Guía de Estudio: Temas Avanzados de Ciberseguridad (Clase 4)

Esta tabla resume los conceptos clave presentados para proporcionar una visión más completa del ecosistema de la ciberseguridad.

Tema	¿Qué es? (Definición)	Concepto Clave / Objetivo	Conexión con el Curso / Herramientas
1. OSINT	**Inteligencia de Fuentes Abiertas.** Es la disciplina de recopilar y analizar información de fuentes públicas (internet, redes sociales, registros de dominios) para construir un perfil de un objetivo.	**Reconocimiento Pasivo:** Obtener la máxima cantidad de información sobre un objetivo sin interactuar directamente con sus sistemas, lo que lo hace indetectable.	**Herramientas:** whois (para registros de dominio), dig (para enumeración de DNS), Google Dorking (búsquedas avanzadas), Shodan.
2. Ingeniería Social	Es el arte de la manipulación psicológica para engañar a las personas y hacer que divulguen información confidencial o realicen acciones que comprometan la seguridad.	**Atacar al "Eslabón Humano":** La persona es a menudo el punto más débil. El objetivo es obtener credenciales, acceso físico o información sensible.	**Ejemplo:** El **Phishing** (correos fraudulentos) es la técnica más común. No se basa en comandos, sino en la confianza y el engaño.
3. Tipos de Malware	Software diseñado específicamente para dañar, interrumpir u obtener acceso no autorizado a un sistema informático.	**Entender la Amenaza:** Conocer los tipos de malware ayuda a identificar el objetivo del atacante (lucro, espionaje, destrucción).	**Tipos Comunes: Ransomware** (cifra datos y pide rescate), **Spyware** (espía al usuario), **Troyano** (se disfraza de software legítimo para crear una puerta trasera).

4. OWASP Top 10	Es un documento de referencia creado por la fundación OWASP que lista los 10 riesgos de seguridad más críticos en aplicaciones web.	**Estándar de Seguridad Web:** Proporcionar una guía para desarrolladores y profesionales de la seguridad sobre las vulnerabilidades más importantes a mitigar.	**Ejemplos: Inyección SQL** (engañar a la base de datos), **Cross-Site Scripting (XSS)** (inyectar scripts en el navegador de otra víctima).
5. Explotación: Shells y Payloads	**Exploit:** El código que aprovecha una vulnerabilidad. **Payload:** La carga maliciosa que el exploit entrega. **Shell:** El objetivo más común del payload, que es obtener una línea de comandos en la víctima.	**Obtener Control (Gaining Access):** El objetivo es pasar de tener conocimiento de una vulnerabilidad a tener control práctico sobre el sistema.	**Tipos de Shell: Reverse Shell** (la víctima se conecta al atacante, bueno para saltar firewalls) y **Bind Shell** (el atacante se conecta a la víctima).
6. Post-Explotación	Son las acciones que realiza un atacante **después** de haber obtenido acceso inicial a un sistema.	**Mantener y Expandir el Acceso:** El objetivo no es solo entrar, sino quedarse y moverse a otros sistemas dentro de la red.	**Técnicas: Persistencia** (cron jobs, servicios de systemd en Linux) y **Movimiento Lateral** (usar el primer equipo como pivote para atacar otros).
7. Fundamentos de Criptografía	Es la ciencia de asegurar la comunicación y la información mediante el uso de códigos, de modo que solo aquellos para quienes está destinada puedan leerla y procesarla.	**Garantizar la Tríada de la CIA** (Confidencialidad, Integridad, Disponibilidad).	**Conceptos: Hashing** (/etc/shadow en Linux), **Cifrado Simétrico** (una clave), **Cifrado Asimétrico** (clave pública/privada, usado en **SSH** y **HTTPS**).
8. Arsenal Defensivo	Son las tecnologías y herramientas que utiliza el **Blue Team** para proteger la infraestructura de una organización.	**Defensa en Profundidad:** Crear múltiples capas de seguridad para que, si una falla, otra pueda detener el ataque.	**Herramientas: Firewall** (filtra tráfico de red), **IDS** (detecta intrusiones), **IPS** (previene intrusiones activamente). Son la contraparte de nmap.

9. SIEM y Análisis de Logs	Un **SIEM** es una plataforma que centraliza y correlaciona logs de múltiples fuentes para detectar amenazas en tiempo real.	**Visibilidad y Detección Centralizada:** Encontrar la "aguja en el pajar" al analizar millones de eventos de seguridad de toda la red desde un solo lugar.	**Conexión:** Es la versión a gran escala de lo que aprendimos en Linux: analizar logs (/var/log) usando grep y tail, pero de forma automatizada y correlacionada.
10. Honeypots	Son sistemas o recursos "señuelo" diseñados para ser atractivos para los atacantes, con el fin de distraerlos y estudiar sus métodos.	**Defensa Proactiva y Engaño:** Atraer a los atacantes a un entorno controlado para analizar sus Tácticas, Técnicas y Procedimientos (TTPs) sin poner en riesgo los sistemas reales.	Es una estrategia avanzada del Blue Team, no se asocia a un comando simple, sino a la configuración de sistemas trampa.
11. Seguridad en la Nube	Es el conjunto de políticas, tecnologías y controles para proteger datos, aplicaciones e infraestructura en entornos de computación en la nube (AWS, Azure, GCP).	**Modelo de Responsabilidad Compartida:** El proveedor de la nube asegura la infraestructura física ("seguridad **de** la nube"), pero el cliente debe asegurar lo que despliega ("seguridad **en** la nube").	Es un área de especialización moderna y con alta demanda laboral que aplica los mismos principios de Linux y redes en un entorno virtualizado.
12. CTFs y Laboratorios	Un **CTF (Capture The Flag)** es una competencia de ciberseguridad. Un **Laboratorio en Casa** es un entorno controlado para practicar.	**Aprendizaje Práctico y Continuo:** La mejor manera de mejorar las habilidades es a través de la práctica constante en entornos seguros y legales.	**Siguiente Paso:** Usar **VirtualBox** para crear máquinas virtuales (como **Kali Linux** para el atacante y **Metasploitable** como víctima) y aplicar todo lo visto en el curso.