✅ Teóricos

1. Purple team y red team

- **Función del Purple Team:** Su función principal es mejorar la seguridad colaborando entre Red Team (atacantes) y Blue Team (defensores), asegurando que ambos equipos aprendan y se fortalezcan mutuamente.
- **Objetivo principal:** Maximizar la eficacia de las pruebas de seguridad y mejorar la detección y respuesta.
- **Fases principales:** Participa durante la ejecución y post-ejecución del pentest (simulaciones de ataque), en la fase de análisis de resultados y en la mejora continua de controles defensivos.
- **Rol del Red Team:** Simular ataques reales (externos o internos) para identificar vulnerabilidades y probar la capacidad de detección y respuesta del Blue Team. Su objetivo es emular a un adversario realista.

🟦 Blue Team (en vez de Purple Team)

- **Función principal:** Defender y proteger la infraestructura de la organización.
- **Objetivo:** Detectar, responder y mitigar incidentes de seguridad.
- **Actividades:**
    - Monitoreo continuo (SIEM, IDS/IPS).
    - Gestión de incidentes.
    - Implementación y control de políticas de seguridad.

---

2. Técnica para evitar ingeniería reversa y diferencia CTF vs Bug Bounty

- **Técnica para evitar ingeniería reversa:**
    - **Ofuscación de código**: técnica que modifica el código (por ejemplo, renombrando variables, funciones o flujos lógicos) para hacerlo ilegible y difícil de analizar.
- **Diferencias:**
    - **CTF (Capture The Flag):** retos diseñados en ambientes controlados para practicar y aprender, con objetivos educativos y competitivos.
    - **Bug Bounty:** programas reales ofrecidos por empresas para que investigadores encuentren y reporten vulnerabilidades en sistemas productivos, a cambio de recompensas.

---

3. Vulnerabilidad Zero Day

- **Definición:** Vulnerabilidad desconocida públicamente, sin parche disponible al momento de ser descubierta.
- **Ciclo de vida:**
    1. Descubrimiento.
    2. Exploitation privado (por actores maliciosos o investigadores).
    3. Divulgación responsable o venta en mercado negro.
    4. Desarrollo y liberación de parche.
    5. Uso público y explotación masiva si no se aplica el parche.
- **Ejemplo:** La vulnerabilidad EternalBlue (MS17-010) explotada por WannaCry antes de ser parchada.

💡 Beneficios de DevSecOps

- Identificar y corregir vulnerabilidades desde el diseño.
- Responder a ataques más rápido.
- Mejor comunicación y mayor conciencia de seguridad en el equipo.

⚫ ⚪ Black box vs White box

- **Black box:**
    - No se conoce nada del sistema (como un atacante externo).
    - Se basa en descubrimiento y enumeración.
- **White box:**
    - Se tiene acceso a información interna (código fuente, diagramas).
    - Simula pruebas más profundas, con contexto.

👨‍⚖️ Rol del perito de parte

- Representa y defiende los intereses de una de las partes en un proceso judicial (puede ser empresa, persona física, etc.).
- Realiza su propio análisis técnico y puede cuestionar el peritaje oficial.
- Puede presentar informes y explicar ante el juez.

🔗 Cadena de custodia

- **Definición:** Registro documentado que detalla quién tuvo acceso a la evidencia digital, cuándo, dónde y cómo se manipuló.
- **Importancia:**
    - Garantiza que la evidencia no haya sido alterada.
    - Permite que sea admisible en un tribunal.
    - Mantiene la integridad y autenticidad de los datos.

🛠️ Fases de un Pentest

1️⃣**Acuerdo de Confidencialidad (NDA)**

Se firma un contrato legal para proteger la información y limitar su uso.

2️⃣Reconocimiento (Información pasiva)

Recolección de información sin interactuar directamente con el sistema para no levantar alarmas.

- Herramientas: Google Dorks, Shodan, Whois, redes sociales.
- Google Dorks: Búsquedas avanzadas (ej: site:ar inurl:passwords filetype:xls para buscar archivos con contraseñas en Argentina).

3️⃣Enumeración (Información activa)

Se interactúa con el sistema para obtener más datos (por ejemplo, escanear puertos y servicios).

- Se usan escáneres de vulnerabilidades y herramientas de análisis.

4️⃣Explotación

Se aprovechan las vulnerabilidades encontradas.

- Repositorios de exploits: exploit-db.com, packetstormsecurity.org, Metasploit.

5️⃣Post-explotación

Payload: Código malicioso ejecutado tras el exploit para tomar control o extraer datos.

