Lamp Security LINUX

Identificación del Objetivo

Aplicación de herramienta NMAP

El nmap es una herramienta que sirve para evaluar la seguridad del sistema en una red,

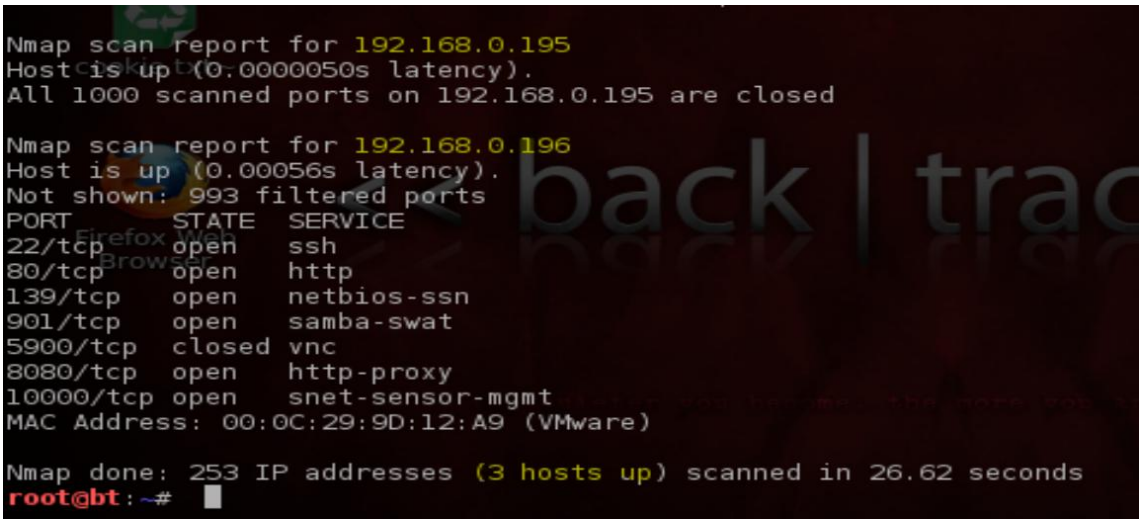
rastrear puertos o detectar objetivo para un ataque

Algunas utilidades de la herramienta nmap son:

-Para averiguar cuántos equipos están conectados en la red, sus ips y los puertos que tienen abiertos, utilizamos el comando nmap y el rangos de ip que queremos que escanea.

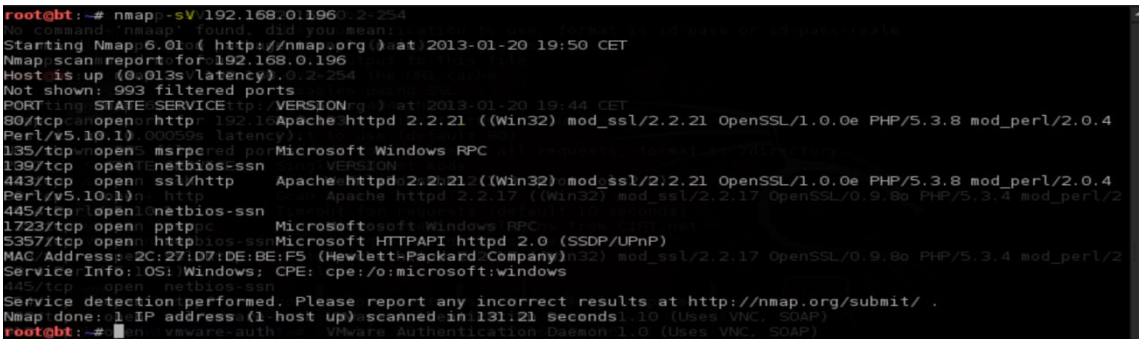
Nota: En este caso escaneamos desde ip 192.168.1.2 hasta 192.168.1.254

nmap 192.168.0.2-254



-Una vez elegido un equipo para averiguar detalles de los puertos que tienes abierto usamos el comando siguiente:

nmap -sV 192.168.0.196



-Para averiguar qué sistema Operativo y más informaciones del sistema del equipo, hacemos un escaneo usando el siguiente comando:

