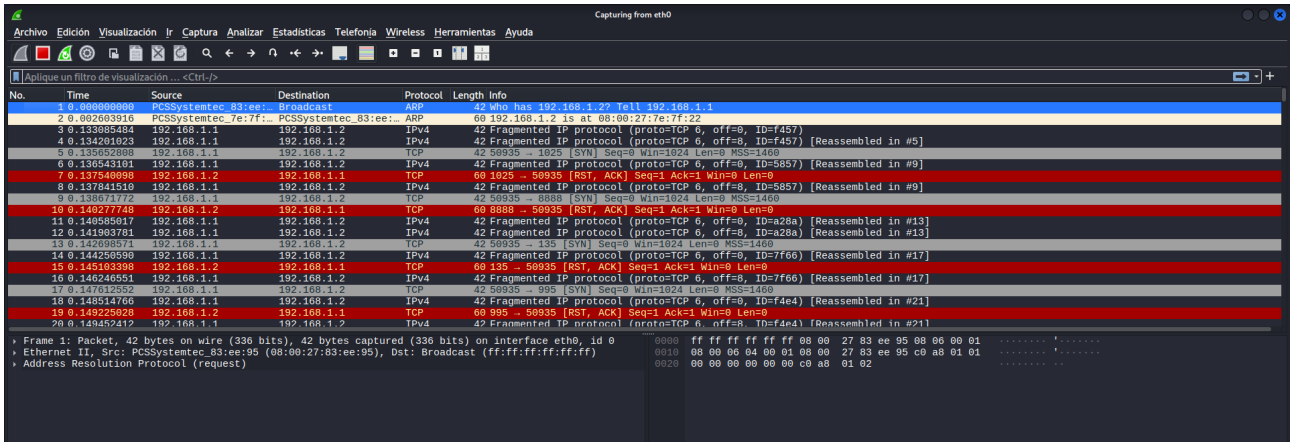
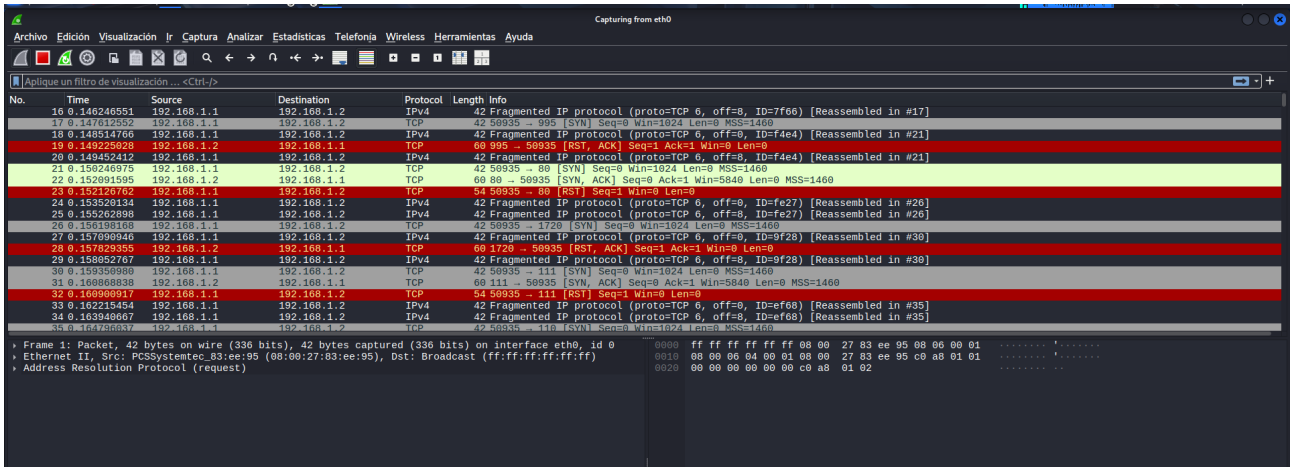
Martin
Dalla Pozza

