Gordon Lyon

Fyodor Vaskovich

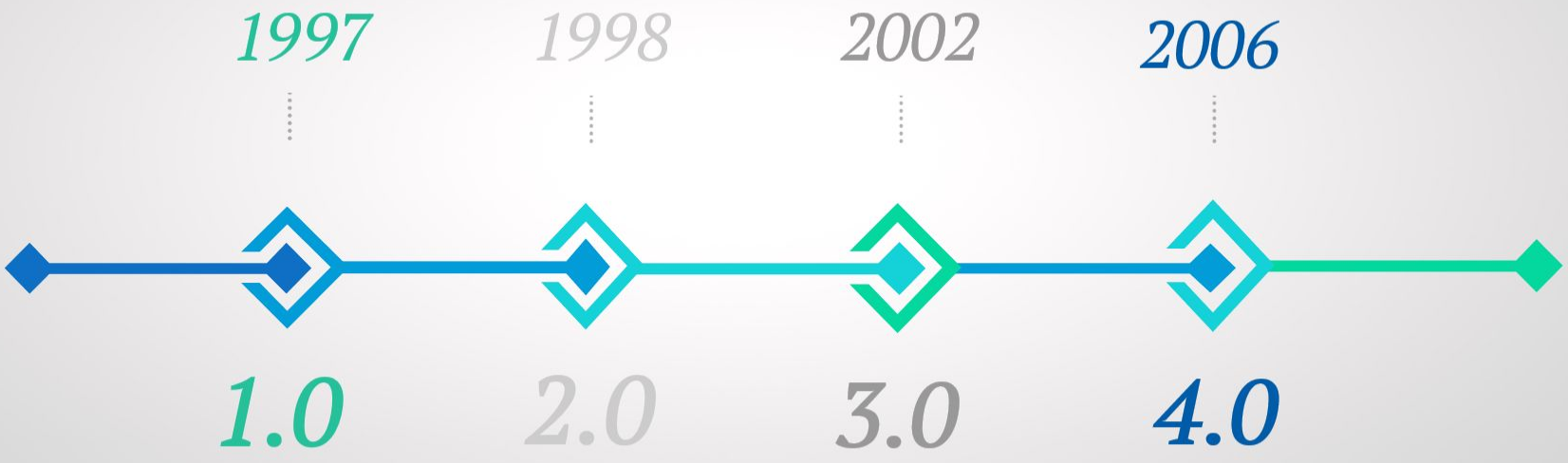
0 1 / 0 9 / 1 9 9 7

Nmap

- Utilidad para el descubrimiento de redes y la auditoría de seguridad.
- Línea de comandos
- Zenmap (GUI)

- Scanning
- OpenSource
  - https://github.com/nmap/nmap
- Gratis

VERSIONES



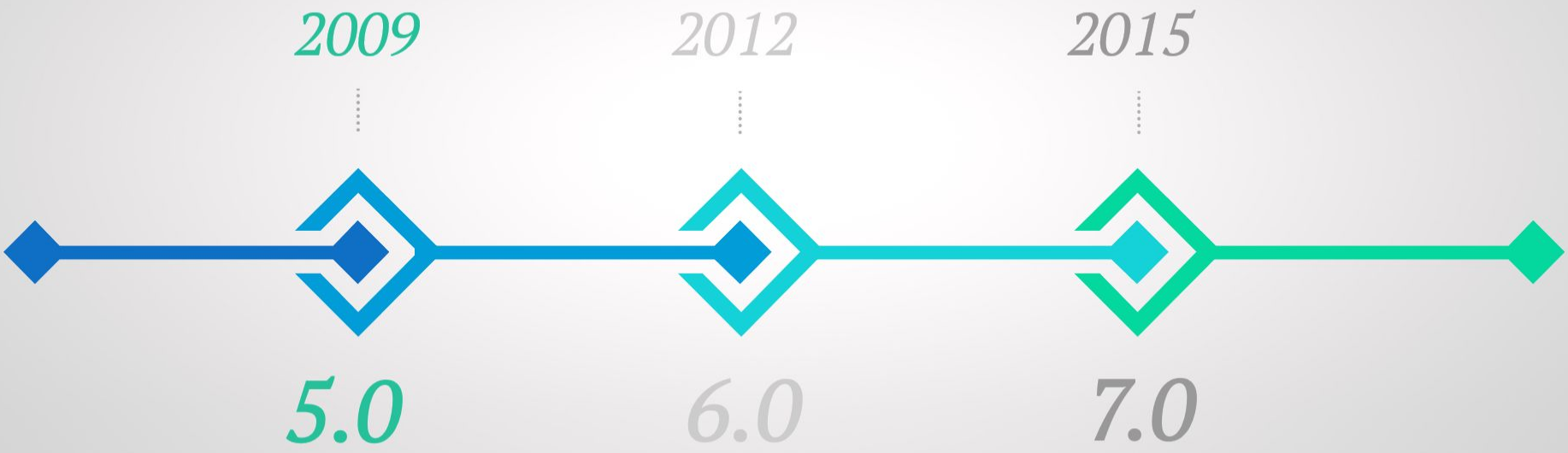
Se publica en la revista Phrack #51, art. 11. No tiene número de versión porque no se planean nuevos lanzamientos. Nmap tiene unas 2.000 líneas

Introduce la detección del sistema operativo. Consta de unas 8.000 líneas de código

Incluye compatibilidad con Mac OS X, salida XML y detección de tiempo de actividad.

