**LABORATORIO N°2 FASE DE ESCANEO**

Durante las fases previas hemos logrado recopilar variada información sobre nuestro objetivo. Bien, ¿cuál es el siguiente paso entonces? Pues identificar los hosts “vivos”, es decir aquellos que están activos dentro de los rangos de IP’s previamente encontrados y una vez realizado esto, proceder a determinar los puertos abiertos en dichos equipos. Si tenemos éxito lograremos determinar la versión del sistema operativo de cada host activo y las aplicaciones o servicios que escuchan requerimientos en dichos puertos.

1. PING SWEEPER (Herramientas de barrido de ping)

Herramientas: Ping Scanner Pro , SoftPerfect Network Scanner

1. HERRAMIENTA DE TCP-PING
2. ESTADO DE PUERTOS

Nos basaremos en las definiciones de estado de puertos de la herramienta de escaneo más popular: NMAP.

* Abierto
* Cerrado
* Filtrado
* No- filtrado
* Abierto|Filtrado
* Cerrado|Filtrado

1. **TECNICAS DE ESCANEO**

Escaneo SYN o Half-Open (medio abierto)

Escaneo Full o Connect-Scan

Escaneo UDP

Escaneos especiales: Null-Scan, Fin-Scan, XMAS-Scan

Escaneo ACK

1. **ESCANER DE PUERTOS: NMAP**

[*http://www.nmap.org/*](http://www.nmap.org/)*.*

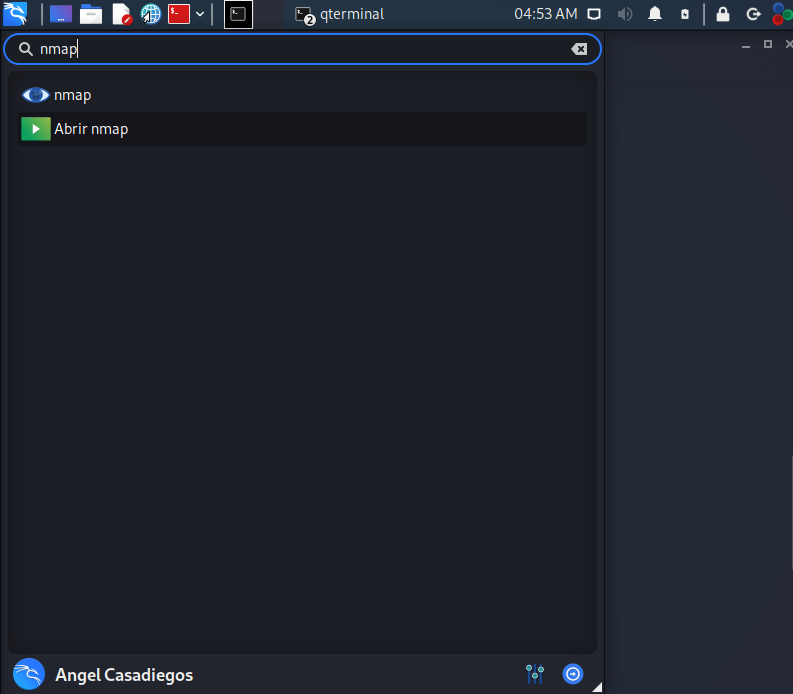
* 1. **Lab: Escaneo de puertos con NMAP**

Recursos:

* **Victima:** Proyecto ScanMe de NMAP, host: scanme.nmap.org
* **Estación Hacker:** 1 PC o VM con sistema operativo Windows o Linux
* **Software:** NMAP con Zenmap disponible en [*http://www.nmap.org*](http://www.nmap.org)*.*

