Modo Bridged en una máquina virtual:

El **modo Bridge** (Adaptador en modo puente) en las máquinas virtuales permite que una máquina virtual se conecte directamente a la red física del anfitrión, como si fuera un dispositivo independiente en esa red. Esto se logra vinculando el adaptador de red virtual al adaptador de red físico del host.

Principales características del modo Bridge:

1. **Dirección IP propia**: La máquina virtual obtiene su propia dirección IP en la red, proporcionada por el servidor DHCP de la red (por ejemplo, un router), lo que la hace independiente del host en términos de conectividad.
2. **Acceso directo a la red local**: La máquina virtual puede interactuar con otros dispositivos en la red local, como computadoras, servidores, impresoras o routers, igual que cualquier dispositivo físico conectado a la misma red.
3. **Visibilidad externa**: La máquina virtual puede ser accesible desde otros dispositivos en la red local, lo que es útil para ejecutar servicios como servidores web, bases de datos o aplicaciones en red.

Fuentes:

Red Hat Documentation

TTL:

En el contexto de ping, el TTL que ves en la respuesta representa el valor del Time To Live (TTL) del paquete de respuesta enviado por el host al que estás haciendo ping. Este valor puede variar según el sistema operativo del host remoto. Por ejemplo, sistemas Linux suelen iniciar con un TTL de 64, mientras que sistemas Windows pueden iniciar con un TTL de 128. El valor que recibes es el TTL inicial menos el número de saltos que el paquete ha recorrido para llegar a ti.

Stack Exchange

NMAP:

Nmap, abreviatura de “Network Mapper”, es una herramienta de código abierto utilizada para la exploración de redes y auditorías de seguridad. Permite descubrir hosts y servicios en una red informática mediante el envío de paquetes y el análisis de las respuestas recibidas.

Entre las principales características de Nmap se incluyen:

- **Descubrimiento de hosts**: Identifica dispositivos activos en la red.
- **Escaneo de puertos**: Enumera los puertos abiertos en los hosts objetivo.

- **Detección de versiones**: Determina el nombre y la versión de las aplicaciones que se ejecutan en los puertos abiertos.
- **Detección de sistemas operativos**: Identifica el sistema operativo y las características del hardware de los dispositivos en la red.
- **Motor de scripting de Nmap (NSE)**: Permite la ejecución de scripts para realizar detección de servicios más avanzada, detección de vulnerabilidades y otras funciones.

Wikipedia

TCP SYN port Scan (-sS):

El parámetro -sS en **Nmap** corresponde al **escaneo SYN** (también conocido como escaneo "semi-abierto" o "Stealth"). Es uno de los métodos de escaneo más utilizados, ya que es rápido, eficiente y menos detectable por los sistemas de registro o firewalls que un escaneo completo de conexiones (-sT).

Cómo funciona el escaneo SYN (-sS):

1. **Envía un paquete SYN**:
   - Nmap envía un paquete TCP con la bandera SYN activada al puerto del objetivo. Este es el primer paso para iniciar una conexión TCP.
2. **Respuestas posibles**:
   - Si el puerto está **abierto**, el host responde con un paquete SYN-ACK.
   - Si el puerto está **cerrado**, el host responde con un paquete RST.
   - Si no hay respuesta o el puerto está filtrado (por un firewall), no se recibe ningún paquete o se recibe un ICMP de tipo "Destino inalcanzable".
3. **No completa la conexión**:
   - Cuando recibe un SYN-ACK, Nmap no completa la conexión con un paquete ACK, sino que envía un paquete RST para abortar el proceso, evitando un registro completo en el sistema objetivo.

Ventajas del escaneo SYN:

- **Más rápido** que otros métodos de escaneo.
- **Menos detectable** por sistemas de seguridad, ya que no completa el "handshake" completo de TCP.
- Funciona en la mayoría de sistemas, siempre que se ejecuten con privilegios suficientes (requiere permisos de superusuario).

nmap Documentation

Feroxbuster:

Feroxbuster es una herramienta de fuerza bruta, es ampliamente utilizada en pentesting y auditorías de seguridad, ya que permite descubrir archivos y directorios ocultos en aplicaciones web. Esto puede ayudar a encontrar rutas expuestas que podrían contener información sensible, paneles de administración o configuraciones incorrectas.

Feroxbuster Cheat Sheet

LFI (Local File Inclusion):

Vulnerabilidad de seguridad web que permite a un atacante incluir y ejecutar archivos locales en el servidor de una aplicación web. Ocurre cuando una aplicación web permite a los usuarios incluir archivos sin sanitización adecuada, lo que significa que un atacante puede manipular la ruta del archivo para acceder a archivos del sistema o incluso ejecutar código malicioso.

OWASP - File Inclusion

ssh2john:

Es una herramienta incluida en John the Ripper (JtR) que se utiliza para convertir claves privadas SSH en un formato compatible con John the Ripper. Esto permite intentar descifrar la contraseña de la clave privada SSH mediante ataques de fuerza bruta o diccionario.

OWASP - SSH Security