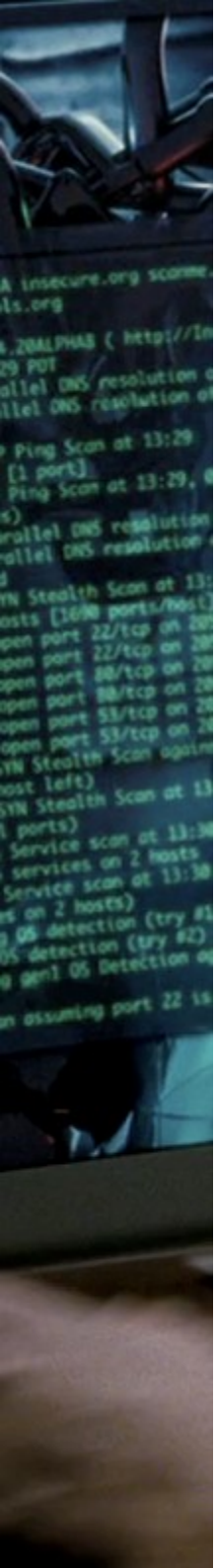


Webinar Gratuito

Nmap

V. 2

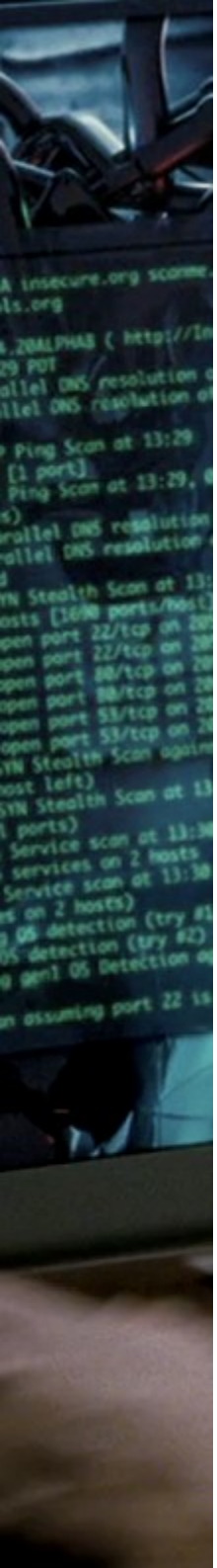
Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

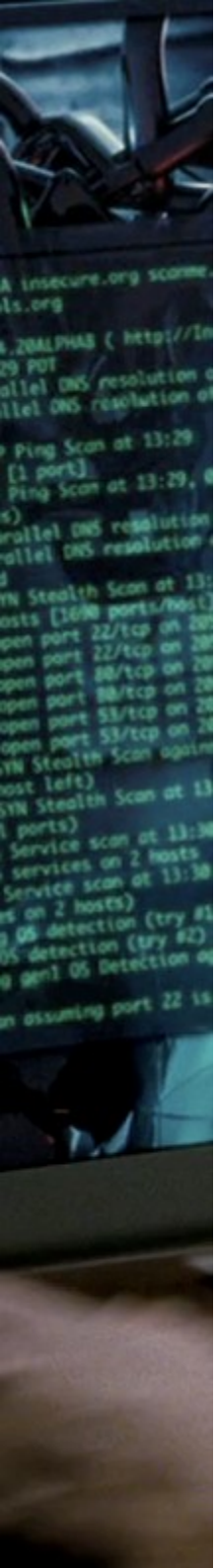
e-mail: ReYDeS@gmail.com

Sábado 25 de Octubre del 2014



¿Quién Soy?

