Listado de Herramientas para Profesionales de Ciberseguridad | Uso Ético (2025)

USO RESPONSABLE Y LEGAL — Declaración de ética

Este documento es una lista informativa dirigida a profesionales y estudiantes de ciberseguridad.

El uso de las herramientas aquí listadas debe realizarse exclusivamente en entornos de laboratorio, con autorización escrita del propietario del sistema o dentro de actividades legales y contractuales. No se promueve, facilita ni legitima actividad ilícita. El autor no se responsabiliza del uso indebido de la información.

1. Reconocimiento y enumeración (recon / footprinting)

- **Nmap / Masscan**: Escaneo de puertos, servicios, fingerprinting de sistemas.
- **Shodan / Censys:** Motores de búsqueda de dispositivos conectados.
- **theHarvester:** Recolección de emails, dominios, metadatos públicos.
- **Amass:** EnumeAración avanzada de subdominios y DNS.
- **Recon-ng:** Framework OSINT modular.
- **Maltego:** Visualización de relaciones entre entidades (redes, personas, dominios).
- **FOFA / ZoomEye:** Alternativas chinas a Shodan, con más detalle industrial.
- **SpiderFoot HX:** OSINT automatizado, reconocimiento completo.

2. Explotación y post-explotación (offensive / Red Team)

- **Metasploit Framework:** Explotación automatizada de vulnerabilidades y payloads.
- **Cobalt Strike / Brute Ratel / Sliver C2:** Plataformas de comando y control (C2).
- **Empire / PowerShell Empire / Covenant:** Frameworks de post-explotación Windows.
- **Impacket**: Scripts Python para NTLM relay, SMB exploitation, pass-the-hash, etc.
- **Mimikatz / LaZagne**: Robo de credenciales, hashes y contraseñas locales.
- **BloodHound + SharpHound**: Análisis de relaciones y privilegios en Active Directory.
- **Responder / Inveigh**: Captura de hashes y ataques LLMNR/NBT-NS en red local.

- **Burp Suite Pro / ZAP Proxy**: Ataques a aplicaciones web (inyecciones, fuzzing, auth bypass).

- **sqlmap**: Automatización de inyecciones SQL y extracción de bases de datos.

- **Hydra / Medusa / CrackMapExec**: Ataques de fuerza bruta a servicios (SSH, RDP, SMB).

- **Bettercap / Ettercap / MITMf**: Ataques MITM, sniffing y manipulación de tráfico.

- **Nishang / Evil-WinRM / PoshC2**: Herramientas PowerShell para post-explotación.

- **MSFVenom / Veil / Unicorn**: Generadores de payloads ofuscados / evasión AV.

- **Beef Project**: Control de navegadores vía XSS.

3. Ingeniería social y phishing

- **Gophish**: Plataforma para campañas de phishing controladas.

- **Evilginx2**: Proxy inverso para robar tokens y sesiones (phishing avanzado).

- **Social-Engineer Toolkit (SET)**: Genera ataques de ingeniería social, clones de webs, payloads.

- **King Phisher / GoPhish Pro / PhishMe**: Herramientas corporativas para simular campañas y entrenar.

4. Análisis de vulnerabilidades y gestión de riesgos

- **Nessus / OpenVAS / Greenbone**: Escaneo de vulnerabilidades general.

- **Qualys / Rapid7 InsightVM / Tenable.sc**: Suites profesionales de gestión de vulnerabilidades.

- **Nikto / Wapiti / Arachni**: Escáneres web (OWASP Top 10).

- **Lynis / Rkhunter / Chkrootkit**: Auditoría de seguridad en Linux.

- **CloudMapper / ScoutSuite / Prowler**: Auditoría de configuraciones cloud (AWS, Azure, GCP).

- **Trivy / Clair / Grype**: Escaneo de vulnerabilidades en contenedores e imágenes Docker.

5. Defensa, monitorización y detección (Blue Team / SOC)

- **Wazuh / OSSEC**: SIEM y monitorización de integridad.

- **ELK Stack (Elasticsearch + Logstash + Kibana)**: Plataforma de análisis de logs.

- **Splunk / QRadar / Sentinel / Chronicle:** SIEM comerciales más potentes.

- **Velociraptor / GRR Rapid Response:** Forense en vivo, respuesta a incidentes.

- **Suricata / Zeek (Bro)**: IDS/IPS para análisis de tráfico de red.

- **Snort / Security Onion**: Detección de intrusiones y análisis completo de red.

