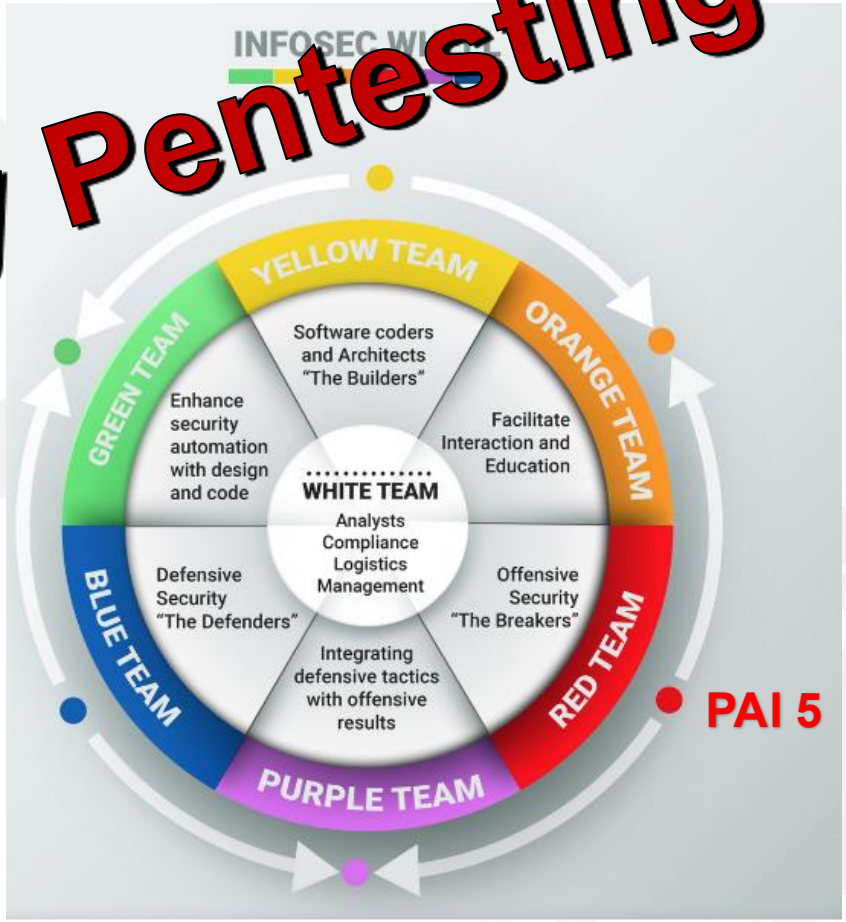
PAI-5. RedTeamPro
Evaluación de la seguridad de la información mediante pruebas de seguridad de una organización pública

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

RedTeamPro

No Toy Pentesting



PAI 5

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

Índice

- 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**.

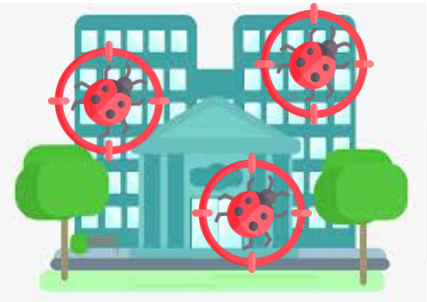
Finalmente han conseguido dicha financiación

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**.

