Laboratorio 2 - Ciberseguridad

Fabián Valero Duque

Integrantes: Alejandra Campo Archbold, María Fernanda Rodríguez, Jham Pool Murillo

12 de agosto de 2022

Introducción

En este laboratorio se describe la definición del phishing con sus pasos, capas de impacto dentro de las empresas, ataques con el navegador de Mitre-Attack. Para ello se incluye un ejercicio práctico de phishing utilizando WampServer son fines educativos.

En primera instancia, se menciona las capas en donde podría incurrir el phishing en una organización. En segunda instancia, se aplica el ejemplo de phishing. Por último, se detalla

algunas mitigaciones y conclusiones.

Capa de reconocimiento

Phishing para obtener información

El phishing es una técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta por correo electrónico o en un sitio web, en la que el perpetrador se hace pasar por una empresa legítima o una persona de confianza.

Todas las formas de phishing son ingeniería social entregada electrónicamente. El phishing puede ser dirigido, conocido como spearphishing. En el spearphishing, el adversario apuntará a una persona, empresa o industria específica. De manera más general, los adversarios pueden realizar phishing no dirigido, como en campañas masivas de recolección de credenciales.

El phishing para obtener información implica con frecuencia técnicas de ingeniería social, como hacerse pasar por una fuente con un motivo para recopilar información (por ejemplo, establecer cuentas o comprometer cuentas) y/o enviar múltiples , mensajes aparentemente urgentes.

Capa de Acceso Inicial

El acceso inicial consta de técnicas que utilizan varios vectores de entrada para obtener su punto de apoyo inicial dentro de una red. Las técnicas utilizadas para afianzarse incluyen el phishing dirigido y la explotación de las debilidades en los servidores web públicos. Los puntos de apoyo obtenidos a través del acceso inicial pueden permitir el acceso continuo, como cuentas válidas y el uso de servicios remotos externos, o pueden ser de uso limitado debido al cambio de contraseñas.

Capa de Movimiento Lateral

El movimiento lateral consiste en técnicas que utilizan los adversarios para ingresar y controlar sistemas remotos en una red. Cumplir con su objetivo principal a menudo requiere explorar la red para encontrar su objetivo y, posteriormente, obtener acceso a él.

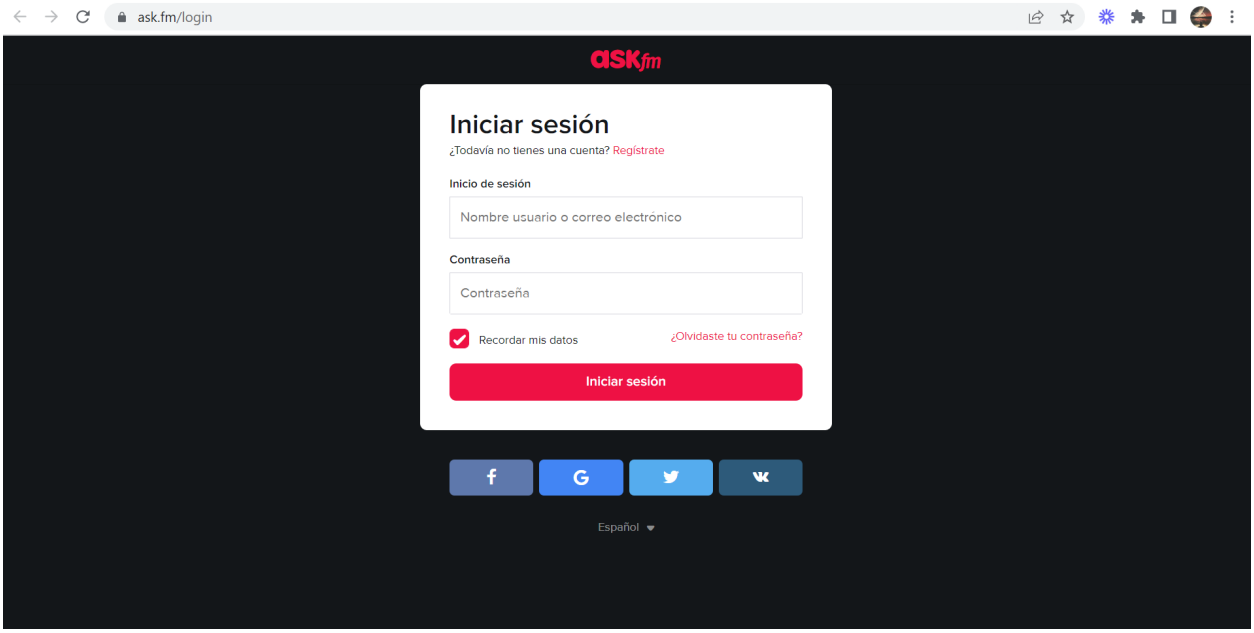
Los adversarios pueden usar el spearphishing interno para obtener acceso a información adicional o explotar a otros usuarios dentro de la misma organización después de que ya tengan acceso a cuentas o sistemas dentro del entorno. El phishing interno es una campaña de varias