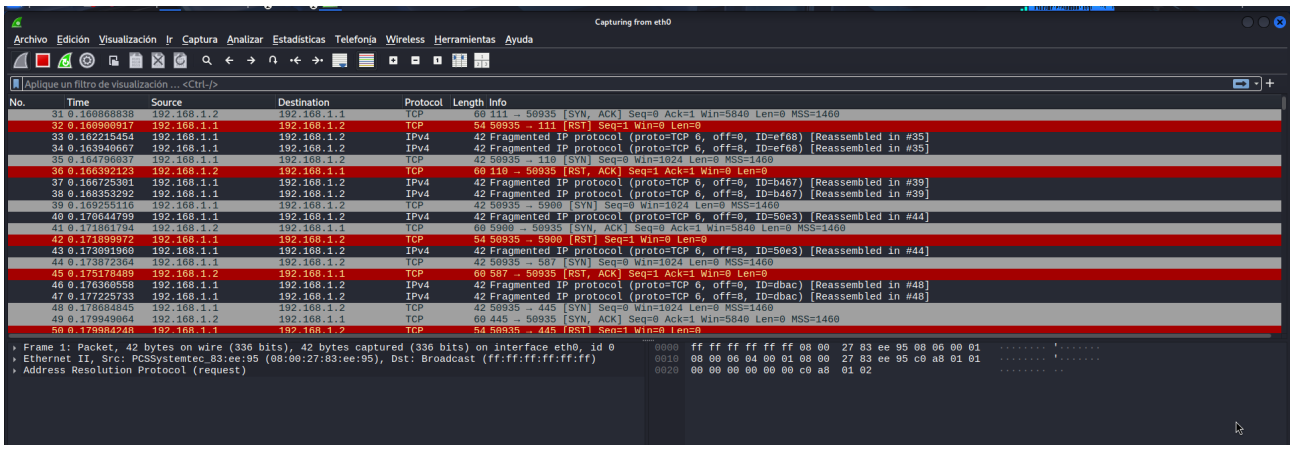
Ejercicio con Nmap con metodologias de evasion

```
Session  Acciones  Editar  Vista  Ayuda
┌──(kali㉿kali)-[~]
└─$ nmap -e eth0 -sS -Pn -n -f --mtu 8 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 21:05 CET
Nmap scan report for 192.168.1.2
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:7E:7F:22 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds
```







El comando:

nmap -e eth0 -sS -Pn -n -f --mtu 8 192.168.1.2

Es una orden de Nmap para realizar un escaneo de puertos con tecnicas de evasion sobre el host 192.168.1.2. A continuación se detalla el significado de cada parametro:

nmap:

Como hemos visto con anteriodidad, es una herramienta de escaneo de red utilizada para descubrir hosts, puertos abiertos y servicios.

-e eth0:

Especifica la interfaz de red que Nmap debe utilizar.

En este caso, la interfaz es eth0.

Útil en sistemas con múltiples interfaces de red.

-sS:

Escaneo TCP SYN (Half-open scan).

Envía paquetes SYN sin completar el handshake TCP.

Es rápido y relativamente sigiloso.

Requiere privilegios de administrador/root.

Respuestas típicas:

SYN/ACK puerto abierto

RST puerto cerrado

-Pn:

Desactiva la detección previa del host (ping).

Nmap asume que el host está activo.

Se usa cuando el objetivo bloquea ICMP o paquetes de descubrimiento.

Hace el escaneo más lento, pero más confiable en redes filtradas.

-n:

No realiza resolución DNS.

Evita convertir direcciones IP en nombres de host.

Acelera el escaneo y reduce tráfico adicional.

-f:

Fragmenta los paquetes IP.

Divide los paquetes en fragmentos pequeños.

Técnica de evasión para evitar firewalls o IDS mal configurados.

Puede causar problemas en redes modernas con inspección profunda.

--mtu 8:

Define el tamaño máximo de unidad de transmisión (MTU) para los fragmentos.

8 bytes es un tamaño extremadamente pequeño.

Aumenta aún más la fragmentación.

Usado específicamente para evadir sistemas de detección

Debe ser múltiplo de 8.

Nota:

-f:

Es equivalente a --mtu 8. Usarlos juntos es redundante, aunque Nmap lo permite.

192.168.1.2:

Dirección IP Metasploitable2

Host dentro de una red privada local.

