Defensa IP

Transcribed on July 31, 2025 at 3:47 PM by Minutes AI

Speaker 1 (00:08)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema del ejercicio de ipetables de ataque y defensa, pero en su segunda parte, en esta parte 2 lo que veremos es que todo lo que hemos aplicado de técnicas de protección funciona correctamente una vez que repetimos los ataques.

Bien, pues ahora pasaríamos a la parte de registro, para ver un registro de los intentos de acceso podemos crear este comando de ip tables, hacemos otro input y ahora decimos p tcp deport porque estamos trabajando con el ssh todo el momento, j y esta vez el comando es log, Lo que vamos a hacer es almacenar en el log prefix, simplemente lo que hace es decirle que le va a poner cuando encuentre un acceso en español, en inglés, como queráis, puesto en inglés, por seguir ya un poco todo en inglés, pero ahí puedes poner intentos ssh y se quedaría como la cabecera.

Bien, pues lo aplicamos y ya también lo tenemos registrado y creo que ya no queda nada más.

El último paso sería guardar las reglas, esto es importante porque hemos puesto muchas y las queremos tener almacenada.

Bien, pues ya hemos visto que era iptable save, le pondríamos la ruta que es etc iptables rule si no tuvierais la carpeta por lo que sea, la de iptable rule, pues nada, la creamos y ya está, y así almacenamos las reglas.

Pues bien, ya hemos visto el ataque, nos hemos defendido, vamos a comprobar que todo ha ido bien y que ahora no podemos hacer todo lo que hicimos antes en la secuencia de ataque, así que volvamos al servidor número 1, a la máquina 1 que es el atacante.

Bien, pues el primero será un ping, vamos a hacer un ping a la 10211 55.17 Bien, pues parece que el ping no está funcionando perfecto, eso era uno de nuestros objetivos, que no respondiera ni siquiera al ping, con lo cual ya el ping no funciona contra esa máquina.

Seguimos viendo si lo que hemos implementado como defensa está funcionando.

El siguiente es un nmap, si os acordáis el nmap devolvía el puerto 80, bien pues vamos a probar con nmap, recuerda que era ip y le poníamos la dirección IP 10.21155.17 y a ver qué nos dice esta vez, ya veis que no aparece el puerto como antes, de hecho dice que está arriba pero se está bloqueando con lo cual, perfecto, otro punto más de la securización que hemos implementado ya Nmap ya no devuelve el puerto 80 como activo o como abierto, estamos ocultando los servicios que tenemos detrás de la máquina.

Bien, vamos ahora con la petición HTTP.

Pues haríamos un CUR como ya vimos antes, HTTP 10.

211.

55 17 nada, se queda pensando, no se está devolviendo ningún paquete en la petición, se están perdiendo, con lo cual correcto, no está dando ningún tipo de información, si incluso ponemos el puerto que era el 8000 tampoco lo va a mostrar, con lo cual otro otro check en nuestra parte de defensa, ya tampoco se pueden hacer ningún tipo de consultas a través de HTTP.

Bien, pues ahora vamos a ir por la de establecer una conexión SSH, pues para eso acordáis que lo que hacíamos era sshuser, que lo conocemos ya, ponemos la dirección 10.

211.

55 17 y vemos qué ocurre, directamente nos echa para atrás.

Bien, para probar Hydra y que nos deje conectar y veamos esa definición de limitaciones.

Bueno, antes vamos a probar Hydra tal y como está ahora mismo, si hacemos un recordar que lo que hemos hecho es que no dejamos conexiones SSH a ninguna IP que no sea la que queramos, de hecho pusimos una ficticia que a esa sí le dimos acceso, pero a la 5 que es esta no, Con lo cual si yo hiciera ahora otra vez el ataque de Hydra que era el Siguiente, era TXT SSH 2 puntos 10 millones 211.55 17 Veis, directamente no deja de nada porque está diciendo que no, Pero supongamos por un momento que tenemos esta IP validada para que pueda hacer la conexión SSH por lo que sea, era una IP que ha sido comprometida y desde ahí están intentando acceder.

Vamos a habilitar la dirección IP, antes como visteis habilité una ficticia, pero voy a habilitar ahora esta que es la que en teoría nos está atacando para ver esta limitación, Es decir, voy a habilitar la IP para que permita el acceso desde esta máquina.

Así que voy otra vez al servidor y si os acordáis el comando era este sudo ip tables guión a input y era guión p tcp de port sh Y aquí voy a habilitar, puse una al azar, ahora voy a poner una que es la del atacante por cualquier motivo, el atacante ya tiene acceso aquí, entonces a este sí que le dejaremos hacer la conexión.

Bien, ya he vuelto a habilitar el acceso, ahora sí que le he dado permisos, con lo cual voy a hacer el ssh, acordaros que era user y la IP 10.211.55.17 nos deja acceder, a ver si funciona Hydra esta.

A ver si funciona hydra esta vez.

Vale, pues lo vamos a ejecutar de nuevo luser, ya que vemos que esto funciona, la clave era password, era listado y era la 10.2117.

Comienza el ataque, recordad que la contraseña estaba en el listado, pero ahora no llegará a buen fin porque le hemos puesto ese límite, Fijaros, ha terminado, pero ha terminado porque no le deja seguir continuando con las pruebas, fijaros, no está dejando, no puede volverse a conectar, con lo cual no puede terminar, así que también está correcto, acordaros que la contraseña era batman 123 y esa estaba aquí antes, vimos cómo la encontró, pero en este caso ya lo hemos securizado.

Bien, pues este es un poco el final del ejercicio, como veis hemos comenzado atacando, hemos después fortalecido hacer un hardening, hemos cerrado nuestro servidor, hemos vuelto a hacer las pruebas y hemos visto que todo está resuelto.

Bien, pues hemos visto que resolver este tipo de ejercicios nos proporciona una comprensión muy práctica de la configuración de reglas de un firewall con iptables, y esto se traduce en que somos mucho más versátiles a la hora de proteger una máquina, ya que sabemos que IP tablets está en prácticamente cualquier equipo, con lo cual con estos comandos al menos ya tenemos una primera capa de protección.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.