NMAP COMO UNA HERRAMIENTA PARA LA SEGURIDAD DE REDES

Santos Ireneo Juchasara Colque, M.Sc.
Docente Ingeniería Informática
Universidad Nacional "Siglo XX"
sijucol@hotmail.com, sijucol@gmail.com

RESUMEN

El Internet es uno de los medios en la cual se puede obtener gran cantidad de información, considerado como una autopista de la información, es utilizado por las empresas y personas, sin embargo la seguridad de la redes es unas de las preocupaciones que enfrentan los administradores de red, en cuanto a quienes se conectan a la red como restringirlos. Favorablemente existen herramientas para la exploración de redes y que a través de esta se pueden denegar accesos, nmap es software libre para el escaneo de redes y que se aplicó para detección de intrusos en la red para luego denegar.

Palabras Claves *– Seguridad informática; redes; nmap; wi—fi; vulnerabilidad;*

ABSTRACT

The Internet is one of the means in which a large amount of information can be obtained, considered as an information highway, it is used by companies and people, however network security is one of the concerns that administrators face network, as to who connects to the network how to restrict them. Favorably, there are tools for network exploration and that through this access can be denied, nmap is free software for network scanning that was applied to detect intrusion in the network and then deny it.

Keywords - *Computer security; networks; nmap; Wifi; vulnerability;*

I. INTRODUCCIÓN

El Internet es uno de los avances más significativos de la sociedad ya que gracias a esta podemos encontrar gran cantidad de información hipertextual (textos formateados, imágenes, audio/video, etc.), por otro lado la interacción social, el comercio electrónico, plataformas educativas, entre otros. Es por tal razón que el Internet se puede considerar como una autopista de la información. Debido a que se considera como una autopista, estamos susceptibles a que ocurra el atraco de datos que fluyen en el Internet, y que la mayor preocupación de las instituciones públicas y privadas es que los datos lleguen a su destino de manera segura, confiable, fidedigna, oportuna.

De lo mencionado anteriormente surge la necesidad de incorporar la seguridad informática en todo aspecto y ámbito, en este caso nos referimos a la seguridad de redes, ya que hoy en día muchas personas o grupos se han dedicado a vulnerar la seguridad de transmisión de datos de las empresas, y que el objetivo de todo administrador de redes es minimizar dichas amenazas, utilizando políticas de seguridad tanto físicas como lógicas, ya que la seguridad informática implica la protección de toda infraestructura computacional.

Una de las preocupaciones más discutidas es sobre la seguridad en las redes inalámbricas (Wi-Fi), ya que uno no sabe quienes acceden a nuestra red, muchas veces uno se pregunta quienes acceden a nuestro router quien es el encargado de proveer internet al resto de las terminales, y ahí donde surgen dudas debido a que cada vez que navega un usuario baja el ancho de banda y emerge ciertas cuestionantes como: ¿Por qué baja la velocidad de descarga?, ¿quiénes están conectados a mi red Wi-Fi?, ¿Si están conectados otros equipos que no son conocidos, como puedo restringir a que ingrese a la red?, ¿Cómo puedo filtrar el acceso a mi red?, ¿Que herramientas aplicar para realizar y monitorear la red?, entre otros cuestionantes que atingen a la seguridad.

En el presente artículo vamos a tratar de responder a las cuestionantes realizadas, pero sin embargo haremos más énfasis en una de las herramientas más utilizadas y conocida por los administradores de red y auditores, hablamos de NMAP, una herramienta que nos permite escanear la red y de igual manera proporciona maneras de restringir o denegar el accesos.

II. DESARROLLO

Seguridad Informática:

La seguridad informática es una forma de proteger los recursos computacionales que implica hardware y software y todos los componentes relacionados a esta. La seguridad informática debe establecer normas políticas en la cual minimicen aquellos riesgos a la información o infraestructura informática. En cuanto estas normas podemos mencionar como: aquellos horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los trabajadores y de la organización en general y como principal contribuyente al uso de programas realizados por programadores.

La seguridad informática está orientada en proteger tres aspectos fundamentales que a continuación se describe de manera breve:

- **Infraestructura computacional**: Velar que los equipos funcionen adecuadamente y anticiparse en caso de fallas, robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.
- **Los usuarios**: Debe protegerse el sistema en general para que el uso por parte de ellos no pueda poner en entredicho la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.
- **La información**: Ésta es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

Seguridad en redes:

Sin importar que estén conectadas por cable o de manera inalámbrica, las redes de computadoras cada vez se tornan más esenciales para las actividades diarias. Tanto las personas como las organizaciones dependen de sus computadoras y de las redes para funciones como correo electrónico, contabilidad, organización y administración de archivos.