Resumen funcional:

Este comando realiza un escaneo SYN sigiloso, sin resolución DNS ni deteccion de host, utilizando fragmentación extrema de paquetes, sobre la interfaz eth0, contra un equipo especifico de la red local. Es tipico de pruebas de penetración, auditorías de seguridad o análisis en entornos restringidos.

Explicacion capturas Wireshark

Escaneo de Puertos (Port Scanning)

El equipo con la IP 192.168.1.1 (el atacante) está intentando conectar a multiples puertos diferentes en la IP 192.168.1.2 (la víctima) en un lapso de tiempo muy corto.

Puertos detectados: Se ve actividad hacia los puertos 1025, 8888, 135, 995, 80, 1720, 111, 110, 5900, 587, 445

Comportamiento:

El atacante envía un paquete [SYN] (solicitud de conexión).

Si el puerto está cerrado, la victima responde con un [RST, ACK] (líneas rojas), indicando que la conexion fue rechazada.

Si el puerto está abierto (como se ve en el puerto 80 en la imagen 2), la victima responde con [SYN, ACK] (linea verde), indicando que acepta la conexion.

Tecnica de Evasion:

Fragmentación de IP

Lo más interesante de estas capturas es que los paquetes de consulta no son paquetes TCP normales, sino que están fragmentados.

Observa las líneas que dicen: "Fragmented IP protocol (proto=TCP 6, off=0, ID=...)".

¿Qué significa?

El atacante ha dividido un solo paquete TCP (el SYN) en dos fragmentos de IP muy pequeños (de unos 42 bytes cada uno).

Objetivo: Muchos sistemas de detección de intrusos (IDS) antiguos no reensamblan los paquetes para analizarlos. Al enviar la cabecera TCP dividida en dos trozos de red, el atacante espera que el firewall no reconozca que se trata de un escaneo de puertos y deje pasar los paquetes.

Analisis por Imagenes:

Paquetes 1-2: Comienzan con una resolución ARP. El atacante pregunta "quien tiene la IP .1.2" para conocer su dirección MAC y poder comunicarse.

Paquetes 3-6:

Se ve el primer intento al puerto 1025. Los paquetes 3 y 4 son los fragmentos de IP, y el paquete 5 es el resultado reensamblado por Wireshark.

Paquete 7:

La victima responde con RST (Reset). El puerto 1025 esta cerrado.

Paquetes 21-22:

Aqui hay un cambio. Al escanear el puerto 80 (HTTP), la victima responde con un paquete verde (SYN, ACK). Esto confirma que el puerto 80 está abierto y escuchando.

Paquete 23:

El atacante envia inmediatamente un RST para cerrar la conexión abruptamente y seguir escaneando sin completar el saludo de tres vias (esto se llama *Stealth Scan* o *Half-open scan*).

Muestra el escaneo sistemático de otros puertos conocidos como el 110 (POP3), 587 (SMTP) y 445 (Microsoft-DS/SMB). La mayoría aparecen en rojo, indicando que están cerrados en el objetivo.

Resumen Tecnico:

Tipo de ataque: TCP SYN Scan (Stealth Scan).

Herramienta probable: nmap con las banderas -sS -f (el -f es el que genera la fragmentacion vista).