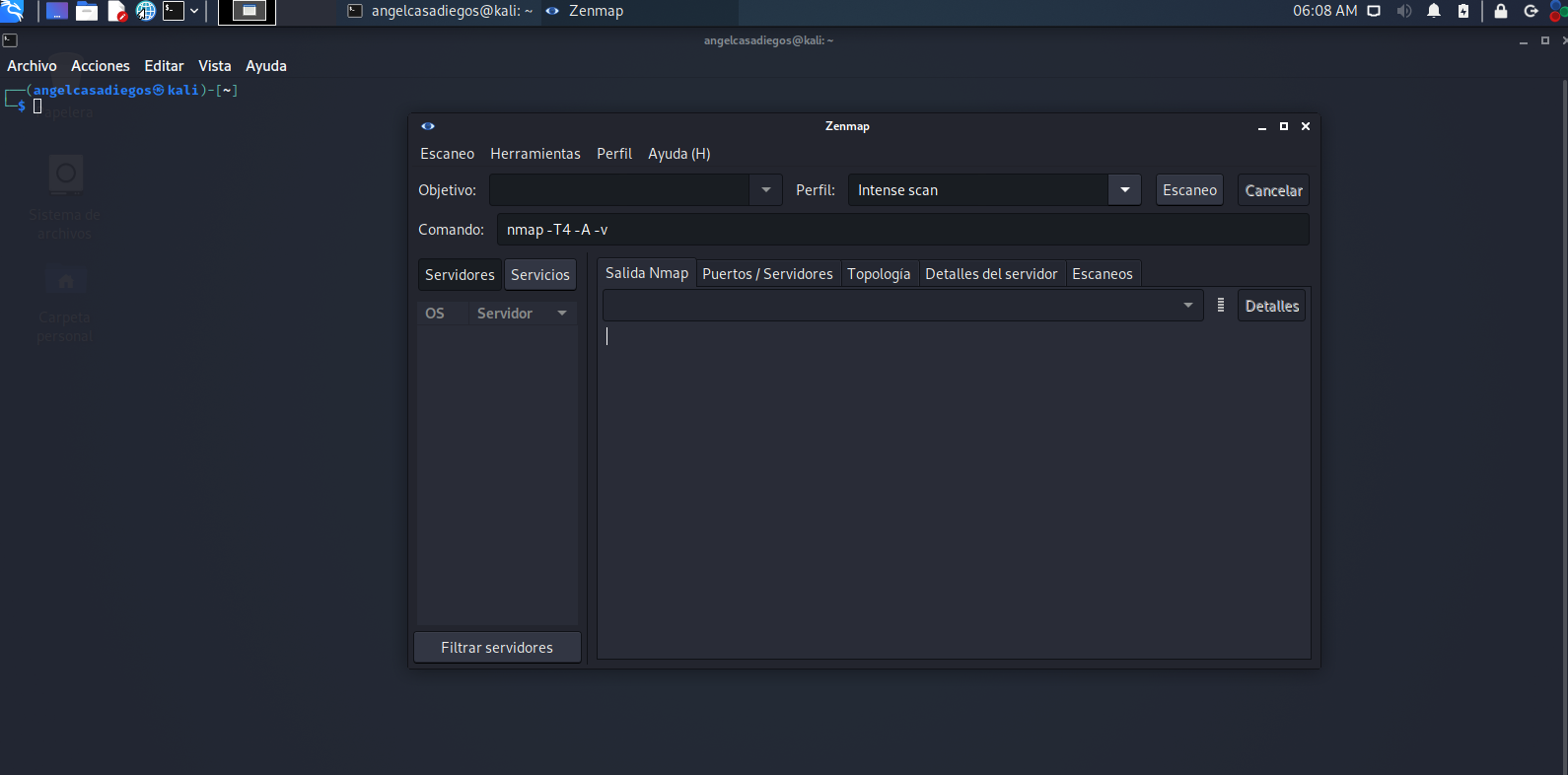
**Pasos para seguir:**

1. Verifique que el aplicativo NMAP se encuentre instalado (en Kali Linux ya viene preinstalado), de lo contrario proceda a realizar la instalación respectiva (en Linux abra un terminal y ejecute como root o con sudo el comando apt-get install nmap).