Las intrusiones de personas no autorizadas pueden causar interrupciones costosas en la red y pérdidas de trabajo, los ataques a una red pueden ser devastadores y pueden causar pérdida de tiempo y de dinero debido a los daños o robos de información o de archivos importantes. (Debish, 2012)

Herramientas para seguridad de redes:

Actualmente existen varias distribuciones orientadas específicamente a auditorías inalámbricas Wi-Fi como Wifislax, Wifiway o Kali Linux, y en algunas ocasiones nos perdemos entre tantas herramientas disponibles. En este artículo nos vamos enfocar a NMAP para realizar la exploración de redes inalámbricas Wi-Fi, de esta manera podremos comprobar si nuestra red inalámbrica es segura. (Benchimol, 2011)

Más allá de las medidas de seguridad que implementemos en nuestras redes WiFi, estas son víctimas potenciales a ser invadidas por conexiones indeseadas que no solo consumirán nuestro ancho de banda, sino que también podrán acceder a nuestros archivos, por eso es mejor estar preparados ante este eventualidad con un script que monitoree nuestra red WiFi.

Nmap:

Nmap (Network Mapper, mapeador de redes) es una sofisticada utilidad para la exploración y auditoría de seguridad de redes TCP/IP. Ha sido diseñado para escanear de forma rápida, sigilosa y eficaz tanto equipos individuales como redes de gran tamaño. Es una herramienta gratuita, de código abierto bajo licencia GPL, bien documentada, multiplataforma, disponible para consola, y que ofrece también una interfaz gráfica para facilitar su uso. (Herrera Joancomartí, García Alfaro, & Perramón Tornil, 2004)

Nmap es una popular herramienta de seguridad utilizada tanto por administradores de red y analistas de seguridad, como por atacantes. Esto es debido a la gran cantidad de información que es capaz de descubrir de una red utilizando una gran variedad de técnicas que la hacen notablemente efectiva y sigilosa. Para ello, Nmap explora equipos remotos mediante secuencias de paquetes TCP/IP tanto convencionales como no convencionales, es decir, paquetes en bruto convenientemente modificados que provocarán o no una respuesta en el objetivo de la cual poder extraer información. Entre esta información se encuentra, por ejemplo: el estado de los puertos y servicios, el sistema operativo, la presencia de cortafuegos, encaminadores u otros elementos de red, así como del direccionamiento IP de la subred. (Chica & Vila, 2012)

III. RESULTADOS

El caso de estudio nace, ya que en un momento menos pensado bajo el ancho de banda de la red Wi-Fi, y de ahí que emerge ciertas dudas sobre si están robando mi ancho de banda otros equipos que no son de conocimiento de nosotros.

Para asegurarnos de no tener intrusos en la red Wi-Fi, vamos poner en práctica lo descrito en el anterior punto, para lo cual contamos con Router 4G LTE el dispositivo que provee Internet a las terminales que se conectan mediante una clave de acceso. Por un lado contamos con una terminal HP Laptop con un sistema operativo Ubuntu 15.04, que vamos a utilizar para la exploración de redes remotas mediante nmap.

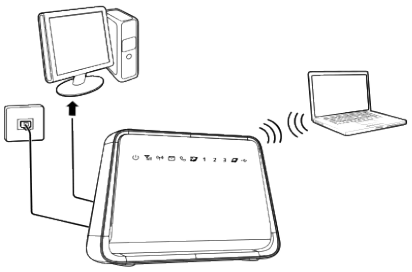

Figura 1: Topología de la red
Fuente: Guía Router Huawei D890

La topología está compuesta por un Router Huawei D890 4G LTE, una Laptop HP y una PC de escritorio.

Instalando nmap e Ubuntu 15.04, la instalación es muy sencilla en el entorno Linux ya que necesitamos aplicar el comando de instalación (apt-get install).

El primer paso es ejecutar el comando desde la línea de comando:

```
santos@HP-15:~$ sudo apt-get update
```

santos@HP-15:~$ sudo apt-get install nmap

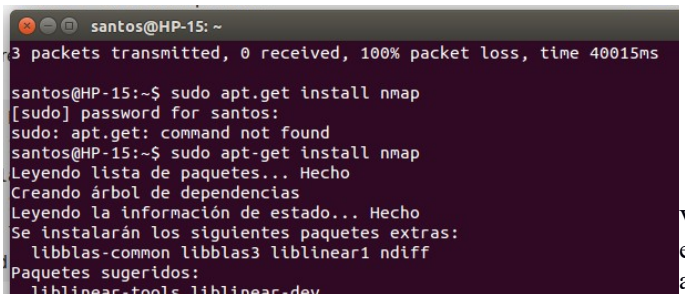

Figura 2: Instalación de nmap en Ubuntu
Fuente: Elaboración propia

Ejecutar nmap:

santos@HP-15:~$ nmap -sP 192.168.1.0/24

Con este comando, le pedimos al nmap que nos muestre sólo (-sP) las IPs de los hosts que estan conectándose a la red.