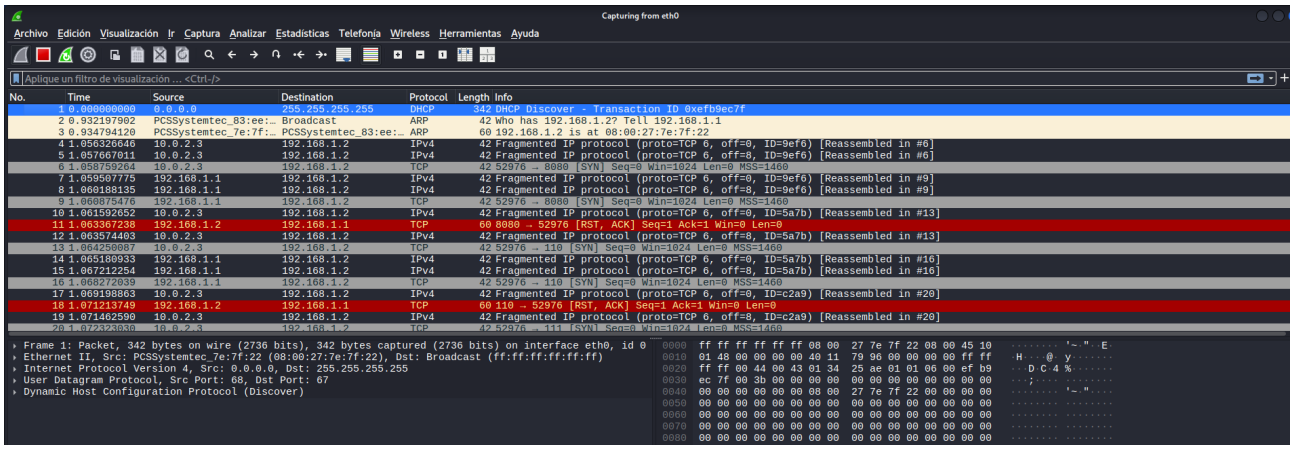
Kali 192.168.1.1 Metasploitable2 192.168.1.2

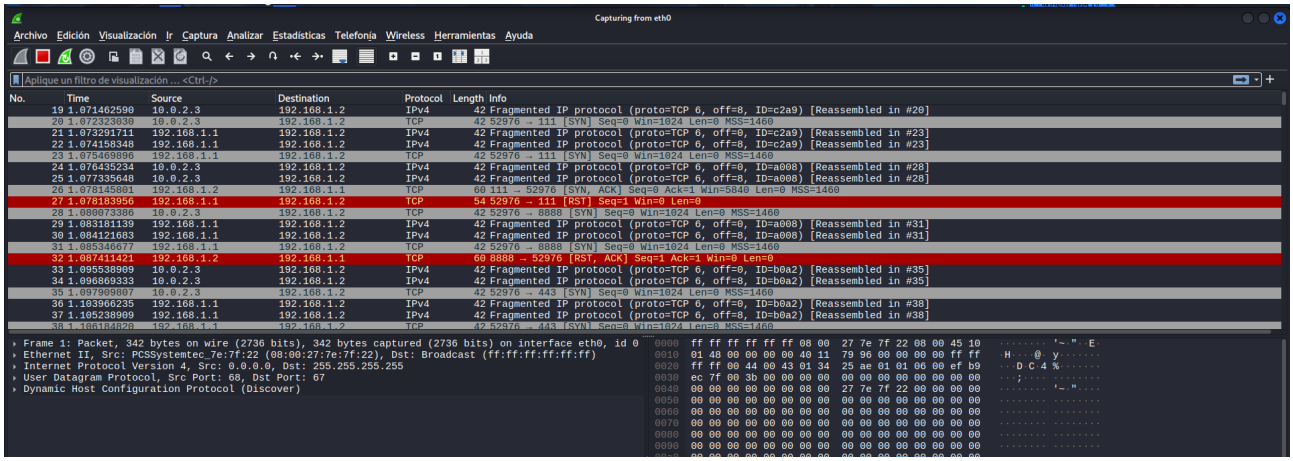
Resultado:

