<h1>Detectives de la Red: monitoreo, diagnóstico y gestión con herramientas profesionales</h1>

Ingeniería | Ingeniería de sistemas | Aprendizaje Invertido

Descripción

Este plan de clase introduce a los estudiantes de educación técnica/tecnológica en el uso básico de herramientas de gestión y diagnóstico de redes. A partir de un caso práctico, los estudiantes analizarán una red con fallas de conectividad, identificarán dispositivos y servicios autorizados, observarán tráfico de red y propondrán acciones de monitoreo. Se trabajará con herramientas como **ping**, **traceroute/tracert**, **Nmap**, **Wireshark** y una demostración de **Zabbix** o una plataforma equivalente.

La sesión aplica la metodología de Aprendizaje Invertido: antes de la clase, los estudiantes revisan un video breve y una guía de lectura sobre la función de cada herramienta, sus principales comandos y las normas de uso ético. Durante la clase, el tiempo se dedica principalmente a resolver un reto técnico en parejas o grupos pequeños, interpretar evidencias y argumentar decisiones.

El tema es relevante porque las redes están presentes en laboratorios, empresas, hogares, centros educativos y servicios en la nube. Un técnico de sistemas debe saber comprobar si un equipo está disponible, identificar dónde ocurre una falla, reconocer tráfico básico y registrar hallazgos sin afectar la infraestructura. Además, se fortalece la capacidad de trabajar con procedimientos, documentar resultados y utilizar herramientas únicamente en redes propias o autorizadas.

Objetivos de Aprendizaje

- **Identificar** la función principal de herramientas básicas de gestión y diagnóstico de red, como ping, tracert/traceroute, Nmap, Wireshark y Zabbix.
- **Aplicar** comandos y filtros básicos para comprobar conectividad, observar rutas, detectar hosts autorizados y analizar tráfico de red.
- **Interpretar** resultados técnicos sencillos para localizar posibles causas de una falla de conectividad.
- **Documentar** hallazgos y proponer una acción de gestión o monitoreo respetando el uso ético y autorizado de las herramientas.

Recursos Necesarios

- Un computador por pareja, con conexión a una red de laboratorio o simulada y permisos de usuario previamente configurados.

- Software instalado: Wireshark, Nmap, terminal de Windows PowerShell o Linux Bash, y acceso demostrativo a Zabbix, Zabbix Appliance o una interfaz de monitoreo equivalente.
- Archivo de captura de tráfico proporcionado por el docente, por ejemplo **diagnostico_red.pcapng**, para trabajar sin capturar información sensible.
- Guía impresa de comandos y filtros básicos: **ping**, **tracert/traceroute**, **nmap -sn**, **ipconfig/ifconfig** y filtro **icmp** en Wireshark.
- Ficha impresa del caso técnico y formato de informe de diagnóstico para cada pareja.
- Proyector, pizarra y marcadores.
- Video previo de 8 a 10 minutos sobre herramientas de gestión de red y lectura previa de dos páginas.
- Conexión a Internet opcional, únicamente para la demostración de la interfaz de monitoreo.

Requisitos Previos

- Reconocer los conceptos de dirección IP, máscara de red, puerta de enlace y dispositivo final.
- Diferenciar, de manera básica, una red LAN de una conexión a Internet.
- Utilizar una terminal para ejecutar comandos sencillos y leer respuestas de texto.
- Conocer normas básicas de seguridad informática, privacidad y autorización de acceso.
- Haber revisado antes de la sesión el video, la lectura y el cuestionario de cinco preguntas asignado por el docente.

Actividades

Fase de Inicio

Tiempo estimado: 10 minutos.

Propósito de la sesión: Activar los conocimientos previos y presentar un reto cercano al trabajo técnico: determinar por qué un computador de una sala de sistemas no puede acceder a un servidor interno. Los estudiantes utilizarán evidencias, no suposiciones, para decidir qué herramienta usar y qué información registrar.

Activación de conocimientos previos: “¿Qué revisarías primero?” — 4 minutos

- **Docente:** Proyecta la situación: “El equipo PC-07 tiene conexión física, pero no puede abrir el sistema de inventario. Otros equipos sí acceden”. Pregunta exactamente: **“¿Qué tres comprobaciones realizarías antes de cambiar cables o reiniciar el servidor?”**
- **Estudiantes:** Responden individualmente en una tarjeta y escriben qué herramienta utilizarían para cada comprobación.
- **Docente:** Solicita tres respuestas y las organiza en la pizarra bajo las categorías *conectividad, ruta, servicios y tráfico*. No corrige todavía; identifica ideas previas y posibles confusiones.

Motivación y enganche: evidencia en lugar de adivinanza — 3 minutos

- **Docente:** Muestra una captura breve de Wireshark con solicitudes ICMP y un resultado de ping exitoso. Pregunta: **“¿Qué puede demostrar esta evidencia y qué no puede demostrar?”**
- **Estudiantes:** Comentan en parejas durante un minuto y mencionan una conclusión válida y una conclusión que sería arriesgada.
- **Docente:** Explica que una herramienta no “arregla” automáticamente la red: ayuda a observar, medir y documentar. Presenta el reto: entregar un diagnóstico breve con evidencias.