Donde la direccion 192.168.1.0 es la red del Router 4G LTE, la salidad es el siguiente:

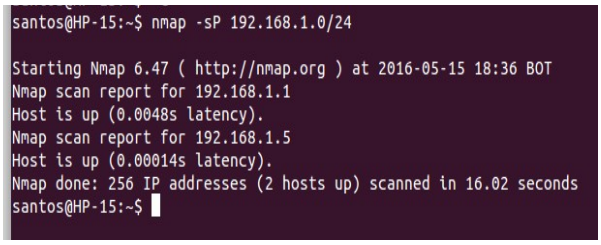

Figura 3: Resultado del comando nmap
Fuente: Elaboración propia

La salida muestra que solo existen dos equipos activos el router y la laptop HP de donde se explora la red con nmap.

Si existen varios host con diferente IP correspondientes, y que sean sospechosos es muy probable que sean intrusos y que están utilizando nuestra red Wi-Fi.

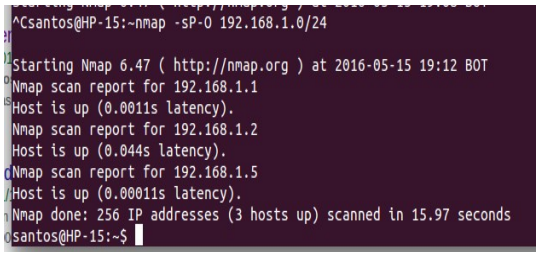

Figura 4: Resultado nmap con un intruso
Fuente: Elaboración propia

Como se puede apreciar la siguiente salida, vemos que se conectó otro equipo en este caso con la IP 192.168.1.2, intruso.

Para nosotros es un intruso ya que estamos conectados solo la Laptop Hp y el router, en este caso para denegar el acceso a la red Wi-Fi debemos descubrir la MAC del equipo conectado, para luego colocar un filtro por MAC, para ello vamos utilizar el siguiente comando para obtener la direccion fisica:

santos@HP-15:~$ arp -n 192.168.1.2

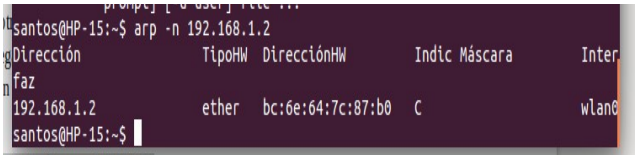

Figura 5: Obtención de dirección MAC
Fuente: Elaboración propia

Vemos que la dirección MAC es bc:6e:64:7c:87:b0, con esta dirección podemos restringir desde el router el acceso a la red.

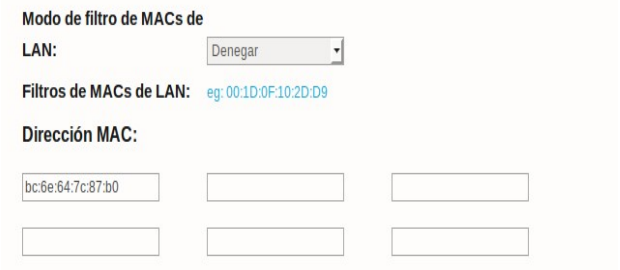

Figura 6: Habilitar filtrado de MAC
Fuente: Elaboración propia

Con esto denegamos el acceso al host 192.168.1.2, recomendable **cambiar la contraseña de nuestra red wifi**, ya que ha sido descifrada y por ello ha dejado de ser segura.

Por otro lado también podríamos cambiar el **filtrado MAC** para que sólo deje conectarse a las MAC conocidas, de esta manera nuestra red aún más segura.

IV. CONCLUSIÓN

La seguridad de las redes es muy importante ya que depende de esta la difusión confiable y oportuna de los datos.

En la actualidad fluye mucha información en el Internet, estas tienden a ser capturados por los famosos llamados hacker.

Sin embargo tanto es el avance científico tecnológico que os proporciona herramientas técnicas para asegurar o proteger nuestra red Wi-Fi ante los intrusos que navegan en el Internet.

La herramienta software libre nmap es un poderoso y sencillo software para exploración de redes conectadas y para el análisis, en los resultados hemos visto que nmap encuentra host conectados a nuestra red, y cualquier host desconocido se puede filtrar su MAC para luego denegar el acceso al Internet, esto lo hemos realizado en el router habilitando la opción Filtros MAC.

Por su puesto a manera de concluir no es a única herramienta existen muchas herramientas que pertenecen a la categoría de software libre, además mencionar que existen distribuciones Linux específicamente para seguridad de redes y auditoria, los cuales son: Wifislax, Kali Linux, etc.

V. REFERENCIAS BIBLIOGRÁFICAS

Benchimol, D. (2011). Hacking desde Cero. Buenos Aires.

Chica, J., & Vila, J. (2012). GUÍA AVANZADA DE NMAP. España.

Debish. (2012). Debian Hackers Elementals.

Herrera Joancomartí, J., García Alfaro, J., & Perramón Tornil, X. (2004). Aspectos avanzados de seguridad en redes. Barcelona.