Universidad Nacional Autónoma de México
Facultad de Ciencias
Criptografía y Seguridad
Práctica 4. SSH multiverse
Semestre 2023-2

Anayanzi Martínez
Fernando Fong
Ivan Galindo

1. Introducción

SSH (Secure Shell) es un protocolo utilizado para establecer una conexión segura y cifrada entre dos dispositivos a través de una red. Se usa comúnmente para el acceso remoto y la administración de servidores y otros equipos conectados. Una de las características clave de SSH es su uso del cifrado para proteger los datos a medida que se transmiten entre dispositivos. Esto ayuda a evitar el acceso no autorizado o que se intercepte información confidencial.

Proteger el servicio SSH es fundamental para garantizar la seguridad de los dispositivos y datos de la red. SSH es un objetivo común para los actores de amenazas porque proporciona una puerta de acceso. Si el servicio SSH se ve comprometido, un atacante podría tomar el control de los dispositivos de red, lo que puede provocar filtraciones de datos, interrupciones del sistema u otros incidentes de seguridad.

El objetivo de esta práctica es conocer y practicar los ataques de diccionario, aprovechando el descuido de los usuarios y una mala implementación de una política para establecer contraseñas seguras.

2. Historia

Se dieron cuenta que los ayudantes tienen un servidor con IP **`44.199.201.139`** y utilizan SSH para administrarlo. Les da curiosidad saber si ahí se encuentra el examen y las respuestas. Por alguna razón todos los inscritos tienen un usuario en el servidor que consiste en su número de cuenta, sólo que no conocen la contraseña. El objetivo es obtener la contraseña y dejar una pequeña huella de que estuvieron ahí.

3. Procedimiento

- Escanear el objetivo:
  Se pueden ocupar técnicas de OSINT si así lo consideran y luego recopilación de información puertos y servicios (utilizando `Nmap` por ejemplo).

- Atacar el objetivo:
  Obtener mediante un ataque de diccionario la contraseña correspondiente a su usuario (utilizando `Hydra` por ejemplo).

- Crear evidencia de haber entrado al sistema:
  La parte más sencilla, basta que ejecuten `$ touch $NumeroDeCuenta` para dejar registro que estuvieron ahí

- ***EXTRA*** Post-explotación:
  Ahora que se tiene un acceso al servidor, ¿qué más se puede hacer?
  Intentar ir más allá, aquí algunas ideas:

  1. Cambiar la contraseña de todos a algo más fácil… o más difícil
  2. Obtener información confidencial contenida en el servidor
  3. Escalar privilegios.
  4. Comprometer otra cuenta
  5. Infectar con algún tipo de malware el servidor (Ransomware por ejemplo)
  6. Minar criptomonedas
  7. Instalar un servidor de minecraft
  8. Instalar un servidor web aprovechando que tiene IP pública
  9. Alguna otra cosa…

4. Entregables

Un PDF con la documentación de todo lo realizado incluyendo capturas de pantalla. Esto incluye todos los puertos y servicios disponibles, cómo hicieron el ataque de diccionario y cómo dejaron huella en el servidor. De igual manera es importante documentar todos sus descubrimientos y, en caso de existir, las dificultades que hayan encontrado y los intentos no exitosos que hayan realizado. Finalmente, incluir los usuarios y contraseñas de los 2 integrantes del equipo con los que entraron al servidor.

Para aquellos que hayan realizado la parte extra, documentar qué fue lo que hicieron y sus descubrimientos.

5. Notas

¡Importante! Ataques de denegación de servicio están explícitamente prohibidos. El servidor tiene que estar disponible para todos.

Aprovechen las 2 semanas y las ayudantías para hacer preguntas, no lo dejen al final.

Está planeado para ser un reto y no ser tan trivial. Hay que tener paciencia y, en su caso, se podrán dar pistas pero debe haber un avance y exponer lo que se haya intentado.

Diviértanse :)