- **Sysmon / Windows Event Forwarding (WEF)**: Monitorización detallada en Windows.

- **Falcon CrowdStrike / Microsoft Defender for Endpoint / SentinelOne / ESET Protect**: EDR/XDR denivel empresarial.

- **pfSense / OPNsense / FortiGate** / Palo Alto: Firewalls avanzados.

- **CloudTrail / GuardDuty / Azure Defender / GCP Security Command Center**: Monitorización nativa cloud.

6. Análisis forense y malware

- **Autopsy / Sleuth Kit:** Análisis de discos y sistemas de archivos.

- **Volatility / Rekall:** Análisis de memoria RAM.

- **FTK / EnCase**: Suites forenses comerciales.

- **IDA Pro / Ghidra / x64dbg / Cutter / Radare2**: Ingeniería inversa y análisis binario.

- **Cuckoo Sandbox / Any.Run / Hybrid Analysis**: Análisis dinámico de malware.

- **YARA / Sigma / Suricata Rules:** Detección basada en firmas y comportamiento.

7. Cloud, DevSecOps y automatización

- **Terraform + Checkov / Tfsec / Terrascan**: Auditoría de seguridad en IaC (Infraestructura como código).

- **Kube-hunter / Kube-bench / Kubescape**: Seguridad en Kubernetes.

- **GitGuardian / TruffleHog:** Detección de secretos en repositorios.

- **AWS Inspector / Azure Security Center / GCP SCC**: Escaneo de vulnerabilidades nativo en la nube.

- **Ansible + Vault / Puppet / Chef**: Automatización segura y configuración reforzada.

8. Frameworks de simulación, Red/Blue/Purple Team

- **Atomic Red Team / MITRE ATT&CK; / Caldera / Prelude Operator**: Simulación de tácticas y técnicas

ATT&CK.;

- **PurpleSharp / Infection Monkey:** Validación de defensas Blue Team.

- **AttackIQ / SafeBreach / Picus Security**: Plataformas de simulación comercial.

9. Gestión de seguridad y cumplimiento

- **OpenSCAP / Lynis / CIS-CAT Pro**: Auditorías de cumplimiento (CIS, NIST, ISO).

- **GRR Rapid Response / Velociraptor / MISP / TheHive / Cortex**: Gestión de incidentes y threat intelligence.

- **Grafana / Prometheus / Loki**: Monitorización avanzada de infraestructuras.

10. Herramientas de inteligencia de amenazas (Threat Intelligence)

- **MISP / OpenCTI / TheHive:** Plataformas de Threat Intel colaborativa.

- **VirusTotal / Hybrid Analysis / Any.Run / AbuseIPDB**: Análisis de muestras y reputación de

IPs/dominios.

- **Maltrail / GreyNoise / ThreatFox / Abuse.ch**: Detección y bloqueo de IoC (Indicators of

Compromise).

BONUS: Herramientas de uso mixto (ofensivo/defensivo)

- **Wireshark / TCPdump**: Análisis de tráfico y protocolos.

- **Netcat / Socat / ProxyChains**: Túneles, redirecciones y debug de red.

- **Python + Scapy / PowerShell / Bash scripting**: Automatización y pentesting personalizado.

- **ChatGPT + GPT Engineer / AutoRecon AI / PentestGPT**: Asistentes IA para pentesting y análisis.

- Red Team (ataque): **Metasploit, Cobalt Strike, BloodHound, Mimikatz, Burp, Responder, Nmap**

- Blue Team (defensa): **Wazuh, Suricata, Zeek, ELK, EDR, SIEM, Sysmon**

- Purple Team (colaboración): **MITRE ATT&CK;, Caldera, Atomic Red Team**

- Forense / Respuesta a incidentes: **Volatility, Autopsy, GRR, Velociraptor**

- Cloud Security: **ScoutSuite, Prowler, Trivy, Checkov, GitGuardian**

- Threat Intel: **MISP, OpenCTI, VirusTotal, Abuse.ch**

Herramientas ofensivas adicionales (2025)

Reconocimiento y OSINT

- **Holehe**: Verifica si un correo electrónico está registrado en servicios populares.

- **Email2phonenumber**: Herramienta OSINT para intentar obtener números de teléfono asociados a correos.
- **GHunt**: Recolecta información pública de cuentas de Google (Drive, YouTube, etc.).
- **PhoneInfoga**: Recolector de datos OSINT sobre números telefónicos.