- Consultor e Instructor Independiente en Hacking Ético, Informática Forense y GNU/Linux.
- Ex Integrante de RareGaZz y actual integrante de PeruSEC.
- Ex Redactor en la Revista Linux+ DVD (ES).
- Creador del II Reto Forense Digital Sudamericano - Chavín de Huantar 2012.
- Brainbench Certified Network Security, Brainbench Certified Computer Forensics (U.S.) & Brainbench Certified Linux Administration (General). CNHE, CNCF, CNHAW.
- Más de 11 años de experiencia en el área.
- @Alonso_ReYDeS
- pe.linkedin.com/in/alonsocaballeroquezada/



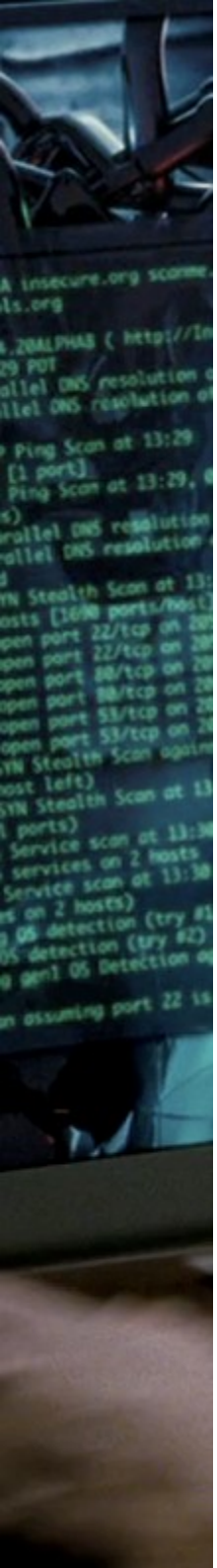
¿Qué es Nmap?

Nmap (Network Mapper) o por su traducción al español “Mapeador de Red”, es una herramienta libre y open source especializada en la exploración de redes y auditorías de seguridad. También es útil para tareas como el inventario de la red, manejo de horarios para la actualización de servicios, y vigilancia de hosts o tiempo de funcionamiento de un servicio.

Nmap utiliza paquetes IP en bruto para determinar cuales son los hosts que están disponibles en la red, cuales servicios (nombre y versión de la aplicación) ofrecen estos hosts, cuales sistemas operativos (y versiones del S.O.) están ejecutando, cual tipo de filtro de paquetes o firewall están utilizando, y docenas de otras características.

Está diseñado para escanear grandes redes de manera rápida, pero trabaja también muy bien con unos pocos hosts. Nmap puede ser ejecutado y utilizado en los principales sistemas operativos.

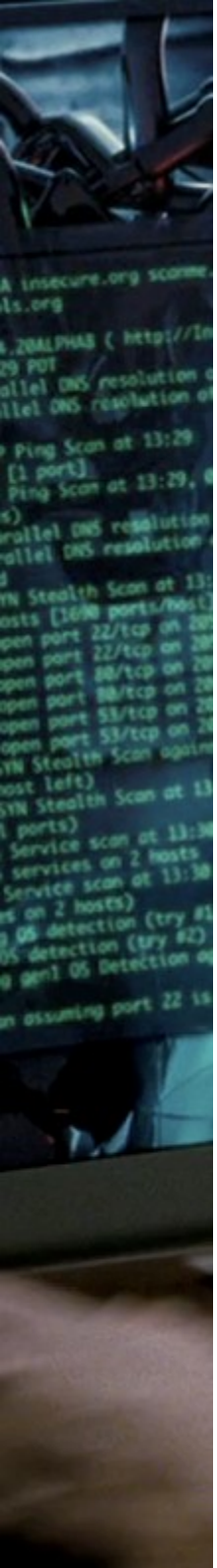
* Nmap: http://nmap.org/



Características de Nmap

1. **Flexible:** Soporta docenas de técnicas y mecanismos avanzados.
2. **Poderoso:** Escaneo redes de cientos de miles de máquinas
3. **Portable:** GNU/Linux, Windows, FreeBSD, Solaris, Mac OS, etc.
4. **Fácil:** Línea de comando tradicional o Interfaz Gráfica (GUI).
5. **Libre:** Descarga gratuita que viene con el código fuente.
6. **Bien Documentado:** Extensa cantidad de documentación.
7. **Soportado:** Existe una vibrante comunidad de ayuda y soporte.
8. **Aclamado:** Numerosos premios y reconocido de muchas formas.
9. **Popular:** Miles de personas lo descargan y utilizan a diario.

* Nmap Documentation: http://nmap.org/nmap_documentation.html



¿Qué son los Escaneos de Red?