ATT&CK® Project

Organización Pública



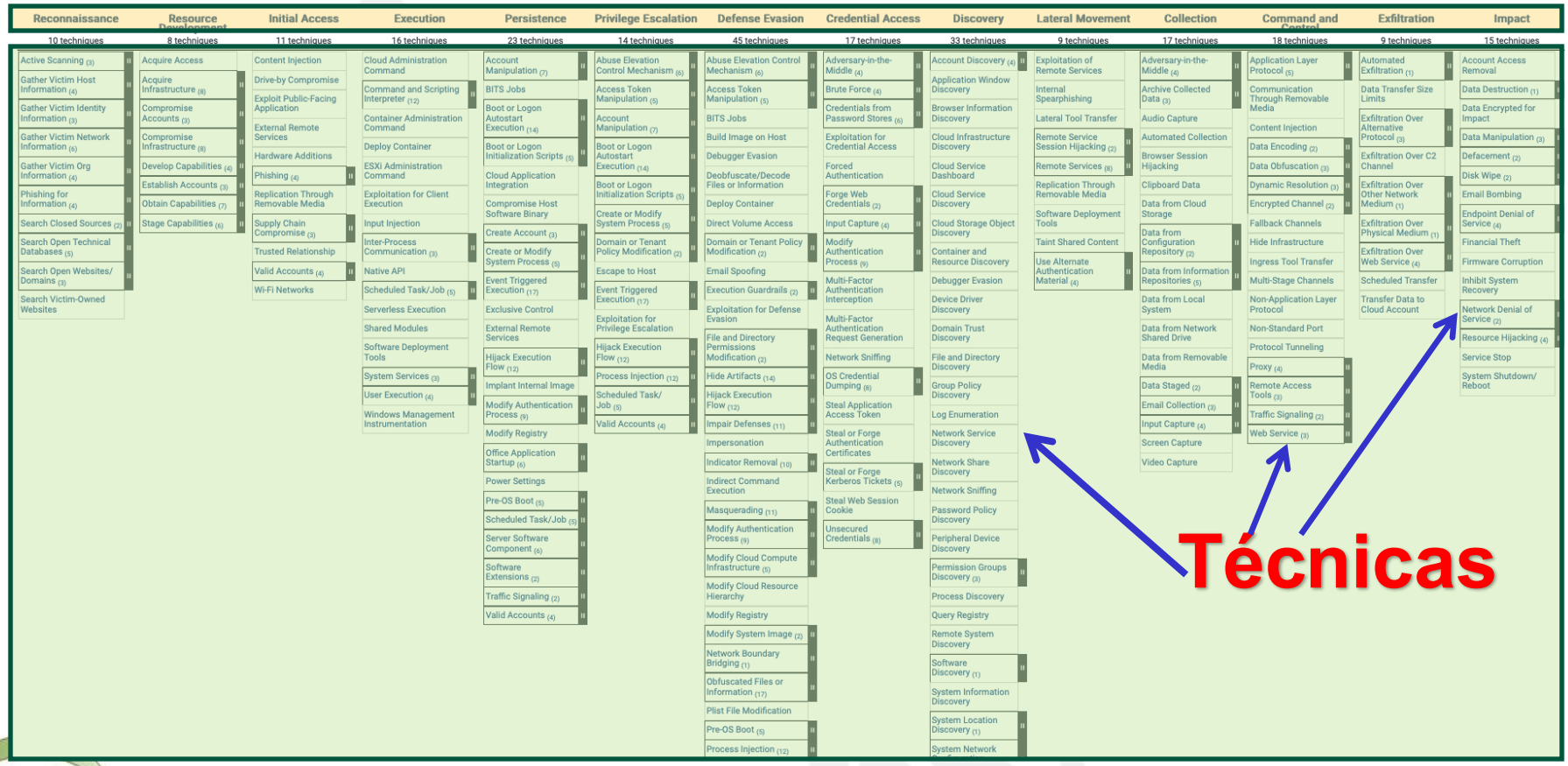
Vulnerabilidades
+
Explotación

ATT&CK® Project

- 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.**

Tácticas

