	I.E. FRANCISCO ABEL GALLEGO **Taller # 1 Tecnología**	**TECH** **2026** **II PERIODO**

Habilidades transferibles y técnicas de ciberseguridad II

Nombre completo: _____ grado: _____

Objetivo:

Identificar y explicar algunas habilidades clave (como comunicación, resolución de problemas y uso de herramientas SIEM) y su aplicación práctica en el campo profesional de la ciberseguridad.

EL PHISHING

es el uso de las comunicaciones digitales para **engañar a las personas** con el fin de que revelen **Datos sensibles o implementen software malicioso**.

Algunos de los **tipos más comunes de ataques de phishing** en la actualidad incluyen:

- **Compromiso de correo electrónico empresarial (BEC):** Un agente de amenaza **envía un mensaje de correo electrónico que parece proceder de una fuente conocida** para realizar una solicitud de información aparentemente legítima, con **el fin de obtener una ventaja financiera.**

- **Spear phishing:** Ataque **malicioso por correo electrónico dirigido a un usuario o grupo de usuarios específico**. El correo electrónico parece proceder de una fuente de confianza.

- **Whaling**: Una forma de phishing dirigido. **Agentes de amenaza** tienen como **objetivo a ejecutivos de la empresa para obtener acceso a datos confidenciales**.

- **Vishing** : El exploit de la comunicación electrónica de voz para obtener información sensible o **hacerse pasar por una fuente conocida**.

- **Smishing** : El uso **de mensajes de texto para engañar a los usuarios**, con el fin de obtener información sensible o hacerse pasar por una fuente conocida.

SOFTWARE MALICIOSO

El software malicioso es un software diseñado **para dañar dispositivos o redes**. Existen muchos tipos de software malicioso. El **objetivo principal del software malicioso es obtener dinero o, en algunos casos, una ventaja de inteligencia que pueda utilizarse contra una persona, una organización o un territorio.**

Algunos de los tipos de ataques de software malicioso más comunes en la actualidad son:

- **Virus:** Código malicioso escrito para **interferir en las operaciones de la computadora y causar daños a los datos y al software**. Un virus debe ser iniciado por un usuario (es decir, un agente de amenaza), que **transmite** el virus a través de un **archivo adjunto** malicioso **o de la descarga de un archivo**. Cuando alguien abre el archivo adjunto malicioso o la descarga, el virus se oculta en otros archivos del sistema ahora infectado. Cuando se abren los archivos infectados, permite al virus insertar su propio código para dañar y/o destruir datos en el sistema.

- **Gusanos (Worm): Software malicioso** que puede **duplicarse y propagarse por los sistemas por sí mismo.** A diferencia de un virus, un gusano no necesita ser descargado por un usuario. En su lugar, se autorreplica y **se propaga desde una computadora ya infectada a otros dispositivos de la misma red.**

- **Ransomware:** Ataque malicioso en el que los agentes de amenazas **encriptan los Datos de una organización y exigen un pago** para restablecer la accesibilidad.

- **Software espía Spyware:** Software malicioso que se utiliza para **recopilar y vender Información sin consentimiento**. El software espía puede utilizarse **para acceder a los dispositivos**. Esto permite a los agentes de amenaza recopilar datos personales, como correos electrónicos privados, textos, grabaciones de voz e imágenes y ubicaciones.

INGENIERÍA SOCIAL

La ingeniería social es una técnica de manipulación que **explota el error humano para obtener información privada, accesibilidad u objetos de valor**. El error humano suele ser el resultado de confiar en alguien sin cuestionarlo. La Misión de un agente de amenaza, actuando como ingeniero social, es **crear un entorno de falsa confianza y mentiras para explotar al mayor número de personas posible.**

Algunos de los tipos más comunes de ataques de ingeniería social en la actualidad incluyen:

- **Phishing en redes sociales:** Un agente de amenaza **recopila información detallada** sobre su **objetivo en los sitios de redes sociales**. A continuación, inician un ataque.

