

Inteligencia activa

Alexis Solis

Inteligencia activa

Conocida como IC 2.0 es la resultante del fuerte desarrollo que está experimentando la conectividad en el entorno de internet. Esto obliga a evolucionar el modelo tradicional de IC hacia un modelo activo contrastado contra los puntos de encuentro entre las marcas y los usuarios.

¡Cómo funciona?

En este caso, va a permitir que la información más actualizada esté disponible en el momento más primordial, ya sea impulsando métricas y conocimientos automatizados en los cuadros de mando o integrándolos específicamente en procesos automáticos, por ende, dicha inteligencia puede combinar datos en reposo con datos en movimiento, por lo cual, refleja el pulso de los datos y proporciona conocimientos en cada oportunidad estratégica de negocio



Análisis de dispositivos y puertos con Nmap

Puertos con NMap.

Nmap utilizará 1 ó 65535 respectivamente. Así se podrá especificar -p- para sondear todos los puertos desde el 1 al 65535. Se permite sondear el puerto cero siempre que lo especifique explícitamente. Esta opción especifica el número de protocolo que quiere sondear (de 0 a 255) en el caso de que esté sondeando protocolos IP (-sO).

Análisis de dispositivos y puertos con Nmap

Escaneo de puertos

Una vez que se haya identificado los hosts activos, a continuación, se debe de realizar un escaneo de puertos en esos hosts para determinar qué puertos están disponibles/abiertos y qué servicios se están ejecutando en ellos. Esto se hace mediante la utilización del siguiente comando:

```
nmap -p <puertos> <dirección IP>
```

Puedes reemplazar <puertos> con una lista de números de puerto separados por comas o rangos (por ejemplo, 80,443 o 1-1024) y <dirección IP> con la dirección IP del host que deseas escanear.

Parámetros opciones de escaneo de *Wmap*

Parámetros de nivel de detalle y depuración

- -v Incrementar el nivel de detalle
- -reason motivos por sistema y puerto
- -d (1-9) establecer nivel de depuración
- -packet-trace ruta de paquetes

Parámetros opciones de escaneo de nMap

Parámetros de nivel de detalle y depuración

- -v Incrementar el nivel de detalle
- -reason motivos por sistema y puerto
- -d (1-9) establecer nivel de depuración
- -packet-trace ruta de paquetes

Opciones interactivas

- v/V aumentar/disminuir nivel de detalle del análisis
- d/D aumentar/disminuir nivel de depuración
- p/P activar/desactivar traza de paquetes

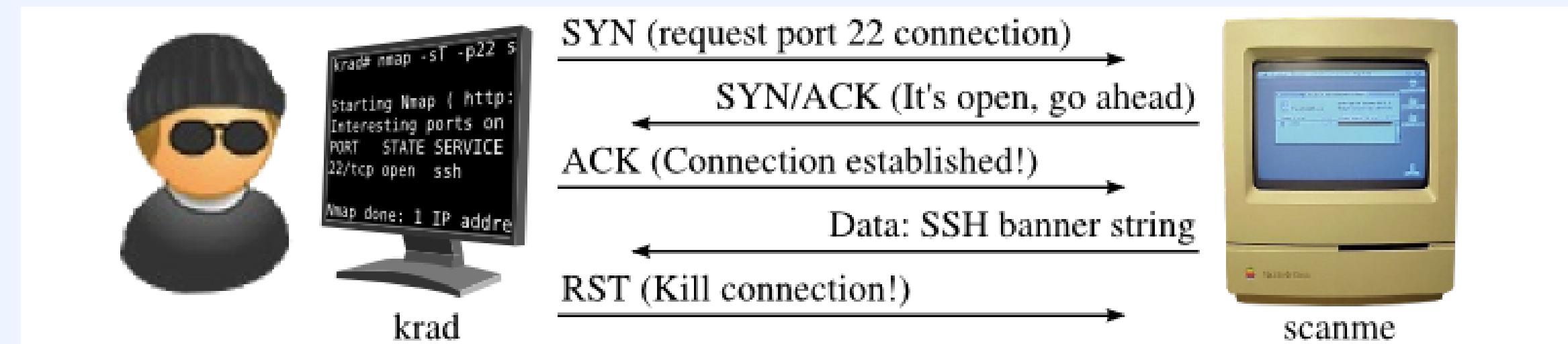
Parámetros opciones de escaneo de *Wmap*

Otras opciones

- -resume file continuar análisis abortado (tomando formatos de salida con -oN o -oG)
- -6 activar análisis IPV6
- -A agresivo, igual que con -O -sV -sC -traceroute

