

PAI-5. RedTeamPro

Evaluación de la seguridad de la información mediante pruebas de seguridad de una organización pública

Ángel Jesús Varela Vaca
Grupo de Investigación **IDEA Research Group**,
Universidad de Sevilla



No Toy Pentesting



Trabajar con enfoque lo más realista posible, basado en amenazas reales, muy bien fundamentado y con impacto estratégico.



- **MITRE: Proyecto CVE y ATT&CK**
- **CISA KEV**
- **NIST 800-115**
- **Tareas del PAI 5**

Vulnerabilidades: CVE

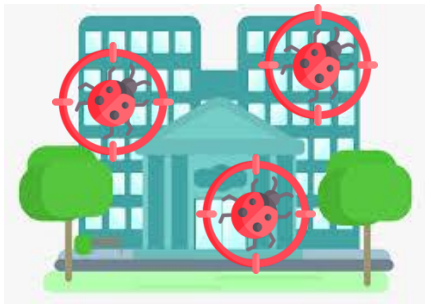
- **Financiación de la ciberseguridad:** Noticia recientemente aparecida: Una de las piezas clave del **ecosistema global de ciberseguridad** está en peligro. El próximo 16 de abril de 2025, el gobierno de Estados Unidos dejará de financiar el programa CVE (Common Vulnerabilities and Exposures), gestionado durante más de dos décadas por la organización sin ánimo de lucro **MITRE**.

Finalmente han conseguido
dicha financiación

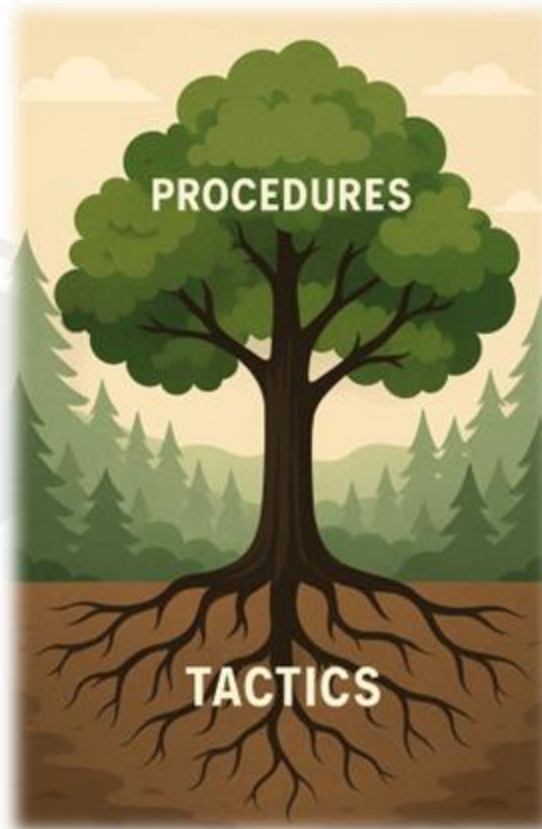
Vulnerabilidades: CVE

- Los **CVEs** pueden ayudar a los Red Team a identificar posibles **vectores de ataques prácticos, reales y bien fundamentados**, ya que contienen información sobre vulnerabilidades específicas en software (**actualmente sobre 276,000 CVE registros**), junto con detalles técnicos tales como:
 - Versión afectada.
 - Condiciones para la explotación.
 - Severidad (CVSS).
 - Enlaces a pruebas de concepto (PoCs) o **exploits conocidos**.

Organización Pública



Vulnerabilidades
+
Explotación



- Offensive Security
- Ethical Hacking
- Exploiting Vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning



- En 2013 el proyecto **ATT&CK®**, tenía como objetivo describir y categorizar los comportamientos de los atacantes en **tácticas, técnicas y procedimientos basándose en observaciones reales**.
- Hoy día, cuenta con diferentes matrices para entornos **Enterprise** (*Windows, macOS, Linux, PRE, Office Suite, Identity Provider, SaaS, IaaS,...*), **Mobile** (*Android/iOS*) y **ICS (Sistemas de Control Industrial)**, donde se recopilan las tácticas y técnicas en cada entorno.
 - **Las Tácticas**, refleja “**por qué**” el atacante realiza una determinada acción (moverse lateralmente, escalar privilegios, acceder a credenciales, command&control ...) ofensiva sobre un objetivo específico.
 - y las **técnicas**, refleja “el cómo” el atacante lleva a cabo la táctica concreta.
 - Ambas poseen un **identificador único asociado que permite hacer una referencia a ellas de forma unívoca**.