Los Escaneos de Red implican el proceso de descubrir hosts activos en la red objetivo e información sobre estos, como puertos activos, información de aplicación y reconocimiento del sistema operativo. Existen cuatro técnica básicas para el escaneo de Red.

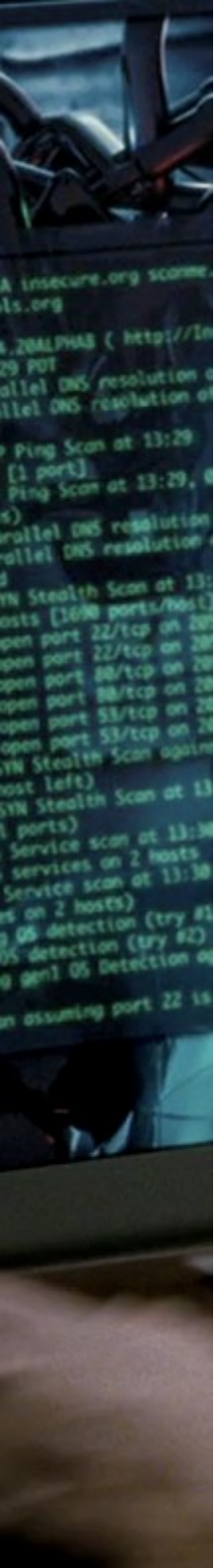
1. Mapeo de Red: Enviar mensajes hacia los hosts para generar una respuesta de los mismos si el host está activo.

2. Escaneo de Puertos: Enviar mensajes hacia un puerto específico para determinar si está activo.

3. Detección de Servicio y Versión: Enviar mensajes especialmente diseñados hacia un puerto activo para generar respuestas indicativas sobre el tipo y versión de servicio en funcionamiento

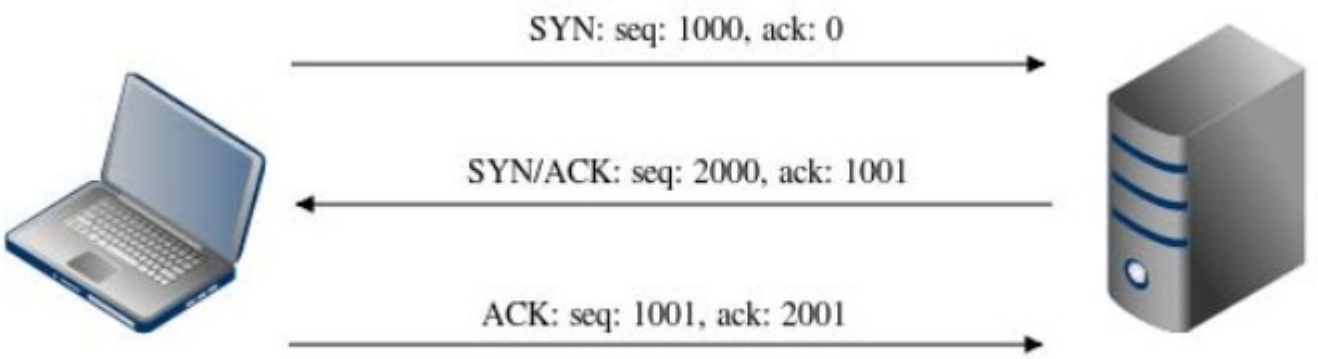
4. Detección del Sistema Operativo: Enviar mensajes especialmente diseñados para generar ciertas respuestas indicativas sobre el tipo de sistema operativo funcionando en el host.

.