Verificamos que tenemos instalado NMAP correctamente en nuestra terminal de LINUX

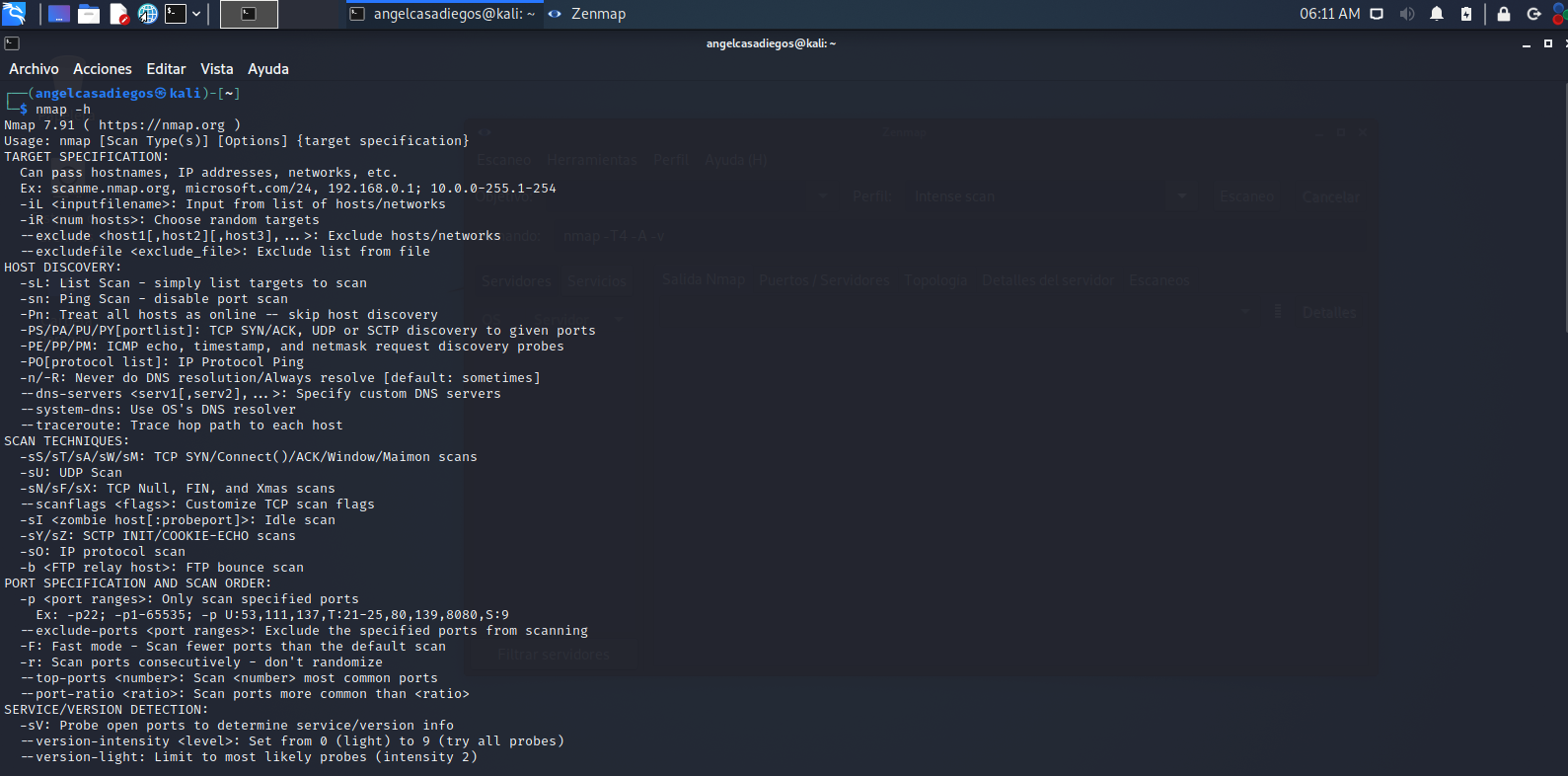
1. Hecho esto, realizaremos un laboratorio en línea de comandos con nmap y compararemos con el uso de la interfaz gráfica Zenmap.