MITRE | ATT&CK®

Tácticas

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	11 techniques	16 techniques	23 techniques	14 techniques	45 techniques	17 techniques	33 techniques	9 techniques	17 techniques	18 techniques	9 techniques	15 techniques
Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Gather Victim Org Information (4) Phishing for Information (4) Search Closed Sources (2) Search Open Technical Databases (5) Search Open Websites/ Domains (3) Search Victim-Owned Websites	Acquire Access Acquire Infrastructure (8) Compromise Accounts (3) Compromise Infrastructure (8) Develop Capabilities (4) Establish Accounts (3) Obtain Capabilities (7) Stage Capabilities (6)	Content Injection Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (4) Replication Through Removable Media Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4) Wi-Fi Networks	Cloud Administration Command Command and Scripting Interpreter (12) Container Administration Command Deploy Container ESXi Administration Command Exploitation for Client Execution Input Injection Inter-Process Communication (3) Native API Scheduled Task/Job (3) Serverless Execution Shared Modules Software Deployment Tools System Services (3) User Execution (4) Windows Management Instrumentation	Account Manipulation (7) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5) Cloud Application Integration Compromise Host Software Binary Create Account (3) Create or Modify System Process (5) Event Triggered Execution (17) Exclusive Control External Remote Services Hijack Execution Flow (12) Implant Internal Image Modify Authentication Process (9) Modify Registry Office Application Startup (6) Power Settings Pre-OS Boot (3) Scheduled Task/Job (3) Server Software Component (3) Software Extensions (2) Traffic Signaling (2) Valid Accounts (4)	Abuse Elevation Control Mechanism (8) Access Token Manipulation (5) Account Manipulation (7) Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5) Create or Modify System Process (5) Domain or Tenant Policy Modification (2) Escape to Host Event Triggered Execution (17) Exploitation for Privilege Escalation Hijack Execution Flow (12) Process Injection (12) Scheduled Task/Job (9) Valid Accounts (4)	Abuse Elevation Control Mechanism (8) Access Token Manipulation (5) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain or Tenant Policy Modification (2) Email Spoofing Execution Guardrails (2) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (14) Hijack Execution Flow (12) Impair Defenses (11) Impersonation Indicator Removal (10) Indirect Command Execution Masquerading (11) Modify Authentication Process (9) Modify Cloud Compute Infrastructure (5) Modify Cloud Resource Hierarchy Modify Registry Modify System Image (2) Network Boundary Bridging (1) Obfuscated Files or Information (17) Plist File Modification Pre-OS Boot (3) Process Injection (12)	Adversary-in-the-Middle (4) Brute Force (4) Credentials from Password Stores (6) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (9) Multi-Factor Authentication Interception Multi-Factor Authentication Request Generation Network Sniffing OS Credential Dumping (8) Steal Application Access Token Steal or Forge Authentication Certificates Steal or Forge Kerberos Tickets (3) Steal Web Session Cookie Unsecured Credentials (8)	Account Discovery (4) Application Window Discovery Browser Information Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource Discovery Debugger Evasion Device Driver Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Log Enumeration Network Service Discovery Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery (3) Process Discovery Query Registry Remote System Discovery Software Discovery (1) System Information Discovery System Location Discovery (1) System Network	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (8) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Adversary-in-the-Middle (4) Archive Collected Data (3) Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Data from Configuration Repositories (3) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2) Email Collection (3) Input Capture (4) Screen Capture Video Capture	Application Layer Protocol (3) Communication Through Removable Media Content Injection Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (3) Encrypted Channel (2) Fallback Channels Hide Infrastructure Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Tools (3) Traffic Signaling (2) Web Service (3)	Automated Exfiltration (1) Data Transfer Size Limits Exfiltration Over Alternative Protocol (3) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (4) Scheduled Transfer Transfer Data to Cloud Account	Account Access Removal Data Destruction (1) Data Encrypted for Impact Data Manipulation (2) Defacement (2) Disk Wipe (2) Email Bombing Endpoint Denial of Service (4) Financial Theft Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking (4) Service Stop System Shutdown/Reboot

