**Práctica Tema 1: Uso de Herramientas – nmap y wireshark**

Monta un escenario con VirtualBox en el que tengamos una máquina virtual con la distribución Kali Linux y otra máquina más con la máquina virtual Metaexploitable distribuida en clase para el seguimiento de las clases prácticas.

Interconecta en RedNat con el nombre P1 (de la rednat) ambas máquinas.

Utilizando nmap, descubre la dirección ip de la MV Metaexploitable.

Lanza, sobre la máquina “Hackeable” distintos nmap y explica cada una de las salidas que obtengas:

1. Haz un escaneo de la ip exclusivamente
2. En el segundo escaneo, busca obtener toda la información posible del escaner, esto es, todos los detalles del análisis del punto anterior.
3. Haz un escaneo de todos los equipos de una red, excepto 2.
4. Realiza un escaneo rápido
5. Realiza un escaneo ruidoso de todos los puertos TCP.
6. Realiza un escaneo ruidoso de todos los puertos UDP.
7. Realiza un escaneo ruidoso de todos los puertos TCP que afectan al servicio web estándar.
8. Descubre el sistema operativo de Hackeable.
9. Descubre la versión de los servicios ofrecidos por Hackeable
10. Realiza un escaneo sigiloso
11. Realiza un escañero utilizando el script Auth
12. Realiza un escañero utilizando el script vuln
13. Realiza un escañero utilizando el script Malware
14. Realiza un escaneo tiran a los flags FIN, XMAS y NULL, cuenta de donde proviene esa información, explica el significado de cada uno de los flags.

Una vez tirados todas estas consultas de escaneo, vuelve a lanzar el escaneo 5, el 10, el 11 y el 14 sobre los puertos 21, 23, 80 y 1200, captura con wireshark las tramas de escaneo, y explica las diferencias entre las capturas en cuanto a las tramas implicadas en las mismas con todo el detalle que te sea posible.

Para el desarrollo de esta práctica empezamos por crear la red NAT de nuestro entorno de trabajo, dejamos por configuración la que usa por defecto

Procederemos a configurar el adaptador de red del propio virtual box, quedando de esta manera

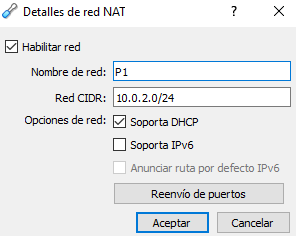


Ilustración Configuración Red

Para descubrir cual es la red que tiene la maquina a explotar, primero debeos de saber cual es **IP A** nos demuestra cual es, procedemos por usar el comando **NMAP** (nuestra dirección ip) y el rango de red para saber que ip tiene la maquina objetivo que queremos escanear, quedando de tal manera