Aplicativo ZENMAP instalado correctamente dentro de la terminal Linux

1. Ejecute una línea de comandos (cmd| Shell).
2. Proceda a ejecutar el comando nmap con la opción de ayuda: nmap -h
3. Tomese un tiempo para revisar todas las opciones disponibles. Luego ejecutaremos un escaneo en modo stealth (half open) hacia el servidor scanme.nmap.org con el comando:

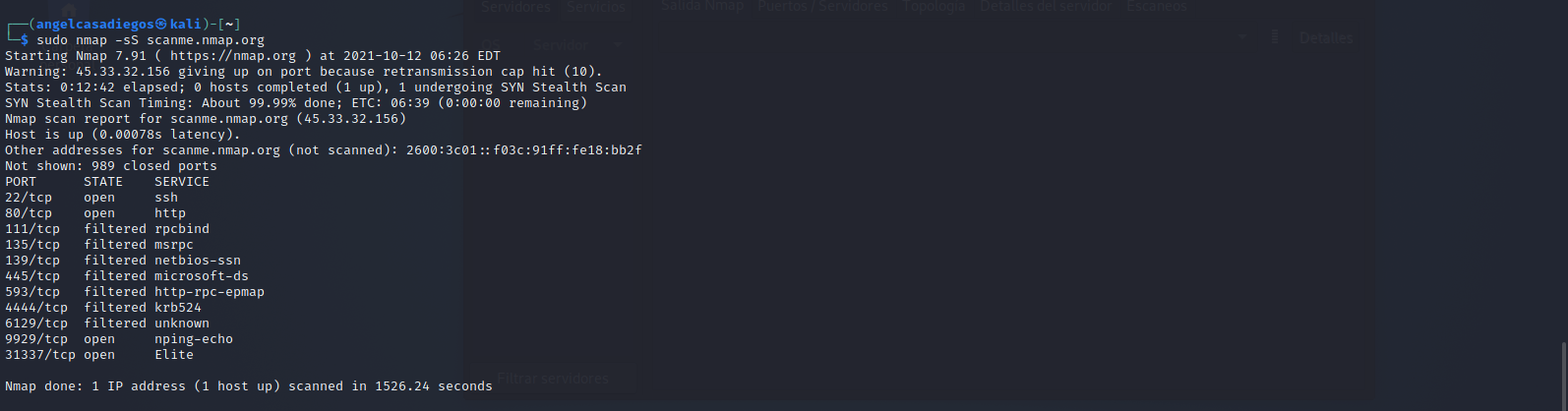
Nmap -sS scanme.nmap.org



Estos son algunos de los comandos que se encuentran luego de ejecutar el comando nmap –h que nos muestra el directorio de la opciones disponibles



Empezamos hacer el escaneo luego de ejecutar el comando nmap a nuestra victima scanme.nmap.org

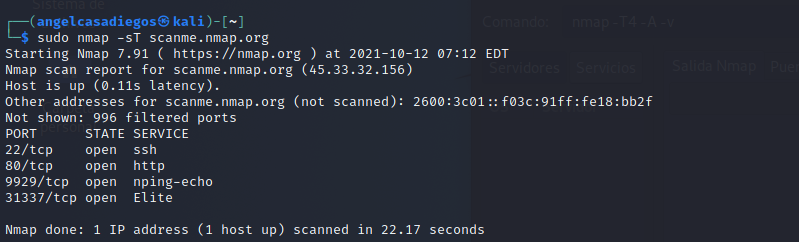


El resultado después de realizado el escaneo es el siguiente:

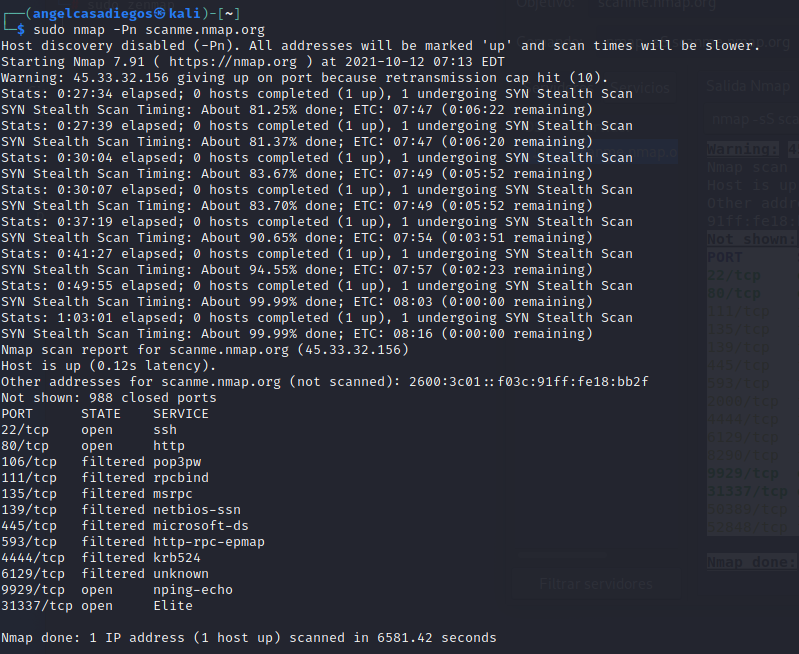
1. Interprete el resultado obtenido. ¿Qué indica el estado “filtered”?

