COMO LOGRAR EL ANONIMATO EN LA RED DE REDES

Toledo Marcelo Alejandro - Licenciado en Sistemas - Profesor Adjunto - Seguridad de la Información.
Puglieso Marcelo Sergio - Licenciado en Gestión Educativa - Profesor Adjunto – Sistemas Inteligentes.
RUIZ DIAZ JAVIER - LICENCIADO EN CIENCIAS DE LA INFORMÁTICA - PROFESOR ADJUNTO -INGENIERÍA DEL SOFTWARE II.
Licenciatura en Sistemas de Información.
Facultad de Ingeniería y Tecnología.
Sede Formosa.
toledomarceloalejandro@gmail.com

Palabras claves: Anonimato en redes, Tor– Proxychains – VPN– DuckDuckGo– Anonsurf

Introducción

La posibilidad de navegar en forma anónima dentro de la red de redes, ha traído beneficios, pero a la par de éstos trajo también la apertura de puertas hacia la Internet profunda también conocida como Deep Web.

En el presente trabajo se detallan diversas maneras de asegurar una navegación anónima en Internet, en aras de mejorar la seguridad a la hora de realizar actividades de hacking ético.

En primer lugar, se describirá que es Tor y como se utilizó, como se configuraron las Proxychains para utilizarlas con el servicio Tor. En segundo lugar, se explicará como se realizó la misma actividad, pero a través de la instalación de un paquete ya configurado para esta tarea, llamada Anonsurf. Por último, se explicará cómo se configuró una VPN gratuita que permitió enmascarar nuestra dirección IP y encriptar nuestro tráfico, con la idea de poder realizar comparaciones. En este sentido, se analizaron las redes de anonimización, TOR, FreeNETe I2P, buscando detectar puntos fuertes y débiles, además de determinar cuáles son sus diferencias.

Desarrollo

Dentro de las redes de anonimización, existen varios software que permitenal usuario una navegación anónima, ya que evitan en muchos casos las restricciones que imponen los gobiernos en países con opresión o accesos a determinados servicios alojados en dicha red. Mediante este tipo de software el usuario puede defenderse del análisis de tráfico, que es una de las formas de vigilancia que atenta contra la libertad y privacidad. Es por ello que muchos usuarios deciden acudir a la Deep Web, conocida, entre otras denominaciones, como la Internet Invisible, y para ello requieren de medios que les garanticen una conexión anónima. Entre esos medios destaca sustancialmente el uso de Tor (Echeverri Montoya, 2016). Tor es el acrónimo de The Onion Router, es decir, el Enrutamiento/Encaminamiento de Cebolla (Panda Security Mediacenter, 2017). Si bien en sus inicios en el Laboratorio de Investigación Naval, se desarrolló como una red mundial de servidores para proteger las comunicaciones

gubernamentales,permitiendo la navegación anónima a través de Internet, en la actualidad,además de los objetivos militares, tiene una gran variedad de usos distintos comoperiodísticos, policíacos, activistas, etc. (David, Mamani, Es, & Su, 2014).

Por otra parte las Proxychains (lit. cadenas de proxys) es un servidor proxy que soporta los protocolos de Internet HTTP(S), SOCKS4 y SOCKS5, funciona sobre distribuciones Linux/GNU, BSD y Mac OS X (plataformas Unix). Permite que cualquier conexión TCP hecha por un programa dado siga una serie de proxies (de los protocolos mencionados) hasta su destino. Donde la lista de proxies se define con anterioridad.Las proxychains funcionan de manera dinámica, moviendo nuestra localización de un proxy a otro por todo el mundo. Con cada servidor proxy nuestra dirección IP cambia.

Al adherir la red Tor, adicionamos una capa de anonimato. La red Tor esconde nuestra identidad moviendo nuestro tráfico a través de diferentes servidores Tor y encriptándolo para que no pueda ser rastreado hasta nosotros. En cambio, para utilizar proxychains, debemos realizar una serie de pasos que incluyen, Editar el archivo "proxychains.conf" y Configurar el proxy tipo SOCKS5 añadiendo la IP 127.0.0.1 y el puerto 9050 al final del archivo.