Payloads y evasión

- **ScareCrow**: Generador de payloads en C++ que evade EDRs modernos.
- **Donut**: Convierte ejecutables PE en shellcode para inyección.
- **ShellcodeRDI**: Inyecta DLLs como shellcode en memoria.
- **Nimcrypt2**: Ofuscador de payloads en lenguaje Nim.

Post-explotación y movimiento lateral

- **Rubeus**: Herramienta para Kerberos abuse (ticket extraction, pass-the-ticket, etc.).
- **SharpHound**: Recolección de datos para BloodHound desde entornos Windows.
- **Seatbelt**: Recolector de información post-explotación en sistemas Windows.
- **SharpUp**: Escalación de privilegios en Windows.
- **PEASS-ng (LinPEAS / WinPEAS)**: Enumeración de privilegios en Linux y Windows.

Ataques a redes y protocolos

- **CrackMapExec (CME)**: Swiss army knife para redes Windows (SMB, RDP, WinRM).
- **PetitPotam**: Ataque NTLM relay para tomar control de controladores de dominio.
- **Coercer**: Fuerza autenticación NTLM desde servicios remotos.
- **Kerbrute**: Fuerza bruta de cuentas Kerberos y enumeración de usuarios.

Ataques a MFA y sesiones

- **Modlishka**: Proxy inverso para robar credenciales y tokens de sesión (bypass MFA).
- **EvilnoVNC**: Phishing visual con sesiones VNC falsas.
- **Browser-in-the-Browser (BitB)**: Ataques visuales que simulan ventanas de login dentro del navegador.

Malware y RATs emergentes

- **LockBit** (en declive pero aún activo): conocido por su modelo RaaS (Ransomware-as-a-Service).
- **BlackCat / ALPHV**: sofisticado, con cifrado rápido y extorsión doble.
- **Phobos**: muy activo en América Latina, con más de 1.1 millones de intentos en 2025
- **Akira**: enfocado en empresas medianas, con tácticas de presión pública.
- **Royal / Black Basta / Play**: variantes agresivas con cifrado rápido y técnicas de evasión.
- **Newcomers**: grupos más pequeños y ágiles que usan tácticas de extorsión sin cifrado (pure extortion).
- Infostealers:
  - **RedLine Stealer:** roba credenciales, cookies, wallets.
  - **Vidar / Raccoon Stealer**: muy usados en campañas masivas.
  - **LummaC2**: nueva generación de stealer con paneles C2 avanzados.
- RATs (Remote Access Trojans):

    - **AsyncRAT / Warzone RAT / NjRAT**: control remoto, keylogger, robo de archivos.
    - **DarkComet / NanoCore**: aún activos en entornos menos protegidos.
- Loaders y droppers:
    - S**mokeLoader / IcedID / Qbot**: usados para cargar ransomware o stealers.
    - **Emotet** (reaparecido): plataforma modular para campañas masivas.
- Botnets y malware persistente:
    - **Mirai variants**: aún usados para DDoS y control de IoT.
    - **Agent Tesla**: persistente, con cifrado y evasión de antivirus.

Tendencias clave en 2025

- **Extorsión sin cifrado**: algunos grupos ya no cifran, solo roban y amenazan con publicar.
- **Ataques a MFA**: uso de proxies inversos como *Modlishka* y *Evilginx2* para robar tokens de sesión.
- **Malware modular**: payloads que se adaptan al entorno, descargan módulos según el objetivo.
- **Uso de IA**: algunos RATs y loaders integran lógica para evasión dinámica y reconocimiento de entorno.

Malware más frecuente según Sophos (2025)

- **Warzone RAT**: Comercializado en foros clandestinos, con keylogger y control remoto.
- **AsyncRAT**: RAT de código abierto con cifrado y persistencia.
- **RAT-el**: RAT en .NET con funciones de evasión y control remoto.

Simulación y automatización

- **Invoke-AtomicRedTeam**: Ejecuta pruebas ATT&CK de forma automatizada en PowerShell.
- **PurpleSharp**: Simula técnicas ATT&CK en entornos Windows para validar detección.
- **Caldera Plugins**: Extensiones como "Manx", "Sandcat" o "Atomic" para simular APTs.