Tenemos la cantidad de 989 puertos cerrados. Pero tenemos además carios puertos OPEN Y FILTERED. Los cuales los puertos OPEN están aceptando conexiones tpc o udp. Osea que el puerto está abierto y se puede utilizar para poder explotar el sistema. Ahora tenemos los puertos con estado FILTERED el cual no nos determina que esos puertos con esos estados están abiertos, ya que puede haber un firewall activo. Lo que hizo que nuestro escaneo durara un poco de tiempo ya que Nmap intento en varias ocasiones conéctanos hacia ese puerto

1. Proceda ahora a ejecutar un escaneo más profundo en modo “connect”, recuerde que, aunque este tipo de escaneo es más exacto que el de tipo half-scan, al completar el 3-way-handshake de TCP nos exponemos a ser detectados. ¿Cuál es el comando que debe ejecutar?

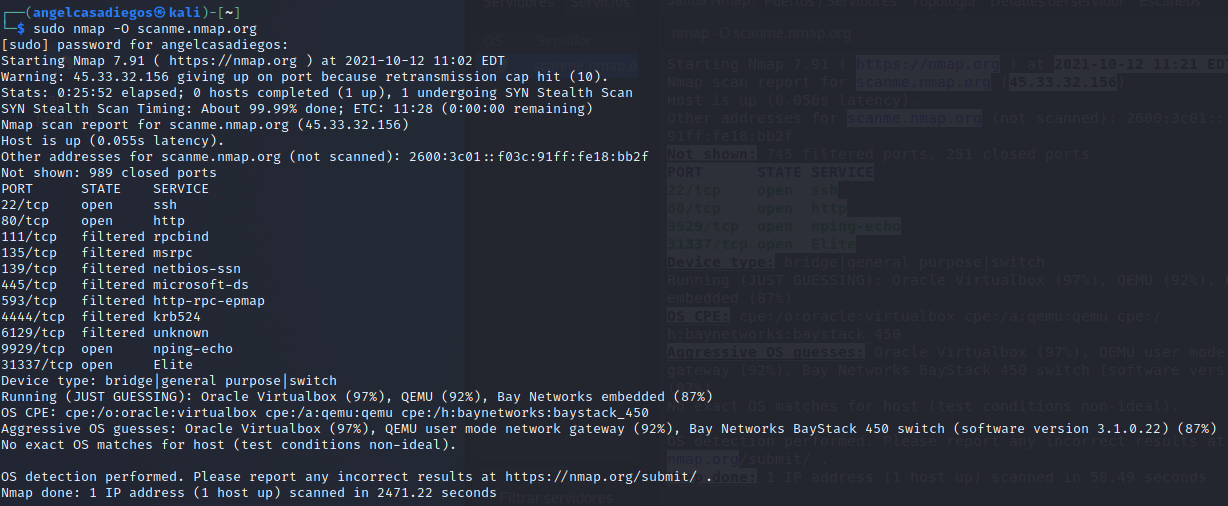


Para ejecutar un escaneo más profundo en modo “Connect” se debe colocar el comando sudo nmap –sT [IP VICTIMA] otro comando que podemos utilizar es sudo nmap –Pn [IP VICTIMA] pero esta llevara mucho más tiempo debido al escaneo más profundo que este hace.



