Imagen que contiene Texto

Descripción generada automáticamenteCOMENTARIOS LECTURA #6

Fundamentos Avanzados Ciber Seguridad

Daniel Alejandro Olarte Ávila

Universidad Sergio Arboleda

Universidad Sergio Arboleda Cl. 74 #14-14

Bogotá, Colombia

Correo: [daniel.olarte01@correo.usa.edu.co](mailto:daniel.olarte01@correo.usa.edu.co)

Escuela de Ciencias Exactas e Ingeniería

Profesor: Juan Carlos Galindo Piraquive

21/03/2022

**“Aprende todo sobre el ataque ARP Poisoning y Protégete”**

La lectura “Aprende todo sobre el ataque ARP Posoning y Protegete” me pareció muy interesante, este tema que ya llevamos viendo desde el principio del semestre me llama mucho la atención y cualquier cosa relacionada a esta me hace leer más artículos como este y seguir investigando por mi parte, lo que me parece interesante de esta lectura es el cómo resalta un montón de aspectos nuevos que normalmente la gente no conoce sobre esto, dándonos a entender lo vulnerables que somos y en la cantidad de riesgos que podemos estar sin darnos cuenta.

El artículo es interesante debido a que nos habla del ataque ARP Poisoning o también conocido como ARP Spoofing el cual son nuevos términos que no hemos visto los cuales se relacionan con unos si vistos anteriormente y mencionados en clase, como Man in the Middle, protocolos HTTPS y Kali Linux. Esto siendo super interesante de leer ya que de esa forma uno comprende de forma mas sencilla y uno aprende más fácil.

Me parece muy interesante como comienza esta lectura, ya que nos empieza hablando como estos ataques ARP Poisoning son de los mas conocidos y mas peligrosos del mundo, mencionando de como un buen Cracker podrá obtener cualquier tipo de información que se pueda interceptar entre la víctima y la conexión a Internet. Lo que me sorprende es que si el atacante es bueno puede convertir la seguridad de la victima de HTTPS a HTTP, dejando mucho mas en riesgo a la victima para los ataques que se puedan hacer.

La lectura resalta que sobre que es el protocolo ARP el cual permite la comunicación entre los dispositivos de la misma red, este mismo protocolo crea la tabla ARP donde muestra las Ips y Macs de los dispositivos conectados a la Red que estamos conectados, también nos informa de como se encarga además de la comunicación entre los dispositivos y el router, esto debido a que el router tiene también una ip que pertenece en la red lo que hará que este en la tabla ARP permitiendo la comunicación entre todos estos. Además los informa de como en el CMD de nuestro dispositivo podemos hacer revisión de esta tabla ARP con el comando arp -a.

Texto

Descripción generada automáticamente

Algo fundamental que nos cuenta el artículo, es sobre esta tabla ARP donde podemos ver la ip del router siendo esta normalmente como la primera dirección IP de la subred (en mi ejemplo 192.168.0.1), en donde ahí es donde se especifican los ataques ARP Poisoning, y mas si se tiene en cuenta como el protocolo ARP no tiene por ningún lado seguridad por lo cual cualquiera se podria hacer pasar por otro host de forma fácil y rápida sin que uno se de cuenta de esto, perfecto para realizar el envenenamiento a la tabla para poder llegar a cumplir su objetivo sea cual sea (DoS o Man in the Middle).

La razón que el ataque sea Dos o Man in the Middle depende de la victima, a la hora de envenenar la tabla y hacer que el ip visto anteriormente que es el router, sea reemplazado por el Malware, esto hace que la victima pueda reenviar las conexiones al router para salir a internet o así mismo no, en el caso que no se vería un ataque DoS negándole la conexión a Internet, pero en el caso que si se vera un ataque MitM, permitiendo obtener toda la información y espiar todas las comunicaciones. Hasta el punto de poder llegarse a hacerse pasar por el sin necesidad de robar Usuarios y Contraseñas.

Para que se pueda realizar este ataque el atacante debe estar en la misma red de la víctima, y el ataque se debe realizar lanzando 2 ataques ARP Poisoning, uno a la victima haciéndonos pasar como el router, y otro al router haciéndonos pasar por la víctima, esto haciendo que ya no se puedan comunicar entre estos si no que directamente con el atacante.

Diagrama

Descripción generada automáticamente

*“Explicación ataques ARP Poisoning” https://www.redeszone.net/app/uploads-redeszone.net/2016/01/mitm\_red.png*

**Referencias:**

* <https://www.redeszone.net/tutoriales/seguridad/que-es-ataque-arp-poisoning/>
* <https://www.ionos.es/digitalguide/servidores/know-how/arp-resolucion-de-direcciones-en-la-red/>
* <https://es.wikipedia.org/wiki/Protocolo_de_resoluci%C3%B3n_de_direcciones>