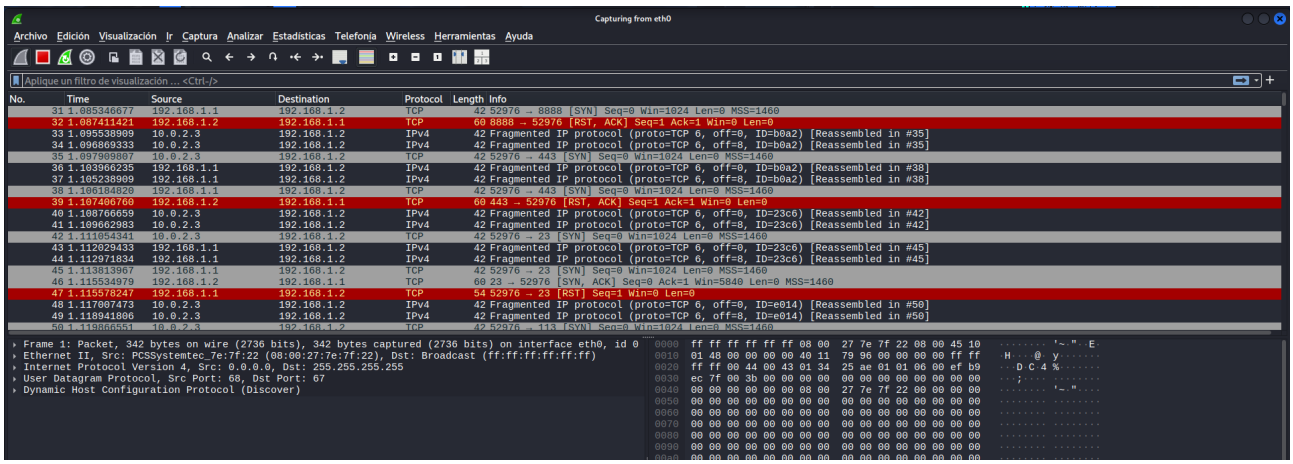
Se confirmo que el puerto 80 esta abierto; la mayoria de los demas estan cerrados.

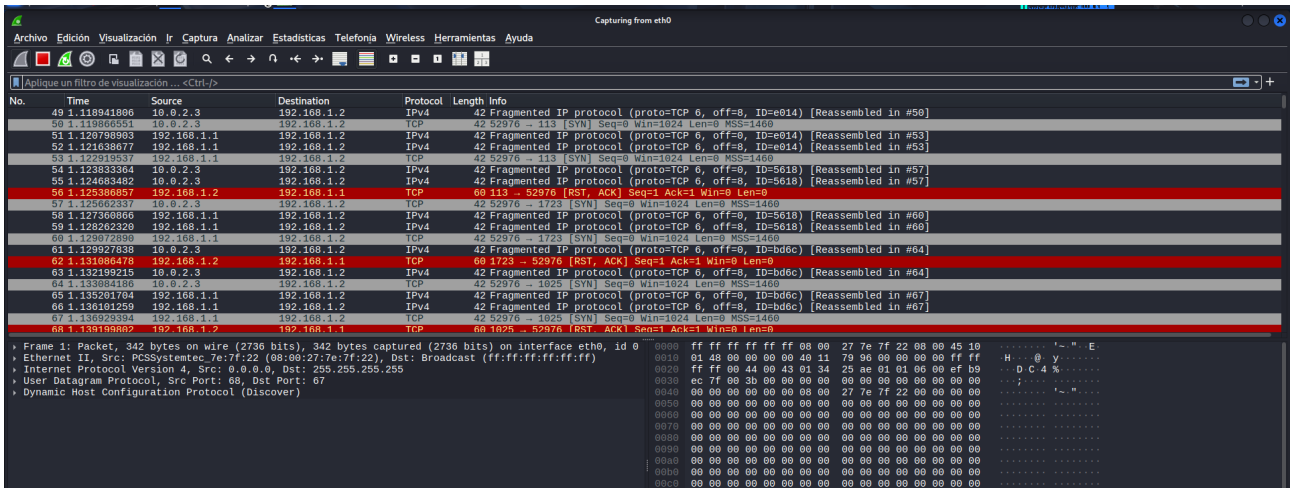
```
Session  Acciones  Editar  Vista  Ayuda
┌──(kali㉿kali)-[~]
└─$ nmap -e eth0 -sS -Pn -n -f --mtu=8 -D 10.0.2.3,ME 192.168.1.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 15:21 CET
Nmap scan report for 192.168.1.2
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:7E:7F:22 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.99 seconds
```









A continuacion se detalla la explicacion tecnica, opcion por opcion, del comando:

nmap -e eth0 -sS -Pn -n -f --mtu=8 -D 10.0.2.3,ME 192.168.1.2

Este comando corresponde a un escaneo Nmap avanzado con tecnicas de evasión y ocultación de origen, típico en contextos de análisis de seguridad ofensiva o laboratorios de ciberseguridad.

