





Resumen Profesional: Módulo de Recursos, Amenazas y Vulnerabilidades

 Portfolio de Ciberseguridad – Michel Macías (M1txel)

Superficie de Ataque: Fundamento de toda Defensa






- La **superficie de ataque** representa todos los puntos vulnerables que pueden ser explotados por un atacante.
 - Puede ser:
 - **Física** (personas y dispositivos).
 - **Digital** (sistemas conectados a la red y servicios en la nube).
 - Cuanto más extensa es, **más difícil es de proteger**.
 -  **Hardening o endurecimiento de seguridad**: proceso de reducción de puntos de entrada.
-

Mentalidad de Atacante: Pensar como el enemigo




- Adoptar el enfoque del adversario permite:
 - Evaluar riesgos de forma proactiva.
 - Diseñar estrategias realistas de defensa.
- Se simulan escenarios mediante:
 -  **Equipos rojos** (simulan ataques reales).
 -  **Equipos azules** (responden a ataques).
-  Utilización de escáneres de vulnerabilidades:
 - Identificación.
 - Análisis.

- Evaluación de riesgos.
- Remediación.

Agentes de Amenaza: ¿Quiénes son los adversarios?

Tipo de Agente	Descripción
 Competidores	Buscan explotar fugas de información para obtener ventajas.
 Actores estatales	Servicios de inteligencia con fines estratégicos o geopolíticos.
 Cibercrimen organizado	Grupos que obtienen beneficios económicos de actividades ilícitas.
 Amenaza interna	Personas con acceso legítimo que ponen en riesgo la organización.
 TI en la sombra	Uso de tecnologías sin supervisión del departamento de IT.








Tipos de Hackers

Tipo	Descripción
 No autorizados	Atacantes maliciosos (script kiddies, criminales, etc.).
 Éticos (white hat)	Profesionales que ayudan a mejorar la seguridad de sistemas.
 Semiautorizados	Activistas o hacktivistas con motivación ideológica o política.

Amenazas Persistentes Avanzadas (APT)


- **Definición:** Accesos no autorizados prolongados, difíciles de detectar.
- Usadas por **grupos patrocinados por estados**.
- Su objetivo: vigilancia, espionaje, robo de datos sensibles.
- Las **empresas privadas** son frecuentemente las primeras víctimas.

Vectores de Ataque: Puntos de entrada comunes

Vector de Ataque	Ejemplo
 Acceso físico directo	Manipulación directa de dispositivos.
 Medios extraíbles	USBs o discos con malware.
 Redes sociales	Ingeniería social, suplantación de identidad.
 Correo electrónico	Phishing, spam malicioso.
 Redes inalámbricas	Ataques de tipo MITM, redes Wi-Fi inseguras.
 Servicios en la nube	Fallos de configuración, exposiciones no intencionadas.
 Cadenas de suministro	Brechas indirectas a través de proveedores comprometidos.

Recomendaciones Clave para Técnicos en Ciberseguridad

- **Piensa como un atacante.**
 - **Simula ataques y estudia respuestas.**
 - **Evalúa vulnerabilidades de forma sistemática.**
 - **Informa de los hallazgos con claridad.**
 - **Adáptate a nuevas amenazas tecnológicas.**
 - Usa recursos como la **NVD del NIST** para estar actualizado.
-

 *Este documento forma parte de mi aprendizaje y práctica como profesional de ciberseguridad. Ha sido elaborado como parte del módulo de evaluación de amenazas y vulnerabilidades, y tiene como objetivo demostrar la aplicación de conceptos clave en entornos reales de defensa de sistemas informáticos.*