“Proxy, Awareness”

Informe N°9

Laboratorio de Seguridad en Redes

Melanny Dávila
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
melanny.davila@epn.edu.ec

Alejandra Silva
Ingeniería en Telecomunicaciones
Facultad de Eléctrica y Eléctronica
Quito, Ecuador
alejandra.silva@epn.edu.ec

***Abstract*—En el siguiente documento se presentará una implementación de Proxy realizado en un entorno controlado con el de poder intermediar tráfico y también poder implementar técnicas de awareness y gestión de contraseñas.**

***Index Terms*—Proxy, squid, gestor de contraseñas, Linux, servidor.**

I. Introducción

Un servidor proxy proporciona una puerta de enlace entre los usuarios e Internet. Es un servidor, denominado “intermediario” porque va entre los usuarios finales y las páginas web que visitan en línea. Los proxies proporcionan una valiosa capa de seguridad para un usuario. Se pueden configurar como filtros web o firewalls, protegiendo al usuario de amenazas de Internet como malware. Sin embargo, así como pueden ser usados para brindar una capa de mayor seguridad, también se puen usar para robar información como por ataques del hombre en el medio por ejemplo, por lo que es una herramienta que debe ser manejada con cuidado y se debe ejercer bastante control sobre la misma.

II. Objetivos

- Instalar, configurar y poner en marcha un servidor básico de proxy para intermediar tráfico web.
- Implementar reglas de control de acceso que permitan y bloqueen el tráfico a nivel de aplicación (web) en función de múltiples parámetros.
- Revisar técnicas de awareness y gestión de contraseñas.

III. Cuestionario

A. Presente la configuración realizada en el laboratorio.

Inicialmente, se realizó una prueba de conocimiento de Phishing que contiene 8 casos de prueba, la misma que puede ser encontrada en el siguiente link: https://phishingquiz.withgoogle.com/

Los casos que se encontraron en dicha prueba fueron los siguientes:

- Correo electrónico: Es importante asegurarse de verificar las URL de los enlaces colocando el mouse o presionando prolongadamente, y explorar las direcciones de correo electrónico. Muchas URLs parecen correctas pero en realidad son similares. Asimismo, es importante tener precauciones con los hipervínculos y archivos adjuntos en correos electrónicos, ya que pueden dirigir a sitios web fraudulentos donde se le solicita que ingrese información confidencial.
- Fax: De manera similar, es importante fijarse en el dominio de correo electrónico del remitente.
- Fotos: De igual manera, parece que se utilizan URL similares, por lo que se debe ser especialmente cauteloso si no se está seguro de conocer al remitente. Muchas veces los archivos adjuntos redirigen a páginas web no conocidad.
- Correo de Dropbox: En este caso, el remitente es ”dropboxmail.com”, que es inusual pero legítimo, y la URL es un enlace seguro (https) a ”dropbox.com”.
- Informe o reporte de una escuela: Los archivos PDF adjuntos en el correo electrónico pueden contener malware o virus. Por lo que se debe utilizar un navegador o un servicio en línea como Google Drive para abrirlos de forma segura.
- Intentos de acceso a una cuenta: Presenta suplantación de identidad debido a que se utilizó una URL similar para hacerse pasar por Gmail, por lo que nuevamente se debe verificar la URL.
- Cuenta bajo ataque nuevamente: Los atacantes intentaron usar Google para ocultar el enlace real, es así como se utilizó un correo electrónico similar a este para apuntar a otros dominios.
- Solicitudes de acceso: Es importante tener cuidado con este tipo de solicitudes de acceso a la cuenta y asegurarse de que confía en el desarrollador.

Donde los resultados obtenidos fueron los siguientes después de dar el test.

Fig. 1. Test de Phishing

Posterior a eso se comenzó a utilizar Dashlane para esto se instaló una extensión del mismo en el navegador, donde se realizó la configuración inicial, para esto se creó y agregó una contraseña.