MITRE | ATT&CK®



ATT&CK® Project

- 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**

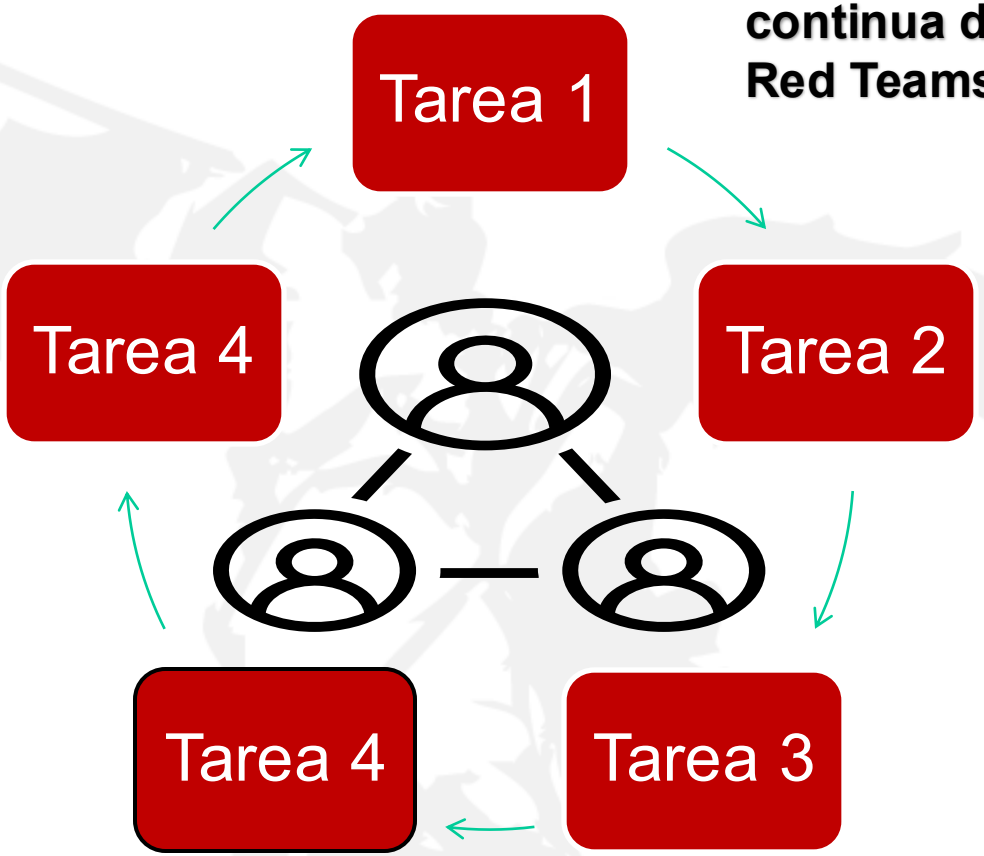
CISA KEV

- **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.