Explicacion global:

Nmap realizara un escaneo SYN (half-open) contra el host 192.168.1.2, usando la interfaz eth0, sin descubrimiento previo, sin resolucion DNS, fragmentando los paquetes, forzando un MTU muy bajo y utilizando señuelos (decoys) para ocultar la IP real del atacante.

Desglose de cada parametro:

-e eth0:

Especifica la interfaz de red a utilizar.

Fuerza a Nmap a enviar el tráfico por eth0

Útil en sistemas con múltiples interfaces (VPN, Docker, Wi-Fi, Tor, etc.)

-sS:

SYN Scan (escaneo semiabierto)

Envia paquetes TCP con la bandera SYN

No completa el three-way handshake

Es rápido y relativamente sigiloso

Requiere privilegios de root

Estados posibles:

SYN/ACK puerto abierto

RST puerto cerrado

Sin respuesta filtrado

-Pn:

Desactiva el descubrimiento de host

Nmap asume que el host esta activo

No envía ping, ARP, ICMP, etc.

Útil si el objetivo bloquea ICMP o firewalls estrictos

-n:

Desactiva resolución DNS

No intenta resolver nombres de dominio

Reduce ruido y acelera el escaneo

Evita consultas DNS detectables

-f:

Fragmentacion de paquetes IP

Divide los paquetes TCP/IP en fragmentos pequeños

Intenta evadir IDS/IPS o firewalls mal configurados

Hace el tráfico más difícil de analizar

--mtu=8

Define el tamaño máximo de los fragmentos

MTU extremadamente bajo (8 bytes)

Genera muchos fragmentos

Alta evasion, pero:

Mas lento

Más sospechoso en redes modernas

Puede romperse en routers estrictos

-f es equivalente a --mtu=8, aquí se estan reforzando explicitamente.

-D 10.0.2.3,ME:

Decoys (señuelos)

Nmap envía paquetes desde IPs falsas ademas de la real

10.0.2.3 actua como señuelo

ME indica tu IP real

El objetivo ve múltiples orígenes y no sabe cuál es el atacante

Ejemplo en logs del objetivo:

10.0.2.3 SYN

TU_IP SYN

192.168.1.2 Host objetivo

IP privada tipica de red local

Probablemente un equipo dentro de la misma LAN o laboratorio

Resumen en una sola frase:

Nmap realiza un escaneo SYN altamente sigiloso contra 192.168.1.2, usando la interfaz eth0, sin ping ni DNS, fragmentando agresivamente los paquetes y ocultando la IP real mediante señuelos.

Consideraciones importantes:

Este comando es ruidoso a nivel de red, aunque evasivo

Puede disparar alertas en:

Firewalls modernos

IDS/IPS (Snort, Suricata)

No es recomendable en redes reales sin autorizacion

Las capturas de Wireshark que has compartido muestran un escenario muy interesante de analisis de trafico de red, especificamente lo que parece ser un escaneo de puertos (port scanning) que utiliza tecnicas de fragmentación de IP para evadir sistemas de seguridad (como un IDS/IPS).

Escaneo de Puertos con Evasion (Fragmentacion)

Lo más llamativo es que cada intento de conexión TCP no se envia en un solo paquete, sino que está dividido.

Fragmentación IP: Veras lineas que dicen Fragmented IP protocol. El atacante esta dividiendo el encabezado TCP en dos fragmentos pequeños.

El primer fragmento contiene parte del encabezado IP.

El segundo fragmento completa el paquete para formar un [SYN].

Proposito:

Esta es una tecnica clasica de evasion. Algunos firewalls antiguos o sistemas de detección de intrusos no reensamblan los paquetes para inspeccionarlos, por lo que el escaneo pasa "desapercibido" para ellos.

Flujo del Escaneo (Target: 192.168.1.2)

El trafico muestra una secuencia de intentos de conexion desde dos fuentes distintas (10.0.2.3 y 192.168.1.1) hacia el objetivo 192.168.1.2.

Analisis de los Puertos:

En las imagenes se observa que se estan probando varios puertos comunes para ver si estan abiertos:

Puerto 8080 (HTTP Alternativo):

Paquetes 6 y 9. El objetivo responde con [RST, ACK] (Paquete 11), lo que significa que el puerto está cerrado.