Añadidas recomendadas (prioritarias)

- **Hashcat** — cracking GPU: imprescindible para romper hashes a gran velocidad.
- **John the Ripper (Jumbo)** — cracking de hashes y wordlists complementario a Hashcat.
- **Mythic** — C2 moderno open-source, alternativa a Cobalt Strike para red teams.
- **Pacu** — framework ofensivo para AWS (ataques y enumeración cloud).
- **AFL / honggfuzz / libFuzzer / Peach Fuzzer** — fuzzers para binarios/servicios; cruciales para descubrir bugs de día cero.
- **Frida + Objection** — instrumentación dinámica para apps móviles y binarios (runtime hooking).

- **MobSF (Mobile Security Framework)** — análisis estático y dinámico de apps Android/iOS.
- **Binwalk / Firmadyne / firmware-mod-kit** — análisis y emulación de firmware (IoT/embedded).
- **pwntools / ROPgadget / ropper** — toolset para explotación binaria y desarrollo de PoCs.
- **Semgrep / CodeQL / Snyk / Dependabot / OWASP Dependency-Check** — SAST/SCA para detección temprana en repos.
- **Pacu + CloudKiller / ScoutSuite** — complementan la caja para ofensiva en la nube (Pacu ya mencionado; CloudKiller como referencia).
- **Mythic / Covenant / Sliver** — C2s modernos (ya mencionas algunos, pero vale la pena añadir Mythic y Sliver concretamente).
- **Ghidra (ya en tu lista) + Binary Ninja (comercial)** — GNIDA está, pero Binary Ninja es útil por su API y flujo moderno.
- **Apm (Application Performance) fuzzing: Burp intruder + Burp Collaborator + Burp extensions (Autor, ActiveScan++)** — para pentesting web a fondo.
- **Hashcat + John + oclHashcat workflows** — añade plantillas y wordlists (RockYou, SecLists) y rules avanzadas.

Especialidades útiles

- **Supply chain / firma y trazabilidad**: **Sigstore / Rekor / In-Toto** — defensa y verificación de cadenas de suministro.
- **Fuzzing de protocolos y IoT**: **Boofuzz / Sulley** — fuzzing de protocolos de red y dispositivos.
- **Firmware reversing & emulación**: **QEMU (user/board mode) + angr** — análisis simbólico y emulación.
- **Mobile runtime / dynamic instrumentation**: **Frida + objection + Xposed frameworks**.
- **Hardware / RF / embedded**: **HackRF / BladeRF / UHF SDR tools, Bus Pirate, JTAGulator** — para pruebas de dispositivos y redes industriales.
- **OT / ICS**: **Metasploit modules para ICS, Censys para ICS fingerprinting, Grid-related tools** — si trabajas OT/ICS deberías añadir frameworks y sensores especializados.
- **Password spraying / AD attack tools adicionales**: **Kerbrute (mencionado), GetNPUsers + ASREProast flows** — detalles para ataques Kerberos.
- **Adversary emulation & purple team**: **Caldera (ya), Atomic Red Team (ya) + AttackIQ** — haz playbooks de emulación con ellos.

Herramientas comerciales / enterprise que podrías considerar (si trabajas con clientes)

- **CrowdStrike Falcon / SentinelOne / Splunk Enterprise / Rapid7 InsightVM / Tenable.io** — ya las mencionas, pero si buscas cobertura completa, añade **Malwarebytes Nebula / Arctic Wolf / Cynet** según el caso de uso.
- **Binary Ninja (licencia)** y **IDA Pro (ya listada)** para reversing profesional.

Notas prácticas / operativas

- **Workflow**: incluye plantillas de Recon → Enum → Explotación → Post-explotación → Detección/Remediation y automatiza con AutoRecon, Pacu, Invoke-AtomicRedTeam.
- **Evasión/EDR**: ten cuidado al usar técnicas y herramientas de evasión (legales y éticas). En entornos de cliente usa acuerdos explícitos y entornos controlados.
- **Prioridad de aprendizaje**: si empiezas, prioriza Hashcat/John + Nmap/BloodHound + Burp/Frida + uno o dos fuzzers.
- **Threat intelligence**: añade feeds comerciales o premium si trabajas en SOC (Recorded Future, Mandiant) — dependen de presupuesto.

1. Planeación y Reconocimiento (Recon / Footprinting)

Objetivo: Obtener información del objetivo sin interactuar directamente.
Ejemplos:

- Nmap, Masscan, Shodan, Censys, Amass, theHarvester, Maltego, SpiderFoot, FOFA, ZoomEye, Recon-ng, GHunt, Holehe, PhoneInfoga.

