Resumen Ejecutivo:

Rudy Roberto Tito Durand ha sido contratado por Google inc. para llevar a cabo una prueba de penetración con el fin de determinar su exposición a un ataque dirigido. Todas las actividades se realizaron de manera que simulaba a un actor malicioso comprometido en un ataque dirigido contra Google inc., con los siguientes objetivos:

Identificar si un atacante remoto podría penetrar las defensas de Google inc..
Determinar el impacto de una violación de seguridad en:

- La confidencialidad de los datos privados de la empresa.
- La infraestructura interna y la disponibilidad de los sistemas de información de Google inc..

Los esfuerzos se centraron en la identificación y explotación de debilidades de seguridad que podrían permitir a un atacante remoto acceder sin autorización a los datos de la organización. Los ataques se llevaron a cabo con el nivel de acceso que tendría un usuario general de Internet. La evaluación se realizó de acuerdo con las recomendaciones establecidas en el NIST SP 800-1151, y todas las pruebas y acciones se llevaron a cabo en condiciones controladas.

Resumen de los Resultados:

El escaneo de Nmap muestra que www.google.com está en línea con el puerto 80/TCP abierto para el servicio de HTTP. Se identifica la dirección IP 172.217.192.104 y se encontraron 180 puertos filtrados. El escaneo se realizó el 5 de noviembre de 2023 a las 03:00.

Narrativa de Ataque:

[nmap -p 20-200 www.google.com]:

Starting Nmap 7.80 (https://nmap.org) at 2023-11-05 03:00 -05
Nmap scan report for www.google.com (172.217.192.104)
Host is up (0.057s latency).
Other addresses for www.google.com (not scanned): 172.217.192.105 172.217.192.103 172.217.192.106 172.217.192.147 172.217.192.99 2800:3f0:4003:c03::67 2800:3f0:4003:c03::69 2800:3f0:4003:c03::93 2800:3f0:4003:c03::63
rDNS record for 172.217.192.104: cf-in-f104.1e100.net
Not shown: 180 filtered ports
PORT STATE SERVICE
80/tcp open http

Nmap done: 1 IP address (1 host up) scanned in 3.20 seconds

El fragmento de texto es un resultado de un escaneo de Nmap usando el comando `nmap -p 20-200 www.google.com`. Aquí está la interpretación:

1. El escaneo fue realizado por Nmap versión 7.80 y comenzó a las 03:00 del 5 de noviembre de 2023, utilizando la zona horaria -05.

2. El informe muestra que se escaneó la dirección IP correspondiente a www.google.com, que es 172.217.192.104.

3. Según el informe, el host (www.google.com en este caso) está en línea y presenta una latencia de 0.057 segundos.

4. Además de la dirección IP escaneada (172.217.192.104), se proporciona una lista de otras direcciones asociadas a www.google.com que no fueron escaneadas en este momento.

5. Se proporciona una entrada de resolución inversa (rDNS) que indica que la dirección IP 172.217.192.104 se resuelve en el nombre de dominio cf-in-f104.1e100.net.

6. El resultado muestra que 180 puertos fueron filtrados y, por lo tanto, no se pudo determinar su estado.

7. Sin embargo, se muestra un puerto abierto: el puerto 80 en el protocolo TCP está abierto y se identifica como el servicio de HTTP.

8. El escaneo finalizó y se determinó que se escaneó una dirección IP, lo que implica que se escaneó un solo host.

En resumen, el escaneo de Nmap revela que www.google.com está en línea y tiene el puerto 80/TCP abierto para el servicio de HTTP.

Resultados:

Como experto en seguridad informática, puedo inferir que el fragmento de texto anterior es el resultado de un escaneo de seguridad utilizando la herramienta Nmap. El objetivo del escaneo fue analizar la disponibilidad y los servicios ofrecidos por el host www.google.com.

El informe indica que el escaneo comenzó a las 03:00 del 5 de noviembre de 2023, utilizando la zona horaria -05. El escaneo se realizó utilizando el comando "nmap -p 20-200 www.google.com", lo que significa que se escanearon los puertos en el rango del 20 al 200.

El informe revela que www.google.com está en línea y presenta una latencia de 0.057 segundos, lo que indica que el host está accesible y responde con prontitud. La dirección IP asociada a www.google.com es 172.217.192.104.

Además de la dirección IP escaneada, se proporciona una lista de otras direcciones asociadas a www.google.com que no se escanearon en este momento. Esto puede ser útil para futuros análisis y penetration testing.

El escaneo también muestra una entrada de resolución inversa (rDNS), lo que significa que la dirección IP 172.217.192.104 se resuelve en el nombre de dominio cf-in-f104.1e100.net.

En cuanto a los puertos escaneados, se identificó que 180 de ellos estaban filtrados, lo que significa que el estado de los mismos no pudo ser determinado. Sin embargo, se encontró un puerto abierto: el puerto 80 en el protocolo TCP, lo que indica que el host ofrece el servicio de HTTP en ese puerto.

En general, este escaneo de Nmap proporciona información valiosa sobre la disponibilidad y los servicios ofrecidos por el host www.google.com. Como experto en seguridad informática, este tipo de análisis ayuda a identificar posibles vulnerabilidades y asegurar que el sistema esté protegido contra ataques.

Recomendaciones:

Basándome en la información proporcionada en el escaneo de Nmap, aquí están algunas recomendaciones de seguridad informática:

1. Actualiza regularmente tus sistemas y aplicaciones para corregir vulnerabilidades conocidas.

2. Configura un firewall adecuado para filtrar y bloquear tráfico no autorizado.

3. Monitorea y revisa constantemente los registros de actividad de red para detectar actividades sospechosas.

4. Implementa medidas de protección adicionales, como sistemas de detección de intrusos y de prevención de intrusiones.

5. Realiza pruebas de penetración regularmente para identificar y corregir posibles vulnerabilidades.

6. Asegúrate de tener políticas de seguridad sólidas, como contraseñas seguras y cambios regulares de contraseñas.

7. Mantén un seguimiento activo de tus servicios expuestos al público y realiza actualizaciones de seguridad según sea necesario.

8. Educa y capacita a tu personal en prácticas seguras de navegación y uso de sistemas informáticos.

Recuerda que la seguridad informática es un proceso constante. Implementar estas recomendaciones puede mejorar la protección de tus sistemas contra posibles amenazas.