Resumen Ejecutivo:

Rudy ha sido contratado por ACME 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 ACME, con los siguientes objetivos:

Identificar si un atacante remoto podría penetrar las defensas de ACME.
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 ACME.

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 texto describe dos escaneos en un host con IP 192.168.1.1. El primero muestra puertos FTP y Telnet filtrados, y otros como SSH abiertos. El segundo escaneo con `snmpwalk` da timeout, tal vez por firewall o servicio deshabilitado. Otro escaneo con Nikto en puerto 80 detecta falta de banner, encabezados inusuales y posibles vulnerabilidades. Recomienda investigar para mejorar la seguridad del sistema.

Narrativa de Ataque:

[nmap -p 20-1200 192.168.1.1]:

Starting Nmap 7.80 (https://nmap.org) at 2024-06-11 18:53 -05
Nmap scan report for 192.168.1.1
Host is up (0.020s latency).
Not shown: 1175 closed ports
PORT STATE SERVICE
21/tcp filtered ftp
22/tcp open ssh
23/tcp filtered telnet
80/tcp open http
161/tcp filtered snmp
443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds

El comando `nmap -p 20-1200 192.168.1.1` ha sido ejecutado. Este comando utiliza la herramienta Nmap para escanear los puertos en el host con dirección IP 192.168.1.1 en un rango que va desde el puerto 20 hasta el puerto 1200.

La salida del escaneo muestra que el host 192.168.1.1 está activo, con una latencia de 0.020 segundos. También muestra el estado de los puertos escaneados:

- El puerto 21 (FTP) está filtrado
- El puerto 22 (SSH) está abierto
- El puerto 23 (Telnet) está filtrado
- El puerto 80 (HTTP) está abierto
- El puerto 161 (SNMP) está filtrado
- El puerto 443 (HTTPS) está abierto

El escaneo ha finalizado, mostrando que se encontró 1 dirección IP con 1 host activo y ha tardado 1.88 segundos en completarse.

[snmpwalk -v 2c -c public 192.168.1.1]:

El comando no existe o se produjo un error:
Timeout: No Response from 192.168.1.1

El mensaje que has proporcionado indica que se intentó realizar un escaneo utilizando el comando snmpwalk con la versión 2c y la cadena comunitaria "public" en la dirección IP 192.168.1.1, pero no se obtuvo respuesta y se agotó el tiempo de espera (timeout). Esto puede deberse a varias razones, como un problema de configuración en el dispositivo objetivo, un filtrado de puertos, un cortafuegos bloqueando las solicitudes SNMP, o incluso a que el dispositivo no tenga habilitado el servicio SNMP.

Para solucionar este problema, se pueden seguir algunas acciones como verificar la configuración del dispositivo objetivo para asegurarse de que el servicio SNMP esté habilitado y configurado correctamente, revisar si hay algún cortafuegos o filtro de puertos bloqueando el tráfico SNMP, y realizar pruebas desde una red local para descartar problemas de conectividad.

Además, es importante tener en cuenta la seguridad al usar el protocolo SNMP, ya que la cadena comunitaria "public" es una cadena comúnmente utilizada pero

insegura. Se recomienda utilizar cadenas comunitarias más seguras y configurar adecuadamente la seguridad en los dispositivos SNMP.

[nikto -h 192.168.1.1 -Tuning 6]:

- Nikto v2.1.5

+ Target IP: 192.168.1.1
+ Target Hostname: 192.168.1.1
+ Target Port: 80
+ Start Time: 2024-06-11 18:54:31 (GMT-5)

+ Server: No banner retrieved
+ Uncommon header 'content-security-policy' found, with contents: frame-ancestors 'self';default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval';style-src 'self' 'unsafe-inline'
+ Uncommon header 'strict-transport-security' found, with contents: max-age=31536000; includeSubDomains
+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
+ Server banner has changed from '' to 'mini_httpd/1.30 26Oct2018' which may suggest a WAF, load balancer or proxy is in place
Use of each() on hash after insertion without resetting hash iterator results in undefined behavior, Perl interpreter: 0x564d20ed42a0 at /usr/share/perl5/LW2.pm line 947.
+ 51 items checked: 1 error(s) and 5 item(s) reported on remote host
+ End Time: 2024-06-11 18:54:39 (GMT-5) (8 seconds)

+ 1 host(s) tested

El comando `nikto` con la bandera `-h` seguido de la dirección IP `192.168.1.1` y la opción `Tuning 6`, se usó para realizar un escaneo de vulnerabilidades en el host con esa dirección IP y puerto 80. Aquí hay un resumen de los hallazgos:

- El servidor no mostró ningún banner.
- Se encontraron encabezados HTTP poco comunes:
- `content-security-policy` con ciertos valores que limitan la ejecución de scripts y contenido.
- `strict-transport-security` con una política de seguridad de transporte estricta.
- `x-frame-options` que indica que el contenido debe mostrarse en el mismo frame.
- `x-content-type-options` que evita la detección incorrecta del tipo de contenido.
- `x-xss-protection` con protección contra ataques XSS.
- El banner del servidor cambió de vacío a 'mini_httpd/1.30 26Oct2018', lo que puede indicar la presencia de un WAF (Firewall de Aplicaciones Web), un balanceador de carga o un proxy.
- Se identificó un error relacionado con el uso de `each()` en un hash en el archivo `/usr/share/perl5/LW2.pm`.

