Ejercicio de Laboratorio – Vulnerabilidades Hum

Objetivo

El objetivo de esta práctica en clase es familiarizarse con la gestión de vulnerabilidaes generadas por los humanos en ICS/SCADA.

DESARROLLO DE LA PRÁCTICA

Paso 1: Actualiza el sistema

Antes de instalar cualquier paquete, asegúrate de que tu sistema esté actualizado. Abre una terminal y ejecuta:

```
sudo apt update && sudo apt upgrade -y
```

Paso 2: Descarga GoPhish

Ve al sitio oficial de GoPhish para descargar la última versión.

1. Abre tu navegador y visita: https://getgophish.com.
2. Descarga la versión de GoPhish para Linux (por lo general, es un archivo `.tar.gz`).

O puedes usar `wget` para descargar directamente desde la terminal. Por ejemplo:

```
wget https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.tar.gz
```

Asegúrate de verificar la versión más reciente en el sitio oficial, ya que puede cambiar.

Paso 3: Extrae el archivo descargado

Descomprime el archivo `.tar.gz` en un directorio de tu elección:

```
tar -xvf gophish-v0.12.1-linux-64bit.tar.gz
```

Paso 4: Ejecuta GoPhish

Navega al directorio descomprimido:

```
cd gophish-v0.12.1-linux-64bit
```

Haz que el archivo de GoPhish sea ejecutable:

```
chmod +x gophish
```

Ejecuta GoPhish:

```
sudo ./gophish
```

Paso 5: Configuración inicial

Una vez que ejecutas el comando anterior, GoPhish iniciará y verás información similar a la siguiente en la terminal:

```
Starting admin server at https://0.0.0.0:3333
Starting phishing server at http://0.0.0.0:80
```

Esto indica que GoPhish está corriendo y que el servidor de administración está disponible en `https://localhost:3333`.

Paso 6: Acceder a la interfaz de administración

1. Abre tu navegador y visita: `https://localhost:3333`.
2. Es probable que recibas una advertencia de seguridad por el certificado SSL autogenerado, ignórala y procede de todos modos.
3. Ingresa el nombre de usuario y la contraseña por defecto:
    - **Usuario**: `admin`
    - **Contraseña**: Aparece en la terminal cuando GoPhish se inicia por primera vez.

Paso 7: Cambiar la contraseña del administrador (opcional)

Es recomendable que cambies la contraseña por defecto después de acceder a la interfaz de administración. Para hacerlo, sigue los pasos dentro del panel de GoPhish.

Paso 8: Configura GoPhish para pruebas de phishing

Una vez que has instalado y ejecutado GoPhish, el siguiente paso es configurar la plataforma para que puedas crear campañas de phishing efectivas. Aquí te explico cómo hacerlo en detalle.

8.1. Accede a la interfaz de administración

1. Abre tu navegador y visita: `https://localhost:3333` o `https://<tu-ip>:3333` si estás accediendo desde otra máquina.
2. Usa las credenciales que obtuviste durante la instalación (usuario: `admin`, contraseña: la que se mostró en la terminal).

Una vez dentro del panel de GoPhish, verás un tablero con diferentes opciones para gestionar tus campañas.

8.2. Configuración de SMTP

Para enviar correos electrónicos a los objetivos, necesitas configurar un servidor SMTP. GoPhish usará esta configuración para enviar los correos de phishing que crees en las campañas.