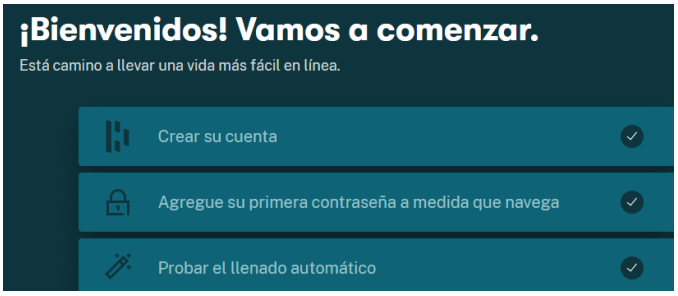

Fig. 2. Configuración inicial

A continuación, se presentó el análisis de las contraseñas.

Fig. 3. Análisis de contraseñas

Para iniciar la realización de la práctica, se procede a instalar *squid* dentro del servidor, que permitirá la implementación del proxy.

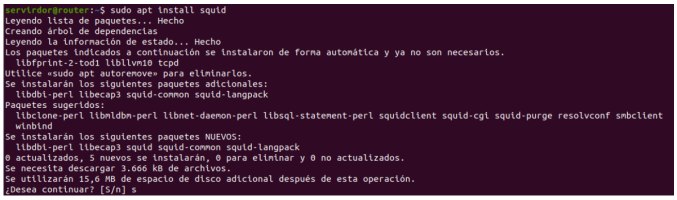

Fig. 4. Instalación de squid

Luego, para verificar el funcionamiento de squid, se ejecuta el comando para visualizar su estado como se muestra en la figura 5.

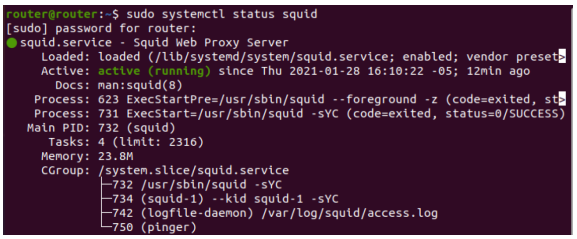

Fig. 5. Visualización del funcionamiento de squid

Posteriormente, dentro del servidor se permite que la dirección 10.10.10.1 haga peticiones por el puerto 3128 que corresponde al puerto donde funciona el proxy, es decir, squid como se ve en la figura 6. Previo a esto se debe realizar una copia de seguridad como se indica en la primera línea de la figura 7.

Fig. 6. Permiso para realizar peticiones concedido

A continuación, se guardan los cambios y se reinicia el servidor squid como se muestra en la figura 7.

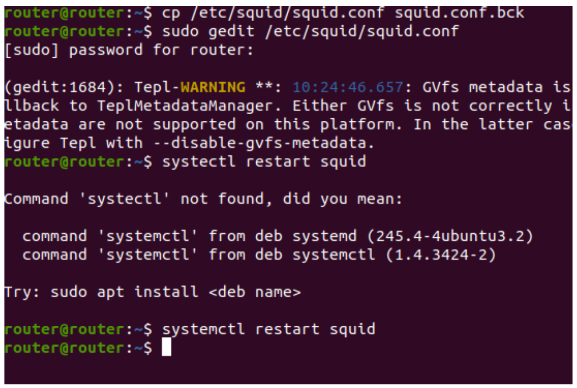

Fig. 7. Realización de la copia de seguridad del documento de configuración de squid y posterior reinicio del servicio

Como un paso adicional se hace telnet a la dirección IP con el puerto correspondiente al proxy, en este caso fue exitosa y se muestra en la figura 8.

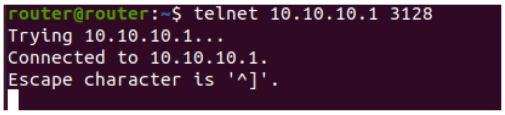

Fig. 8. Conexión con telnet exitosa

Luego, para realizar la primera actividad de la práctica, se debe crea un archivo llamado *permitidos.txt* en el cual se encuentran las direcciones IP que pueden hacer peticiones al proxy. Las direcciones IP permitidas son colocadas de la manera en que se muestra en la figura 10.