Contextualización — 3 minutos

Docente: Relaciona el contenido con situaciones reales: pérdida de conexión al aula virtual, lentitud del Wi-Fi, impresoras que desaparecen, servidores que no responden y necesidad de vigilar la disponibilidad de servicios. Aclara: **“En esta clase solo analizaremos el laboratorio y los archivos proporcionados. No se permite escanear redes externas ni equipos sin autorización”**.

Estudiantes: Observan el mapa simple de la red del laboratorio y responden oralmente: **“¿Qué diferencia existe entre comprobar que un host responde y saber qué servicio está disponible?”** El docente recoge una respuesta para enlazar con la actividad práctica.

Fase de Desarrollo

Tiempo estimado: 40 minutos.

Presentación del contenido: Se parte del material invertido revisado en casa. El docente no repite toda la lectura; realiza una demostración guiada de seis minutos y luego los estudiantes aplican el procedimiento. En la pizarra presenta esta secuencia: **1) comprobar configuración local, 2) probar conectividad, 3) revisar la ruta, 4) identificar activos autorizados, 5) analizar tráfico, 6) registrar y monitorear**.

Presentación interactiva y demostración — 8 minutos

- **Docente:** Ejecuta en un equipo de demostración **ipconfig** o **ifconfig**, **ping 127.0.0.1**, **ping [puerta_de_enlace_del_laboratorio]** y **tracert [servidor_autorizado]**. Pregunta después de cada comando: **“¿Qué componente estamos comprobando y qué resultado indicaría una posible falla?”**
- **Estudiantes:** Comparan la demostración con su guía y levantan una tarjeta verde si comprenden la función o amarilla si necesitan aclaración.
- **Docente:** Explica que Nmap se utilizará solamente contra el rango autorizado del laboratorio o contra localhost, por ejemplo **nmap -sn 192.168.10.0/24**, y que Wireshark permitirá revisar el archivo entregado aplicando el filtro **icmp**. Finalmente muestra en Zabbix dónde se consulta disponibilidad, último dato recibido y estado de un host.

Actividad 1: Ruta de diagnóstico por comandos — 12 minutos

Objetivo específico: Aplicar comandos básicos e interpretar resultados de conectividad y ruta.

Organización: Parejas, con roles de operador y relator; se intercambian a mitad de la actividad.

- **Docente dice:** “Trabajen únicamente con las direcciones impresas en la ficha. Ejecuten los comandos en orden y no modifiquen configuraciones”.
- **Estudiantes:** Ejecutan **ipconfig/ifconfig**, hacen ping a la propia máquina, a la puerta de enlace y al servidor autorizado; después ejecutan **tracert/traceroute** al servidor.
- Registran en la tabla: destino, respuesta, latencia aproximada, número de saltos y primera hipótesis.
- Responden: **“Si responde la puerta de enlace, pero no el servidor, ¿qué segmento o servicio investigarían después?”**
- **Docente:** Observa la lectura de resultados y pregunta: **“¿Están confundiendo que un host responda con que una aplicación funcione?”** y **“¿Qué evidencia respalda su hipótesis?”**

Producto: Tabla de resultados y una hipótesis técnica de dos líneas.

Actividad 2: Detectar y observar — 14 minutos

Objetivos específicos: Identificar activos autorizados y analizar tráfico básico.

Organización: Grupos de tres; operador, analista y encargado de evidencias.

- **Docente dice:** “Usen Nmap solamente sobre el rango escrito en la ficha. El propósito es reconocer hosts del laboratorio, no buscar vulnerabilidades”.
- **Estudiantes:** Ejecutan **nmap -sn [rango_autorizado]** o, si no hay red disponible, analizan la salida previamente preparada por el docente.
- Comparan los hosts encontrados con el mapa del laboratorio y marcan cuáles son conocidos, desconocidos o requieren verificación.
- Abren **diagnostico_red.pcapng** en Wireshark, aplican el filtro **icmp** y responden: **“¿Qué dirección origina la solicitud?, ¿qué dirección responde?, ¿se observan solicitudes sin respuesta?”**
- Guardan una captura de pantalla o anotan el número de paquete que sustenta su conclusión.
- **Docente:** Verifica que no se realicen escaneos externos y pregunta: **“¿Qué diferencia hay entre un host detectado por Nmap y un paquete observado en Wireshark?”**

Producto: Lista de hosts autorizados, filtro usado y dos evidencias de tráfico.

Actividad 3: Informe y decisión de gestión — 6 minutos

Objetivo específico: Documentar hallazgos y proponer una acción de gestión o monitoreo.

- **Estudiantes:** Completan en grupo la ficha: problema observado, evidencia, causa probable, nivel de certeza y siguiente acción.
- Eligen una acción: verificar cableado, revisar configuración IP, comprobar servicio, crear un host en monitoreo o establecer una alerta de disponibilidad.
- **Docente:** Solicita que cada grupo prepare una explicación de 30 segundos usando la estructura: **“Observamos…, por eso inferimos…, proponemos…”**

Transición: El docente indica: “Ya no necesitamos más comandos; ahora convertiremos los resultados en una decisión técnica comunicable”.

