Guía de Estudio en Español

CompTIA Security+ (SY0-701) — Capítulo 6

Comparing Threats, Vulnerabilities, and Common Attacks — Amenazas, Vulnerabilidades y Ataques Comunes

---

Este material es un **resumen conceptual elaborado con palabras propias**, pensado como guía de apoyo para estudiar junto al libro original en inglés. No es una traducción ni una reproducción del texto original; cubre los mismos temas, en el mismo orden, para facilitar el repaso en español.

Incluye: resumen por secciones, tablas comparativas, glosario EN↔ES y preguntas de práctica originales.

1. Actores de Amenaza (Threat Actors)

Actor	Motivación principal	Características
Nación-estado / APT	Intereses geopolíticos, espionaje.	Alta sofisticación y financiamiento; ataques dirigidos y prolongados.
Crimen organizado	Dinero.	Estructura jerárquica similar a una empresa (ej. ransomware Ryuk).
Atacante sin habilidad (script kiddie)	Aburrimiento, curiosidad.	Poca sofisticación y financiamiento; usa herramientas ya hechas.
Hacktivista	Causa política o social.	Busca visibilidad, no beneficio propio.
Insider (interno)	Codicia, venganza, o accidental.	Tiene acceso legítimo; el riesgo depende de su nivel de acceso.

Atributos de los atacantes: interno vs. externo, nivel de recursos/financiamiento, y nivel de sofisticación/capacidad. **Shadow IT:** sistemas o aplicaciones no autorizados dentro de una organización, que quedan fuera de la gestión de IT y por lo tanto sin parches ni monitoreo.

Motivaciones comunes: exfiltración de datos, espionaje, interrupción de servicio, chantaje, ganancia financiera, creencias filosóficas/políticas, ética (hackers de sombrero blanco), venganza, caos/disrupción, y guerra.

2. Vectores de Amenaza y Superficie de Ataque

Un vector de amenaza es el camino que usa un atacante para acceder a un sistema. La **superficie de ataque** es el conjunto total de vectores a los que está expuesta una organización — reducirla es una de las tareas clave de un profesional de seguridad.

- **Basado en mensajes:** email, SMS, mensajería instantánea — se estima que el 91% de los ataques comienza con un correo.
- **Basado en imágenes / archivos:** código malicioso oculto en imágenes (esteganografía) o documentos.
- **Llamadas de voz, dispositivos removibles, software vulnerable, sistemas sin soporte, redes inseguras, puertos abiertos, credenciales por defecto, cadena de suministro (proveedores, MSPs).**

3. Tipos de Malware

Tipo	Característica clave
Virus	Se adhiere a una aplicación anfitriona; necesita ejecutarse para activarse y replicarse.
Gusano (worm)	Se autorreplica por la red sin necesidad de anfitrión ni interacción del usuario; consume ancho de banda.
Troyano	Parece útil pero es malicioso; suele llegar por drive-by download o scareware.
RAT (Remote Access Trojan)	Troyano que da control remoto total del sistema al atacante.
Ransomware	Cifra los datos y exige un rescate para la clave de descifrado.
Keylogger	Captura las pulsaciones del teclado; el MFA lo neutraliza parcialmente.
Spyware	Monitorea al usuario sin su consentimiento; a menudo incluye un keylogger.
Rootkit	Obtiene acceso a nivel raíz/kernel; oculta sus procesos ('hooking') para evadir el antivirus.
Logic bomb	Se activa ante un evento específico (fecha, acción, ausencia de un nombre en nómina).
Bloatware	Software no deseado instalado junto con otro programa; puede secuestrar el navegador.

Indicadores generales de malware: tráfico extra en la red, exfiltración de datos, tráfico cifrado inusual, conexiones a IPs conocidas de comando y control, y envío de spam saliente desde equipos que normalmente no envían correo masivo (indica que forman parte de una botnet).

4. Ingeniería Social y Vectores Humanos

La ingeniería social usa tácticas sociales (no técnicas) para obtener información o hacer que alguien actúe de forma que normalmente no lo haría.