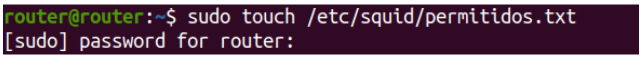

Fig. 9. Creación del archivo *permitidos.txt*

Fig. 10. Direcciones IP permitidas para realizar peticiones

Como siguiente paso, para concretar la primera actividad, se debe añadir una regla nueva al archivo de configuración de squid como se muestra en la figura 11, donde se especifica que se de acceso a las direcciones que se encuentran dentro del archivo permitidos.txt.

Fig. 11. Establecimiento de la lista de acceso dentro del archivo de configuración de squid

Para aplicar los cambios realizados se reinicia el servicio de squid como se muestra en la figura 12

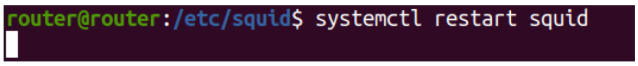

Fig. 12. Reinicio de squid

Para realizar las pruebas, dentro del cliente se debe configurar el navegador de manera que haga uso del proxy establecido. En el caso de firefox, esto se realiza dentro de las configuraciones donde se coloca la dirección IP del servidor proxy. Esta configuración se muestra en la figura 13.

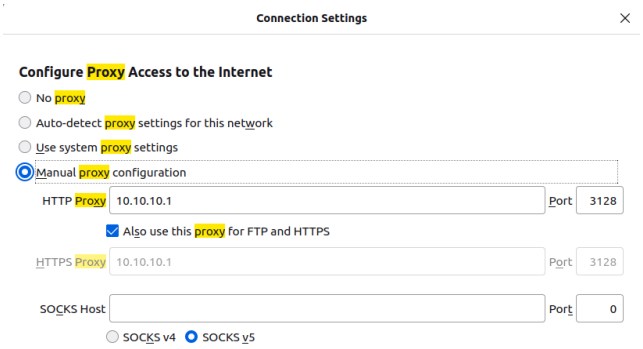

Fig. 13. Configuración dentro del cliente para utilizar el proxy

Como siguiente paso y para continuar con la práctica se crea un nuevo archivo de nombre *noAccess.txt* que contendrá los dominios de servidores a los que no se desea dar permisos. En este caso se colocaron los dominios de Facebook y de Youtube como se muestra en la figura 14.

Fig. 14. Dominios sin permiso de acceso

A continuación se muestran las pruebas de funcionamiento de las reglas recientemente aplicadas.

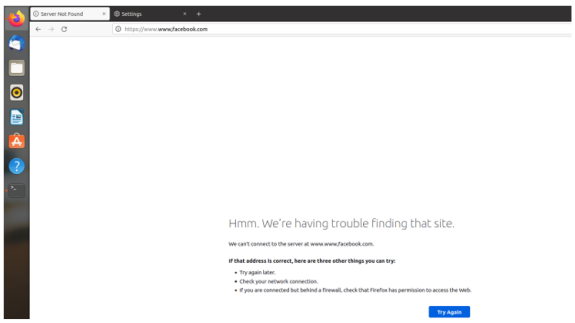

Fig. 15. Prueba de funcionamiento de las reglas establecidas

Fig. 16. Prueba de funcionamiento de las reglas establecidas

Nuevamente, para agregar la nueva regla que rechace a las direcciones establecidas previamente se agrega la línea *acl noAccess url_regex* junto con el path donde se encuentran los

dominios rechazados y se añade a la lista de acceso con el identificador de signos de exclamación en la última línea de la figura 17.

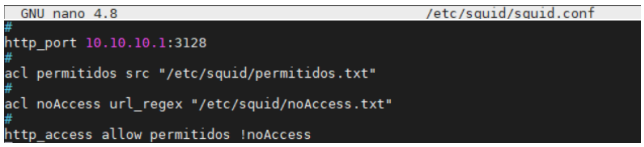

Fig. 17. Reglas de lista de acceso actualizadas

Con el fin de pedir un usuario y una contraseña al usuario, se generan estas credenciales con el comando *printf "USER:$(openssl passwd -crypt USER:PASSWORD)"* donde se cambian los campos correspondientes, como se muestra en la figura 18

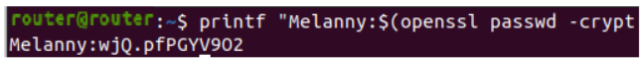

Fig. 18. Generación de un usuario y una contraseña

Luego de esto, se debe añadir la cadena generada con el comando dentro de un archivo de nombre *htpasswd* como se muestra en la figura 19.