Con el Comando nmap –Pn scanme.nmap.org el escaneo es mas profundo pero ala vez mas demorado incluso con el doble de tiempo pero podemos recopilar más información sobre los puertos que podemos visualizar además de sus estados

1. Ahora pruebe a detectar la versión del sistema operativo. ¿Qué comando debe ejecutar?

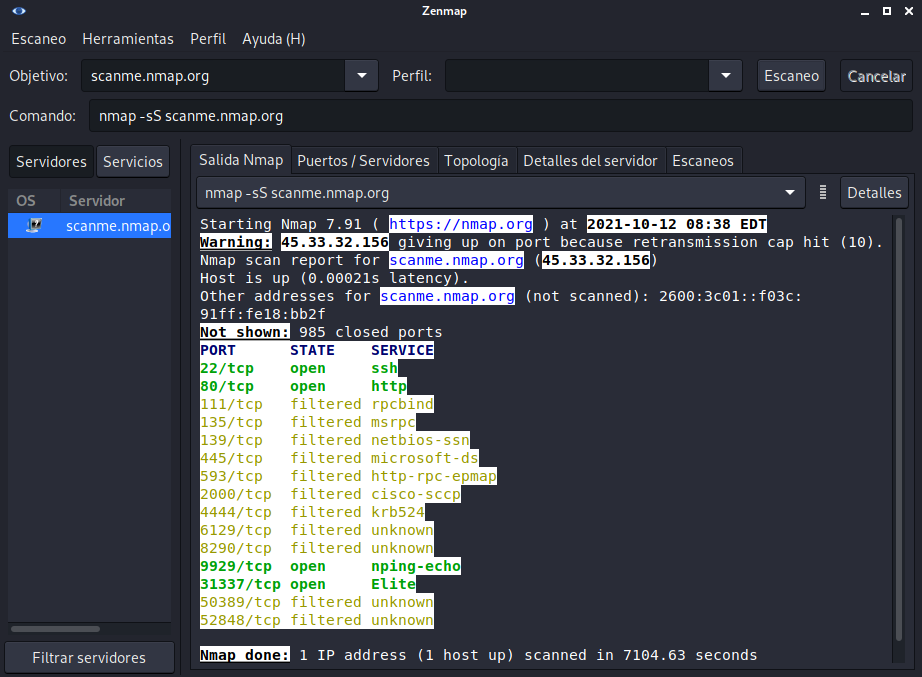


El resultado fue impreciso ya que no existen coincidencias exactas del sistema operativo para el host. El comando con que se obtuvo esta información fue nmap –O scanme.nmap.org

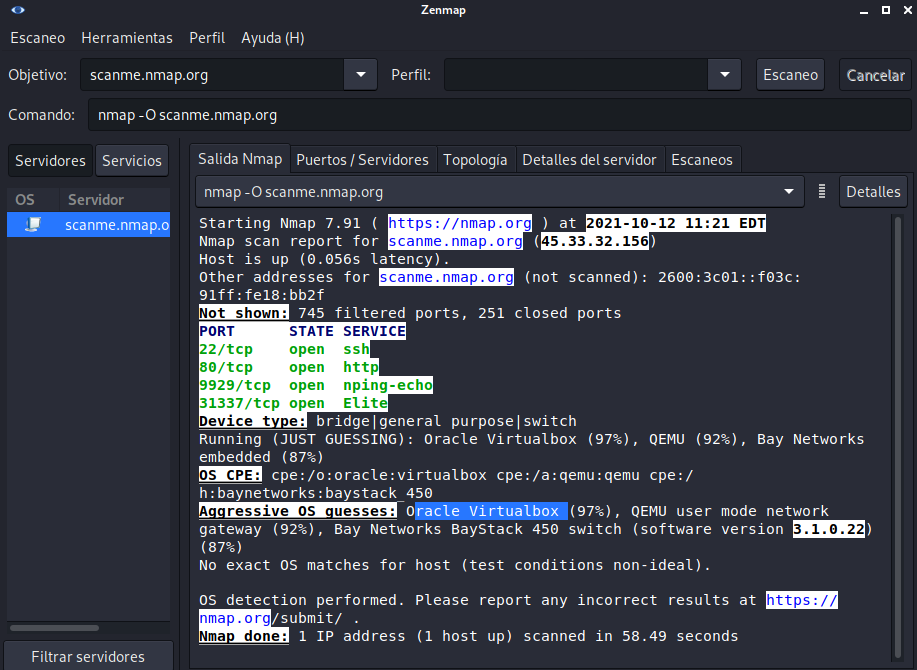
1. Compare los nuevos resultados con los obtenidos previamente. ¿Coinciden? Registre sus nuevos resultados en la bitácora.