etapas en la que se posee una cuenta de correo electrónico controlando el dispositivo del usuario con malware instalado previamente o comprometiendo las credenciales de la cuenta del usuario. Los adversarios intentan aprovechar una cuenta interna de confianza para aumentar la probabilidad de engañar al objetivo para que caiga en el intento de phishing.

Ejercicio de phishing con fines educativos

En este ejercicio buscamos conseguir datos de ingreso suplantando una página web, en este caso ask.fm.

Detalle del proceso



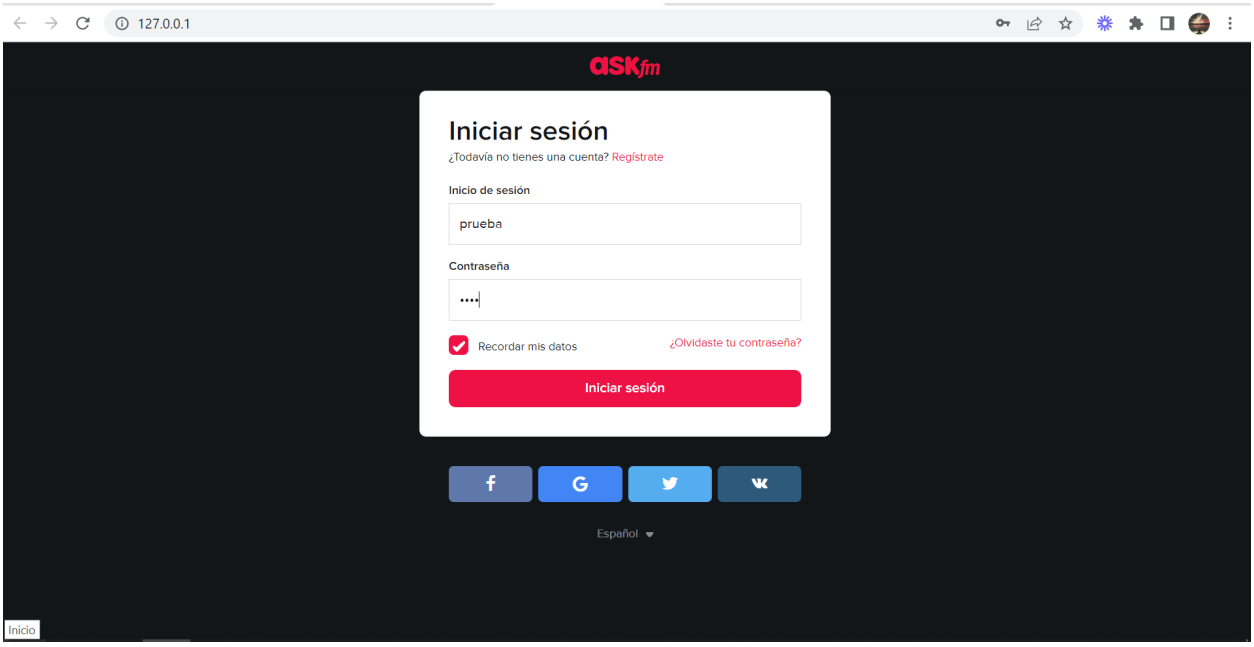
En la fase de **búsqueda** escogimos una pagina web, ask.fm una red social hoy en día muy poco usada. Luego, para generar confianza de acceso usamos WampServer.