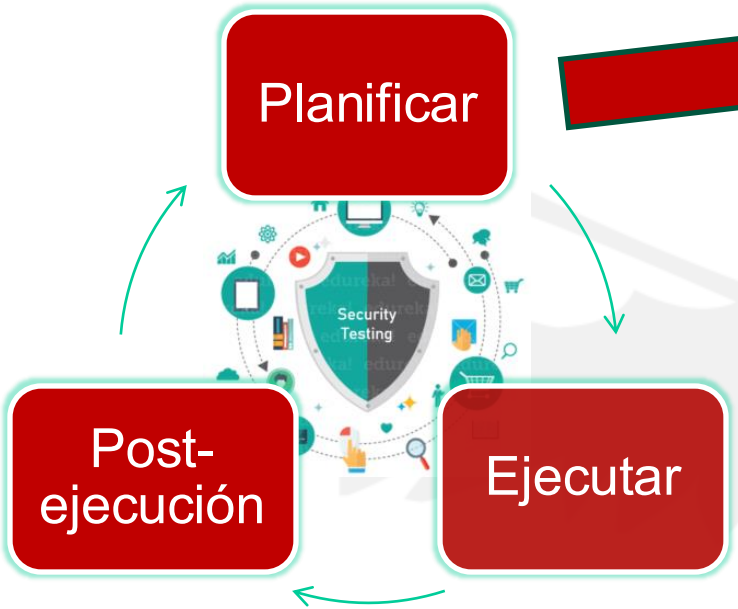
Workflows de los Red Teams

Todo lo anterior representa el conocimiento para los Red Teams

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



NIST 800-115

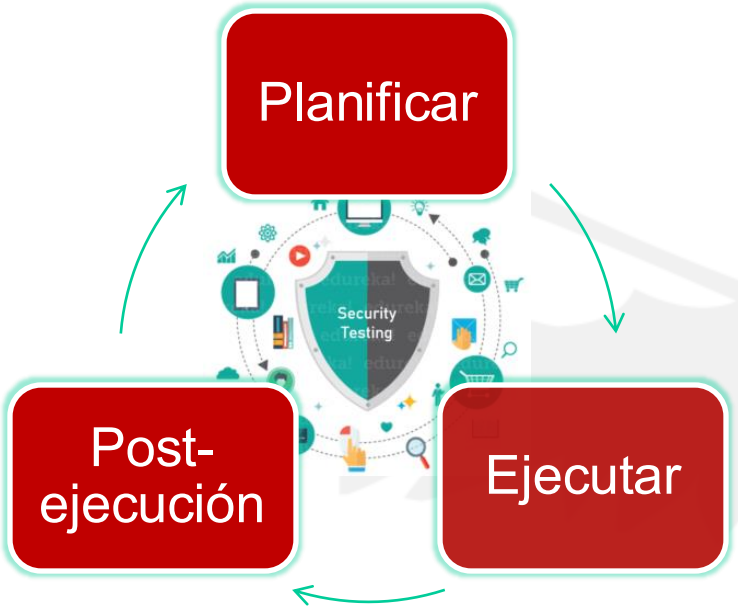


Technical Guide to Information Security Testing and Assessment, 2008

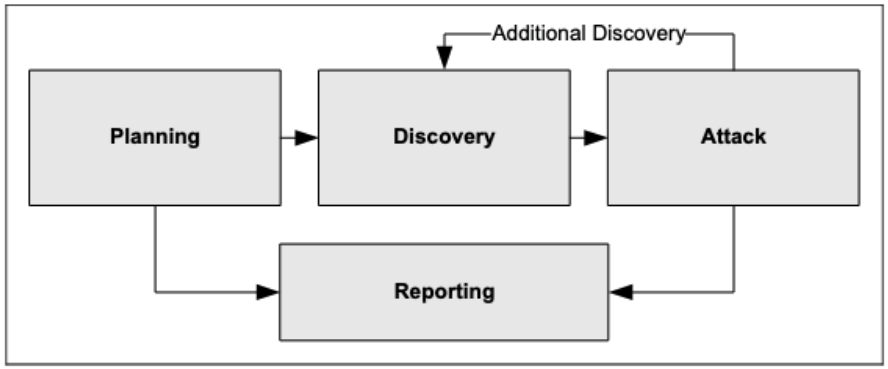
TÉCNICAS

- **Técnicas de revisión**
  - Revisión doc.
  - Revisión registros
  - Revisión config.
- **Identificación activos y técnicas de análisis**
  - Código fuente
  - Protocolos
  - Analsis vulnerabilidades
- **Técnicas validación**
  - Web security testing
  - Penetration testing