2. Enumeración y Mapeo de Superficie de Ataque

Objetivo: Interactuar con los servicios y sistemas para identificar vectores vulnerables.
Ejemplos:

- Nmap (profundo), SMBmap, SNMPwalk, LDAPSearch, enum4linux, Netdiscover, DNSrecon, Sublist3r, dirsearch, Gobuster, Nikto.

3. Análisis de Vulnerabilidades (Vulnerability Scanning)

Objetivo: Detectar debilidades conocidas o configuraciones inseguras.
Ejemplos:

- Nessus, OpenVAS, Qualys, Rapid7 InsightVM, Tenable.sc, Nikto, Wapiti, Arachni, Lynis, Trivy, Clair, Grype, ScoutSuite, Prowler, CloudMapper.

4. Explotación (Exploitation)

Objetivo: Obtener acceso inicial o ejecutar código malicioso aprovechando vulnerabilidades.
Ejemplos:

- Metasploit, Cobalt Strike, Brute Ratel, Sliver C2, Burp Suite, ZAP Proxy, sqlmap, Hydra, Medusa, Bettercap, Ettercap, MITMf, Evilginx2, Modlishka, MSFVenom, Veil, Unicorn.

5. Escalada de Privilegios y Movimiento Lateral (Privilege Escalation / Lateral Movement)

Objetivo: Elevar privilegios locales y expandirse por la red.
Ejemplos:

- Mimikatz, LaZagne, PEASS-ng (LinPEAS / WinPEAS), SharpUp, Rubeus, Impacket, CrackMapExec, Responder, Inveigh, PetitPotam, Coercer, Kerbrute, Evil-WinRM, Nishang, PowerShell Empire, Covenant, PoshC2.

6. Post-explotación y Persistencia (Post-Exploitation / Persistence)

Objetivo: Mantener el control, recolectar información y preparar la exfiltración.
Ejemplos:

- BloodHound + SharpHound, Seatbelt, Mythic, Sliver, Empire, Cobalt Strike, Veil, Donut, ShellcodeRDI, Nimcrypt2, ScareCrow, Beef Project, AsyncRAT, Warzone RAT, NjRAT, Agent Tesla, SmokeLoader.

7. Evasión y Ofuscación (Defense Evasion / EDR Bypass)

Objetivo: Evadir antivirus, EDR y defensas de endpoint o red.
Ejemplos:

- ScareCrow, Donut, Nimcrypt2, ShellcodeRDI, Obfuscator-LLVM, Mythic plugins, Empire Obfuscation modules, AMSI bypass scripts, payloads de Veil / Unicorn.

8. Exfiltración y Command & Control (C2 / Exfiltration)

Objetivo: Control remoto y extracción de datos.
Ejemplos:

- Mythic, Sliver, Covenant, Brute Ratel, Cobalt Strike, Metasploit Meterpreter, Netcat, Socat, ProxyChains, Wireshark (para monitorear tráfico C2).

9. Detección, Monitorización y Defensa (Blue Team / SOC)

Objetivo: Detectar, analizar y bloquear ataques en tiempo real.
Ejemplos:

- Wazuh, OSSEC, ELK Stack, Splunk, QRadar, Sentinel, Chronicle, Zeek, Suricata, Snort, Security Onion, Sysmon, Windows Event Forwarding (WEF), pfSense, OPNsense, Palo Alto, GuardDuty, Azure Defender.

10. Contención, Respuesta y Recuperación (Incident Response / Forensics)

Objetivo: Aislar incidentes, analizar evidencia y restaurar la operación.
Ejemplos:

- Velociraptor, GRR Rapid Response, Autopsy, Sleuth Kit, Volatility, Rekall, FTK, EnCase, Cuckoo Sandbox, Any.Run, Hybrid Analysis, YARA, Sigma, Suricata Rules.

11. Threat Intelligence y Análisis de IoC (Threat Intel / Detection Engineering)

Objetivo: Identificar, correlacionar y anticipar amenazas.
Ejemplos:

- MISP, OpenCTI, TheHive, Cortex, VirusTotal, Hybrid Analysis, AbuseIPDB, GreyNoise, ThreatFox, Abuse.ch, Recorded Future, Mandiant Intel.

12. Gestión de Riesgos, Cumplimiento y Gobernanza (GRC / Compliance)

Objetivo: Alinear seguridad con normativas (CIS, NIST, ISO, GDPR, ENS).
Ejemplos:

- OpenSCAP, Lynis, CIS-CAT Pro, Qualys Policy Compliance, Rapid7 InsightVM, Tenable.io, Audit Scripts, Ansible + Vault, Terraform + Checkov / Tfsec / Terrascan.

