Asignatura	Datos del alumno	Fecha
Seguridad en los Sistemas de Información	Apellidos: Bocanegra Capera	24/03/2025
	Nombre: Oscar David	

Actividad 2. Vectores de ataque

Objetivos

Con esta actividad vas a conseguir documentar un ciberdelito, analizándolo al máximo en su funcionamiento, bien a través de código, vídeos, artículos científicos, prensa, etc.

Descripción de la actividad

Podemos definir un vector de ataque como el camino que usa un ciberdelincuente para acceder al activo objetivo del ataque.

A lo largo de esta asignatura conocerás la existencia de múltiples ciberdelitos: *phising, smishing*, inserción de *malware*, *keyloggers, botnets, pharming, carding, skimming,* fraude del CEO, *rogues* y un largo etcétera, pero en todos estos casos, ¿cómo es el vector de ataque? o al menos ¿cómo creemos que haya podido ser?, es esta la tarea que se os asigna en esta actividad.

Un pequeño ejemplo concreto: si quisieras entender un *ransomware* y dar respuesta a cómo infecta una máquina, primeramente, verías un vector de ataque en forma de ingeniería social, convenciendo al usuario que haga *click* en algún sitio determinado, a partir empieza a recorrer directorios del disco, haciendo el cifrado correspondiente, para a continuación recibir un mensaje de rescate de la clave de descifrado. Esto es un proceso cíclico y bien se puede encontrar como es en Internet, aunque cuando lo veas en clase, lo acabarás de entender.

Asignatura	Datos del alumno	Fecha
Seguridad en los Sistemas de Información	Apellidos: Bocanegra Capera	24/03/2025
	Nombre: Oscar David	

Evalúa la calidad de la información que dan estas herramientas, y si crees que, en manos no deseadas, pudieran ser el inicio de un delito contra la persona. ¿Crees que es fácil realizar un delito informático con la información recopilada?, en caso afirmativo, ¿Cómo crees que se podrían evitar?

Rúbrica

Delitos informáticos en fuentes abiertas	Descripción	Puntuación máxima (puntos)	Peso %
Criterio 1	Información recopilada	4	40
Criterio 2	Explicación detallada del ataque	4	40
Criterio 3	Recomendaciones para evitar el ataque	2	20
		10	**100 %**

Extensión de la actividad

Sin delimitación de extensión. Puede ser viable entregar código fuente, vídeos demostrativos o tantos recursos como se estime oportuno.

Asignatura	Datos del alumno	Fecha
Seguridad en los Sistemas de Información	Apellidos: Bocanegra Capera	24/03/2025
	Nombre: Oscar David	

Para el desarrollo de esta actividad he elegido el método de phishing en donde desarrollare una investigación sobre esta modalidad de cibercrimen, daré algunas recomendaciones para evitar ser víctima de esta.

¿Como funciona el phishing?

Para este caso puedo indicar que el phishing es un método o una técnica de ingeniería social en donde los ciberdelincuentes buscan obtener información privada o delicada de su objetivo, ya sea una persona en especial o una empresa, la mayoría de las veces buscan encontrar contraseñas, datos bancarios o números de tarjetas de crédito, por ende, se puede decir que este método se basa en el engaño, donde los atacantes se hacen pasar por entidades legítimas para así poder manipular a los usuarios y que realicen acciones que comprometan su seguridad.

A continuación, voy a poner un paso a paso de cómo es que los ciberdelincuentes realizan el proceso de este método de ciberataque.

1. Selección del objetivo (empresa o persona)
2. Creación del mensaje fraudulento (Pagina web, SMS, enlace a su correo)
3. Envío del mensaje
4. Interacción de la víctima
5. Robo de información

Y para dar un contexto de este método encontré que en España se involucró una estafa de phishing relacionada con la cadena de tiendas de Costco en donde los atacantes enviaron correos electrónicos fraudulentos a las víctimas en donde se les informaba que habían ganado un iPhone 16 Pro y que debían seguir un enlace para reclamar el premio pero al hacer clic en el enlace, las víctimas eran dirigidas a páginas web falsas que solicitaban información personal, la cual era posteriormente utilizada por los ciberdelincuentes para realizar compras no autorizadas o instalar programas maliciosos en los dispositivos de las víctimas.

