

curso “Experto en Ciberseguridad de Redes y Sistemas”

TEMAS

1. Fingerprinting
2. Footprinting
3. IDSs - Snort
4. Nessus
5. Firewalls
6. SGSI
7. Antiphishing
8. MITRE
9. Red Team y Blue Team
10. Principales procesos de Seguridad



Red Team y Blue Team

9.1. Red Team

Red Team

Es el equipo que simula ataques reales.

Su objetivo es **pensar y actuar como un atacante**.

Ya hemos visto muchas de sus herramientas y técnicas en este ciclo, por ejemplo:

- Desde el principio Wireshark.
- **Videos 36 a 39** → crack WiFi.
- **Video 47 a 49** → Configuración de Routers
- **Desde el video 52** → varios sobre: SCAPY, generando tráfico.
- **Video 61 a 63** → Ataques VoIP.
- **Video 71 a 76** → Fingerprinting.
- **Video 77 a 87** → Auditoría remota con Raspberry Pi
- **Video 88 a 99** → Footprinting.
- **Video 101 a 109** → Snort.
- **Video 111–119** → Nessus. Escaneo de vulnerabilidades. Nmap y reconocimiento activo.
- **Video 121 a 139** → Firewalls

- **Video 141 a 149** → SGSI (ISO 27001).
- **Videos 151–159** → GoPhish, campañas de ingeniería social y phishing.
- **Video 161 a 178** → MITRE ATT&CK, Navigator, Caldera D3FEND.

Herramientas típicas del Red Team:

- Nmap, Nessus, Wireshark, Metasploit, GoPhish, Burp Suite, Hydra, etc.

Cómo trabajan Blue y Red Team en la vida real

Un flujo profesional típico a ejercitar puede ser el siguiente:

1. Planificación

- Objetivos del ejercicio
- Alcance permitido (reglas de enganche)

2. Ejecución del Red Team

- Simula amenazas
- Usa tácticas reales (MITRE ATT&CK)

3. Defensa del Blue Team

- Monitorea
- Correlaciona eventos
- Aplica respuesta a incidentes

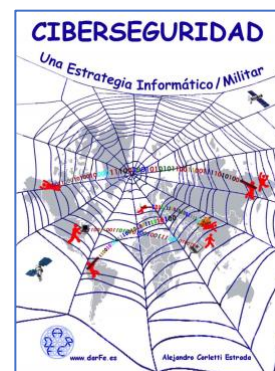
4. Reporte y lecciones aprendidas

- Qué falló
- Qué funcionó
- Qué mejorar

5. Reentrenamiento

- Hardening
- Nuevas políticas
- Nuevas reglas de detección

En el video se hace mención al punto 11.3 “Resumen de la doctrina militar sobre Juegos de guerra” de nuestro libro: **Ciberseguridad, una estrategia Informático/Militar**, al cual recomendamos que le des una mirada. Recordad que lo podéis descargar gratuitamente de: www.darFe.es



Este tema lo desarrollamos en detalle en el video 179 (**Obligatorio**).

🌐 **Red Team - Charla 179** - Aprendiendo Ciberseguridad paso a paso
<https://youtu.be/tSzkR4q--Lo>

9.2. Blue Team

Blue Team

Es el equipo que **defiende**, analiza, investiga, detecta, responde y protege.

Principales actividades:

- Monitorización continua.
- Revisión de logs.
- Uso de SIEM.
- Correlación de eventos.
- Reglas de detección.
- Respuesta a incidentes.
- Análisis forense.
- Hardening y controles de seguridad.

Metodologías del Blue Team:

- **NIST CSF**
- **ISO 27001 e ISO 27002**
- **CIS Controls**
- **MITRE D3FEND**
- **Ciclo de Respuesta a Incidentes**

Herramientas de Blue Team:

- SIEM (Splunk, Wazuh)
- Firewalls (iptables, nftables, pf)
- IDS/IPS (Snort, Suricata)
- Sysmon + Elastic
- Herramientas forenses: Autopsy, Volatility, etc.

Relación con vídeos previos de nuestro ciclo:

- Videos 140–145 → Análisis de tráfico, detección.
- Videos sobre iptables/nftables → Hardening y control de red.
- Video 120 → Análisis forense básico.
- Videos 100–110 → Logs y monitorización.



info@darfe.es

- Vídeos 97–101 → Gestión de vulnerabilidades.

Este tema lo desarrollamos en detalle en el video 181 (**Obligatorio**).

🌐 **Blue Team - Charla 181** - Aprendiendo Ciberseguridad paso a paso

https://youtu.be/4O_wPIFuF-Y