Puerto 110 (POP3 - Correo): Paquetes 13 y 16. También responde con [RST, ACK] (Paquete 18). Cerrado.

Puerto 111 (RPCbind):

Paquetes 20 y 23. Curiosamente, aquí vemos un [SYN, ACK] en el paquete 26, lo que indica que el puerto 111 está ABIERTO. Sin embargo, luego aparece un [RST] (paquete 27), posiblemente porque el escaneador cortó la conexión abruptamente (escaneo tipo *Stealth* o *Half-open*).

Puerto 8888: Paquetes 28 y 31. Responde con [RST, ACK]. Cerrado.

Puerto 443 (HTTPS): Paquetes 35 y 38. Intentos de conexión.

Direcciones IP Involucradas:

0.0.0.0 / 255.255.255.255: Al principio (paquete 1) se ve una solicitud DHCP Discover, que es un dispositivo buscando una dirección IP en la red.

192.168.1.1: Kali

Parece ser la puerta de enlace o un equipo en la red local participando en el escaneo.

10.0.2.3: Es una dirección IP de una red distinta (posiblemente una máquina virtual en modo NAT en VirtualBox), que también está enviando fragmentos.

192.168.1.2: Metasploitable2

Es la victima o el objetivo que esta siendo analizado.

Resumen Tecnico:

Estas presenciando un IP Fragmented Port Scan.

Tecnica:

El atacante usa fragmentación de paquetes (ID=0x9ef6, ID=0x5a7b, etc.) para ocultar la bandera SYN del encabezado TCP.

Resultado:

El atacante ya sabe que el puerto 111 está abierto y que los puertos 8080, 110 y 8888 están cerrados.

Herramienta probable: Este tipo de tráfico es muy característico de herramientas como nmap cuando se usan banderas de fragmentación (como -f).

Continuacion del Escaneo de Puertos:

El atacante sigue probando diferentes servicios en la dirección objetivo 192.168.1.2. Los nuevos puertos identificados son:

Puerto 443 (HTTPS):

Paquetes 35 y 38 envian el [SYN] fragmentado. La victima responde con [RST, ACK] en el paquete 39. Estado: Cerrado.

Puerto 23 (Telnet):

Paquetes 42 y 45. En este caso, la víctima responde con un [SYN, ACK] (paquete 46), lo que indica que el puerto 23 está ABIERTO. Inmediatamente después, el atacante envía un [RST] (paquete 47) para cerrar la conexión sin completarla.

Puerto 113 (Ident/Auth):

Paquetes 50 y 53. La víctima responde con [RST, ACK] (paquete 56). Estado: Cerrado.

Puerto 1723 (PPTP VPN):

Paquetes 57 y 60. Responde con [RST, ACK] (paquete 62). Estado: Cerrado.

Puerto 1025 (Microsoft RPC / NFS): Paquetes 64 y 67. Responde con [RST, ACK] (paquete 68). Estado: Cerrado.

Patron de Evasion Detallado:

En las imágenes se observa claramente cómo se manipula la capa de red (IP) para ocultar la capa de transporte (TCP):

Doble Envio:

Cada intento de conexión se envía dos veces, una desde la IP 10.0.2.3 y otra desde 192.168.1.1. Esto sugiere que el atacante podría estar usando decoy IPs (señuelos) para confundir a los administradores de red sobre el origen real del ataque.

Fragmentacion IP:

Fíjate en los paquetes como el 40 y 41. Ambos tienen el mismo ID de identificación (ID=0x23c6).

Offset 0: Contiene la primera parte del paquete.

Offset 8: Contiene el resto del paquete.

Wireshark indica [Reassembled in #42], lo que significa que solo al unir ambos fragmentos se puede ver que se trataba de un paquete TCP dirigido al puerto 23.

Conclusion:

El tráfico analizado es un escaneo de tipo Stealth (o SYN scan) que utiliza fragmentación de IP y posiblemente direcciones señuelo. El atacante ha logrado identificar servicios vulnerables potenciales, como Telnet (23) y RPCbind (111), que suelen ser objetivos comunes debido a su falta de cifrado o configuraciones inseguras.