Práctica 1. Análisis forense de correo electrónico.

El correo electrónico es uno de los métodos de comunicación más comunes en la actualidad. Los sitios de redes sociales han comenzado recientemente a superar al correo electrónico, pero las redes sociales todavía se utilizan principalmente en comunicaciones privadas.

Las empresas utilizan el correo electrónico para comunicarse con clientes futuros, actuales y pasados.

- Las empresas utilizan el correo electrónico para brindar servicio al cliente, soporte de productos y comunicación continua sobre cambios de productos o políticas.
- Las aplicaciones del servicio de asistencia reciben correos electrónicos para iniciar tickets de problemas.
- Las computadoras y las aplicaciones envían alertas por correo electrónico a los administradores.

Por un momento, piensa en cómo te afectaría si el correo electrónico dejara de funcionar por un día.

El correo electrónico no se diseñó originalmente teniendo en cuenta la seguridad. Originalmente fue diseñado para enviar mensajes de texto a personas designadas en una sola máquina y luego a través de redes simples. El diseño permite que alguien malintencionado redirija el correo electrónico. También permite que alguien que tiene acceso a un sistema que procesa correo electrónico modifique un correo electrónico. Cualquiera que tenga acceso a redes donde se transmiten correos electrónicos o computadoras donde se procesan correos electrónicos puede ver los correos electrónicos que están allí.

No hay un mecanismo incorporado para hacer que el correo electrónico sea confidencial (como el cifrado), para verificar que el contenido del correo electrónico no se haya alterado (como un hash) o para verificar quién envió el correo electrónico (como un digital firma).

El correo electrónico no tiene un método integrado para verificar la identidad de un remitente. Aunque se confía en nosotros para ingresar nuestra identidad correcta en nuestros programas de correo electrónico, nada nos impide usar direcciones fraudulentas.

Alguien puede configurar un programa de correo electrónico para enviar correos electrónicos con direcciones falsas, e incluso sin un programa de correo electrónico, es bastante trivial utilizar herramientas simples como Telnet para crear mensajes de correo electrónico fraudulentos con direcciones de remitente falsas. Algunos proveedores de correo electrónico intentan solucionar este problema con configuraciones especiales en sus servidores de correo, pero muchos otros no lo hacen.

El correo electrónico nunca se creó para mantener la confidencialidad y la privacidad del contenido de un correo electrónico. El texto de un mensaje se transmite de forma clara, lo que significa que cualquier persona con una herramienta que pueda monitorear la red puede ver el correo electrónico.

Las herramientas básicas, como la supervisión de la red o la herramienta de rastreo de la red, pueden ver los correos electrónicos. Se pueden utilizar herramientas básicas como los clientes de correo electrónico ordinarios y Telnet para crear correos electrónicos fraudulentos.

La buena noticia es que existen herramientas disponibles que pueden superar estos desafíos.

Objetivos:

- Tomar conciencia de todos los aspectos de seguridad importantes que tienen que ver con el correo electrónico.
- Aprender a estudiar las evidencias forenses que aportan las cabeceras de los email.

Materiales

- Webmail
- Herramientas online
- Clientes de correo: Thunderbird y outlook.

Se pide:

1) Familiarización con las cabeceras de los correos electrónicos.
    a) Abre tu webmail particular.
    b) Accede al formato completo de uno de tus correos.
    c) Copia el formato completo y aplica alguna herramienta para analizar las cabeceras del mismo.
    d) Comenta el significado que tienen las cabeceras.
    e) Aprende a comprobar la información DKIM (selector, dominio y DKIM pública) que aparece en la cabecera (https://dkimcore.org/tools/).

2) Spoofing
    a) Utiliza alguna herramienta online para enviarte correo valiéndote de la técnica de suplantación de personalidad. Por ejemplo, envíate correo electrónico con origen billgates@microsoft.com y destino tu cuenta de correo.
    b) ¿Comenta qué herramientas impiden que te llegue el correo electrónico?
    c) Ahora repite el envío del apartado a), pero esta vez con origen billgates@microsoft.com y como destino utiliza la cuenta de correo que te proporcione la siguiente dirección: https://dkimvalidator.com/
    d) Estudia el correo electrónico recibido.
    e) Comenta a qué conclusiones has llegado y qué papel tienen las tecnologías SPF, DKIM y DMARK en evitar el spoofing.

3) Instala los clientes de correo electrónico más comunmente utilizados: Mozilla Thunderbird y Outlook.
    - Aprende a configurar tu cuenta de correo electrónico en ellos. Te recomiendo que uses IMAP.
    - Investiga los ficheros que utilizan como almacenamiento y son susceptibles de almacenar evidencias forenses.
    - Ponte en la tesitura de que, en un clonado de un disco al que estamos realizando una pericial, localizamos una carpeta de Thunderbird. Seria intereante acceder a esos correos, verdad? Busca herramientas “genéricas” que sirvan para visualizar (interpretar) la información contenida en el directorio de almacenamiento que usa tu Thunderbird.