13. Automatización, Cloud Security y DevSecOps

Objetivo: Integrar la seguridad en pipelines CI/CD y entornos cloud-native.
Ejemplos:

- Terraform, Checkov, Tfsec, Terrascan, Kube-bench, Kube-hunter, Kubescape, GitGuardian, TruffleHog, Ansible, Puppet, Chef, AWS Inspector, Azure Security Center, GCP SCC, Pacu, CloudKiller.

14. Simulación y Validación de Defensas (Purple Team / Emulación de Ataques)

Objetivo: Probar la eficacia de detecciones y respuestas.
Ejemplos:

- MITRE ATT&CK, Atomic Red Team, Caldera, Prelude Operator, PurpleSharp, Infection Monkey, AttackIQ, SafeBreach, Picus Security, Invoke-AtomicRedTeam.

15. Tendencias y Evolución de Amenazas (2025+)

Objetivo: Entender el panorama cambiante de amenazas y adaptarse.
Ejemplos y tendencias destacadas:

- Extorsión sin cifrado, ataques a MFA, malware modular, evasión con IA, RATs con lógica adaptativa, payloads dinámicos, supply chain attacks, seguridad cuántica emergente.

16. Reporting, Lessons Learned y Continuous Improvement

Objetivo: Documentar hallazgos, indicadores, recomendaciones y lecciones aprendidas para mejorar procesos.

- Herramientas: **Dradis, PlexTrac, Serpico, Markdown con templates de OWASP, Jira, Confluence.**
- Frameworks de mejora: PDCA (Plan-Do-Check-Act), NIST CSF Tier Evolution, MITRE D3FEND.

  Resultado: Cierre de ciclo profesional, comunicación con dirección o cliente y base para auditorías futuras.

17. OSINT avanzado y geoespacial

- **GeoIntOSINT**: framework para correlación de datos geográficos, imágenes satelitales y redes sociales
- **Creepy / GeoSpy**: geolocalización de imágenes y metadatos en redes sociales

- **SocialNet / SpiderFoot HX plugins**: enriquecimiento de relaciones entre perfiles, ubicaciones y dispositivos

18. Evasión y payloads avanzados

- **NimPlant**: payload modular en Nim con evasión de EDR y persistencia
- **OffensiveNim / Nimcrypt3**: evolución de ofuscadores Nim con soporte para payloads dinámicos
- **SharpBlock**: bypass de AMSI y ETW en entornos Windows modernos
- **EDRSandblast**: bypass de EDRs mediante técnicas de inyección y manipulación de syscalls

19. Fuzzing y análisis binario

- **Fuzzowski / Fuzzotron**: fuzzers para protocolos industriales y SCADA
- **Angr + Triton**: análisis simbólico y ejecución condicional para binarios complejos
- **DeepFuzzer / FuzzBench AI**: fuzzing asistido por IA para detección de bugs lógicos
- **Binsec / Manticore**: análisis formal y simbólico de binarios en entornos críticos

20. Threat Intelligence y detección avanzada

- **Yeti / IntelMQ**: automatización de ingestión y correlación de feeds de amenazas
- **OpenCTI plugins: MITRE D3FEND / ATT&CK Navigator**: visualización y mapeo de defensas vs tácticas
- **ThreatMapper / DeepFence**: detección de amenazas en tiempo real en entornos cloud-native
- **Sigma2 / TTPFlow**: evolución de Sigma para correlación de TTPs y detección basada en comportamiento

21. Simulación adversaria y validación de defensas

- **RedHunt OS**: entorno ofensivo preconfigurado con herramientas de emulación y evasión
- **Pentera / BreachLock**: plataformas comerciales de validación continua de seguridad
- **MITRE Caldera plugins: Sandcat AI / Manx**: simulación de APTs con lógica adaptativa
- **PurpleSharp + Elastic Detection Rules**: simulación + validación directa en entornos ELK

22. Seguridad en cadena de suministro y DevSecOps

- **Sigstore / Cosign / Rekor**: verificación de firma y trazabilidad en pipelines CI/CD
- **In-Toto / TUF (The Update Framework)**: protección de integridad en actualizaciones y despliegues
- **ChainGuard / SLSA Verifier**: cumplimiento de Supply Chain Levels for Software Artifacts