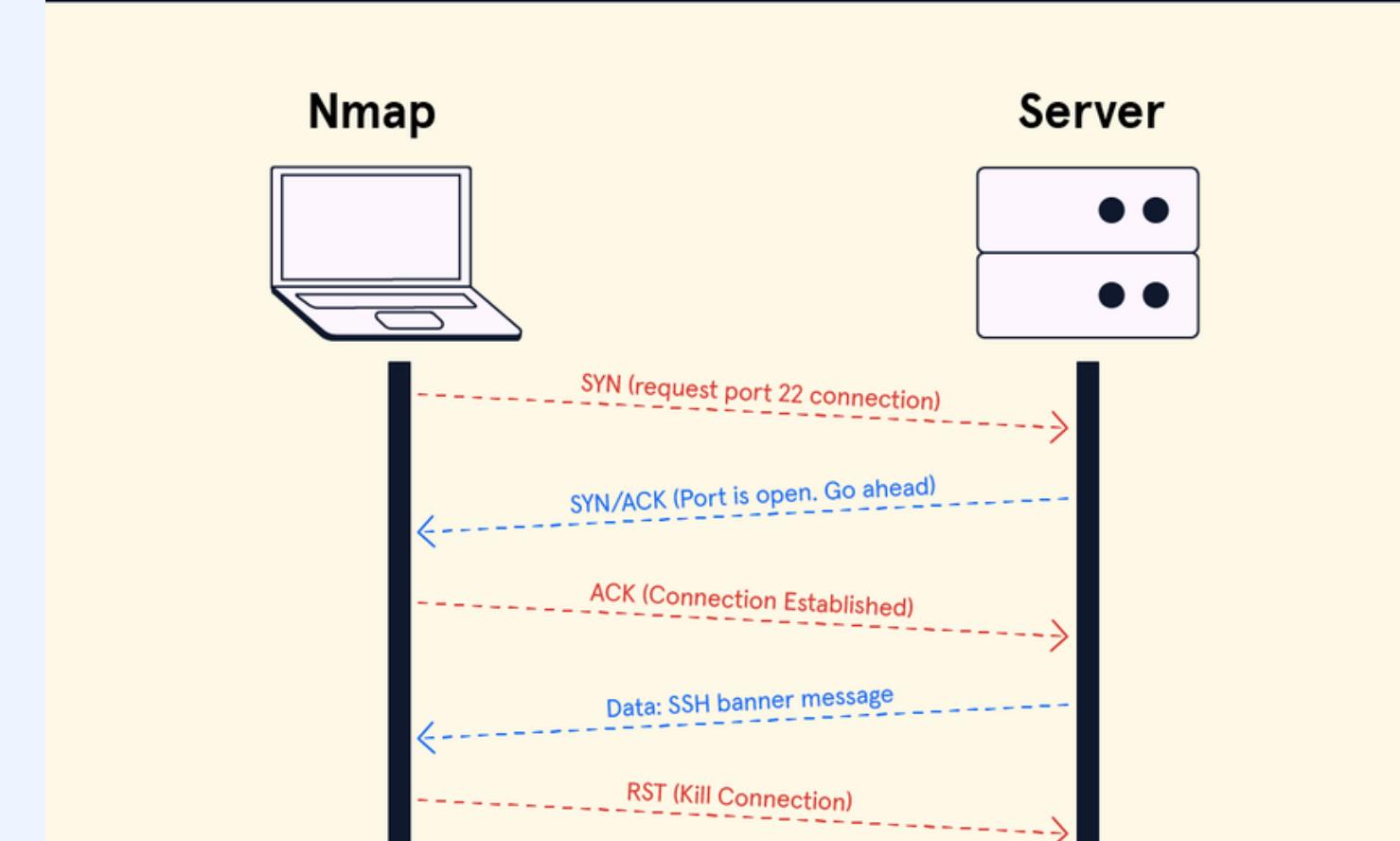
Full TCP Scan

Es una técnica de exploración de puertos que consiste en enviar un paquete FIN a un puerto determinado, en donde después de haber realizado eso, se deberá recibir un paquete de reset, (mayormente conocido como 'RST') si dicho puerto esta cerrado. Cabe destacar que esta técnica se aplica principalmente sobre implementaciones de pilas TCP/IP de sistemas Unix



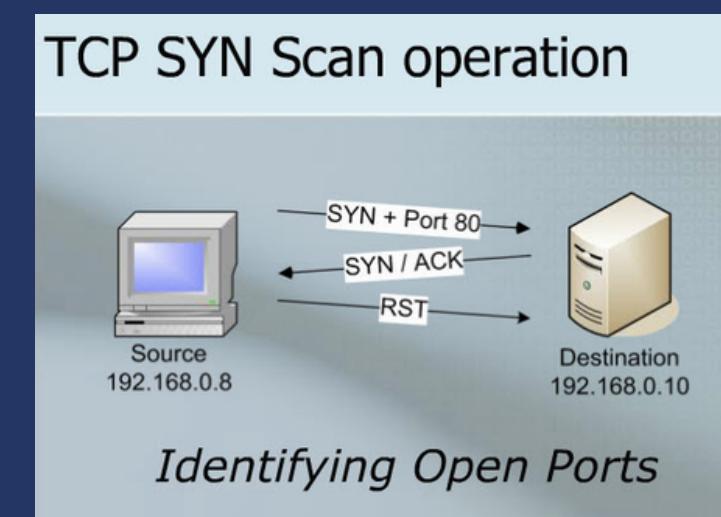
Full TCP Scan

Este tipo de escaneo implica que Nmap intentará conectarse a todos los 65,535 puertos TCP posibles en cada dirección IP o host en el rango especificado. Entonces, a causa a la gran cantidad de puertos y la duración que podría tomar, este tipo de escaneo puede llevar mucho tiempo y de igual manera, muchos recursos.



