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:

Los resultados muestran posibles problemas de seguridad en www.unsa.edu.pe. El escaneo de Nmap revela puertos HTTP/HTTPS abiertos, pero el ping falló, posiblemente por un firewall. El uso de credenciales predeterminadas representa un riesgo de seguridad grave.

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.

[fuente propia]:

se descubrio que se usaban credenciales por defecto, como admin y 1234

Esto significa que los usuarios o administradores de un sistema o red están utilizando contraseñas y nombres de usuario predeterminados, como "admin" para el nombre de usuario y "1234" para la contraseña. Este es un problema de seguridad grave, ya que estos son generalmente los primeros conjuntos de credenciales que un atacante probará al intentar acceder a un sistema. Esto pone al sistema en un riesgo altísimo de ser violado y explotado. Utilizar credenciales seguras y únicas, y cambiar las que se proporcionan por defecto, es esencial para la seguridad cibernética.

Resultados:

Como experto en seguridad informática, mi interpretación global del texto introducido implica varias preocupaciones de seguridad y posibles vectores de ataque:

1. Primero, el escaneo de puerto Nmap indica que el servidor www.unsa.edu.pe está en línea. El puerto 80 y el puerto 443 están abiertos, lo que sugiere que está alojando un sitio web accesible tanto en protocolos HTTP como HTTPS. Sin embargo, también muestra que muchos otros puertos están filtrados, posiblemente cerrados o no respondiendo. Esto puede ser una política de seguridad para reducir la superficie de ataque, pero debe verificarse.

2. A pesar de esto, los pings al mismo servidor www.unsa.edu.pe están fallando, indicando una posible inconsistencia. Esto podría deberse a las prácticas de seguridad de bloqueo de paquetes ICMP, algún problema de red, u otra configuración en el servidor que esté interfiriendo con el comando ping.

3. Finalmente, se menciona el uso de contraseñas y nombres de usuario predeterminados, que es una falla o negligencia de seguridad. Los atacantes a menudo intentarán usar estas credenciales comunes para intentar acceder a un sistema. Aquellos a cargo de la seguridad del sistema deberían ser instados a cambiar estos valores predeterminados a conjuntos de credenciales seguros y únicos.

En general, estos resultados demuestran la importancia de una seguridad informática sólida y las múltiples dimensiones a tener en cuenta al evaluar la seguridad de un sistema.

Recomendaciones:

1. Mantenga actualizado: Asegúrese de que todos los sistemas operativos y aplicaciones estén actualizados con los últimos parches de seguridad.

2. Monitoreo de Puertos: Monitoree regularmente los puertos abiertos y asegúrese de cerrar todos los puertos no esenciales. Cualquier puerto innecesario debe estar seguro y cerrado.

3. Hardening: Realizar 'hardening' de sus sistemas. Esto incluye la desactivación de servicios innecesarios, la eliminación de cuentas de usuario innecesarias y la configuración de firewalls.

4. Contraseñas: No utilice contraseñas y nombres de usuario por defecto. Siempre utilice contraseñas robustas y únicas y cambie regularmente estas contraseñas.

5. Firewall: Configurar un firewall adecuado que pueda bloquear conexiones no deseadas.

6. Monitoreo de Red: Realice un monitoreo regular de la red y revise los registros para detectar cualquier actividad sospechosa.

7. Autenticación: Implementar una autenticación de dos factores siempre que sea posible.

8. Conciencia de Seguridad: Brinde capacitación regular en seguridad de la información a todos los usuarios del sistema.

9. Pruebas Regulares: Realizar pruebas de penetración y auditorías de seguridad regulares para identificar y solucionar cualquier vulnerabilidad existente.

10. Respuesta a Incidentes: Tener un plan de respuesta a incidentes de seguridad listo para cualquier eventualidad.