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

Dcode Brainfuck:

Dcode Brainfuck es una página web que ofrece herramientas para programadores y criptógrafos. En el contexto de Brainfuck, la página se centra en facilitar la codificación, decodificación y ejecución de programas escritos en este lenguaje.

Brainfuck es un lenguaje de programación minimalista e intencionalmente complicado creado por **Urban Müller** en 1993. Se caracteriza por tener solo 8 comandos y trabajar directamente con un array de memoria (generalmente de 30,000 celdas). Su propósito original era demostrar que un lenguaje podía ser extremadamente pequeño y aún ser Turing completo.

web
Fuentes: wikipedia

Enum4linux:

Enum4linux es una herramienta de enumeración utilizada para extraer información de sistemas Windows y Samba. Está escrita en Perl y actúa como un envoltorio para herramientas de Samba como smbclient, rpcclient, net y nmblookup.
La opción -a ejecuta una serie de comandos de enumeración predeterminados para recopilar información detallada del sistema objetivo. Es equivalente a ejecutar las opciones -U -S -G -P -r -o -n -i juntas. Estas opciones permiten:

- -U: Obtener la lista de usuarios.
- -S: Obtener la lista de recursos compartidos.
- -G: Obtener la lista de grupos y sus miembros.
- -P: Obtener información sobre la política de contraseñas.
- -r: Enumerar usuarios mediante el ciclo RID.
- -o: Obtener información del sistema operativo remoto.
- -n: Realizar una búsqueda de nombres NetBIOS.
- -i: Obtener información de direcciones IP.

Al utilizar la opción -a, enum4linux realiza una enumeración exhaustiva del sistema objetivo, recopilando información valiosa para análisis de seguridad o pruebas de penetración.

Documentación Oficial

Kali linux

Netcat:

Netcat, a menudo abreviado como nc, es una herramienta de red versátil que permite leer y escribir datos a través de conexiones de red utilizando los protocolos TCP o UDP. Debido a su amplia funcionalidad, se le conoce como la “navaja suiza del TCP/IP”**.**

Definición

Sus principales funciones son:

- **Conexiones**: Abre conexiones TCP/UDP para probar servicios y verificar conectividad.
- **Escucha de puertos**: Recibe conexiones entrantes, útil para depuración.
- **Transferencia de archivos**: Facilita el intercambio de archivos sin configuraciones complejas.
- **Escaneo de puertos**: Detecta puertos abiertos en sistemas remotos.
- **Proxy básico**: Redirige tráfico de red.
- **Comandos remotos**: Ejecuta comandos en sistemas remotos para administración o pruebas.

Usos

Reverse Shell:

Una **reverse shell** es una conexión en la que una máquina víctima abre una conexión hacia el atacante, permitiéndole al atacante ejecutar comandos en el sistema víctima. A diferencia de una shell tradicional, donde el atacante se conecta a la víctima, en una reverse shell es la víctima quien se conecta al atacante, lo que puede ser útil para evadir firewalls o filtros de red.
Usos comunes:

- **Acceso remoto**: Permite a un atacante controlar remotamente una máquina, ejecutando comandos.
- **Evitar firewalls**: Utiliza puertos salientes (permitidos en redes) para evadir restricciones de entrada.
- **Exploits de vulnerabilidades**: Es utilizada en ataques de penetración para tomar control de sistemas comprometidos.
- **Administración remota no autorizada**: Usada en pruebas de penetración para simular accesos no autorizados a sistemas.

Fuente

TTI:

En Linux, TTI se refiere a un tipo de **interfaz de entrada/salida de terminal**. En general, es un mecanismo que ayuda a identificar qué tipo de terminal se está utilizando para la comunicación con el sistema, como tty o pts (para terminales virtuales).