Técnica	Descripción
Impersonación	Hacerse pasar por otra persona (técnico, autoridad) para obtener acceso o información.
Shoulder surfing	Espiar por encima del hombro para ver credenciales o PINs.
Desinformación / hoax	Mensajes falsos (a menudo por email) sobre amenazas inexistentes que inducen a actuar mal.
Tailgating / piggybacking	Seguir a alguien autorizado sin mostrar credenciales propias; los mantraps lo previenen.
Dumpster diving	Buscar información en la basura; se mitiga triturando o incinerando documentos.
Watering hole	Infectar un sitio que el grupo objetivo visita habitualmente y en el que confía.
BEC (Business Email Compromise)	Suplantar a un ejecutivo por email para autorizar transferencias fraudulentas.
Typosquatting	Registrar un dominio con una ligera falta de ortografía del original.
Suplantación de marca	Imitar el logo/diseño de una empresa confiable para engañar a la víctima.
Elicitación	Obtener información sin pedirla directamente (escucha activa, preguntas reflexivas, afirmaciones falsas, 'bracketing').
Pretexting	Inventar una historia convincente para manipular a la víctima.

4.1 Ataques basados en mensajes

- **Spam / SPIM:** correo no deseado / spam por mensajería instantánea o SMS.
- **Phishing:** correos que buscan engañar al usuario para revelar información o hacer clic en un enlace malicioso.
- **Spear phishing:** phishing dirigido a un grupo específico. **Whaling:** spear phishing dirigido a ejecutivos de alto nivel.
- **Vishing:** phishing por teléfono/VoIP. **Smishing:** phishing por SMS.

4.2 Principios psicológicos que explotan estos ataques

Autoridad, intimidación, consenso (prueba social), escasez, urgencia, familiaridad y confianza — reconocer estos principios ayuda a los usuarios a identificar cuándo están siendo manipulados.

5. Bloqueo de Malware y Otros Ataques

- **Filtros de spam** en el gateway de correo, en el servidor y en el cliente.
- **Antivirus/antimalware:** detección por *firmas* (patrones conocidos) o *heurística* (comportamiento sospechoso, útil contra malware polimórfico y amenazas de día cero).
- **Monitores de integridad de archivos:** calculan hashes de archivos críticos y alertan si cambian — útil para detectar rootkits.

6. Fuentes de Inteligencia de Amenazas

- **OSINT (Open-Source Intelligence):** información disponible públicamente (sitios web, redes sociales).
- **Bases de datos de vulnerabilidades:** NVD (NIST) y CVE (MITRE).
- **STIX / TAXII:** STIX define qué información compartir sobre amenazas; TAXII define cómo compartirla.
- **Dark web:** zona de Internet no indexada por buscadores, usada por criminales para vender herramientas de hacking y datos robados; a veces revela vulnerabilidades antes de que aparezcan en bases de datos oficiales.
- **Indicadores de compromiso (IoC):** evidencia de que un ataque ocurrió o está ocurriendo (ej. alertas de antivirus, URLs de malware conocidas).
- **Organizaciones de intercambio de información:** como InfraGard (FBI).

7. Glosario de Términos Clave (Inglés ↔ Español)

Inglés	Español	Definición breve
Threat actor	Actor de amenaza	Cualquiera que lanza un ciberataque.
APT (Advanced Persistent Threat)	Amenaza persistente avanzada	Grupo organizado, generalmente patrocinado por un estado.
Unskilled attacker / script kiddie	Atacante sin habilidad	Usa herramientas ya creadas, poca sofisticación.
Hacktivist	Hacktivista	Ataca por una causa política o social.
Insider threat	Amenaza interna	Persona con acceso legítimo que representa un riesgo.
Shadow IT	TI en la sombra	Sistemas o apps no autorizados dentro de la organización.
Attack surface	Superficie de ataque	Conjunto de vectores a los que está expuesta la organización.
Ransomware	Ransomware	Malware que cifra datos y exige rescate.
Trojan / RAT	Troyano / RAT	Malware disfrazado de algo útil / con control remoto.
Worm	Gusano	Malware autorreplicante sin necesidad de anfitrión.
Rootkit	Rootkit	Malware con acceso a nivel raíz que oculta su actividad.
Keylogger	Registrador de teclas	Captura las pulsaciones del teclado.
Logic bomb	Bomba lógica	Código que se activa ante un evento específico.
Bloatware	Software basura	Programas no deseados instalados junto a otro software.
Social engineering	Ingeniería social	Tácticas sociales para obtener información o acceso.
Phishing / spear phishing / whaling	Phishing / phishing dirigido / caza de ballenas	Variantes de correo malicioso dirigidas a distintos públicos.
Vishing / smishing	Vishing / smishing	Phishing por teléfono / por SMS.

