# Ipetables Defense

Transcribed on July 31, 2025 at 10:40 AM by Minutes AI

Speaker 1 (00:01)

En esta sesión vamos a tratar el tema de ipetables, pero esta vez vamos a proponer un ejercicio práctico que está orientado a la defensa de nuestra arquitectura, es decir, un ejercicio muy práctico que nos va a enseñar a defendernos de diferentes ataques utilizando ipetables.

Pues básicamente es eso, tratar de defender nuestra máquina virtual de una variedad de ataques y para eso nos hará falta tener un entorno de laboratorio en el que es muy sencillo, serán dos máquina virtuales que estén en la misma LAN y también conocer sus direcciones IP, en otras palabras, que ambas máquinas se vean en la misma LAN.

Bien, pues desde el punto de vista del atacante, recordemos que hemos dicho que hay dos máquinas, una que defiende y una que ataca, nos vamos a centrar sobre todo en la que defiende.

Los ataques lo vamos a explicar ahora, son muy fáciles, son muy sencillos de ejecutar, porque realmente solo uno de ellos es realmente un ataque, que es el último, que es el ataque de fuerza bruta en el que usaremos Hydra, pero el primero que es un escaneo de puertos, es muy simple, utilizaremos nmap con el comando más sencillo para escanear los puertos de la máquina que queremos defender, y esto lo haremos desde la máquina atacante.

Después simplemente haremos una petición HTTP para ver algún tipo de servicio web en la máquina que estamos defendiendo, utilizando por ejemplo CUR.

Después haremos una simple y sencilla conexión SSH, lo que haremos será intentar establecer una conexión SSH desde el atacante contra la máquina que estamos defendiendo.

Y ya por último sí que usaremos Hydra.

Hydra es una pequeña aplicación que no permite hacer ataques de fuerza bruta sobre el servicio SSH que es el que está ejecutando el defensor.

Hydra es muy sencillo de usar, ahí podéis ver un ejemplo, solo hay que poner el nombre de usuario con el parámetro L, aquí pondremos el nombre de usuario que queremos probar contra la máquina atacante, aquí podemos suponer incluso que lo sabemos, que ya sabemos cuál es el usuario.

Después pondremos con guión p un fichero txt que es un listado de diferentes contraseñas, esto es lo que se llama en argot un diccionario de contraseñas, aquí puedes poner una gran variedad de diferentes textos que son diferentes contraseñas que Hydra va a intentar utilizar para acceder al servicio ssh.

Y ya finalmente lo único que hay que poner es la dirección IP de de la máquina que está sirviendo el proceso SSH para intentar conectarnos.

Como veis es muy sencillo, solo hay que ejecutarlo y esto lo hacemos para ver si somos capaces de defendernos nosotros de ataques de fuerza bruta, limitando las conexiones, etc.

Esto ya lo vimos en anteriores vídeos.

Bien, pues ahora sí, en la parte de defensa, que es la que vamos a intentar implementar nosotros, tenemos que seguir esos cuatro puntos.

El primero es crear algún tipo de reglas con iptable que nos detecte y nos bloquee cualquier intento de escaneo de puertos, o sea de descubrimiento de pentesting, o sea de que, o sea, evitar dar información nosotros de nuestro sistema.

Después tenemos que bloquear cualquier petición HTTP que no sea lícita o que no permitamos.

Y también tenemos que limitar el acceso a ssh, sólo a IPs conocidas.

Pues bien, ya por último, esto va orientado al tema de Hydra, tenemos que limitar el número de accesos justamente para que no puedan hacer ataques de fuerza bruta, que es lo que hace directamente Hydra.

Y como siempre en cualquier tipo de sistema, como ya he hecho hincapié anteriormente, tenemos que tener siempre un log, un registro, hay que almacenar todo lo que está ocurriendo para después analizarlo y poder aprender de esos problemas y solucionarlos.

Este pequeño esquema lo que intenta es representar gráficamente el entorno y las acciones que vamos a tomar.

Arriba podéis ver que está el atacante y abajo el defensor.

Los cuatro diferentes ataques entre comillas, que son el nmap, el CAR, SSH y hydra, irán contra la máquina que estamos defendiendo, que tiene como herramientas ipetables para evitar cualquiera de esos ataques, pero todo tiene que estar registrado en unos locs, en un sistema de registro.

Bien, pues este ejercicio tiene muchas ventajas, ya que ofrece un escenario real de ataque y defensa.

Además la defensa se realiza utilizando únicamente iptables, una herramienta que podemos encontrar prácticamente en cualquier entorno Linux, y con esto demostramos la eficacia que tiene iptables ante ataques tan populares como los que hemos visto durante el ejercicio.

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