Ya teniendo el acceso de la información de sus víctimas se encontró que estas enfrentaron diversas consecuencias, como pérdidas financieras, robo de identidad y compromisos de seguridad en sus cuentas personales y/o laborales. Adicional a esto,

la organización afectada puede sufrir daños reputacionales y pérdidas económicas significativas.

Vector de ataque

Como ya lo mencioné anterior mente cual era como funcionaba este método, o como es que se planificaba, el cual también se entiende como el vector de ataque, pero en este apartado voy a especificar un poco más sobre esta información en donde encontré que:

El primer paso es la selección del objetivo, y este es el punto en el que los ciberdelincuentes identifican a sus víctimas, estas pueden ser parte de una compañía o una persona en particular, ya teniendo esto claro los delincuentes investigan a fondo a sus objetivos para personalizar el ataque y aumentar su efectividad en el proceso del ataque.

Ya el segundo paso es la creación de un mensaje fraudulento, y acá es donde empiezan a elaborar un mensaje que aparente ser legitimo y confiable, esto ya lo hacen dependiendo de su objetivo, en donde lo pueden realizar mediante mensaje SMS vía teléfono, o un correo con ciertos enlaces para ver si la victima cae en estos, además de esto en muchas ocasiones usan instituciones gubernamentales para que caigan con mayor facilidad.

Ya teniendo el mensaje listo, es donde añaden los enlaces o los archivos maliciosos para realizar el respectivo robo de información, ya que estos enlaces los dirigen a sitios web falsos diseñados para parecerse a los legítimos lugares o archivos adjuntos que, al ser descargados, instalan un malware en el dispositivo de la víctima haciendo que estos sitios o archivos están diseñados para capturar información sensible o comprometer la seguridad del dispositivo.

El siguiente paso ya es la distribución de dicho mensaje en donde los ciberdelincuentes envían el mensaje a las víctimas seleccionadas a través de correo electrónico, mensajes de texto (SMS), aplicaciones de mensajería instantánea o incluso redes sociales cabe aclarar que la distribución de dicho mensaje puede ser masiva o dirigida, dependiendo del objetivo del ataque definido anteriormente.

Enviado el mensaje y si la víctima logra ser engañada por la apariencia legítima del mensaje este puede hacer clic en el enlace proporcionado o descargar el archivo adjunto. Al hacer esto, la victima va a ser redirigida a un sitio web falso que solicita información personal o se instala malware en su dispositivo sin su conocimiento.

Y ya por último habiendo logrado su objetivo los ciberdelincuentes realizan el respectico robo y explotación de la información obtenida

Para el caso presentado anteriormente, podemos decir que este se ejecutó vía correo electrónico en donde enviaban un mensaje que indicaba que habían ganado un iPhone 16 Pro y que debían seguir un enlace para reclamar el premio.

Ya la persona al hacer clic en dicho enlace para reclamar el premio las víctimas eran dirigidas a páginas web falsas que solicitaban información personal, la cual era posteriormente utilizada por los ciberdelincuentes para realizar compras no autorizadas o instalar programas maliciosos en los dispositivos de las víctimas.

Accesibilidad de la Información sobre Phishing

Para este apartado voy a evaluar la calidad de la información sobre el phishing la cual es esencial para comprender su funcionamiento y las medidas de prevención adecuadas, por ende, a continuación, se analiza la accesibilidad y confiabilidad de la información disponible en donde encontré que:

La información sobre el phishing es muy accesible a través de diversas fuentes en la web como lo pueden ser instituciones gubernamentales y de seguridad, empresas de seguridad informática, medios de comunicación y educaciones educativas.

