando los puertos 2 veces, y es posible que los resultados sean idénticos. Además incrementará el tiempo total del análisis. Este plugin tiene el código 11219.

**Scan for LaBrea tarpitted hosts**: mediante el uso de este scanner, podremos analizar sistemas que tengan instalado el software de LaBrea. Este análisis se realizará enviando paquetes ACK modificados, y paquetes SYN para intentar detectar máquinas inexistentes que están siendo simuladas por LaBrea.
La web del soft es labrea en sourceforge. LaBrea funciona utilizando direcciones IP que no están en uso en la red, y crea sistemas virtuales respondiendo a intentos de conexiones desde dichas direcciones IP inexistentes.
Este funcionamiento permite prolongar el tiempo de análisis del sistema de forma indefinida, además de provocar resultados inconsistentes.
Resulta curioso que la interpretación que algunos dan sobre la funcionalidad de LaBrea Tarpits es tarros de miel pegajosos, cuando Tar Pits se traduce como Hoyos de Alquitrán, y siendo la Brea, resina de pino. El código de este plugin es 10796.

**Nessus TCP scanner**: realiza un análisis TCP de los puertos del host destino, una vez se establece la conexión se obtienen los banners de los servicios para los plugins de

identificación de servicios. Si empleamos el plugin de Nmap, estaremos analizando los hosts destino 2 veces. Este plugin esta identificado con el número 10335.

**Ping the remote host**: activando este plugin se analizaran los host destino enviando paquetes TCP Ping. La técnica de TCP ping, envía paquetes SYN, y analiza la respuesta en función de esta sea RST o SYN/ACK.
Este plugin está identificado como 10180, también permite utilizar un ICMP tradicional.

**SNMP port scan**: consulta los puertos abiertos a través de peticiones SNMP, requiere que snmpwalk este instalado en el sistema. Este plugin está identificado con el número 10841.