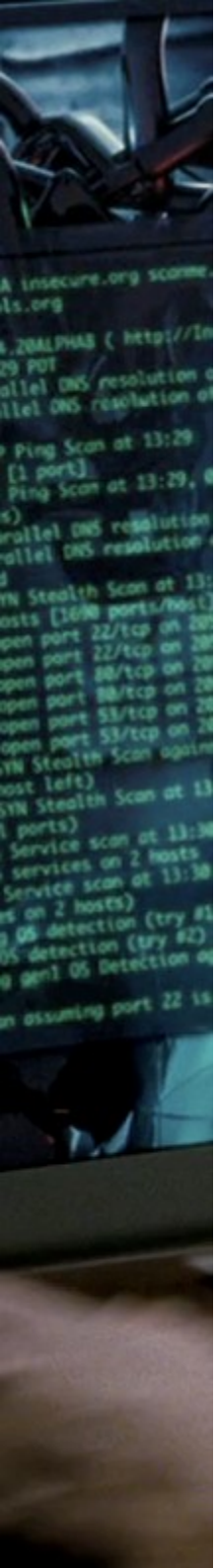


TCP Handshake

Una sesión TCP inicia típicamente con un host (Cliente) enviando un paquete de sincronización (SYN) hacia otro host (Servidor). El SYN contiene un número inicial de secuencia (ISN), un número pseudoaleatorio el cual representa el principio de una sesión TCP desde la perspectiva de el cliente. Luego el Servidor reconoce el SYN del Cliente, y genera su propio SYN. Este paquete "SYN/ACK" contiene el ISN del Servidor, como también el número de reconocimiento igual al ISN del Cliente mas 1. Finalmente el Cliente reconoce el SYN/ACK del Servidor, y envía un paquete con su propio ISN incrementado en uno, como también su número de reconocimiento igual al ISN del servidor más 1.



* http://nmap.org/misc/split-handshake.pdf



Cursos Virtuales

Todos los Cursos están disponibles en Video.

Curso Virtual de Hacking Ético
http://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web
http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense
http://www.reydes.com/d/?q=Curso_de_Informatica_Forense

Más Información:

caballero.alonso@gmail.com

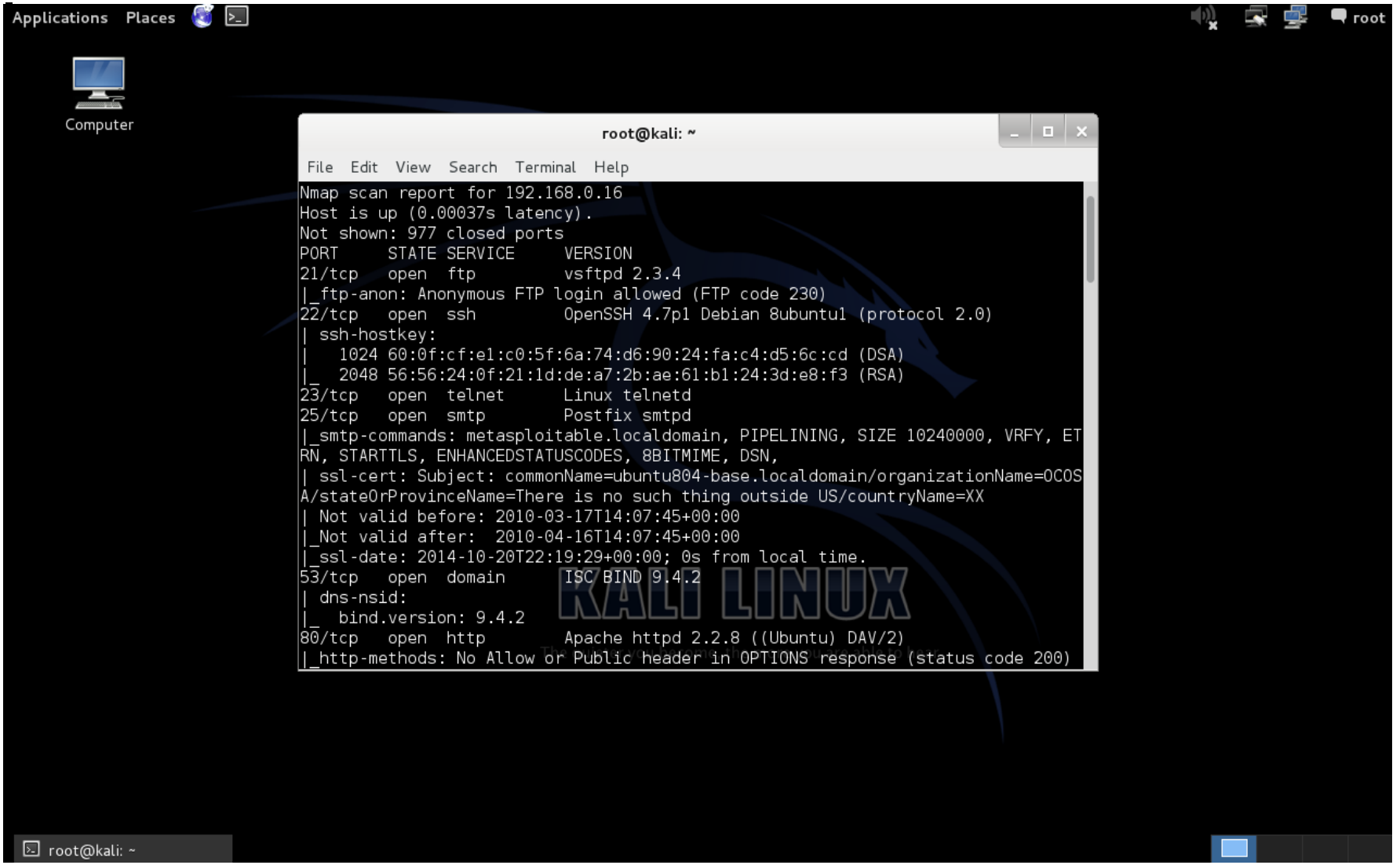
@Alonso_ReYDeS

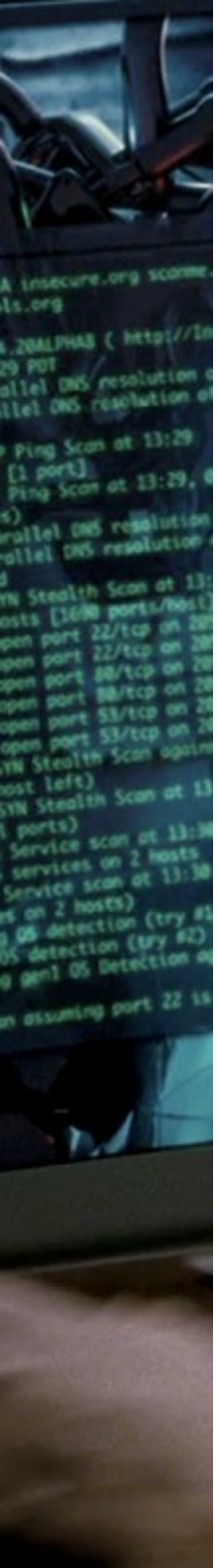
http://pe.linkedin.com/in/alonsocaballeroquezada/

ReYDeS

http://www.reydes.com

Demostraciones





Mas Material

Videos de 22 Webinars Gratuitos que he dictado sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

http://www.reydes.com/d/?q=videos

Todas las diapositivas utilizadas en los Webinars Gratuitos las encuentran en la siguiente página.

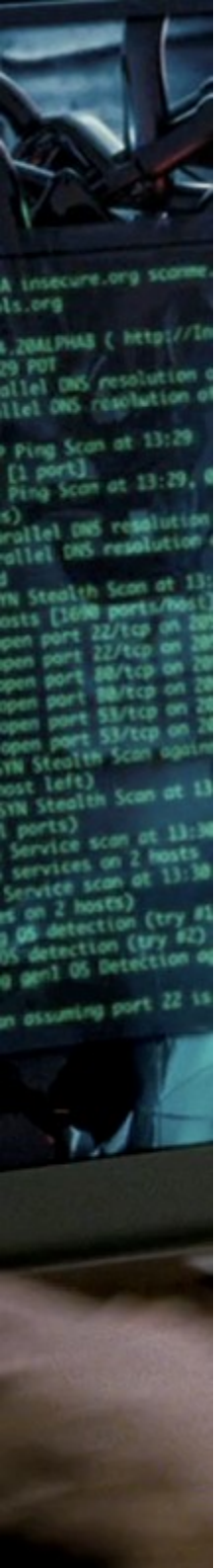
http://www.reydes.com/d/?q=node/3

Todos los artículos y documentos que he publicado.

http://www.reydes.com/d/?q=node/2

Mi Blog sobre temas de mi interés.

http://www.reydes.com/d/?q=blog/1



Muchas Gracias

Nmap

V. 2

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: http://www.ReYDeS.com

e-mail: ReYDeS@gmail.com

Sábado 25 de Octubre del 2014