

El Día a Día del Administrador de Sistemas: Nmap 4

LA DIETA DE FYODOR

Muchas herramientas van creciendo con cada versión nueva, pero Nmap 4.00 ha perdido peso gracias al proyecto Diet-Nmap. La última encarnación de Nmap no es sólo más rápida, sino que también consume menos memoria. **POR CHARLY KÜHNAST**

La herramienta Network Mapper, o Nmap [1], es mi compañera preferida. Recientemente, su inventor Fyodor celebró el octavo cumpleaños de su invención y como regalo ha recibido una dieta de código con muchas funciones nuevas y útiles. Una de las más interesantes es el escaneado de ARP.

El sistema operativo utiliza peticiones ARP para preguntar la dirección MAC de la tarjeta de red. Nmap realiza esta tarea para el sistema operativo y como resultado, el escáner Nmap genera una colección útil de datos fiables del número y tipo de equipos activos en la red.

Esta característica elimina la necesidad de hacer ping o trucos parecidos. (Pinging es una técnica imprecisa, de todas formas, no es necesario que el host responda). No necesita familiarizarse con una nueva sintaxis. Cuando escanea la red local, Nmap escoge automáticamente el escaneado ARP más efectivo, incluso si se especifica `-sP` (Ping Scan) en la línea de comandos. De acuerdo a las páginas de ayuda, esto sólo ocurre si ejecuta Nmap con los privilegios de superusuario. Si quiere indicarle a la herramienta que guarde su comportamiento anterior, necesita especificarle el parámetro `—send-ip`.

SYSADMIN

AppArmor56
AppArmor construye una cárcel virtual para proteger las aplicaciones que se están ejecutando en su ordenador.

Clusters Tomcat60
Vemos cómo ejecutar aplicaciones críticas con alta disponibilidad y balanceo de carga con Apache Tomcat.

Engañar es Placentero

El parámetro `—badsum` también es nuevo. Le indica a Nmap que envíe paquetes TCP o UDP con un checksum incorrecto a la tarjeta del host. La mayoría de los ordenadores que reciben un paquete como éste lo suprimen inmediatamente, pero si Nmap recibe una respuesta, puede suponer que la tarjeta sea un cortafuegos o IDS que no tiene problemas con la inspección de checksums. Ahora la herramienta puede alterar fácilmente su propia dirección MAC utilizando la opción de la línea de comandos `—spoof-mac dirección MAC`.

Nmap soporta diversas versiones de sistemas operativos utilizando el parámetro `O`. Por ejemplo, he escaneado un router en mi laboratorio utilizando el comando `nmap -O 10.0.0.50`. He obtenido la siguiente salida de Nmap 3.70 (reducido a lo esencial):

```
MAC Address: 00:05:5E:96:3D:00
(Cisco Systems)
No exact OS matches for host
```

Nmap 4.0 proporciona un mensaje más detallado:

```
Device type: router
Running: Cisco IOS 12.X
OS details: Cisco 2600
router running IOS 12.2(3),
Cisco router running IOS 12.1
```

Lo mismo se aplica a las versiones. Si quiero encontrar la versión del servicio IMAP que se está ejecutando en un servidor, puedo teclear `nmap -sV 10.0.0.88 -p143` para obtenerla:

```
143/tcp open imap
UW imapd 2004.352
```

Nmap siempre ha sido un medio fantástico de detección de gente no deseada en tu red, y de evitar la pérdida de toneladas de papel mediante el escaneado de impresoras. Las impresoras de red a menudo escuchan en el puerto 9100, y más de unos cuantos modelos convierten cualquier dato para enviarlo a este puerto como copia impresa. Los desarrolladores de Nmap 4.00 han incluido actualmente una característica para ahorrar papel de manera elegante. Cuando introduzco `nmap -sV printer -p 9100`, primero estoy preguntando:

```
9100/tcp open jetdirect?
Excluded from version scan
```

que evita la avalancha de papel. Pero esta técnica para ahorrar papel no significa que Fyodor sea un aguafiestas. Si realmente decide que quiere gastar papel, puede decirle al cerebro de ocho años de Fyodor que escanee `—allports`, extendiendo la avalancha de papel durante siete años en la siguiente generación. ■

RECURSOS

[1] Nmap: <http://www.insecure.org/nmap/>

EL AUTOR

Charly Kühnast es Administrador de Sistemas Unix del centro de datos de Moers, cerca del famoso río Rin. Sus tareas incluyen velar por la seguridad del cortafuegos y ocuparse de la DMZ.