En resumen, se escanearon 51 elementos en el host, se reportó 1 error y se identificaron 5 aspectos en el servidor. El escaneo comenzó a las 18:54:31 y terminó en 8 segundos, probando un solo host.

Resultados:

Como experto en seguridad informática y pentesting, mi interpretación de este texto se centra en la descripción de dos escaneos realizados en un host con la dirección IP 192.168.1.1. En el primer escaneo con el comando `nmap -p 20-1200 192.168.1.1`, se identificó la activación del host con una latencia de 0.020 segundos. Se encontraron los puertos 21 (FTP) y 23 (Telnet) como filtrados, lo que puede indicar que hay un firewall bloqueando el acceso a estos servicios. Por otro lado, los puertos 22 (SSH), 80 (HTTP), 443 (HTTPS) y 161 (SNMP) estaban abiertos o filtrados. La presencia de puertos abiertos como SSH, HTTP y HTTPS indica posibles servicios en funcionamiento, mientras que los puertos filtrados sugieren una configuración más restrictiva para esos servicios.

En un segundo escaneo utilizando el comando `snmpwalk` con la cadena comunitaria "public" en la misma IP, se experimentó un timeout sin respuesta. Esto puede ser debido a varias razones, como una configuración incorrecta, filtrado de puertos, bloqueo de SNMP por un firewall o la deshabilitación del servicio. Se recomienda investigar más a fondo la causa de esta falta de respuesta para garantizar la correcta configuración y seguridad del servicio SNMP.

Por último, se llevó a cabo un escaneo de vulnerabilidades en el puerto 80 del host con la IP 192.168.1.1 utilizando el comando `nikto -h 192.168.1.1 -Tuning 6`. En este análisis se detectó la ausencia de un banner, algunos encabezados HTTP inusuales que podrían obstaculizar la ejecución de scripts, y un cambio en el banner que sugiere la posible presencia de un WAF, balanceador de carga o proxy. Se identificó un error en un archivo específico, se analizaron 51 elementos, se encontró 1 error y se reportaron 5 aspectos relacionados con el servidor. Esto sugiere posibles vulnerabilidades o configuraciones inseguras en el servidor web alojado en el puerto 80.

En resumen, estos resultados revelan información valiosa sobre la configuración y seguridad del host escaneado, señalando posibles áreas de mejora y vulnerabilidades que requieren atención para fortalecer la seguridad del sistema.

Recomendaciones:

Basándonos en la información proporcionada, aquí tienes algunas recomendaciones de seguridad informática:

1. **Configuración de firewall:** Dado que los puertos 21 (FTP), 23 (Telnet) y 161 (SNMP) fueron detectados como filtrados, es importante revisar la

configuración del firewall para asegurarse de que solo los servicios necesarios estén permitidos y que los puertos no esenciales estén correctamente bloqueados.

2. **Seguridad en SNMP:** Ante la falta de respuesta al intentar acceder mediante SNMP con la cadena comunitaria "public", sería recomendable revisar la configuración de SNMP en el host, evitar el uso de cadenas comunitarias genéricas y establecer medidas de seguridad adicionales, como limitar el acceso a la información sensible.

3. **Escaneo de vulnerabilidades:** Como se identificó la presencia de encabezados HTTP inusuales y un posible cambio en el banner relacionado con un WAF, balanceador de carga o proxy en el puerto 80, es esencial realizar escaneos regulares de vulnerabilidades en el servidor para identificar posibles puntos débiles y aplicar las correcciones necesarias.

4. **Banner e información reveladora:** Dado que se observó la ausencia de un banner y la presencia de un banner específico durante el escaneo en el puerto 80, se recomienda revisar la configuración del servidor web para asegurarse de que la información revelada públicamente sea la mínima necesaria y no revele detalles sensibles.

5. **Actualización y monitoreo constante:** Mantener actualizados todos los servicios y aplicaciones en el servidor, además de monitorear de forma constante la seguridad y la integridad del sistema, es crucial para prevenir posibles brechas de seguridad y asegurar la protección de la red.

Estas recomendaciones pueden ayudar a fortalecer la seguridad del sistema y a prevenir potenciales vulnerabilidades o problemas de configuración en el entorno de red.