



FIE

FACULTAD DE INGENIERIA DEL EJERCITO
Universidad de la Defensa Nacional

CIBERDEFENSA

¿Cómo enfrentar este nuevo dominio militar?
Nivel Táctico & Técnico

Mayor Eduardo Malvacio
Investigador - Facultad de Ingenieria del Ejercito



Nivel Táctico / Técnico (Abordaje Militar)

TEMARIO

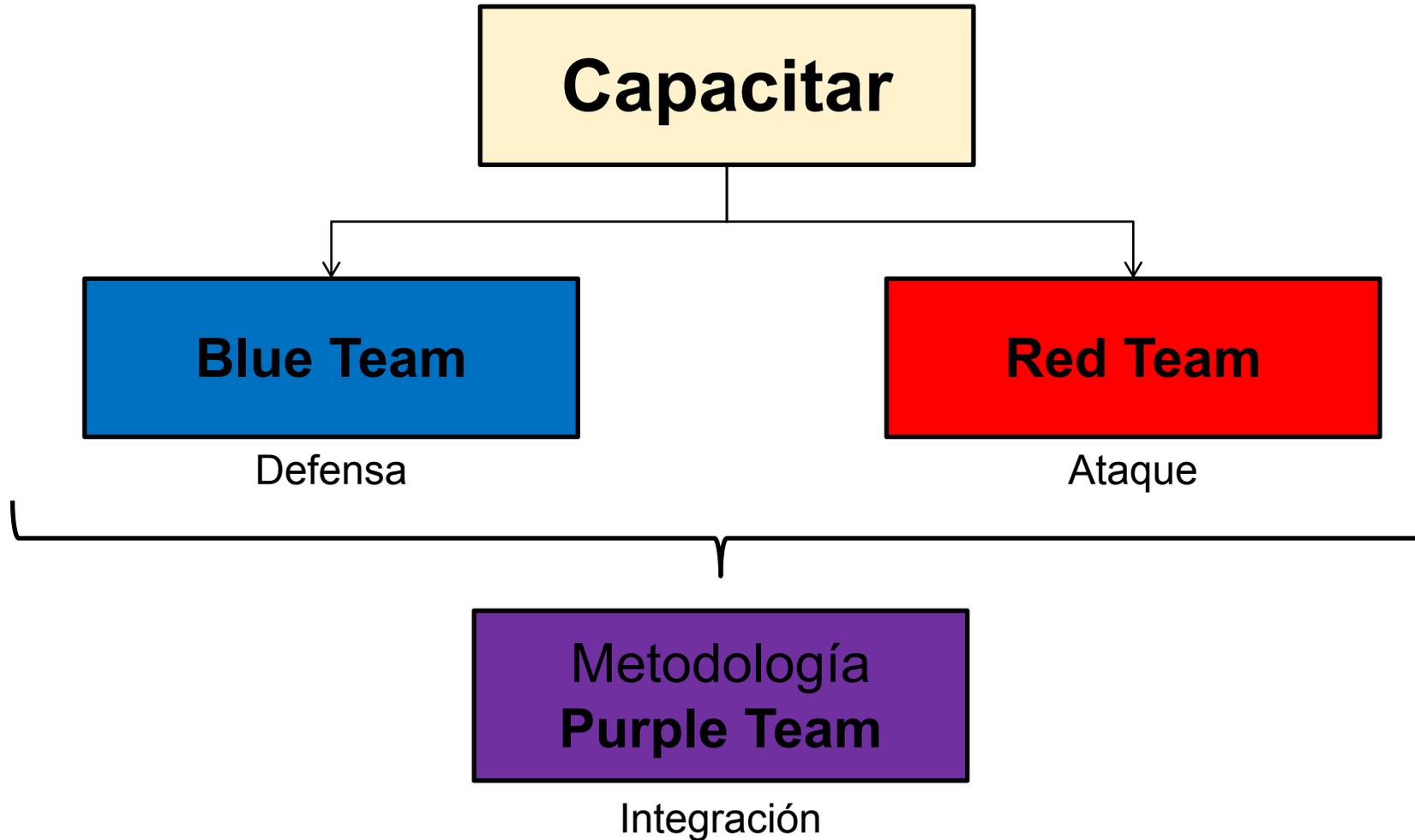
- Ámbito (nivel) en el que se encuadra.
- Objetivo de la capacitación a este nivel.
- Metodología de formación/capacitación en este nivel.
- Técnicas principales empleadas.
- Diferentes escuelas o líneas de formación (referentes).