Mantener el acceso: Se instalan backdoors, troyanos o rootkits para seguir accediendo.

Borrar rastros: Se eliminan logs y huellas para evitar ser detectados.

6️⃣Informe final

Informe ejecutivo: Resumen claro y no técnico, dirigido a directivos. Explica riesgos y conclusiones con gráficos y estado general.

Informe técnico: Detallado, incluye herramientas usadas, vulnerabilidades encontradas (nombre, gravedad, descripción, impacto, recomendación, referencias y CVEs), evidencias y capturas.

---

4. Tipos de sombreros y fases omitidas

- **Tipos:**
  - **White Hat:** ético, autorizado, realiza pruebas controladas.
  - **Black Hat:** malicioso, sin permiso, con fines dañinos.
  - **Gray Hat:** sin permiso, pero sin intención maliciosa (a veces informa la vulnerabilidad).
- **Fases que no realiza un Black Hat:**
  - No hace informes detallados al cliente.
  - No ejecuta pruebas con planificación ni acuerdo previo.
  - No remedia ni ayuda a mejorar la seguridad.

---

5. Puntos de pericia y perito

- **Puntos de pericia:** Conjunto de cuestiones técnicas específicas que debe responder el perito para el juez. Son determinadas por el juez o la autoridad judicial.
- **Rol del perito oficial:** Profesional designado por el poder judicial para analizar evidencia digital, emitir informes técnicos y asistir al tribunal como experto.

✅ Prácticos

1. Informe técnico — vulnerabilidad crítica

Alcance:
Pentest externo a la plataforma de trámites online municipal, centrado en la identificación de fallas de exposición de datos sensibles.

Técnicas y herramientas:

- Escaneo de directorios y archivos públicos usando **Dirb**, **Dirbuster** o **Gobuster**.
- Validación manual de los hallazgos.

Impacto sobre CID:

- **Confidencialidad:** total pérdida; datos personales expuestos.

- **Integridad:** posibilidad de manipulación indirecta.
- **Disponibilidad:** potencial riesgo si los datos son eliminados o alterados.

Recomendaciones:

- Eliminar inmediatamente `backup.mdb` del servidor público.
- Restringir acceso por controles de permisos y autenticación.
- Configurar revisiones automáticas de directorios y backups expuestos.
- Implementar políticas estrictas de gestión de respaldos.

---

2. Caso Banco de Bangladesh

a) Segmentación y accesos

- Segmentar redes evita que un atacante lateralice desde un sistema comprometido.
- La gestión de accesos limita privilegios mínimos necesarios, reduciendo superficie de ataque.

b) Vectores y técnicas (APT Lazarus)

- Uso de spear phishing para ingresar.
- Movimientos laterales a sistemas SWIFT.
- Instalación de malware especializado para ocultar rastros (ej: wiper y backdoors).

c) Vulnerabilidades explotadas

- **Humanas:** phishing y credenciales robadas.
- **Técnicas:** falta de segmentación, sistemas obsoletos.
- **Organizativas:** falta de controles y monitoreo de transacciones.

---

3. Entorno Windows 7 y SQL Server 2000

a) Errores evidentes

- Sistema sin parches.
- Servicios innecesarios habilitados.
- Cuentas con contraseñas débiles o por defecto.

b) Nmap

- Herramienta de escaneo de red y puertos.
- Se usa en la **fase de reconocimiento y enumeración**.

c) Plan de hardening

Técnicos:

- Desactivar servicios innecesarios.
- Restringir acceso remoto.
- Aplicar parches de seguridad donde sea posible.

Organizativos:

- Revisar contraseñas y roles.
- Segmentar red.
- Supervisión de logs y alertas.

d) Medidas Blue Team

- Monitoreo constante de logs y tráfico.
- Implementación de IDS/IPS.
- Aplicar políticas de autenticación robustas.

---

4. Caso Organismo público

a) Técnicas de relevamiento

- **Entrevistas:** para conocer procesos actuales.
- **Revisión documental y técnica:** análisis de cuentas y accesos en el sistema.

b) Evidencia

- Listado de usuarios activos.
- Logs de acceso y modificaciones.
- Políticas internas escritas (o ausencia).

c) Riesgos

- Acceso no autorizado.
- Robo o manipulación de información.
- Compromiso de sistemas críticos.

---

5. Google Dorks

- **Fase:** Reconocimiento pasivo.
- **Ejemplo de consulta:**

```
site:.edu.ar filetype:doc "curriculum"
```

Este dork busca archivos Word con currículums en sitios educativos argentinos.