Para instalar TOR, primero comprobamos si ya estaba instalado el servicio, ingresando ala terminal el comando:service tor status.Luego de verificar que no estaba instalado, lo instalamos a través del comando:apt install tor. Una vez instalado,iniciamos el servicio con el comando:service tor start y comprobamos su ejecución con el comando:service tor status.

Para comprobar la configuración de Proxychains y TOR utilizamos el buscador DuckDuckGo, éste no guarda un registro de las IP cuando se realizan búsquedas, lo que añade una capa más de anonimato.A su vez, podemos visualizar en la terminal los encadenamientos de proxys.En el cuadro de búsqueda de DuckDuckGo ingresamos:check dns leaks; el primer resultado de la búsqueda,es un sitio web que realiza una comprobación para saber si las peticiones DNS de nuestra conexión están siendo filtradas, el cual representa una amenaza crítica para la seguridad.

Además, se pudo comprobar que nuestra IP actual pertenecía a Irlanda (esto siempre cambia), cuando debería haber sido una IP de Argentina. Volvimos a repetir los mismos pasos, para verificar que efectivamente nos asigna otra dirección IP.

Otra herramienta que utilizamos fue Anonsurf, que es un script creado por el equipo de ParrotSec (los desarrolladores de Parrot Linux) que anonimiza completamente y de manera sencilla utilizando proxys TOR. Ésta automáticamente dirige el tráfico a través de TOR, incluyendo las solicitudes de DNS para impedir filtraciones.Para utilizar Anonsurf se tuvo que instalar, descargando el código fuente desde Github con el comando:git clone https://github.com/Und3rf10w/kali-anonsurf. Como Anonsurf es un servicio, lo tuvimos que iniciar con el comando:anonsurf start. Y se pudo comprobar la IP, anónima, que nos asignó con el comando:anonsurf myip

Con estas significaciones Blazquez analiza a la música de cuarteto en la ciudad de Córdoba. Una música que se representa y simboliza a si misma como extremadamente masculina, donde la mujer cumple una función de complemento y tal vez de adorno en sus letras, melodías y baile.

Conclusiones

De acuerdo a lo analizado precedentemente: se pudo constatar queuno de los mejores métodos para permanecer anónimos, es el uso de TOR, aunque no asegura un 100% de anonimato. El servicio de TOR se puede reiniciar las veces que se quiera para obtener nuevas direcciones IP evitando que nos detecten. También hay que considerar que buscadores como DuckDuckGo no llevan un registro de cada búsqueda que hacemos, el cual nos favorece por no dejar nuestros rastros.

Como desventaja se pudo comprobar que nuestra conexión se hace más lenta debido a todos los saltos que se deben dar para llegar de un destino a otro.

Bibliografía

- Beaver, K. (2018). Hacking for Dummies (Sexta ed.). Hoboken, Nueva Jersey, Estados Unidos de América: John Wiley & Sons, Inc. Recuperado el 20 de Marzo de 2019.
- Bradley, P. (2019). Hacking with Kali Linux: A Comprehensive, Step-By-Step Beginner's Guide to Learn Ethical Hacking With Practical Examples to Computer Hacking, Wireless Network, Cybersecurity and Penetration Testing.Estados Unidos de América: Publicación Independiente. Recuperado el 20 de Marzo de 2019.
- Echeverri Montoya, D. (2016). Deep Web: TOR, Freenet & I2P. Privacidad y Anonimato. (Zeroxword). Madrid.
- Mamani, David, F. (2014). ¿ Qué es TOR , Revista de Información, Tecnología Y Sociedad, 9, 1–3.
- Roa Buendía, J. F. (2013). Seguridad Informática. Madrid: McGraw-Hill Interamericana de España S.R.L. Recuperado el 20 de Marzo de 2019.