1. **Ir a la sección "Sending Profiles"**
   - En el menú superior, haz clic en **Sending Profiles**.
   - Haz clic en **New Profile**.
2. **Configura el perfil de envío** Aquí debes ingresar los detalles de tu servidor SMTP. Un ejemplo sería el uso de un servidor de correos público (como Gmail), aunque en entornos reales se recomienda configurar tu propio servidor SMTP.
   - **Name**: Pon un nombre descriptivo (por ejemplo, “Gmail SMTP” o “Servidor de prueba”).
   - **Interface Type**: Deja la opción por defecto ("SMTP Plain").
   - **From Address**: La dirección de correo desde la que los correos serán enviados (por ejemplo, `tu-correo@gmail.com` o `phishing@ejemplo.com`).
   - **Host**: El servidor SMTP que utilizarás. Por ejemplo:
     - Para Gmail: `smtp.gmail.com:465`
   - **Username**: El correo electrónico o nombre de usuario que autenticará el envío (por ejemplo, `tu-correo@gmail.com`).
   - **Password**: La contraseña de tu correo o la contraseña específica de aplicaciones en Gmail (debes habilitar "Contraseñas de Aplicaciones" en tu cuenta de Google para esto https://myaccount.google.com/apppasswords) debes tener el doble factor de autenticación habilitado).
   - **Ignore Cert Errors**: Actívalo solo si tu servidor SMTP tiene un certificado inválido o autofirmado (útil para pruebas en servidores locales).
   - **Send Test Email**: Puedes probar la configuración enviando un correo de prueba.

   Haz clic en **Save**.

8.3. Creación de Plantillas de Correo

Las plantillas de correo son el contenido que se enviará a los objetivos de phishing. Puedes crear correos personalizados con enlaces maliciosos u otras técnicas para engañar a las víctimas.

1. **Ir a la sección "Email Templates"**
   - En el menú superior, selecciona **Email Templates**.
   - Haz clic en **New Template**.
2. **Configura la plantilla**
   - **Name**: Dale un nombre descriptivo a la plantilla (por ejemplo, "Plantilla de Phishing de Actualización de Seguridad").
   - **Subject**: El asunto del correo (por ejemplo, "Actualización de Seguridad Crítica. Acción Requerida").
   - **HTML Content**: Aquí puedes diseñar el contenido del correo. Puedes usar HTML para formatear el correo y hacer que se vea más auténtico. Ejemplo básico:

     ```
     <h1>Alerta de Seguridad</h1>
     <p>Estimado usuario,</p>
     <p>Es necesario que actualices tu contraseña debido a una
     vulnerabilidad crítica. Haz clic en el siguiente enlace para
     proceder:</p>
     <a href="{{.URL}}">Actualizar Contraseña</a>
     <p>Gracias,</p>
     <p>Equipo de Seguridad</p>

     Nota: Use ChatGPT para crear una plantilla más sofisticada
     ```

   - **Text Content**: Si prefieres enviar un correo en texto plano, escribe aquí el contenido del mensaje.
   - **Tracking Options**:
     - **Track clicks**: Actívalo si quieres rastrear quién hace clic en el enlace de phishing.
     - **Track opens**: Actívalo si quieres rastrear quién abre el correo.

   Haz clic en **Save** cuando termines.

8.4. Creación de Páginas de Phishing

El siguiente paso es crear la página a la que serán redirigidos los objetivos al hacer clic en los enlaces del correo. Esto podría ser una página de inicio de sesión falsa (login page) u otro tipo de página para capturar datos.

1. **Ir a la sección "Landing Pages"**
   - En el menú superior, selecciona **Landing Pages**.
   - Haz clic en **New Page**.
2. **Configura la página de destino**
   - **Name**: Dale un nombre descriptivo (por ejemplo, "Página de Phishing de Inicio de Sesión").

- **Capture Submitted Data**: Actívalo si quieres capturar las credenciales que los usuarios ingresen en la página.
- **Redirect to URL**: Si quieres que los usuarios sean redirigidos a una página legítima después de ingresar sus credenciales, especifica la URL aquí (por ejemplo, la página de inicio de sesión real de la empresa).