Stealth Scan

Es una técnica de escaneo en Nmap que busca minimizar la detección de actividad de escaneo por parte de los firewalls del host objetivo y otras medidas de seguridad. También, otro punto importante de este scan, es que se implementan para eludir los cortafuegos o descubrir hosts vivos sin ser detectados.



Stealth Scan

Técnicas para escaneos TCP SYN (Stealth) de nmap El usuario debe usar el indicador -sS (SYN) para hacer un escaneo SYN o Stealth como el que se muestra en la segunda imagen anterior. La conexión terminará al seleccionar esta opción. Nota: use el comando sudo en lugar del escaneo SYN si tiene acceso de root. A continuación, se muestra un ejemplo de escaneos sigilosos usando nmap contra la red 192.168.0.0/24 en Linux:

Sintaxis: \$ sudo nmap -sS 192.168.0.0/24

ZenMap

Se define como la interfaz gráfica de usuario oficial de NMap, la cual va a permitir usar el programa de manera práctica, clara, cómoda y mucho más organizada. Algo que hay que tomar en cuenta es que esta interfaz es ideal para expertos y principiantes, aunque también depende del gusto de cada usuario.

ZenMap.

Zenmap permite la creación de perfiles de ejecución y de esa forma hacer más sencilla la repetición de órdenes. También permite guardar los informes obtenidos de la exploración en una base de datos.

¡Cómo se instala?

Zenmap está disponible en el repositorio de Ubuntu y la podemos instalar directamente desde Synaptic o desde el Centro de Software de Ubuntu (según versiones de Ubuntu). Una vez instalada está disponible en Aplicaciones > Internet o en el Centro de Software de Ubuntu (Ubuntu 12.04) La ejecución conviene hacerla con privilegios de administrador. En cuyo caso lanzamos la aplicación desde una terminal de la forma:

```
$ sudo zenmap
```

Análisis traceroute

Conocido como Traceroute porque este es el nombre que recibe esta función en GNU/Linux, UNIX y Mac. Se trata de un comando que se ejecuta directamente en la consola del sistema operativo, en donde tiene como finalidad el encontrar y solucionar problemas que pueda haber en una red doméstica o empresarial, o por ejemplo con lo que es la conexión con el Internet.

De igual forma, puede servir cuando hay problemas para conectarse con una web.

los derechos reservados.
11 para obtener nuevas
informaciones.

¡Cómo utilizarlo!

Lo único que tienes que hacer para utilizar este comando en su función básica es abrir el Símbolo de sistema o Windows PowerShell en tu ordenador. Una vez en él, escribe el comando tracert <nombre dominio o IP>, poniendo en <nombre dominio o IP> la dirección a la que quieras enviar los datos de prueba, ya sea una web como www.xataka.com o una dirección IP concreta.

Bibliografía

Srl, A. E. (2021, 11 noviembre). Inteligencia activa. AnalyticaEmpresarial.
<https://www.analyticaempresarial.com/post/inteligencia-activa>

De Luz, S. (2023, 3 agosto). Realiza escaneos de puertos con NMAP a cualquier servidor o sistema. RedesZone. <https://www.redeszone.net/seuridad-informatica/listado-de-parametros-de-nmap/>

S.a. (2017, 21 diciembre). Técnicas de exploración - TCP Port Scanning. TCP. https://www.seguridadyfirewall.cl/2017/12/tecnicas-de-exploracion-tcp-port_21.html#:~:text=TCP%20FIN%20Scan%3A%20Es%20una,TCP%2FIP%20de%20sistemas%20Unix.

Laureta, G. (2022, 8 noviembre). How to do stealth scans with NMAP on Linux - Distroid. Distroid. <https://distroid.net/stealth-scans-nmap-linux/>

Vallejo, C. (s. f.). MONOGRÁFICO: ZenMap | Observatorio Tecnológico. <http://recursostic.educacion.es/observatorio/version/v2/eu/software/software-general/1050-zenmap?showall=1>

Fernández, Y. (2020). Tracert o TraceRoute: qué es, cómo funciona o cómo se utiliza. Xataka. <https://www.xataka.com/basics/tracert-traceroute-que-como-funciona-como-se-utiliza#:~:text=Se%20trata%20de%20un%20comando,en%20tu%20conexi%C3%B3n%20con%20Internet>