**Laboratorio 3**

**Paso 1 buscar el vector de ataque**

El **phishing** es un tipo común de ciberataque que utiliza correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web falsos para engañar a las personas y hacer que compartan datos confidenciales, como contraseñas o información financiera. Los atacantes se hacen pasar por entidades de confianza para manipular a las víctimas y obtener información sensible. Para protegerse contra el phishing, es importante estar atento a correos electrónicos sospechosos, no hacer clic en enlaces desconocidos y verificar la autenticidad de las solicitudes de información personal.

**Simulación**

**Gophish**: Una herramienta de código abierto para la simulación de phishing que permite crear campañas de phishing controladas y analizar las respuestas.

**Escenario de Ataque – Phishing Corporativo Dirigido (Spear Phishing)**

**Contexto General:**

**Empresa:** HealthTech S.A.S. **Sector:** Salud **Empleado afectado:** Andrea López (asistente administrativa) **Herramientas usadas:** Correo corporativo, Microsoft 365, Teams

**Inicio del Ataque: Correo Malicioso**

**Fecha:** 22 de abril de 2025 **Asunto del correo:** ¡Acción urgente! Documento pendiente de firma electrónica  
**Remitente:** notificaciones@healthtech-firma.com **Contenido del correo:**

**Estimada Andrea,**

Tiene un documento importante pendiente de firma relacionado con su contrato laboral. Por favor, revíselo y fírmarlo en un plazo de 24 horas**.**

**Revisar Documento**

Este mensaje ha sido generado automáticamente, por favor no responda.

**Enlace malicioso:**

https://healthtech-firma.com/inicio-sesion(Sitio clonado visualmente al login oficial de Microsoft 365)

**Acciones del Usuario:**

1. Andrea hace clic en el enlace.
2. Introduce sus credenciales en el sitio falso (login + contraseña).
3. Recibe un error ("Contraseña incorrecta, intente de nuevo"), y lo ignora.
4. El atacante recibe sus credenciales en tiempo real.

**Acciones del Atacante:**

1. Se conecta al correo corporativo de Andrea desde una IP en Colombia (pero en horario no laboral).
2. Revisa correos, archivos de OneDrive y Teams buscando documentos sensibles.
3. Reenvía un correo de la empresa con adjunto confidencial a su propia dirección personal.
4. Intenta usar las credenciales en otros sistemas (VPN, ERP) sin éxito.

**Evidencias Detectadas:**

| **Fuente** | **Evidencia** |
| --- | --- |
| Logs de acceso O365 | Inicio de sesión exitoso desde IP desconocida: 190.25.86.144 |
| Logs de tráfico web | Acceso previo al sitio: healthtech-firma.com |
| Historial del navegador | Formulario de login en sitio no oficial |
| Análisis de URL | Página clónica con formulario falso conectado a servidor externo |
| SIEM / Alerta interna | Detección de comportamiento anómalo fuera del horario laboral |

**Vector de Ataque Confirmado:**

**Phishing con Ingeniería Social Dirigida (Spear Phishing)**

**Medidas de Contención y Recomendaciones:**

* Cambio inmediato de contraseñas del usuario afectado.
* Monitoreo de accesos inusuales a otros sistemas.
* Bloqueo del dominio malicioso desde firewall/proxy.
* Capacitación en concientización sobre correos sospechosos.
* Implementación de MFA en todos los accesos sensibles.

**Paso 2 Analizar Los Logs Del Sistema Para Encontrar Evidencias De Actividad Maliciosa**

**Log del Servidor de Correo Electrónico**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Fecha y Hora (UTC)** | **Usuario** | **Dirección IP** | **Acción Realizada** | **Cliente/Dispositivo** | **Resultado** | **Detalles Adicionales** |
| 2025-04-22 17:41:58 | andrea.lopez@healthtech.com | 190.25.86.144 | Inicio de sesión (OWA) | Chrome - Windows 10 | Éxito | Inicio de sesión desde ubicación no habitual (Colombia) |
| 2025-04-22 17:43:12 | andrea.lopez@healthtech.com | 190.25.86.144 | Lectura de correo | Outlook Web Access | OK | Asunto: “Firma electrónica pendiente” |
| 2025-04-22 17:44:06 | andrea.lopez@healthtech.com | 190.25.86.144 | Click en enlace externo | Outlook Web Access | OK | URL: http://healthtech-firma.com/inicio-sesion |
| 2025-04-22 17:45:03 | andrea.lopez@healthtech.com | 190.25.86.144 | Cambio de contraseña | OWA | Fallido | Error: contraseña incorrecta |
| 2025-04-22 17:45:59 | andrea.lopez@healthtech.com | 190.25.86.144 | Acceso a OneDrive | Chrome - Windows | OK | Descarga de archivo: “listado-clientes.xlsx” |
| 2025-04-22 17:47:11 | andrea.lopez@healthtech.com | 190.25.86.144 | Envío de correo externo | Outlook Web Access | OK | Destinatario: attacker@gmail.com |

**Análisis del Log:**

**IP sospechosa: No corresponde al rango corporativo ni ubicación usual de Andrea.**

* Actividad fuera de horario laboral.
* Acceso al enlace malicioso antes del login.
* Transferencia de información posterior al acceso.