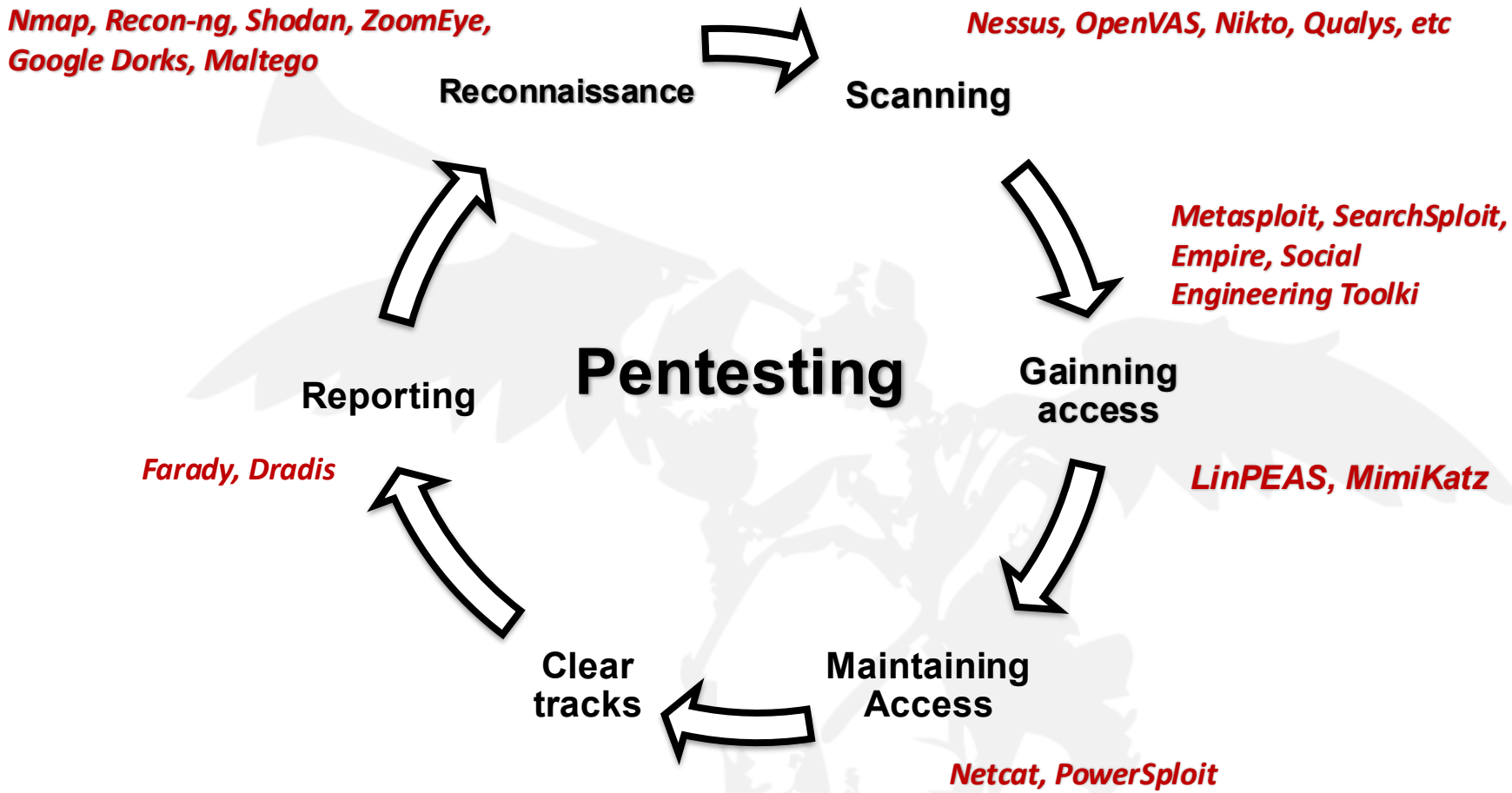
NIST 800-115



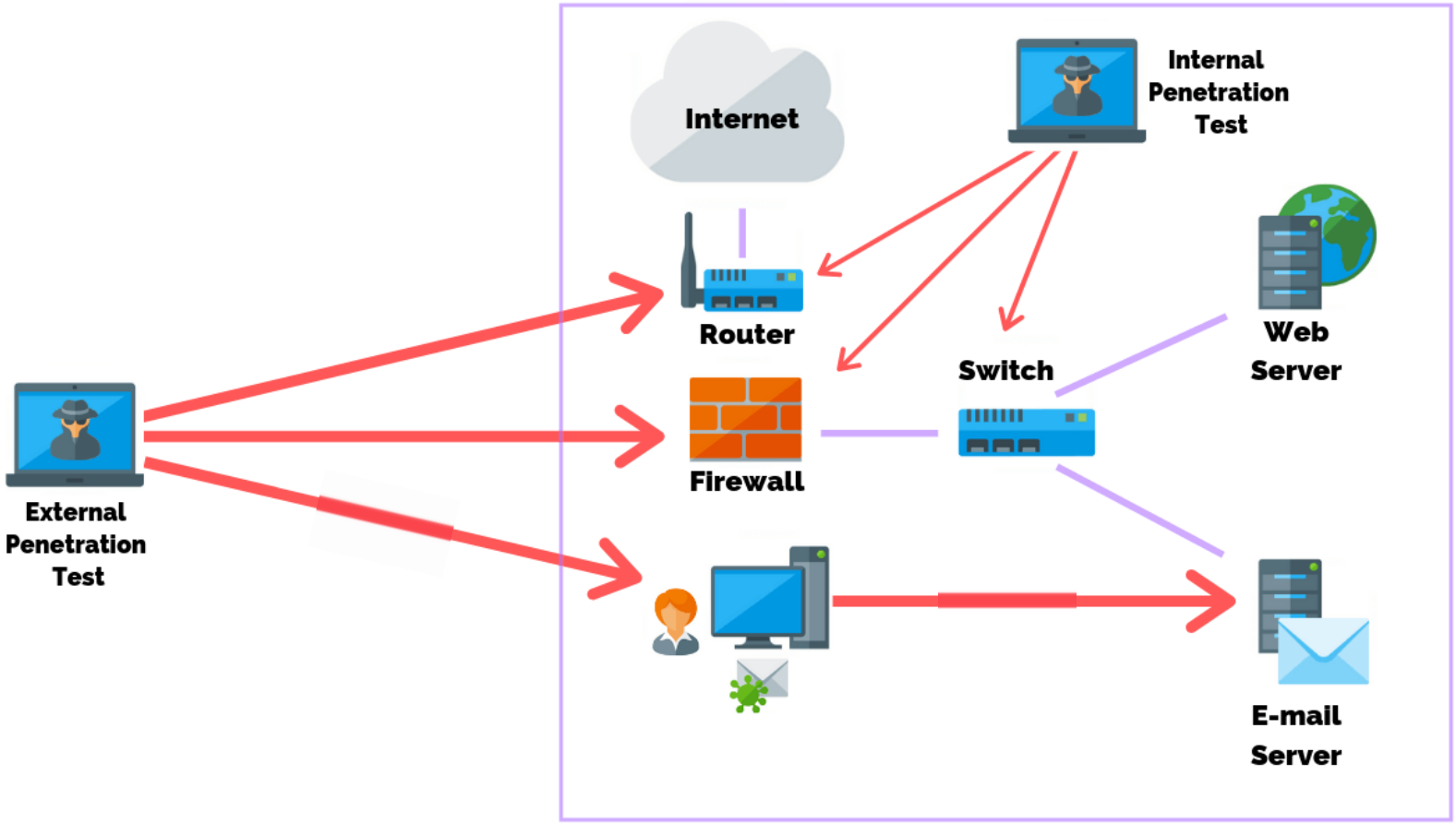
Penetration testing



NIST 800-115

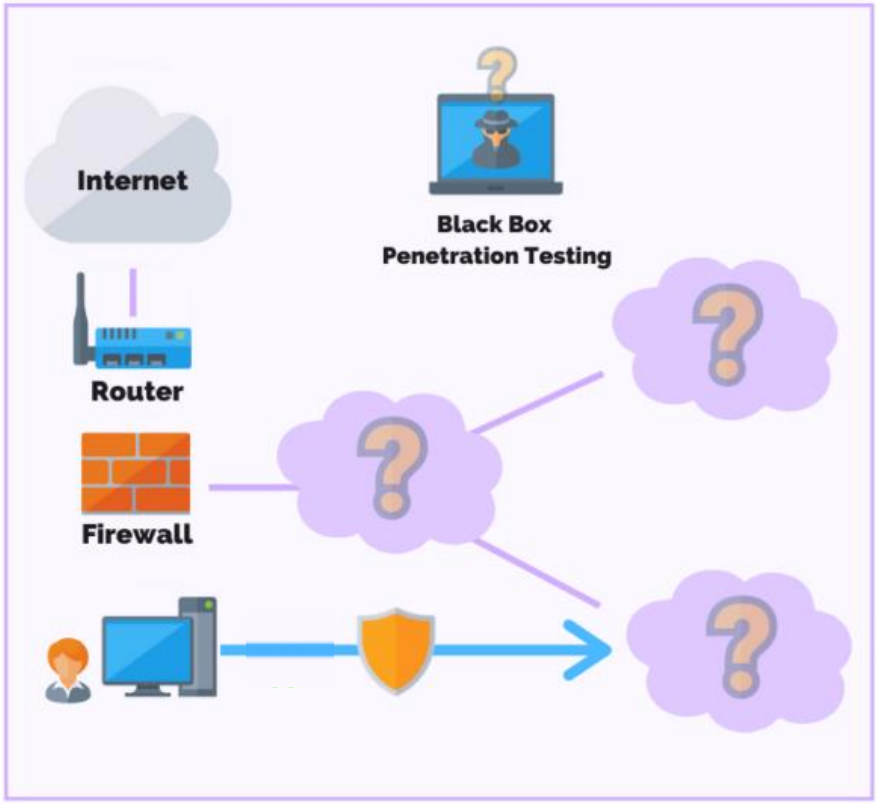

Nmap, Recon-ng, Shodan, ZoomEye, Google Dorks, Maltego
Reconnaissance
Nessus, OpenVAS, Nikto, Qualys, etc
Scanning
Metasploit, SearchSploit, Empire, Social Engineering Toolki
Gainning access
LinPEAS, MimiKatz
Maintaining Access
Netcat, PowerSploit
Clear tracks
Farady, Dradis
Reporting
Pentesting

White Box



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

Black Box



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

Open-Source Tools

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)

Objetivos

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