Los resultados coinciden y podemos afirmar que estamos trabajando con la misma ip y nuestro escaneo está ejecutándose exitosamente. Aunque con algunas diferencias en cuanto a lo que es el escaneo Half-open y connec ya que uno es más profundo que otro y podemos obtener cierta información de diferencia. En cuanto en el comando para obtener el sistema operativo nos arroja la misma bitácora aun que con la diferencia que nos arroja las posibles coincidencias de sistemas operativos en los que funciona nuestra victima.

1. Ahora pruebe a realizar lo mismo pero en la interfaz grafica Zenmap (en Kali abra el menú: **“Application->Information Gathering->Zenmap”**). ¿Es más fácil? ¿Qué ventajas o desventajas presenta vs la línea de comandos?



Por medio el programa Zepman es más fácil en cierto modo, ya que este nos da una cantidad de comandos a ejecutar al mismo tiempo, que por medio de consola ya podríamos hacerlo. En cuanto a la diferencia de tiempo, es más demorado hacer el mismo trabajo aunque el escaneo es más profundo que por medio de la consola ya que nos arrojas mas información sobre mas puertos y sus estados que simplemente por medio de la consola a primera vista no nos los muestra.



Es esta caso se registra que este comando en especifico es menos demorado en realizar. Pero la precisión de este es menor ya que nos da datos de sistemas en los que esta basado nuestra victima que lo que nos hace ver a simple vista que no es 100% concreta la información que nos suministra en cuanto al sistema operativo. Por lo tanto no hay coincidencias exactas del sistema operativo para el host.

Por lo tanto ventajas objetivas seria:

Ventajas

Escaneo mas completo

Capacidad de ejecutar más comandos a la vez

Mejor uso y adaptabilidad para el usuario ya que el aprendizaje es mas rápido

Desventajas

Mayor tiempo de ejecución de los comandos

Menor eficiencia y rapidez en los comandos

Ejecución de varias instancias del programa

1. **ANALIZADORES DE VULNERABILIDADES**

Los analizadores facilitan la labor del auditor porque permite ejecutar desde una sola interfaz escaneos y enumeraciones sobre el objetivo, a la vez que identifican las vulnerabilidades presentes en dichos sistemas y las clasifican de acuerdo con el nivel de riesgo presente.

Los niveles de riesgo se clasifican usualmente en: bajo, medio y alto.

Existen muchas herramientas de análisis de vulnerabilidades en el mercado, tanto comerciales como de código abierto. Podemos mencionar algunas de las más populares:

* **OpenVas:** Analizador de código abierto, multiplataforma, disponible para descarga desde <http://www.openvas.org/>.
* **Nexpose:** Analizador desarrollado por la empresa Rapid 7 (<http://www.rapid7.com>), tiene una versión Community de código abierto y una versión comercial. Además de ser multiplataforma.
* **Nessus:** analizador popular y uno de los más antiguos, catalogado por fuentes independientes como el analizador # 1 de vulnerabilidades, es patrocinado por la empresa Tenable Network Security (<http://www.tenable.com/>) y tiene varias versiones, 1) una gratuita llamada Nessus Home dirigida a los usuarios de hogar y de oficinas pequeñas y otras dos con costo.
  1. **Lab: Análisis de vulnerabilidades con OpenVAS**

En este laboratorio usaremos la herramienta OpenVAS en Kali Linux para ejecutar un escaneo de vulnerabilidades sobre un host objetivo.

Recursos

* **Host victima:** 1 dispositivo de su preferencia con cualquier sistema operativo instalado. Se puede usar como víctima *Metasploitable2*.
* **Estaciónhacker:** 1 PC o VM con Kali Linux.
* **Software:** Analizador de vulnerabilidades OpenVAS.
* **Requisitos:** El host victima debe ser alcanzable desde la estación hacker y debe tener algunos servicios publicados a través del firewall.