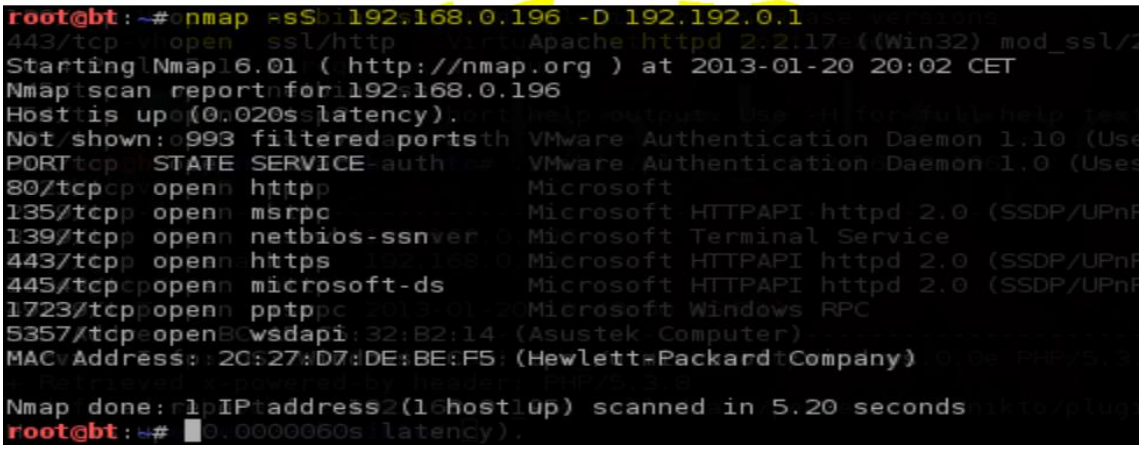
Nota: en este escaneo tambien estamos asegurando de que nonos detectan, en caso de que el equipo escaneado tiene algún programa que nos puedes detectar.

nmap –O –sS 192.168.0.196

-Otra forma de confundir el equipo que queremos escanear de que no nuestra deirecion y hacerlo creer que se trata de otro equipo, por ejemplo el router. Usamos el comando nmap con la opción siguiente:

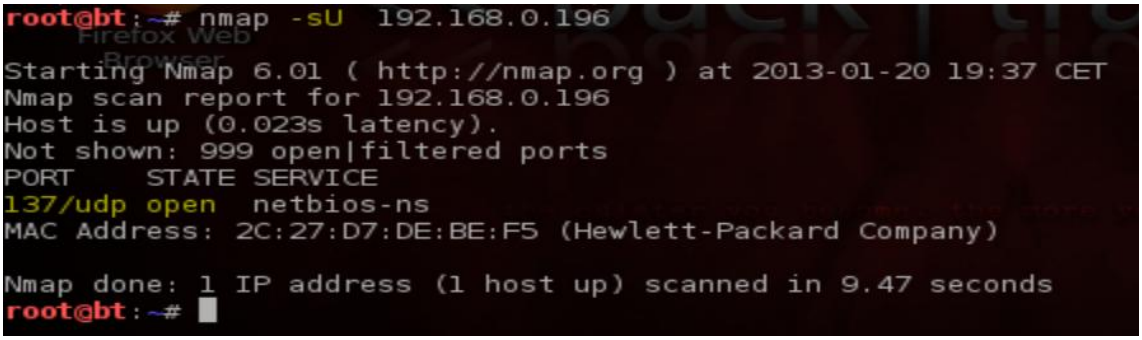
Nota: Escaneamos al 192.168.0.19 y le hacemos creer que está siendo escaneado por 192.168.1.196

nmap sS 192.168.0.196 –D 192.168.0.1



-Para ver el puerto UDP abierto

nmap –sU 192.168.0.196



Nota: La herramienta nmap tiene muchos más opciones para evaluar la seguridad de una red.

Exploración del Objetivo

Aplicación de la Herramienta NIKTO

Una vez tenemos localizado el objetivo con la herramienta NMAP, ahora podemos explorar el objetivo en busca de vulnerabilidades utilizando las direcciones y los puertos abiertos anteriormente encontrado.

En este casso vamos a comentar sobre la herramienta NIKTO.

Para abrir nikto vamos al menú Backtrack->Vulnerabilityu assessment->Web application assessment->Web vulnerability scanner->nikto

Se abrirá una ventana de linea de commando de nikto.

-Para explorar hacer una exploración con nikto usamos en comando:

./nikto.pl –host 192.168.0.195

En el caso anterior, nikto va a hacer automáticamente la exploración en el puerto 80. Para hacer exploración en otro puerto, como por ejemplo 8080, habrá que indicarlo de la siguiente manera:

./nikto.pl –host 192.168.0.195 –port 8080

Nota: Con las acciones anteriores de la herramienta nikto se puede encontrar vulnerabilidades

que pueden ser utilizados para un ataque, como por ejemplo inyección de Sql con la herramienta MySQLmap.