Las entidades mencionadas anteriormente ofrecen recursos (lecturas, documentos, videos) detallados sobre información de que es el Phishing, como podemos prevenirlo, como identificarlo, además de esto compañías grandes, por comentar una Microsoft proporcionan guías y herramientas para detectar y prevenir ataques de phishing, lo cual hace que tengamos la información necesaria en la web para enterarnos que es este método de ciberataque, como funciona y demás información que consideremos pertinente.

Dejare los enlaces de las páginas mencionadas anteriormente

1. https://www.incibe.es/aprendeciberseguridad/phishing?utm_source=chatgpt.com
2. https://www.microsoft.com/es-mx/security/business/security-101/what-is-phishing?utm_source=chatgpt.com
3. https://as.com/meristation/betech/el-fbi-lanza-un-aviso-a-todos-los-usuarios-de-chome-safari-y-edge-cuidado-con-estas-paginas-web-n/?utm_source=chatgpt.com

Con esta información como base puedo decir que la calidad de la información disponible es en términos generales alta debido a que proviene de fuentes oficiales y reconocidas en el ámbito de la ciberseguridad. Además de esto cabe aclarar que estas fuentes suelen proporcionar datos actualizados, ejemplos reales y consejos prácticos para la prevención.

Preguntas clave

¿Crees que es fácil realizar un delito informático con la información recopilada?, en caso afirmativo, ¿Cómo crees que se podrían evitar?

Personalmente considero que si es fácil realizar un delito de este modelo debido a que para individuos con conocimientos básicos de informática les es fácil llevar a cabo ataques de phishing por su bajo grado de complejidad hoy en día ya que pueden perfeccionar sus modelos con diferentes tipos de inteligencias artificiales y además

de esto la abundancia de información disponible en línea, incluyendo tutoriales y herramientas diseñadas para este propósito, facilita la ejecución de estos delitos.

Y para dar respuesta a la segunda pregunta considero que para evitar caer en este método debemos de educarnos de una mejor manera a la hora de todo esto de los robos cibernéticos, ya que con el avance de la tecnología día a día son más comunes, pero sí de igual manera tenemos esa curiosidad de saber como es que se efectúan y cómo podemos hacer nosotros para no caer, los riesgos van a ser mucho menores, además de esto deberíamos de aplicar aspectos como la educación y la concienciación para poder detectar y aprender a reconocer señales de alerta, como errores gramaticales, solicitudes de información personal o enlaces sospechosos además de esto debemos de dudar mucho sobre las fuentes que recibimos y que no hemos solicitado.

Recomendaciones de prevención

Formación Continua: Acá lo que se va a buscar es que los empleados y usuarios reciban formación regular sobre las tácticas de phishing y cómo identificarlas para así lograr reconocer correos electrónicos sospechosos, enlaces fraudulentos y solicitudes inusuales de información.

Simulacros de Phishing: Al realizar pruebas periódicas mediante simulaciones de ataques de phishing ayuda a evaluar la preparación y respuesta de los empleados, fortaleciendo la cultura de seguridad dentro de la organización. (globallogic, 2023)

Verificar la autenticidad de los mensajes: No confiar en correos electrónicos o mensajes que soliciten información personal o financiera y aún más cuando estos provienen de fuentes no verificadas.

No hacer clic en enlaces sospechosos: Evitar seguir enlaces o descargar archivos adjuntos de remitentes desconocidos o inesperados.

Utilizar medidas de seguridad adicionales: Implementar autenticación de dos factores (2FA) en cuentas sensibles y mantener actualizados los sistemas y programas de seguridad.

Asignatura	Datos del alumno	Fecha
Seguridad en los Sistemas de Información	Apellidos: Bocanegra Capera	24/03/2025
	Nombre: Oscar David	