Incluye la interacción en tiempo de ejecución para proporcionar estimaciones de terminación a petición, un instalador ejecutable de Windows

VERSIONES



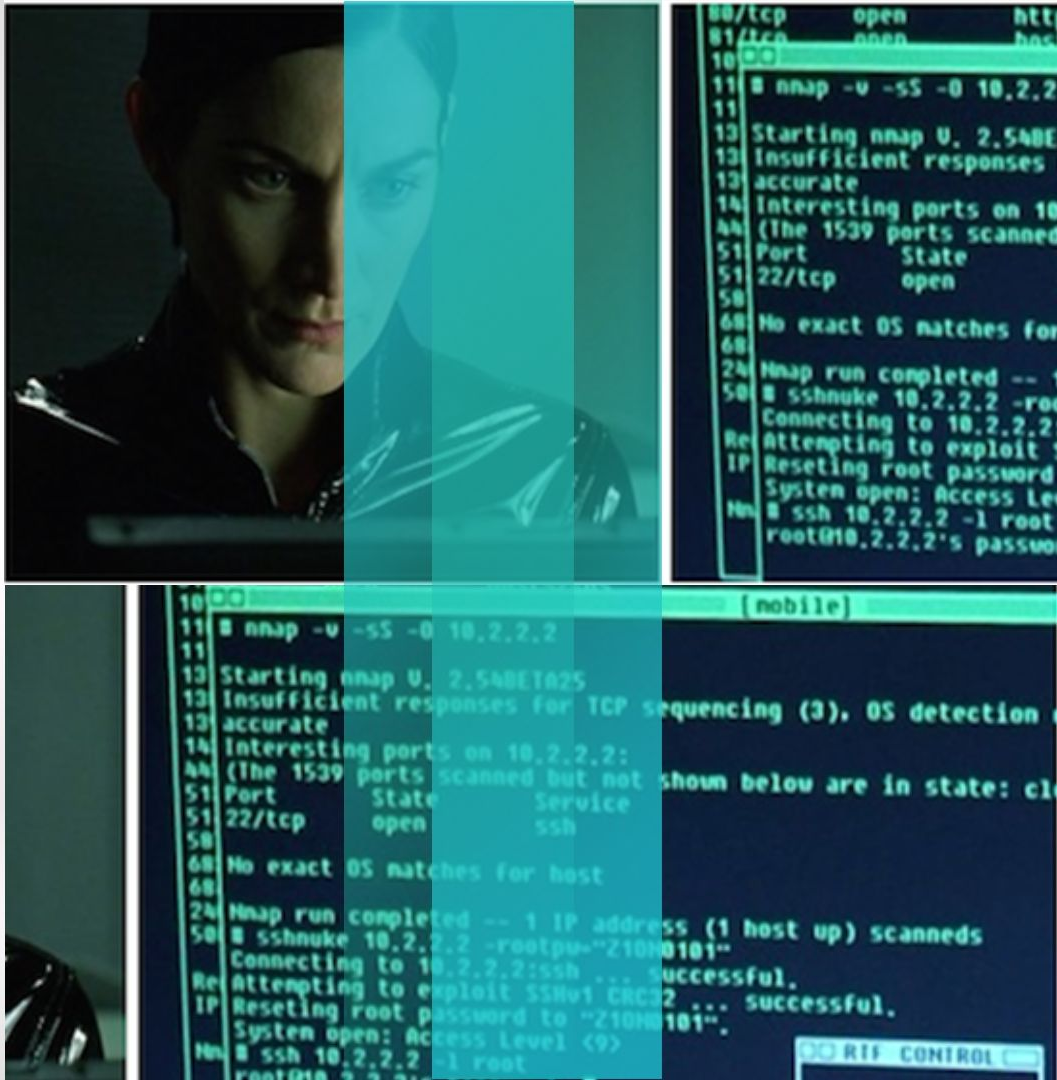
¿Qué hace?

Utiliza paquetes IP sin procesar para determinar:

- Qué hosts están disponibles en la red,
- Qué servicios (nombre y versión de la aplicación) ofrecen,
- Qué sistemas operativos (y versiones del sistema operativo) ejecutan,
- Qué tipo de filtros / firewalls de paquetes usan,

Nmap Suite incluye:

- Zenmap
- Ndiff
- Ncat
- Nping



¿Cómo funciona?

Scanning - Conjunto de procedimientos para identificar hosts, puertos y servicios en una red.

TCP 'Flags'

El encabezado TCP contiene 6 indicadores que controlan la transmisión de datos a través de una conexión TCP. El tamaño de cada 'flag' es 1 bit.

URG, PSH, FIN, ACK, RST, SYN

Escaneo de Puertos

- TCP
  - Abierto
    - TCP Connect / Full open
  - Sigiloso
    - Half open
    - ACK (SYN/ACK)
    - Inverso (XMAS, FIN, NULL)
  - Spoofed
    - IDLE / IPID
- UDP

Checar si hay sistemas activos

- Escaneo ICMP
- Ping Sweep

Escaneo pasando IDS

- Fragmentación de paquetes

Banner Grabbing (OS fingerprinting)

Detección del Sistema operativocon base en la comprobación de huellas TCP/IP.