Técnicas

- Por ejemplo para la táctica **Credential Access(TA0006)** una de las técnicas de ataque es **Brute Force(T1110)** y hay 4 subtécnicas (aparece como subíndice en la matriz)
 - Password Guessing
 - Password Cracking
 - Password Spraying
 - Credential Stuffing
- Además, aparecen en cada técnica los procedimientos ejemplos ya usados por grupos de atacantes.

- **Integración MITRE ATT&CK y CVE**

- MITRE vincula algunos CVEs con técnicas ATT&CK, lo que permite:
 - Integrar una Vulnerabilidad en una Cadena de Ataque Realista
 - Actuar cómo un actor específico real (APT, ransomware, etc.) que podría aprovechar una CVE.
 - Correlacionar tácticas y técnicas con vulnerabilidades específicas.
- Por ejemplo:
 - La vulnerabilidad CVE-2021-34527 (PrintNightmare) si se busca en ATT&CK “Print Spooler”, “CVE-2021-34527” aparece relacionado con las técnicas:
 - **T1543.003 Create or Modify System Process: Windows Service**
 - **T1055 Process Injection**
 - **T1068 Exploitation for Privilege Escalation**

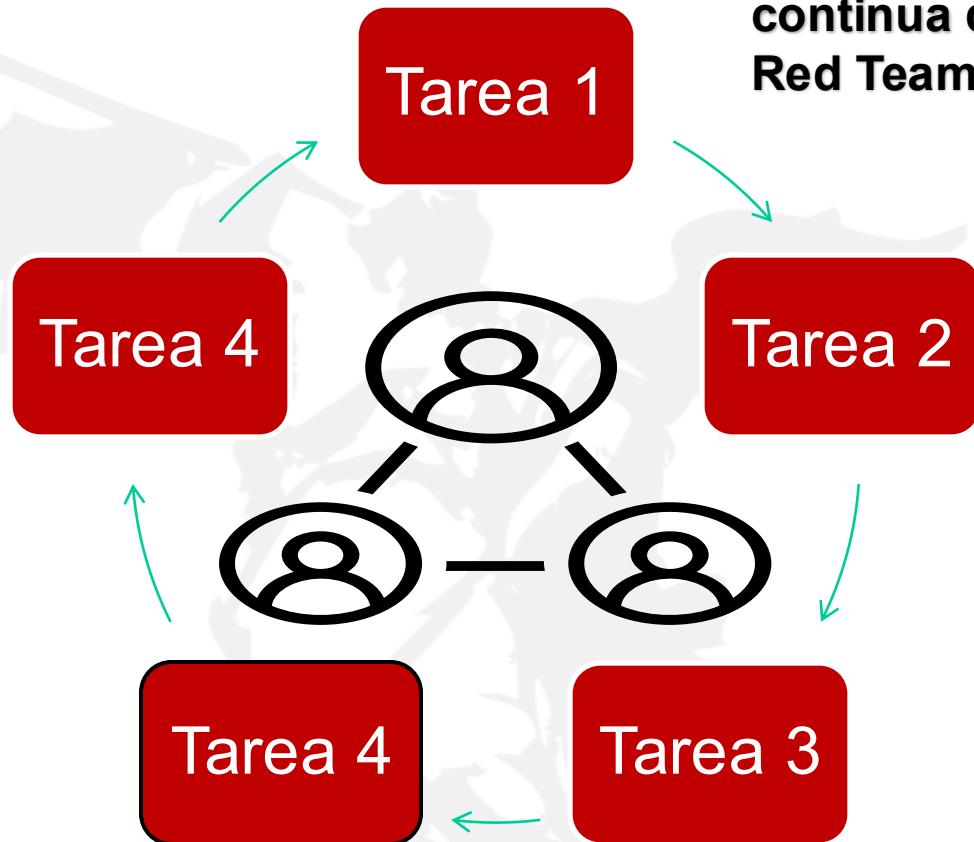
- **CISA KEV (Known Exploited Vulnerabilities)** es un catálogo no de “potenciales amenazas”, sino de vulnerabilidades del software que ya están siendo explotadas por grupos de ciberdelicuentes y que mantiene actualizada la ***Cibersecurity & Infrastructure Security Agency en US***
 - Confirmadas en el mundo real (por agencias como FBI, NSA, CISA).
 - Riesgo real inmediato y por tanto se ha debido priorizar su parcheo por los Blue Team.

