Gobierno de Canarias
Consejería de Educación y Universidades
Unión Europea
Fondo Social Europeo
"El FSE invierte en tu futuro"
CIFP César Manrique

DEPARTAMENTO DE INFORMÁTICA Y COMUNICACIONES

Análisis y explotación de vulnerabilidades (SAD01)

CICLO: 1 DAW
Alumno: Pedro Pérez Jaramillo
CURSO: 2020 / 2021

INDICE GENERAL

Enunciado:

Apartado 1: FingerPrinting

Utilizando las máquinas virtuales Kali Linux y metasploitable, ejecuta los comandos Nmap necesarios para los casos planteados a continuación, capturando la pantalla resultante de dicha ejecución y volcando los resultados sobre fichero.

1.1 Ver los hosts que se encuentran activos en la red.
1.2 Para cada uno de los equipos de dicha red, verifica sistema operativo, puertos y servicios.
1.3 Realiza un escaneo de tipo TCPconnect sobre la máquina metasploitable para determinar qué puertos están abiertos.
1.4 Determina la versión concreta de los servicios que tienen activados la máquina metasploitable.
1.5 Repite el escaneo de puertos realizando un escaneo silencioso.
1.6 Utiliza Zenmap para averiguar el sistema operativo que tienen instalado cada uno de los equipos de la red.

Apartado 2: Pentesting. Análisis y explotación de vulnerabilidades

2.1 Instala en la máquina.
2.2 Utilizando la herramienta elegida.

Desarrollo de la actividad:

1. Resumen:

La realización de este proyecto fue definida del siguiente modo, se realizará en tres fases, en la primera fase se realizará la definición del proyecto como tal, los objetivos, la justificación, el problema, y demás. La segunda fase contendrá la definición del sistema de información con el cual se realizará la prueba piloto del procedimiento que se propondrá, se creará el procedimiento, se escogerán las herramientas con las cuales se realizarán las pruebas de penetración y posterior a esto se realizará la ejecución del procedimiento propuesto y se mostrarán resultados. A partir de la segunda parte se interpretarán los resultados y se generarán recomendaciones.

2. Apartado 1: FingerPrinting

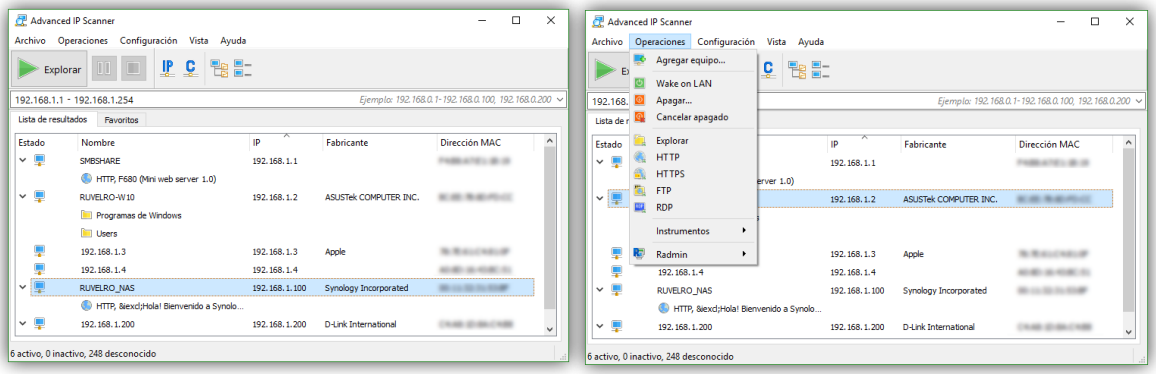
Utilizando las máquinas virtuales Kali Linux y metasploitable, ejecuta los comandos Nmap necesarios para los casos planteados a continuación, capturando la pantalla resultante de dicha ejecución y volcando los resultados sobre fichero.

2.1. Ver los hosts que se encuentran activos en la red.

Muchas veces tenemos que encontrar qué equipos activos tenemos en una red local o que IP acaba de ser asignada a un equipo sobre el que no tenemos acceso directo, sino que tenemos que acceder a él por SSH, Terminal Server,…

Para encontrar la IP resulta muy cómodo el siguiente escaneo con nmap (como administrador)

*(en este caso **NO** es necesario poner la imagen al ancho completo para que se visualice bien el texto)*



nmap -sP 192.168.0.1/24
En este caso estamos escaneando una red de tipo C 192.168.0.0, 192.168.0.0/24 o 192.168.0.0 con máscara de red 255.255.255.0, como queramos verla.