- **Ataque de "agujero de agua":** Un agente de amenaza **ataca un sitio web visitado con frecuencia** por un grupo específico de usuarios. Ejemplo: social engineering

- **USB baiting:** Un agente de amenaza deja estratégicamente una **memoria USB con software malicioso** para que un empleado la encuentre e instale, con el fin de **infectar una red sin saberlo**.

- **Ingeniería social física:** Un agente de amenaza se **hace pasar por un empleado, cliente o proveedor para obtener acceso no autorizado a un lugar físico.**

PRINCIPIOS DE LA INGENIERÍA SOCIAL

La ingeniería social es increíblemente eficaz. Esto se debe a que la **gente suele ser confiada y está condicionada a respetar la autoridad**. El número de **ataques** de ingeniería social **aumenta con cada nueva aplicación de Redes sociales que permite el acceso público a los datos de las personas**. Aunque compartir datos personales -como su ubicación o sus fotos- puede resultar cómodo, también supone un Riesgo.

Entre las razones por las que los ataques de ingeniería social son eficaces se incluyen:

- **Autoridad**: Agentes de amenaza se **hacen pasar por personas con poder**. Esto se debe a que la gente, en general, ha sido condicionada a respetar y seguir a las figuras de autoridad.
- **Intimidación**: Los Agentes de amenaza utilizan **tácticas de intimidación**. Esto incluye persuadir e intimidar a las víctimas para que hagan lo que se les dice.
- **Consenso/Prueba social:** Dado que la gente a veces hace cosas que cree que muchos otros están haciendo, los agentes de amenaza **utilizan la confianza de los demás para fingir que son legítimos**. Por ejemplo, un Agente de amenaza podría intentar obtener acceso a datos privados diciéndole a un empleado que otras personas de la empresa le han dado acceso a esos datos en el pasado.
- **Escasez**: Táctica utilizada para dar a entender que la **oferta** de bienes o servicios es limitada.
- **Familiaridad**: Agentes de amenaza establecen una **falsa conexión emocional** con los usuarios que puede ser explotada.
- **Confianza**: Los agentes de amenaza **establecen una relación emocional con los usuarios que puede ser explotada a lo largo del tiempo**. Utilizan esta relación para desarrollar la confianza y obtener información personal.
- **Urgencia**: Un agente de amenaza **persuade a los demás para que respondan rápidamente** y sin hacer preguntas.

ACTIVIDAD GRUPAL

En grupos de Max. 3 estudiantes, realizar la actividad grupal.

1. **Un gerente financiero recibe un correo aparentemente enviado por el director general solicitando una transferencia urgente. El mensaje incluye lenguaje formal y datos reales de la empresa. ¿Qué tipo de ataque se evidencia principalmente y cuál es el factor psicológico explotado?**

A. Spear phishing – Escasez

B. BEC – Autoridad

C. Whaling – Familiaridad

D. Smishing – Urgencia

2. **Una organización detecta que varios equipos comenzaron a comportarse de forma anómala sin que los usuarios descargaran archivos. El malware se propagó automáticamente dentro de la red. ¿Cuál es el tipo de software malicioso más probable?**

A. Virus

B. Ransomware

C. Gusano (Worm)

D. Spyware

3**. Un atacante deja memorias USB infectadas en el parqueadero de una empresa, esperando que algún empleado las conecte a su equipo. Este ataque corresponde a:**

A. Ataque de agujero de agua

B. Ingeniería social física

C. USB baiting

D. Phishing en redes sociales

4**. Una víctima recibe una llamada telefónica donde el atacante se hace pasar por soporte técnico y solicita credenciales argumentando una falla crítica inmediata. ¿Qué combinación de ataque y principio de ingeniería social se está aplicando?**

A. Vishing – Urgencia

B. Smishing – Confianza

C. Phishing – Autoridad

D. Spear phishing – Escasez

5**. Un atacante investiga a fondo a un grupo específico de empleados en redes sociales para diseñar un correo altamente personalizado que parece legítimo. ¿Cuál es la característica clave que diferencia este ataque de otros tipos de phishing?**

A. Uso de mensajes de texto

B. Enfoque masivo sin segmentación

C. Alto nivel de personalización del objetivo

D. Uso exclusivo de llamadas telefónicas