3. **Página HTML** Puedes crear una página desde cero o copiar el HTML de una página legítima para hacerla más convincente. Un ejemplo básico sería una página de inicio de sesión falsa:

```
<!DOCTYPE html><html lang="es"><head><meta charset="UTF-8"/><meta name="viewport" content="width=device-width,
initial-scale=1.0"/><meta http-equiv="X-UA-Compatible" content="ie=edge"/>
   <title>ICS Control System - Login</title>
   <style type="text/css">body {
            font-family: Arial, sans-serif;
            background-color: #f4f4f4;
            display: flex;
            justify-content: center;
            align-items: center;
            height: 100vh;
            margin: 0;
        }

        .login-container {
            background-color: #ffffff;
            padding: 40px;
            border-radius: 10px;
            box-shadow: 0 4px 8px rgba(0, 0, 0, 0.1);
            width: 400px;
            text-align: center;
        }

        .login-container h2 {
            color: #004c8c;
            margin-bottom: 20px;
        }

        .login-container input[type="text"],
        .login-container input[type="password"] {
            width: 100%;
            padding: 12px;
            margin: 8px 0;
            display: inline-block;
            border: 1px solid #ccc;
            border-radius: 4px;
            box-sizing: border-box;
        }

        .login-container input[type="submit"] {
            background-color: #004c8c;
            color: white;
            padding: 14px 20px;
            margin: 10px 0;
            border: none;
            cursor: pointer;
            width: 100%;
            border-radius: 4px;
        }

        .login-container input[type="submit"]:hover {
            background-color: #003366;
        }

        .login-container .footer {
            margin-top: 20px;
            font-size: 12px;
            color: #777;
        }

        .login-container .logo {
            margin-bottom: 20px;
        }

        .login-container .logo img {
            max-width: 150px;
        }
   </style>
</head>
<body>
<div class="login-container">
<div class="logo"><img alt="ICS Logo" src="https://cdn3.vectorstock.com/i/1000x1000/68/47/industrial-control-
systems-concept-icon-vector-36066847.jpg"/> <!-- Puedes cambiar la URL por la imagen de tu elección --></div>

<h2>ICS Control System Login</h2>

<form action="" method="POST"><label for="username">Username:</label><br/>
<input id="username" name="username" required="" type="text"/><br/>
```

```
<label for="password">Password:</label><br/>
<input id="password" name="password" required="" type="password"/><br/>
<input type="submit" value="Login"/> </form>

<div class="footer">
<p>© 2024 ICS Inc. All rights reserved.</p>
</div>
</div>


</body></html>
```

Haz clic en **Save** cuando termines, use ChatGPT para personalizar la plantilla.

8.5. Importar Grupos de Objetivos

Necesitarás un grupo de personas a quienes enviar los correos. Puedes importar una lista de objetivos.

1. **Ir a la sección "Users & Groups"**
   - En el menú superior, selecciona **Users & Groups**.
   - Haz clic en **New Group**.
2. **Añade los objetivos**
   - **Name**: Dale un nombre al grupo (por ejemplo, “Grupo de Prueba de Phishing”).
   - **Targets**: Puedes agregar objetivos manualmente o importar una lista de correos en formato CSV. Ejemplo de un archivo CSV:

     ```
     first_name,last_name,email,position
     John,Doe,john.doe@empresa.com,Manager
     Jane,Smith,jane.smith@empresa.com,Developer
     ```

3. Haz clic en **Save**.

8.6. Crear la Campaña de Phishing

Ahora que has configurado el servidor SMTP, la plantilla de correo, la página de phishing y los grupos de objetivos, puedes crear una campaña.

1. **Ir a la sección "Campaigns"**
   - En el menú superior, selecciona **Campaigns**.
   - Haz clic en **New Campaign**.
2. **Configura la campaña**
   - **Name**: Dale un nombre a la campaña (por ejemplo, “Campaña de Phishing de Octubre”).
   - **Email Template**: Selecciona la plantilla de correo que creaste.
   - **Landing Page**: Selecciona la página de destino que creaste.
   - **URL**: Esta es la URL del servidor que utilizarás para la página de phishing (debe estar configurada en tu red o servidor).

- **Sending Profile**: Selecciona el perfil SMTP que configuraste.
- **Group**: Selecciona el grupo de objetivos al que quieres enviar la campaña.
- **Launch Date**: Puedes programar la campaña para que se envíe en una fecha específica o lanzarla de inmediato.

Haz clic en **Launch Campaign**.

8.7. Monitoreo de la Campaña

Una vez que la campaña esté en marcha, puedes monitorear el progreso:

1. **Visualizar resultados** En la pestaña **Campaign Results**, verás detalles sobre quién abrió los correos, quién hizo clic en los enlaces y quién ingresó información en la página de phishing.
2. **Reporte y análisis** Puedes descargar los reportes o visualizarlos directamente desde el panel de GoPhish. Esto te permite identificar el nivel de exposición de los usuarios y ajustar futuras campañas.