Ámbito (nivel) en el que se encuadra



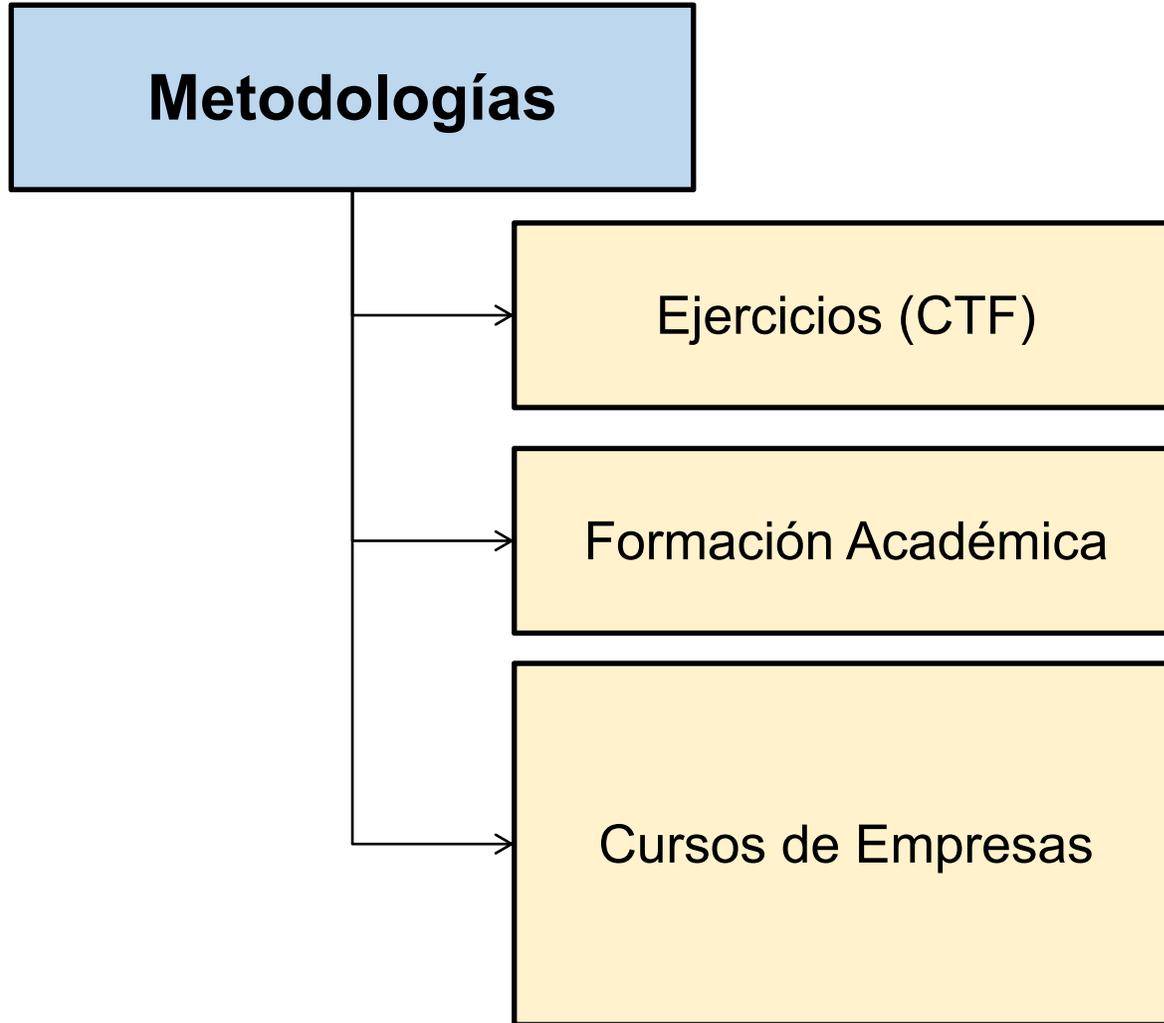


Objetivo de la capacitación a este nivel





Metodología de formación/capacitación en este nivel



Carreras de grado
Carreras de posgrado
Cursos

Cursos:

- Penetration Test
- Ethical Hacker
- Linux
- Redes
- Etc

Técnicas principales empleadas

Ofensivas

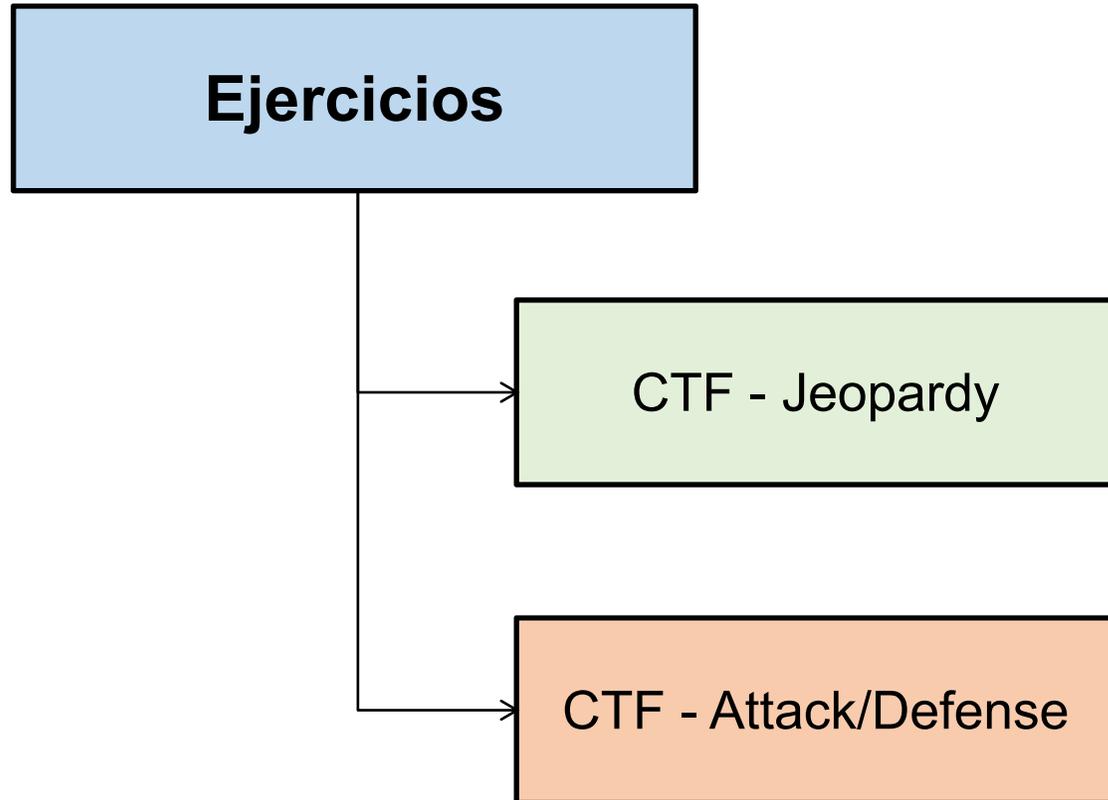
- Penetration Test
- Ethical Hacking
- Exploits
- Ciberarmas

Defensivas

- Threat Hunting
- Análisis de Malware
- Inteligencia de Amenazas
- Informática Forense
- Hardening



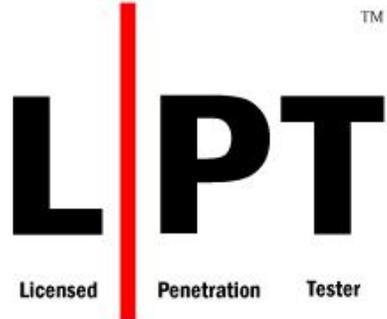
Técnicas principales empleadas



Rooters CTF (<https://rootersctf.in/>)
HITCON CTF (<https://ctf.hitcon.org/>)
Newbie CTF (<https://nctf.vulnerable.kr/>)
M*CTF Quals (<https://board.mctf.moscow/rules>)

SibirCTF (<https://sibirctf.org/>)
M*CTF (<http://mctf.moscow/>)

Diferentes escuelas o líneas de formación (referentes)



Empresas (Certificaciones)

- EC-Council (CEH)
- EC-Council (LPT)
- GIAC (Penetration Tester)
- GIAC (Advanced Penetration Tester)
- Offensive Security
- ISC2 (CISSP)
- ISACA (CISM)