Workflows de los Red Teams

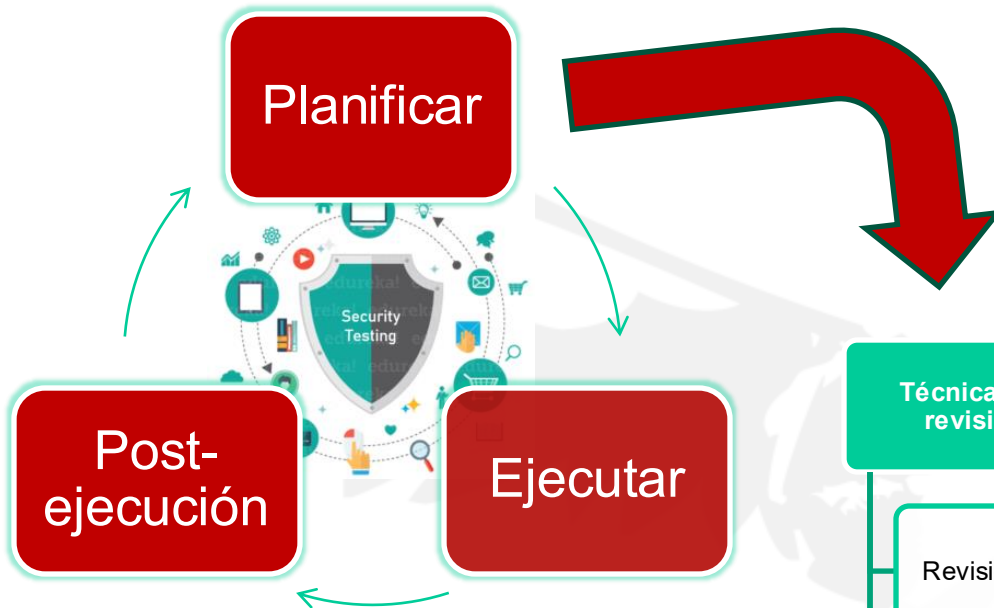
Todo lo anterior
representa el
conocimiento
para los Red
Teams



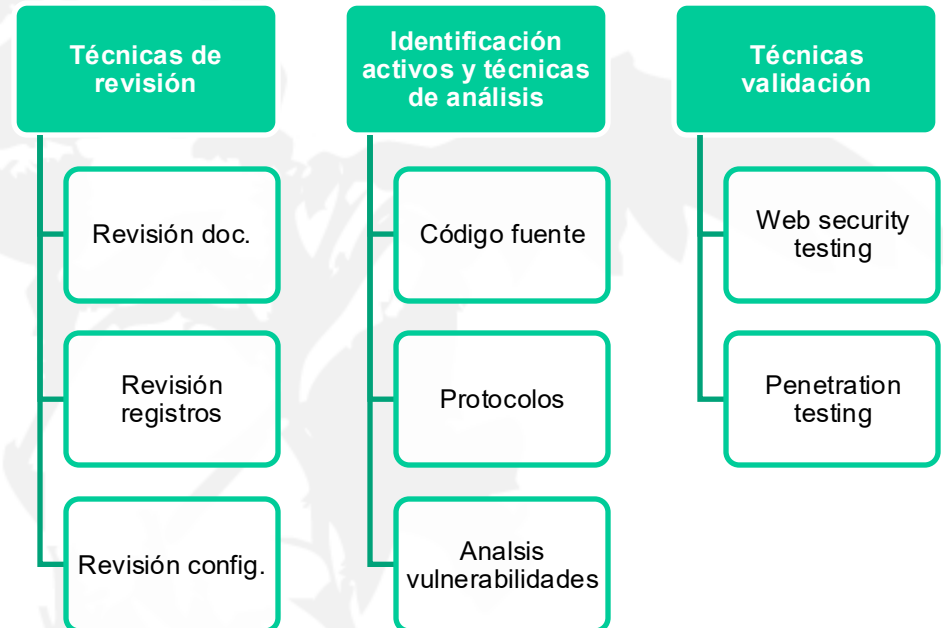
¿¿Cuál es el
flujo de trabajo
para la mejora
continua de los
Red Teams???