Criterios de Corrección

1. **Precisión en la Ejecución de Comandos y Configuración**
   - **Calificación Completa**: Todos los comandos fueron ejecutados correctamente y en el orden indicado, sin errores de sintaxis ni configuración.
   - **Parcialmente Completo**: Algunos comandos se ejecutaron con éxito, pero hubo errores o desviaciones menores que no afectaron significativamente el desarrollo del laboratorio.
   - **Incompleto**: Hubo errores considerables en la ejecución de los comandos o la configuración, afectando el funcionamiento de GoPhish.
2. **Configuración del Servidor SMTP**
   - **Calificación Completa**: La configuración del perfil de envío SMTP es precisa y permite el envío exitoso de correos de prueba. Todos los campos están completos y configurados de acuerdo con las instrucciones.
   - **Parcialmente Completo**: La configuración del servidor SMTP fue exitosa pero presenta configuraciones incompletas o errores menores que pueden afectar el envío en ciertos casos.
   - **Incompleto**: La configuración del SMTP es incorrecta o incompleta, lo que impide el envío de correos.
3. **Calidad de las Plantillas de Phishing**
   - **Calificación Completa**: La plantilla de correo es convincente y bien diseñada, con lenguaje y formato que simulan un correo auténtico. Las opciones de seguimiento de apertura y clic están habilitadas.
   - **Parcialmente Completo**: La plantilla es funcional pero carece de ciertos detalles de realismo o formato que podrían mejorar su efectividad.

- **Incompleto**: La plantilla es poco convincente o incorrectamente diseñada, con errores importantes en el formato o en la configuración de seguimiento.

4. **Desarrollo de Páginas de Destino de Phishing**
   - **Calificación Completa**: La página de destino es realista y permite capturar datos ingresados por los usuarios, simula adecuadamente una página legítima de inicio de sesión.
   - **Parcialmente Completo**: La página funciona, pero presenta elementos de diseño que restan realismo o faltan configuraciones menores en la captura de datos.
   - **Incompleto**: La página de destino tiene errores importantes que afectan su funcionalidad o no logra simular un entorno realista para el usuario.
5. **Importación y Organización de Grupos de Objetivos**
   - **Calificación Completa**: Los grupos de objetivos fueron creados e importados correctamente en el formato solicitado, con todos los datos necesarios y bien organizados.
   - **Parcialmente Completo**: Los grupos fueron importados, pero hay datos incorrectos o faltantes que afectan la segmentación.
   - **Incompleto**: La importación de grupos de objetivos es incorrecta o incompleta, dificultando la segmentación y envío de la campaña.
6. **Configuración y Lanzamiento de la Campaña de Phishing**
   - **Calificación Completa**: La campaña está configurada correctamente, con todos los elementos (SMTP, plantilla de correo, página de destino y grupo de objetivos) vinculados de manera precisa.
   - **Parcialmente Completo**: La campaña está lanzada, pero existen errores menores en la configuración o en la vinculación de algunos elementos.
   - **Incompleto**: La campaña no fue lanzada correctamente o falta la configuración adecuada de uno o más elementos críticos.
7. **Monitoreo y Análisis de Resultados**
   - **Calificación Completa**: Los resultados de la campaña están documentados con precisión, incluyendo análisis detallado de las métricas (aperturas, clics, capturas de datos) y observaciones sobre la efectividad de la campaña.
   - **Parcialmente Completo**: La documentación de los resultados es funcional pero carece de detalles en el análisis o presenta algunas métricas incompletas.
   - **Incompleto**: No se documentaron los resultados de manera adecuada o no se realizó un análisis crítico de las métricas obtenidas.
8. **Documentación y Análisis Final**
   - **Calificación Completa**: El reporte final es claro, organizado y analiza críticamente la efectividad de la campaña, proponiendo mejoras para futuras iniciativas.
   - **Parcialmente Completo**: El reporte es comprensible, pero carece de profundidad en el análisis o en las recomendaciones para mejorar.
   - **Incompleto**: El reporte es confuso, incompleto o carece de análisis crítico sobre los resultados.

¡Amino!