Resumen Ejecutivo:

3GPTesting 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 dominio www.unsa.edu.pe fue sometido a un escaneo de puerto, donde se descubrió que de los puertos 20 a 1200, solo los puertos 80 y 443 estaban abiertos. Un intento de ping a la misma dirección resultó en una pérdida total de paquetes.

Narrativa de Ataque:

[nmap -p 20-1200 www.unsa.edu.pe]:

Starting Nmap 7.80 (https://nmap.org) at 2023-11-05 22:18 -05
Nmap scan report for www.unsa.edu.pe (45.231.83.3)
Host is up (0.045s latency).
Not shown: 1178 filtered ports
PORT STATE SERVICE
80/tcp open http
113/tcp closed ident
443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 7.19 seconds

El texto es la salida de un escaneo de puerto usando la herramienta Nmap. Esta herramienta se utiliza regularmente para auditorías de seguridad y la detección de servicios o servidores en una red. El comando utilizado para este proceso ha especificado un rango de puertos de 20 a 1200 en el dominio www.unsa.edu.pe.

Según la salida obtenida:

- El servidor www.unsa.edu.pe está en línea (Host is up) con una latencia de 0.045 segundos.
- De los puertos escaneados, 1178 fueron filtrados (probablemente cerrados o no responden a ningún intento de conexión).
- Los puertos 80 y 443 están abiertos. Estos son típicamente usados ??por los protocolos HTTP y HTTPS, respectivamente, lo que sugiere que este servidor está alojando un sitio web.
- El puerto 113 (generalmente usado por el servicio Ident) está cerrado.

El escaneo tomó un total de 7.19 segundos para completarse. Teniendo estos puertos abiertos no necesariamente significa una vulnerabilidad pero siempre es una buena práctica asegurarse de que solo los puertos necesarios para las operaciones del servidor estén abiertos y que cualquier puerto innecesario esté seguro y cerrado.

[ping -c10 www.unsa.edu.pe]:

El comando no existe o se produjo un error:
PING www.unsa.edu.pe (45.231.83.3) 56(84) bytes of data.

--- www.unsa.edu.pe ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9221ms

El resultado del comando "ping -c10 www.unsa.edu.pe" indica que se intentó hacer un ping a la dirección www.unsa.edu.pe 10 veces. Cada ping intenta enviar 56 bytes de data a la dirección especificada y después espera una respuesta de ese host.

Desafortunadamente, todos los paquetes enviados (10 en total) fueron perdidos. Esto se evidencia por el "100% packet loss" que significa que ninguna respuesta fue recibida de www.unsa.edu.pe. Los paquetes perdidos podrían ser debido a varias razones, como problemas de red o firewall que bloquean los paquetes ICMP (Internet Control Message Protocol), los cuales se utilizan en el comando ping.

El "time 9221ms" indica el tiempo total que tardó el comando ping en completarse, el cual es 9221 milisegundos.

Un resumen de este resultado sería que no se pudo establecer una conexión con www.unsa.edu.pe utilizando el comando ping.

Resultados:

En base a los textos presentados, miraremos algunos puntos específicos:

1. Nmap: Se realizó un escaneo de seguridad con Nmap a la dirección www.unsa.edu.pe en los puertos 20 a 1200. El escaneo reveló que el único puerto abierto es 80 y 443. El puerto 80 y 443 son usados típicamente por los protocolos HTTP y HTTPS, sugiriendo que el dominio está alojando un sitio web. El hecho de que estos puertos están abiertos no es necesariamente una mala práctica, siempre y cuando se le apliquen las medidas de seguridad necesarias. Por otro lado, el puerto 113, usado por el servicio Ident, está cerrado y no representa una vulnerabilidad. Por último, se menciona que el host está activo y la latencia de conexión a este es de 0.045 segundos.

2. Ping: A continuación, se realizó un comando ping a la misma dirección www.unsa.edu.pe pero no se obtuvo ninguna respuesta, indicando una pérdida de paquetes del 100%. Esto puede suceder por varias razones como problemas en la red, o la dirección IP objetivo puede estar bloqueando paquetes ICMP utilizados por el comando ping.

En resumen, parece ser que el servidor www.unsa.edu.pe tiene habilitado los servicios web pero bloquea los pings o está experimentando problemas de red.

Recomendaciones:

1. Mantén Actualizado el Sistema: Asegúrate de que todos tus sistemas y software estén actualizados, pues las actualizaciones suelen incluir parches para vulnerabilidades de seguridad recién descubiertas.

2. Seguridad en Puertos: Implementa políticas de seguridad de red para cerrar y bloquear puertos innecesarios, o configurarlos adecuadamente si deben dejar abiertos puertos (como 80 y 443).

3. Protocolos Seguros: Utiliza siempre protocolos de comunicación seguros (como HTTPS en lugar de HTTP) para proteger la integridad y la confidencialidad de los datos durante su transmisión.

4. Monitoreo Constante: Realiza periódicamente escaneos y auditorías de red para detectar posibles amenazas y vulnerabilidades.

5. Gestión de Firewall: Se ha observado que los paquetes ICMP están siendo bloqueados. Asegúrate de que tu firewall solo está bloqueando tráfico que realmente necesitas bloquear.

6. Crea un Plan de Respuesta: En caso de que se detecte una amenaza o brecha de seguridad, debes tener un plan de acción que detenga el ataque lo más rápido posible, minimice el daño y recupere el sistema a su estado seguro normal.