Para comenzar el entorno de **infiltración**, guardamos el sitio web elegido (ask.fm) como un archivo .html, lo abrimos como block de notas y modificamos todos los *action* por el nombre del shell en este caso writhe.php y los métodos deben quedar en post. En el write.php modificamos y ponemos el link (https://ask.fm/login)

Dentro de www creamos la carpeta de la página web:

index_files	8/08/2022 5:26 p. m.	Carpeta de archivos	
index	8/08/2022 5:52 p. m.	Chrome HTML Docu...	9 KB
write	8/08/2022 5:42 p. m.	Archivo PHP	1 KB

Para la víctima, recibiría el link 127.0.0.1 (en la realidad es modificado para que sea más realista)



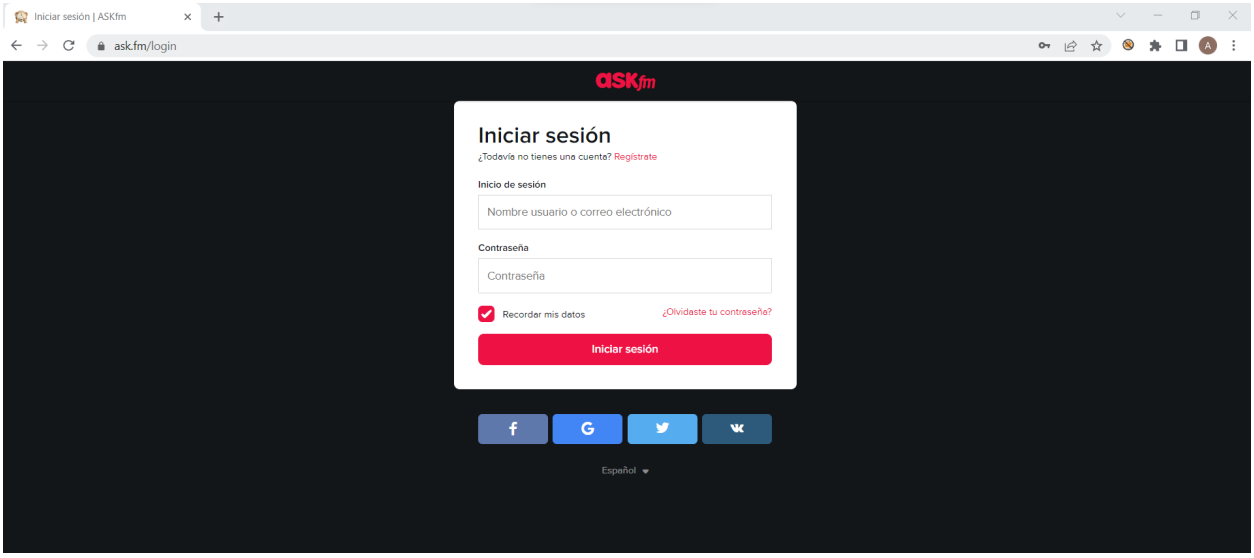
En la página falsa, ingresamos un usuario y una contraseña.

index_files	12/08/2022 7:27 p. m.	Carpeta de archivos	
index	8/08/2022 5:52 p. m.	Chrome HTML Docu...	9 KB
passes	12/08/2022 7:33 p. m.	Documento de texto	1 KB
write	8/08/2022 5:42 p. m.	Archivo PHP	1 KB

Luego, se crea un archivo txt con los datos del *login*.

```
utf8=✓
authenticity_token=mLmfMQd1s0xD6R
+1muV4KU71rWFgTzrGOnrtgIiQrX5RUiTYVGUX4arfdsicDEPF2yiW1KtShIVgRes2k7NDjw==
login=prueba
password=123
remember_me=1
```

Cuando el usuario termina de ingresar los datos y hace click en iniciar sesión lo envía a la página principal.



En la fase de **descubrimiento** se evidencia la captura del sitio comprometido (la página web) y cómo el clonar páginas puede llegar a tener un impacto crítico en la víctima.

Al final logramos **capturar** los datos del usuario, cuando es engañada por la página clonada.