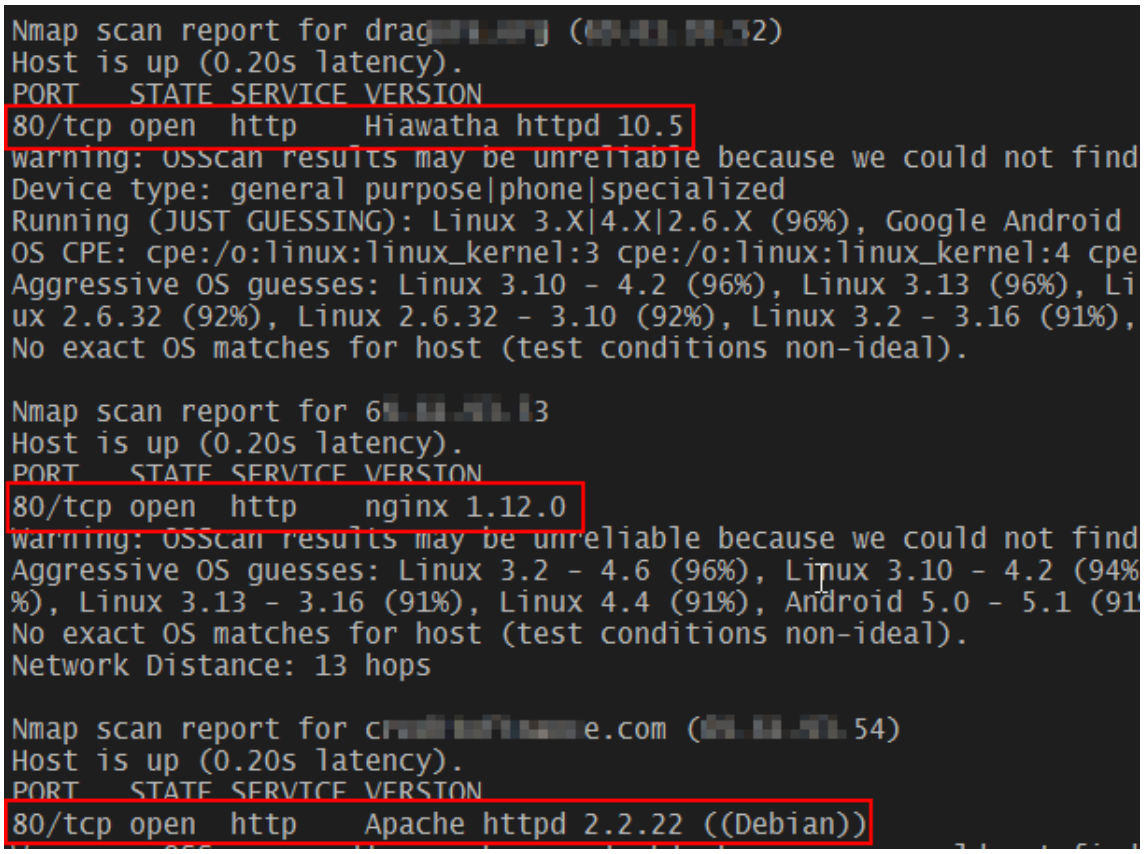
Este tipo de escaneos no van a funcionar si algún equipo tiene bloqueado en el firewall el ping, ya que lo que hace el parámetro "-sP" es un sondeo ping.

En el escaneo de la máquina podemos ver que tiene abiertos varios puertos como 135, 139 o 445. También esto nos ayuda a identificar el sistema operativo, por ejemplo el puerto 445, utilizado en máquinas Windows para compartir recursos de red nos indica que se trata de una máquina Windows,

2.2. Para cada uno de los equipos de dicha red, verifica sistema operativo, puertos y servicios.

Las herramientas vistas hasta ahora se basaban únicamente en las características de los protocolos de Internet. Ahora presentamos otra serie de herramientas de análisis de red algo más sofisticadas. Su finalidad es la de evaluar los sistemas informáticos desde el punto de vista de la seguridad, y no tanto la depuración de errores en la configuración, si bien también pueden ser detectados con ellas.

*(en este caso **SI** es necesario poner la imagen al ancho completo para que se visualice bien el texto)*



Nmap ha llegado a ser una de las herramientas imprescindibles para todo administrador de sistema, y es usado para pruebas de penetración y tareas de seguridad informática en general.

Como muchas herramientas usadas en el campo de la seguridad informática, es también una herramienta muy utilizada para hacking. Es decir que mientras los administradores de sistema lo usan para verificar la presencia de posibles aplicaciones no autorizadas ejecutándose en el servidor, los crackers pueden usarlo para descubrir objetivos potenciales de ataque en dichas vulnerabilidades.

… de esta manera se van desarrollando todos los apartados según el enunciado…

3. CONCLUSIÓN.

Realice una síntesis de los resultados obtenidos aportando experiencias y criterios propios sobre el trabajo realizado.

Tanto nmap como su interfaz gráfica Zenmap son herramientas muy útiles para los administradores de sistemas. Permiten hacer, de forma rápida, intuitiva y sencilla, una auditoría del sistema en el ámbito de su competencia, que es la exploración de puertos. Y no hace falta ser responsable de un gran sistema para

verle la utilidad a nmap. Cualquiera de nosotros, al fin y al cabo, somos administradores de nuestro propio sistema y debemos vigilar la integridad, disponibilidad y confidencialidad de nuestros datos.

4. Bibliografía / Webgrafía

Certificados digitales: una herramienta muy útil a tu alcance Por CI2CRUE

Fecha: 5 noviembre 2013.
En: YouTube [vídeo en línea]. Disponible en: https://youtu.be/8ab88NLomY8 [Consulta: 8 junio 2020].

Ley Orgánica de Protección de Datos de Carácter Personal Por colaboradores de Wikipedia

Fecha: 2017.
En: Wikipedia, la enciclopedia libre. Disponible en: https://es.wikipedia.org/wiki/Ley_Org%C3%A1nica_de_Protecci%C3%B3n_de_Datos_de_Car%C3%A1cter_Personal_(Espa%C3%B1a) [Consulta: 8 junio 2020].

Seguridad informática Por colaboradores de Wikipedia

Fecha: 2017.
En: Wikipedia, la enciclopedia libre. Disponible en: https://es.wikipedia.org/w/index.php?title=Seguridad_inform%C3%A1tica&oldid=102021318. [Consulta: 8 junio 2020].