UNIVERSIDAD DE GUAYAQUIL

INGENIERIA INDUSTRIAL

INGENIERÍA EN SISTEMAS DE INFORMACIÓN

TALLER 5

TÍTULO

RESUMEN DEL ARTÍCULO “HABLEMOS DE SPOOFING”

ALUMNO:

MADELINE MUÑOZ VILLEGAS

MATERIA:

SEGURIDAD DE SISTEMAS INFORMÁTICOS

DOCENTE:

ING. OTTO GONZALES MENDOZA

CURSO:

8VO SEMESTRE NOCTURNO

AÑO LECTIVO:

CICLO I

2023-2024

Desarrollo

El spoofing es una técnica de suplantación de identidad utilizada en seguridad de redes con fines maliciosos o de investigación. Consiste en falsificar el origen de los paquetes de datos para que la víctima crea que provienen de un host de confianza o autorizado, evitando así su detección. Se utilizan principalmente tres tipos de spoofing en este contexto:

1. ARP Spoofing: Se falsifica la dirección MAC asociada a una dirección IP en una red local para redirigir el tráfico a un host malicioso en lugar del destino legítimo.

2. IP Spoofing: Se falsifica la dirección IP origen de un paquete TCP/IP para hacer creer que proviene de otra fuente, lo que puede utilizarse para engañar a la víctima y comprometer la seguridad de la comunicación.

3. TCP Spoofing: Es un tipo de ataque que aprovecha las vulnerabilidades del protocolo TCP para suplantar la personalidad de otro host y establecer una comunicación falsa con un tercero.

El IP Spoofing puede ser utilizado para varios fines, como el secuestro de sesiones, ataques de negación de servicio (DoS) y ataques de hombre en el medio (man-in-the-middle). Los ataques pueden ser de dos tipos:

- Non-Blind Spoofing: El atacante está en la misma subred que la víctima, lo que facilita el acceso a la secuencia y números de reconocimiento de los paquetes. El secuestro de sesión es una de las amenazas más comunes en este tipo de ataque.

- Blind Spoofing: En este caso, el atacante no puede acceder fácilmente a la secuencia y números de reconocimiento, lo que dificulta el ataque. Sin embargo,

mediante el envío de múltiples paquetes con diferentes números de secuencia, el atacante puede intentar comprometer los datos enviados al objetivo.

El spoofing también se utiliza en ataques de denegación de servicio (DOS) para inundar a la víctima con una gran cantidad de paquetes en un corto período de tiempo, dificultando su detección y mitigación. Cuando varios hosts comprometidos participan en el ataque y envían tráfico spoofeado, el ataque se vuelve más efectivo rápidamente.