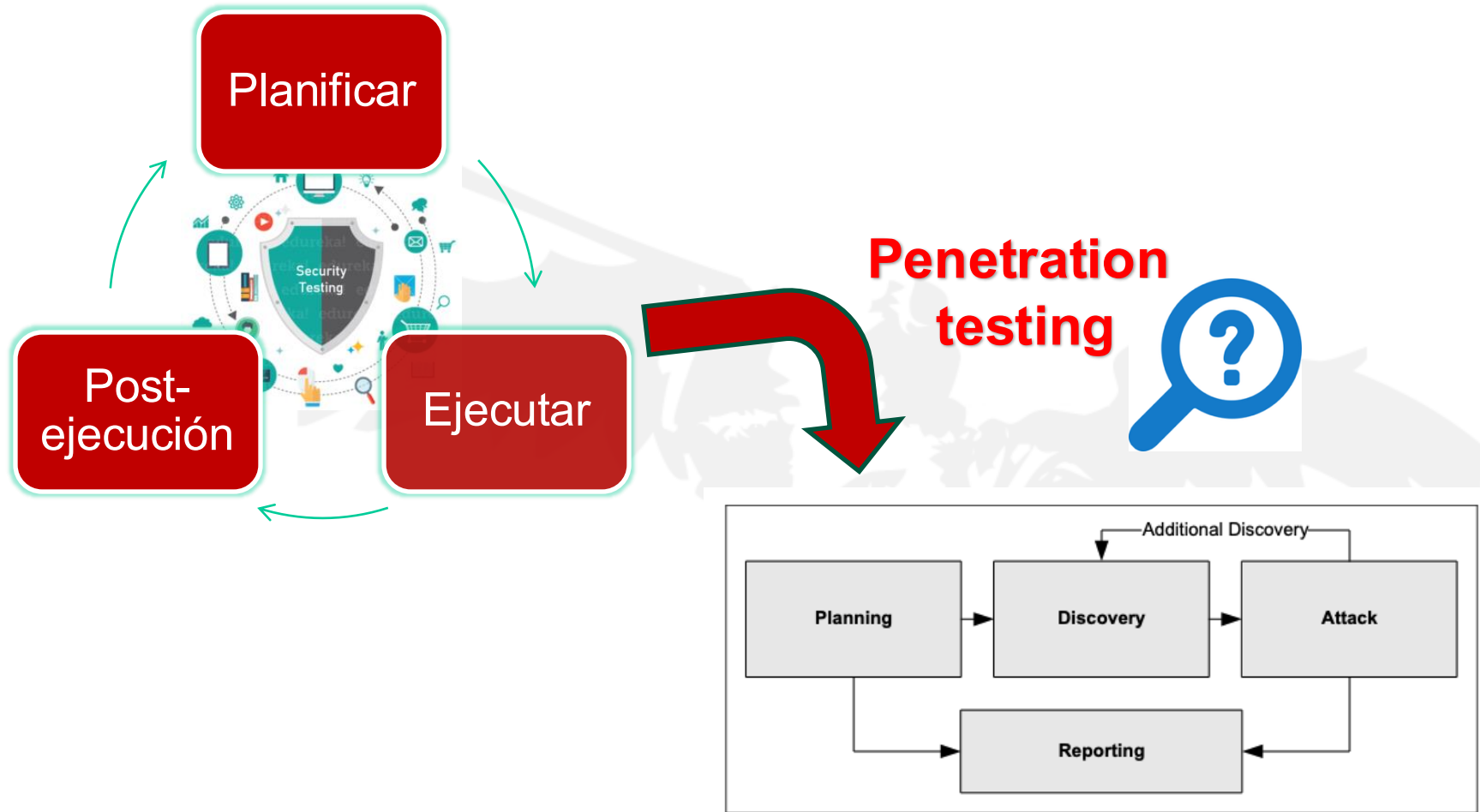


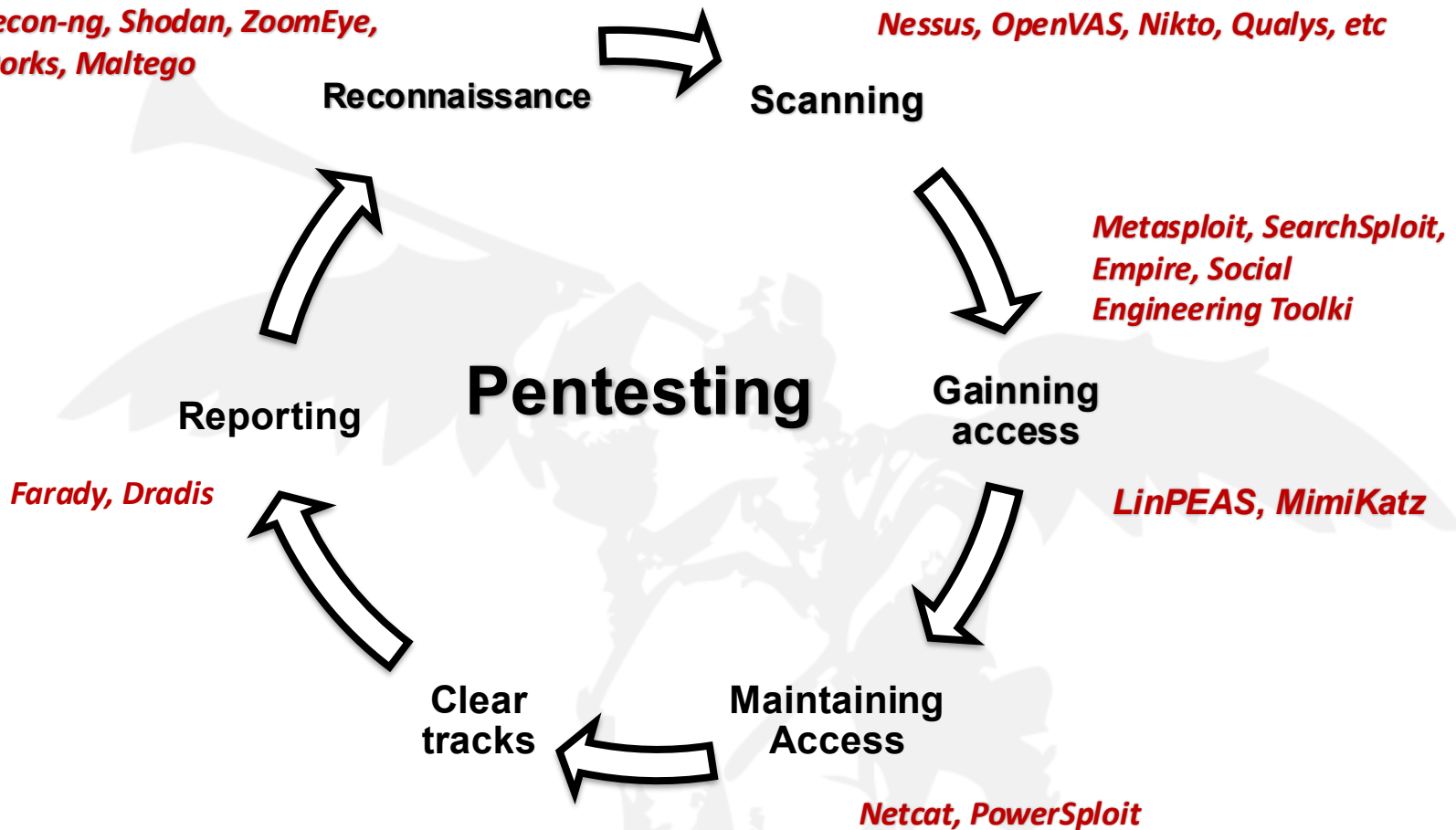
Technical Guide to Information Security Testing and Assessment, 2008