Pasos para seguir:

1. En las ultimas versiones de Kali Linux, OpenVAS no viene preinstalado. Por tanto, debemos instalarlo. Para configurar Open VAS ejecute el comando: Openvas-setup
2. Una vez finalizada la configuración, los servicios de OpenVAS se inician automáticamente, se crea además una cuenta de usuario llamada admin y se le asigna una clave aleatoria y se abre un navegador web conectado a la interfaz administrativa (<https://localhost:9392>). Busque en la salida esta información y guarde la clave para que pueda usarla luego para autenticarse en la interfaz de administración de OpenVAS.
3. Dado que el certificado digital instalado por el proceso de configuración de OpenVAS es auto-generado, es posible que reciba una alerta de seguridad del navegador web. Simplemente dele clic a las opciones avanzadas y agregue una excepción para el certificado. Luego ingrese a la interfaz administrativa Greenbone security Assistant con el usuario admin y la clave asignada. Puede usar como victima una VM con Metasploitable2, pero usted también podría usar como blanco cualquiera de sus maquina virtuales.
4. Empezaremos por crear un nuevo escaneo. Para ello escogemos el menú

“Scans->Tasks”, y luego daremos clic sobre el icono del asistente (wizard) ubicado a la izquierda en color morado y optaremos por seleccionar “Task Wizard”.

1. El asistente abrirá una caja de dialogo en la que ingresaremos el nombre de host o la dirección IP de nuestro objetivo y finalmente daremos clic en el botón “Start Scan”. Ahora solamente esperamos que finalice el escaneo para poder analizar los resultados y generar el reporte.
2. Para ver todos los reportes generados damos clic en el menú **“Scan->Reports”**
3. OpenVAS permite exportar el reporte en distintos formatos aparte de XML.
   1. **Lab: Análisis de vulnerabilidades con Nessus**

En este ejercicio instalaremos la herramienta Nessus Home en Kali Linux.

Recursos

* Victima: 1 dispositivo a su elección con cualquier sistema operativo.

Puede ser como victima usar el proyecto ScanMe de NMAP.

* Estación hacker: 1 PC o VM Windows o Linux.
* Software: Nessus Home disponible en <https://www.tenable.com/products/nessus-home>.

Pasos a seguir:

1. Para el sistema hacker podemos escoger Kali Linux, pero Nessus Home puede instalarse en sistemas Windows server, Windows 7/8/10, Linux y Mac OS.
2. Registrese con Tenable y descargue el instalador, transfieralo a su nestación hacker y ejecute el programa de instalación con privilegios administrativos. Puede ser Kali Linux de 64 bits.
3. Una vez instalado procederemos a iniciar el servicio desde la línea de comandos.

/etc/init.d/nessusd start

Otra forma de iniciar el servicio: service nessusd start

1. La interfaz grafica de Nessus se accede desde un navegador web conectándose al host local en el puerto 8834. La primera vez nos va a pedir crear un usuario administrador, póngale sus nombre y asígnele una clave.
2. Luego de eso Nessus se conectara con los servidores de Tenable para descargar los plugins, es decir los módulos utilizados para detectar vulnerabilidades en los sistemas remotos.
3. Para agregar un nuevo escaneo, podemos hacerlo desde la carpeta “My Scans” haciendo clic en el botón “New Scan”, a partir de una plantilla (template)
4. Podemos usar la plantilla básica “Basic Network Scan” y dejaremos las opciones por defecto para auditar el host scanme.nmap.org. Usted es libre de experimentar con las distintas plantillas.
5. Lo único que cambiaremos serán las opciones avanzadas respecto a rendimiento (opción “Custom”). Esto lo haremos por dos motivos principales: 1) evitar ser detectados por un dispositivo de protección perimetral y 2) para evitar congestionar los equipos remotos. Luego de esto grabaremos el escaneo dando clic en el botón “save” ubicado en la parte inferior de la página web.
6. El escaneo creado aparecerá en la carpeta “My Scans”. Para iniciarlo daremos click en el botón “play” o “Launch”. Elk análisis de vulnerabilidades puede tomar varios minutos, horas o días inclusive, dependiendo de la cantidad de hosts escaneados.
7. Cuando el escaneo se haya completado veremos un símbolo de visto en la tercera columna. Para ver los resultados daremos click en el nombre del escaneo.
8. Finalmente podremos generar reportes en distintos formatos para su posterior análisis (menú “Export”).