Diferenciación y apoyo

Para quienes necesitan apoyo, se entrega una guía con capturas de la terminal, comandos incompletos para completar y un glosario de *host, latencia, ruta, paquete y servicio*. El docente puede asignarles el archivo de captura en lugar de una captura en vivo. Para quienes terminan antes, se plantea el reto: comparar una respuesta con latencia alta y una solicitud ICMP sin respuesta, y explicar cuál evidencia sería necesaria antes de concluir que existe una falla permanente.

Fase de Cierre

Tiempo estimado: 10 minutos.

Síntesis: tablero de decisiones — 4 minutos

- **Docente:** Dibuja cuatro columnas en la pizarra: *conectividad, ruta, descubrimiento y análisis de tráfico/monitoreo*.
- **Estudiantes:** Cada pareja pega o escribe una herramienta en la columna correcta y añade una frase sobre la evidencia que produce. Por ejemplo: “ping: confirma respuesta ICMP” o “Wireshark: permite observar paquetes capturados”.
- **Docente:** Corrige colectivamente dos errores frecuentes: usar Nmap sin autorización y afirmar que un ping exitoso garantiza que una aplicación funcione.

Reflexión metacognitiva y retroalimentación — 5 minutos

Los estudiantes responden individualmente en un ticket de salida:

- **“¿Qué herramienta elegirías primero si un equipo no responde en la red? Explica por qué.”**
- **“¿Qué evidencia de tu práctica permitió distinguir entre un problema de conectividad y un problema de servicio?”**
- **“¿Qué procedimiento de seguridad debes cumplir antes de ejecutar un descubrimiento con Nmap?”**

Docente: Revisa dos o tres respuestas en voz alta, reconoce evidencias bien interpretadas y corrige inmediatamente respuestas que confundan disponibilidad del host con disponibilidad de una aplicación. Entrega retroalimentación breve usando la fórmula: **fortaleza observada + ajuste necesario + siguiente paso**.

Transferencia y reto — 1 minuto

Docente: Conecta el aprendizaje con la siguiente práctica de administración de servicios: “En la próxima sesión diseñaremos una alerta de monitoreo para detectar cuándo un servidor deja de responder”. Como tarea, cada estudiante elaborará una tabla de tres filas con una herramienta, el problema que ayuda a investigar y la evidencia que debe registrarse. Deberá incluir una regla ética de uso.

Evaluación

Estrategia de evaluación

Se aplicará evaluación **diagnóstica, formativa y de cierre**. La evaluación diagnóstica se realiza en el Inicio, durante la pregunta “¿Qué revisarías primero?”, para identificar conocimientos sobre conectividad y herramientas. La evaluación formativa se aplica durante las actividades 1, 2 y 3 mediante observación directa, revisión de tablas, evidencias de Wireshark y preguntas de razonamiento. La evaluación de cierre se realiza con el ticket de salida y la ficha de diagnóstico entregada por cada pareja.

Criterios de evaluación

- **Identificación de herramientas:** relaciona correctamente cada herramienta con su función principal. Vinculado con el objetivo 1.
- **Aplicación técnica:** ejecuta o interpreta correctamente comandos de conectividad, ruta, descubrimiento y filtros básicos de Wireshark, respetando el rango autorizado. Vinculado con el objetivo 2.
- **Interpretación de evidencias:** diferencia entre respuesta de un host, ruta de red, paquete observado y disponibilidad de un servicio. Vinculado con el objetivo 3.
- **Documentación y ética:** registra resultados, formula una hipótesis razonable y propone una acción de gestión segura y autorizada. Vinculado con el objetivo 4.

Instrumentos sugeridos

- Lista de cotejo para observar la ejecución segura de comandos y el trabajo colaborativo.
- Rúbrica breve de la ficha de diagnóstico, con niveles: logrado, en proceso y requiere apoyo.
- Observación directa durante la interpretación de resultados.
- Autoevaluación mediante el ticket de salida.
- Coevaluación oral de la explicación “Observamos…, por eso inferimos…, proponemos…”.

Evidencias de aprendizaje

- Tabla de comandos con destinos, respuestas, latencias y rutas: evidencia del objetivo 2.
- Lista de hosts autorizados y análisis de paquetes ICMP en Wireshark: evidencia de los objetivos 1 y 2.
- Ficha grupal con problema, evidencias, causa probable y acción propuesta: evidencia de los objetivos 3 y 4.
- Ticket de salida con selección justificada de herramientas y norma ética: evidencia de los objetivos 1, 3 y 4.

Lista de cotejo rápida

- Identifica correctamente al menos cuatro de las cinco herramientas trabajadas.
- Usa o interpreta los comandos indicados sin salir del entorno autorizado.
- Registra al menos dos evidencias técnicas verificables.
- Explica una causa probable diferenciándola de una certeza absoluta.
- Propone una acción de monitoreo o diagnóstico coherente y segura.