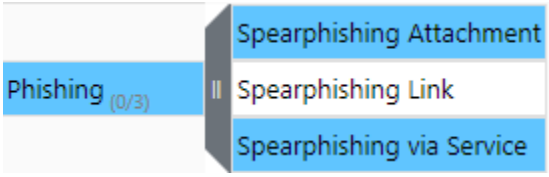
Elementos de investigación que permitan mitigar este procedimiento

Dentro del phishing encontramos estas subtécnicas:

- **Spearphishing Attachment:** Consiste en enviar un correo electrónico con un archivo adjunto malicioso. Utiliza ingeniería social para que el usuario piense que es una fuente confiable y lo ejecute.
- **Spearphishing link:** A diferencia del anterior, esta subténica envía un enlace malicioso evitando las defensas que pueden inspeccionar archivos adjuntos a los correos. También usa ingeniería social para que el usuario ingrese al link.
- **Spearphishing via Service:** Emplea el uso de servicios de terceros como redes sociales personales en vez de hacerlo con servicios controlados por la empresa. El objetivo es

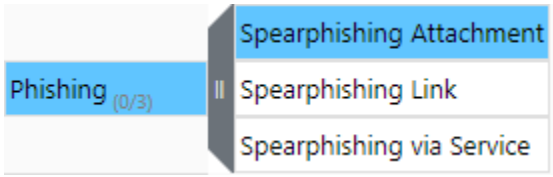
generar una relación con el objetivo o captar el interés del objetivo para sacar información importante o enviar enlaces o archivos maliciosos.

Antivirus/Antimalware:



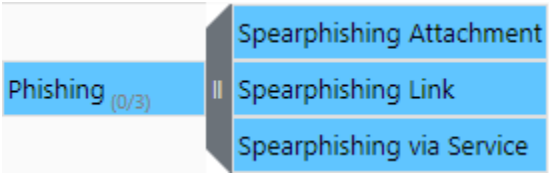
El antivirus puede poner en cuarentena automáticamente los archivos sospechosos, tanto en Spearphising Attachment como en Spearphishing via Service; Sin embargo no puede analizar enlaces web.

Network Intrusion Prevention:



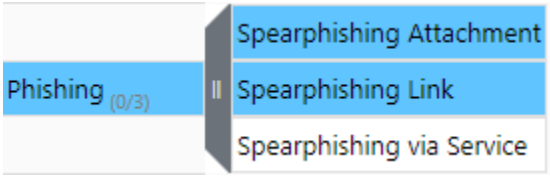
Los sistemas de prevención de intrusiones en la red y los sistemas diseñados para escanear y eliminar archivos adjuntos o enlaces de correo electrónico maliciosos se pueden usar para bloquear la actividad.

Restrict Web-Based Content:



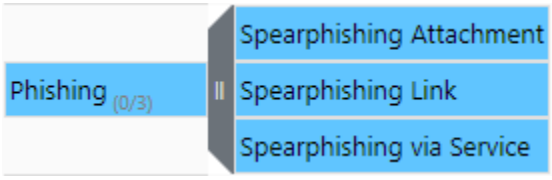
Mitiga el phishing al bloquear el acceso a ciertos sitios web o archivos adjuntos si la actividad no se puede monitorear bien o plantea un riesgo significativo. El usuario es responsable de ejecutar el posible riesgo luego de recibir el aviso.

Software Configuration:



Software configuration usa mecanismos de autenticación de correo electrónico y contra la suplantación de identidad para filtrar los mensajes validando el dominio del remitente y la integridad de los mensajes. No funciona si el ataque se envía en medios externos (via Service).

User Training:



User training se trata de proveer una capacitación a los usuarios para identificar técnicas de ingeniería social y correos electrónicos de phishing. Es efectivo en las tres subtécnicas.

