

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:

La interpretación de todo el texto es que se ha detectado un riesgo de seguridad en la página web debido al uso de las credenciales por defecto "admin" y "1234". Se recomienda cambiar las credenciales por unas más seguras y realizar pruebas de penetración para identificar y corregir vulnerabilidades.

Narrativa de Ataque:

[nmap -p 20-1200 192.168.0.100]:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-05 15:16 -05
Nmap scan report for 192.168.0.100
Host is up (0.023s latency).
Not shown: 1178 closed ports
PORT STATE SERVICE
23/tcp open telnet
53/tcp open domain
80/tcp open http
```

Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds

El fragmento de texto es una salida de un escaneo realizado con la herramienta Nmap. El comando utilizado fue "nmap -p 20-1200 192.168.0.100", lo que indica que se escaneó el rango de puertos desde el 20 hasta el 1200 en la dirección IP 192.168.0.100.

La salida del escaneo muestra que el host en la dirección IP 192.168.0.100 está activo, ya que responde a los paquetes enviados por Nmap con una latencia de 0.023 segundos.

De los puertos escaneados, se muestra el estado y el servicio asociado a cada uno. En este caso, se encontraron los siguientes puertos abiertos:

- Puerto 23/tcp: está abierto y se identifica como el servicio Telnet.
- Puerto 53/tcp: está abierto y se identifica como el servicio de dominio (DNS).
- Puerto 80/tcp: está abierto y se identifica como el servicio HTTP.

La última línea indica que se ha terminado el escaneo, se ha escaneado una dirección IP y se encontró un host activo. El escaneo en total tomó 0.91 segundos.

[ping -c10 192.168.0.100]:

```
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=63 time=4.32 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=63 time=4.16 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=63 time=4.57 ms
64 bytes from 192.168.0.100: icmp_seq=4 ttl=63 time=4.16 ms
64 bytes from 192.168.0.100: icmp_seq=5 ttl=63 time=4.99 ms
64 bytes from 192.168.0.100: icmp_seq=6 ttl=63 time=4.70 ms
64 bytes from 192.168.0.100: icmp_seq=7 ttl=63 time=4.11 ms
64 bytes from 192.168.0.100: icmp_seq=8 ttl=63 time=7.32 ms
64 bytes from 192.168.0.100: icmp_seq=9 ttl=63 time=4.21 ms
64 bytes from 192.168.0.100: icmp_seq=10 ttl=63 time=4.10 ms
```

--- 192.168.0.100 ping statistics ---

10 packets transmitted, 10 received, 0% packet loss, time 9010ms
rtt min/avg/max/mdev = 4.095/4.664/7.321/0.929 ms

El fragmento de texto corresponde a una salida de la herramienta de línea de comandos "ping" que envía paquetes de solicitud de eco ICMP a la dirección IP 192.168.0.100.

Aquí hay una explicación de cada línea relevante:

- "PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data." indica que se está enviando una solicitud de eco ICMP a la dirección IP 192.168.0.100 y que los paquetes tienen un tamaño de 56 bytes (incluyendo la cabecera).

- "64 bytes from 192.168.0.100: icmp_seq=1 ttl=63 time=4.32 ms" muestra una respuesta del host 192.168.0.100 indicando que ha recibido el paquete correctamente. También muestra el número de secuencia del paquete ICMP, el valor del TTL (Tiempo de Vida) del paquete y el tiempo de respuesta en milisegundos.

- "--- 192.168.0.100 ping statistics ---" indica el inicio de las estadísticas de ping.

- "10 packets transmitted, 10 received, 0% packet loss, time 9010ms" muestra que se transmitieron y recibieron correctamente 10 paquetes de eco ICMP sin pérdida de paquetes. El tiempo total de ejecución fue de 9010 milisegundos.

- "rtt min/avg/max/mdev = 4.095/4.664/7.321/0.929 ms" proporciona información sobre los tiempos de ida y vuelta (RTT) de los paquetes ICMP. "min" representa el tiempo mínimo, "avg" representa el tiempo promedio, "max" representa el tiempo máximo y "mdev" representa la desviación estándar de los tiempos de respuesta en milisegundos. En este caso, el tiempo mínimo fue de 4.095 ms, el tiempo promedio fue de 4.664 ms, el tiempo máximo fue de 7.321 ms y la desviación estándar fue de 0.929 ms.

[fuente propia]:

se detecto que usa las credenciales por defecto en el login de su web : admi y 1234

Según la información proporcionada, se ha detectado que el sistema utiliza las credenciales por defecto en el login de su página web, con el nombre de usuario "admi" y la contraseña "1234". Esto es un riesgo de seguridad, ya que las credenciales por defecto son conocidas por muchas personas y pueden ser utilizadas para acceder ilegalmente a su sistema. Se recomienda encarecidamente cambiar las credenciales por defecto y utilizar combinaciones seguras de nombre de usuario y contraseña para mejorar la seguridad de su sistema.

[fuente propia]:

se detecto que usa las credenciales por defecto en el login de su web : admin y 1234

Este fragmento de texto indica que se ha detectado que en la página web en cuestión se están utilizando las credenciales por defecto para el inicio de sesión, que son "admin" y "1234". Esto puede representar un riesgo de seguridad, ya que las credenciales por defecto son ampliamente conocidas y pueden facilitar el acceso no autorizado a la web. Como asistente experto en seguridad informática, recomendaría encarecidamente cambiar las credenciales por defecto por unas más seguras y difíciles de adivinar. Esto puede incluir el uso de contraseñas más complejas, combinaciones únicas de caracteres y la implementación de políticas de autenticación más rigurosas. Además, es importante llevar a cabo un monitoreo constante de la seguridad de la aplicación y realizar pruebas de penetración regulares para identificar y remediar posibles vulnerabilidades.

Resultados:

Mi interpretación como experto de todo el texto introducido previamente es que se trata de una salida de un escaneo realizado con la herramienta Nmap, específicamente el comando "nmap -p 20-1200 192.168.0.100" para escanear el rango de puertos desde el 20 hasta el 1200 en la dirección IP 192.168.0.100.

El escaneo reveló que el host en la dirección IP 192.168.0.100 está activo y responde a los paquetes con una latencia de 0.023 segundos.

Además, se identificaron tres puertos abiertos y se asociaron con los siguientes servicios: el puerto 23/tcp con Telnet, el puerto 53/tcp con el servicio DNS y el puerto 80/tcp con HTTP.

Por último, se muestra una línea indicando el final del escaneo, se escaneó una dirección IP y se encontró un host activo. El escaneo en total tomó 0.91 segundos.

Como experto en seguridad informática, puedo inferir que este escaneo fue realizado con el fin de verificar la disponibilidad y los servicios activos en el host escaneado. La presencia de servicios como Telnet, DNS y HTTP puede tener implicaciones en la seguridad del sistema, ya que estas aplicaciones pueden presentar vulnerabilidades conocidas. Es importante realizar análisis y pruebas de seguridad adicionales, así como implementar medidas de seguridad adecuadas, como actualizar y parchear los sistemas, configurar correctamente los servicios y utilizar autenticación segura, para mitigar los posibles riesgos de seguridad identificados.

Recomendaciones:

Basado en la información proporcionada, aquí están algunas recomendaciones de seguridad informática:

1. Realiza escaneos de seguridad regulares en tu red y sistemas utilizando herramientas como Nmap para identificar puertos abiertos y posibles vulnerabilidades.
2. Mantén los sistemas y aplicaciones actualizados con los últimos parches de seguridad. Esto ayudará a mitigar posibles riesgos conocidos.

3. Evita el uso de credenciales por defecto y utiliza combinaciones seguras de nombre de usuario y contraseña. Asegúrate de que las contraseñas sean complejas y únicas para cada cuenta.
4. Implementa medidas de control de acceso adecuadas, como autenticación de dos factores y políticas de bloqueo de cuentas en caso de intentos de inicio de sesión fallidos.
5. Realiza pruebas de penetración y auditorías de seguridad de forma regular para identificar y solucionar posibles vulnerabilidades.
6. Educa y concientiza a los usuarios sobre las mejores prácticas de seguridad, como la importancia de no compartir información confidencial y no hacer clic en enlaces o descargar archivos sospechosos.
7. Utiliza soluciones de seguridad, como firewalls, antivirus y sistemas de detección y prevención de intrusiones, para proteger tus sistemas y datos contra amenazas externas.
8. Mantén copias de seguridad regulares de tus datos críticos en caso de incidentes de seguridad o pérdida de información.
9. Establece políticas de seguridad y cumplimiento que regulen y promuevan prácticas seguras dentro de la organización.
10. Considera la contratación de expertos en seguridad informática para evaluar y fortalecer aún más la postura de seguridad de la organización.