Resumen Ejecutivo:

Rudy Tito ha sido contratado por UNSA 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 UNSA, con los siguientes objetivos:

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

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 red revela que el host 192.168.0.100, con nombre "DD-WRT", tiene los puertos 23/tcp (telnet), 53/tcp (DNS) y 80/tcp (HTTP) abiertos. El análisis de ping muestra 0% de pérdida de paquetes y los tiempos de respuesta mínimo, promedio y máximo. Se encontró un archivo de contraseñas en la ruta 192.168.0.100/passwords.txt que requerirá protección adecuada.

Narrativa de Ataque:

[nmap -p 20-1200 192.168.0.100]:

Starting Nmap 7.80 (https://nmap.org) at 2023-11-09 09:05 -05
Nmap scan report for DD-WRT (192.168.0.100)
Host is up (0.014s 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 0.48 seconds

El fragmento de texto corresponde a la salida de un escaneo de red realizado con la herramienta Nmap. El comando utilizado fue "nmap -p 20-1200 192.168.0.100", lo que indica que se escanearon los puertos desde el 20 hasta el 1200 en la dirección IP 192.168.0.100.

La salida muestra que el escaneo se realizó con éxito y se obtuvo un informe de escaneo para el host con nombre "DD-WRT" y dirección IP 192.168.0.100. El host se encuentra activo, con una latencia de respuesta de 0.014 segundos.

Se indican los puertos abiertos en el host, que son:

- El puerto 23/tcp está abierto y se identifica como el servicio de "telnet".
- El puerto 53/tcp está abierto y se identifica como el servicio de "domain" (DNS).
- El puerto 80/tcp está abierto y se identifica como el servicio "http" (HTTP).

Además, se indica que hay 1178 puertos cerrados que no se muestran en la salida.

Finalmente, se informa que se ha completado el escaneo de 1 dirección IP (1 host activo) en un tiempo de 0.48 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=64 time=1.72 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=1.72 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=1.71 ms
64 bytes from 192.168.0.100: icmp_seq=4 ttl=64 time=1.76 ms
64 bytes from 192.168.0.100: icmp_seq=5 ttl=64 time=1.84 ms
64 bytes from 192.168.0.100: icmp_seq=6 ttl=64 time=1.77 ms
64 bytes from 192.168.0.100: icmp_seq=7 ttl=64 time=1.74 ms
64 bytes from 192.168.0.100: icmp_seq=8 ttl=64 time=1.88 ms
64 bytes from 192.168.0.100: icmp_seq=9 ttl=64 time=1.79 ms
64 bytes from 192.168.0.100: icmp_seq=10 ttl=64 time=1.77 ms

--- 192.168.0.100 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 1.711/1.769/1.879/0.052 ms

El comando "ping -c10 192.168.0.100" se utiliza para enviar 10 paquetes ICMP de prueba de conectividad a la dirección IP 192.168.0.100.

En la respuesta, cada línea representa una respuesta ICMP recibida del host 192.168.0.100. Cada respuesta muestra el tamaño de los datos enviados, la dirección IP de origen, un número de secuencia, el tiempo de vida (TTL) y el tiempo de respuesta en milisegundos.

Al final del resultado, se muestra un resumen de las estadísticas del comando ping. En este caso, se transmitieron 10 paquetes, se recibieron los 10 sin pérdida de paquetes (0% de pérdida), el tiempo total de prueba fue de 9015 ms y se muestran estadísticas adicionales sobre los tiempos de respuesta mínimo, promedio, máximo y la desviación estándar.

[fuente propia]:

se encontro un archivo llamado passwords en el host , el cual se accede a 192.168.0.100/passwords.txt , posee ids y passwords

Basado en la información proporcionada, parece que encontraste un archivo llamado "passwords" en el host con la dirección IP 192.168.0.100. Este archivo se puede acceder a través de la ruta 192.168.0.100/passwords.txt y contiene identificaciones (IDs) y contraseñas. Es importante tener en cuenta que la seguridad de este archivo debe ser evaluada y, si es necesario, tomar medidas para protegerlo adecuadamente para evitar el acceso no autorizado a la información confidencial contenida en él.

Resultados:

Como experto en seguridad informática, mi interpretación de todo el texto previamente mencionado es la siguiente:

1. Se realizó un escaneo de red utilizando la herramienta Nmap para la dirección IP 192.168.0.100. El escaneo mostró que el host DD-WRT está activo y responde con un tiempo de latencia de 0.014 segundos.

2. Se identificaron puertos abiertos en el host: el puerto 23/tcp está abierto para el servicio telnet, el puerto 53/tcp está abierto para el servicio DNS y el puerto 80/tcp está abierto para el servicio HTTP.

3. Además, hubo 1178 puertos cerrados que no se mostraron en la salida del escaneo.

4. Se realizó una prueba de conectividad (ping) a la dirección IP 192.168.0.100, enviando 10 paquetes ICMP. Los resultados mostraron que los 10 paquetes fueron recibidos sin pérdida y se proporcionaron estadísticas adicionales sobre los tiempos de respuesta.

5. Se encontró un archivo llamado "passwords" en la ruta 192.168.0.100/passwords.txt. Este archivo contiene ID y contraseñas, lo que indica un posible riesgo de seguridad. Se recomienda evaluar la seguridad de este archivo y tomar medidas para protegerlo adecuadamente para evitar el acceso no autorizado.

En general, se sugiere mejorar la seguridad del host y la red, considerando la posible exposición de servicios como telnet y HTTP, y revisando la protección de archivos sensibles como "passwords.txt".

Recomendaciones:

Basado en la información proporcionada, te recomendaría lo siguiente:
1. Asegúrate de tener contraseñas seguras y únicas para todos tus sistemas y servicios.
2. Realiza regularmente escaneos de red para identificar puertos abiertos y vulnerabilidades en tus sistemas.
3. Mantén actualizados tus sistemas y aplicaciones con los últimos parches de seguridad.
4. Implementa medidas de seguridad como firewalls y sistemas de detección de intrusiones.
5. Protege adecuadamente los archivos y datos confidenciales, limitando el acceso y utilizando cifrado si es necesario.
6. Realiza copias de seguridad de forma regular y almacénalas en ubicaciones seguras.
7. Educa a los usuarios sobre las prácticas de seguridad, como no hacer clic en enlaces sospechosos o abrir archivos adjuntos desconocidos.
8. Mantente actualizado sobre nuevas amenazas y vulnerabilidades, y adapta tus medidas de seguridad en consecuencia.