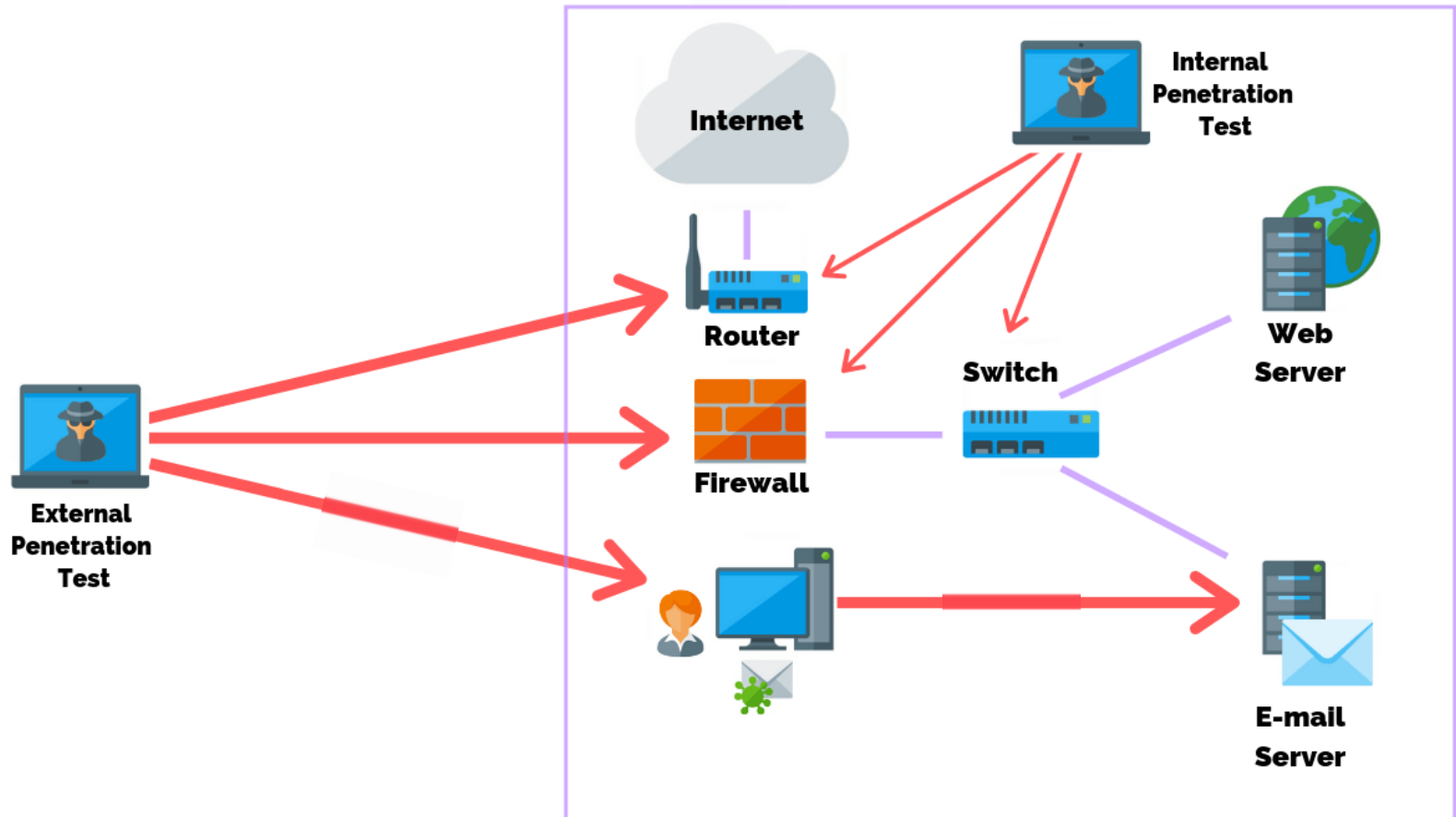


TÉCNICAS

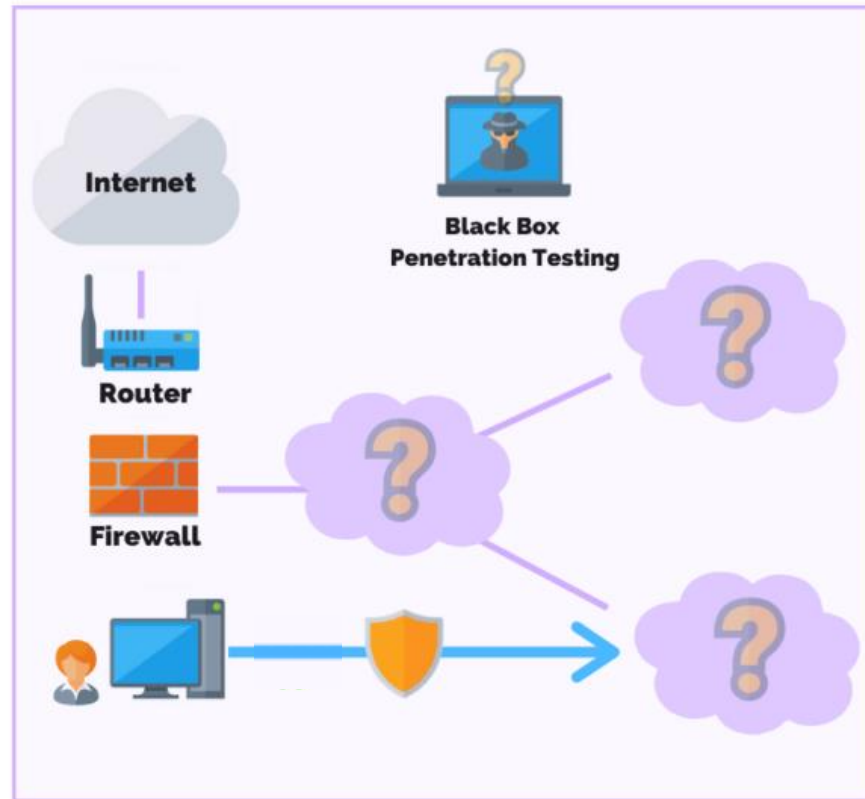








*Origen de las imágenes: <https://purplesec.us/>



*Origen de las imágenes: <https://purplesec.us/>

Otras herramientas open-source con el foco específico del desarrollo de las actividades propias de Red Team y también de Blue Team son:

- **MITRE Caldera**: basada en MITRE- ATT&CK y que dispone de un agente ligero para el trabajo de Red Team.
- **Uber Metta**: más ligero que CALDERA, pero no tan completo, también basado en MITRE- ATT&CK.
- **Atomic Red Team de Red Canary**: permite ejecutar **pruebas pequeñas, específicas y controladas** llamadas "**atomics**", similarea a las técnicas del marco MITRE ATT&CK.

Las anteriores herramientas son integrables en los pipelines de CI/CD (security validation as code)

1. Planificar:

- a. Definir un **escenario sobre el que se desarrollarán pruebas de seguridad**.
- b. **Identificación de los servicios y aplicaciones** sobre los que se desarrollarán las pruebas de seguridad.
- c. Analizar vulnerabilidades y los controles de seguridad desplegados.
- d. **Definir las pruebas de seguridad a realizar.**

2. Ejecutar Explotación, Escalada de Privilegios y Post-explotación:

- a. Ejecutar las pruebas e identificar potenciales brechas de seguridad.
- b. Tomar evidencias de todas las pruebas de seguridad.

3. Generar informes técnicos de pentesting:

- a. Analizar los resultados de las pruebas de seguridad y definir un plan de mitigación.
- b. Generar un informe técnico tanto del proceso llevado a cabo como los resultados obtenidos en las diferentes tareas de las pruebas de seguridad.



**Muchas gracias por
vuestra colaboración**