Detección:

- Supervisar el registro de aplicaciones de terceros, mensajes y/u otros artefactos que pueden enviar mensajes de phishing para obtener acceso a los sistemas de las víctimas. El filtrado basado en DKIM+SPF o el análisis de encabezado puede ayudar a detectar cuándo se falsifica al remitente del correo electrónico. La inspección de URL dentro del correo electrónico (incluida la expansión de enlaces acortados) puede ayudar a detectar enlaces que conducen a sitios maliciosos conocidos. Las cámaras de detonación se pueden usar para detectar estos enlaces e ir automáticamente a estos sitios para determinar si son potencialmente maliciosos, o esperar y capturar el contenido si un usuario visita el enlace.
- Supervisar los archivos recién creados a partir de mensajes de phishing para obtener acceso a los sistemas de las víctimas.
- Monitorear y analizar patrones de tráfico SSL/TLS e inspección de paquetes asociados a protocolos que no siguen los estándares de protocolo y flujos de tráfico esperados (por ejemplo, paquetes extraños que no pertenecen a flujos establecidos, patrones de tráfico gratuitos o anómalos, sintaxis anómala o estructura).
- Supervisar los datos de la red en busca de flujos de datos poco comunes. Los procesos que utilizan la red que normalmente no tienen comunicación de red o nunca antes se han visto son sospechosos.

Phishing en Android

Los dispositivos Android tienen mas posibilidad de sufrir ataques a su privacidad en comparación con los Iphone ya que tienen un sistema operativo de código abierto.

Hay algunas señales que nos ayudan a identificar si somos victimas de phishing en nuestro Android:

- Consumo excesivo de batería o datos.
- Redirección a paginas web que no se han buscado o comportamiento sospechoso al navegar por el internet.
- Recibir publicidad extraña o anuncios atípicos.
- Bloqueo o fallo de aplicaciones, o que estas aparezcan sin que el usuario las descargue.
- Recalentamiento o lentitud inusuales.

Una técnica sencilla para realizar el phishing en Android es la siguiente:

1. Instalar una terminal de Linux en nuestro dispositivo, **Termux** puede servir en este caso.
2. Instalar python con el comando **pkg install python,** ya que muchas librerías y frameworks son de python**.**
3. Instalar github con el comando **pkg install git,** para realizar una clonación de frameworks alojados en Github.
4. Instalar OpenSsh con el comando **pkg install openssh**, esto para utilizar una web App con conexión local a través de este protocolo.
5. Instalar un editor de texto con el comando **pkg install nano** para utilizar los archivos.

Una vez tenemos todo lo necesario instalado podemos utilizar un Framework para realizar el ataque Phishing. Algunos que nos sirven son:

▼ **Nexphisher:** Tiene plantillas de servicios como Google, Netflix, Paypal y Facebook. Se usa mediante servidores de servicios como Ngrok, Serveo o LocalExpose.

▼ **Zphisher:** Tiene mas de 30 plantillas para su uso de forma instantánea en distintos servicios (no solo localhost).

Como pudimos observar realizar este ataque en Android es relativamente sencillo, por lo cual debemos seguir las recomendaciones para evitarlo; entre estas descargar aplicaciones de fuentes confiables, revisar permisos de aplicaciones, revisar un enlace antes de hacer clic, etc.

Conclusiones

- Podemos destacar que el phishing como modalidad de estafa informática ha ido adoptando perfiles cada vez más complejos, existiendo una mayor dificultad para detectar la sustracción de datos personales y requiriendo mecanismos cada vez más sofisticados para defenderse de ellos.
- Existen mecanismos de mitigación al phishing como: el Antivirus/Antimalware, Prevención de intrusiones en la red, Restringir contenido basado en la web, Configuración de software y Entrenamiento de usuario. Estos mecanismos son importantes para prevenir y detectar el phishing a tiempo.
- Consideramos como mecanismo de mitigación más importante el entrenamiento al usuario, ya que el phishing depende mucho de la ingeniería social; el usuario debe ser ingenuo para no revisar un archivo o enlace antes de abrirlos o para decidir compartir información personal con desconocidos.

Referencias

MITRE ATT&CK Navigator. https://mitre-attack.github.io/attack-navigator/

Enterprise Mitigations. https://attack.mitre.org/mitigations

Phishing. COMPUTER SECURITY RESOURCE CENTER. https://csrc.nist.gov/glossary/term/phishing

¿Qué es el phishing en el teléfono móvil y cómo evitarlo?. https://willistowerswatsonupdate.es/ciberseguridad/13-pasos-para-evitar-el-phishing-en-tu-telefono-movil/

¿Cómo hacer phishing en Android? https://comoinstalar.xyz/como-hacer-phishing-en-android/