Inglés	Español	Definición breve
Pretexting	Pretextos	Historia inventada para manipular a la víctima.
Tailgating	Colarse detrás (tailgating)	Seguir a alguien autorizado sin mostrar credenciales.
Watering hole attack	Ataque de abrevadero	Infectar un sitio que el objetivo visita con frecuencia.
Business Email Compromise (BEC)	Compromiso de correo empresarial	Suplantación de ejecutivos para fraude financiero.
Typosquatting	Typosquatting	Registrar dominios similares con errores tipográficos.
OSINT	Inteligencia de fuente abierta	Información de amenazas disponible públicamente.
Indicators of compromise (IoC)	Indicadores de compromiso	Evidencia de un ataque en curso o pasado.
Dark web	Dark web / internet oscura	Zona de Internet no indexada, usada por criminales.

8. Preguntas de Práctica (Autoevaluación)

Preguntas de elaboración propia, en español, para repasar los conceptos del capítulo 6. Las respuestas están al final.

1. Una empresa sufre un ataque muy sofisticado y prolongado, con evidencia de que proviene de un gobierno extranjero. ¿Qué tipo de actor de amenaza es el más probable?

2. Un exempleado deja un fragmento de código en el sistema de nómina que borra archivos importantes si su nombre deja de aparecer en la lista de empleados. ¿Cómo se llama este tipo de malware?

3. Un usuario recibe un mensaje de texto que dice ser de su banco, pidiéndole que responda con un código de verificación para evitar el bloqueo de su cuenta. ¿Qué tipo de ataque es?

4. Un atacante identifica que los desarrolladores de una empresa visitan frecuentemente cierto foro técnico y coloca malware en ese sitio para infectarlos. ¿Cómo se llama esta técnica?

5. Un empleado recibe un correo que parece venir del CEO pidiendo una transferencia urgente de dinero a una cuenta desconocida. ¿Cómo se llama este tipo específico de ataque?

6. Un atacante registra el dominio 'gmial.com' esperando que usuarios que escriben mal 'gmail.com' terminen en su sitio. ¿Cómo se llama esta técnica?

7. Un antivirus detecta un archivo que se comporta de forma sospechosa (crea copias con variaciones) aunque no coincide con ninguna firma conocida. ¿Qué método de detección lo identificó?

8. Una empresa recibe alertas porque varios de sus equipos de escritorio, normalmente silenciosos, están enviando grandes cantidades de correo saliente. ¿Qué es lo más probable que haya pasado?

9. Un investigador de seguridad quiere consultar información sobre vulnerabilidades conocidas y parches disponibles para un software específico, usando una fuente pública y confiable. ¿A qué tipo de base de datos debería recurrir?

10. Un atacante logra hacer que la recepcionista de una empresa le entregue acceso a la sala de servidores, haciéndose pasar por un técnico de mantenimiento con una historia convincente. ¿Qué técnica de ingeniería social combina impersonación con una historia inventada?

Respuestas

1. Un actor de nación-estado (posiblemente una APT) — por el nivel de sofisticación y el origen extranjero.

2. Una bomba lógica (logic bomb) — se ejecuta en respuesta a un evento específico.

3. Smishing — phishing realizado por mensaje de texto (SMS).

4. Un ataque de abrevadero (watering hole attack).

5. Compromiso de correo empresarial (Business Email Compromise, BEC).

6. Typosquatting — registrar un dominio con una falta de ortografía similar al original.

7. Detección heurística (heuristic-based) — identifica comportamiento sospechoso sin necesitar una firma conocida.

8. Es probable que los equipos formen parte de una botnet y estén enviando spam/phishing como zombis.

9. Bases de datos de vulnerabilidades como el NVD (NIST) o el CVE (MITRE).

10. Pretexting combinado con impersonación — el atacante se hace pasar por otra persona usando una historia inventada.