Fig. 19. Adición del usuario y la contraseña que se desean pedir al usuario

Finalmente, para que se apliquen estos cambios se añaden las nuevas reglas al archivo de configuración de squid.conf como se muestra en la figura 20

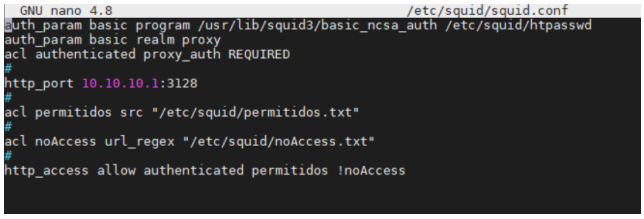

Fig. 20. Nuevas reglas añadidas a la lista de acceso del proxy

A continuación, en la figura 15, se muestra la petición de usuario y contraseña dentro del navegador Firefox.

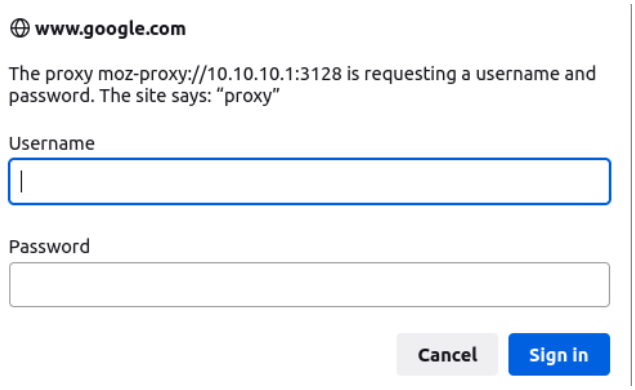

Fig. 21. Prueba de funcionamiento de las reglas establecidas

Luego, se monitorea el funcionamiento de squid consultando el archivo */var/log/squid/cache.log*, cuyos resultados se muestran en la figura 22

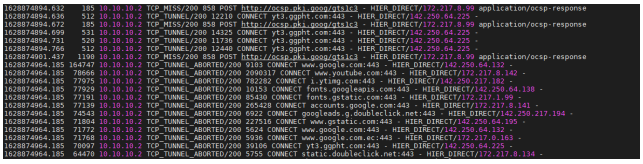

Fig. 22. Registro del funcionamiento de squid

También, los registros de navegación de los usuarios pueden ser monitoreados consultando el archivo */var/log/squid/access.log* cuyas ultimas líneas son mostradas en la figura 23

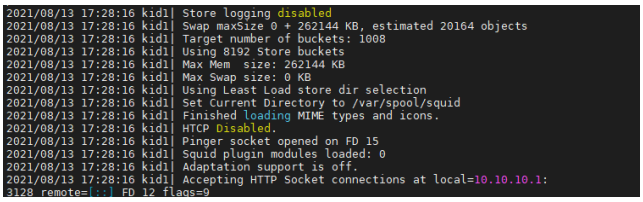

Fig. 23. Registro de la navegación de los clientes en el servidor squid

B. Explique los resultados obtenidos durante la práctica.

Los resultados obtenidos para la parte del establecimiento de un servidor proxy varían de acuerdo a la aplicación de las reglas de control de acceso establecidas. Estas reglas fueron capaces de limitar el acceso a internet por parte del cliente, desde no permitirle acceder a las páginas establecidas en el archivo de páginas prohibidas, hasta pedir un usuario y una contraseña para acceder de manera general a internet. Asimismo el servidor fue capaz de monitorear la actividad del usuario permitiendo ver al administrador de la red hasta que direcciones fueron rechazadas. Por lo que se concluye que el alcance de un proxy es bastante amplio y puede ser usado para evitar que los empleados de una empresa, por ejemplo, se distraigan o ingresen a sitios peligrosos.
Durante el análisis de lasposibles amenazas de phising se pudo percibir que existen varios tipos y algunos son mas detectables

que otros, en algunos casos fue difícil detectarlos ya que la forma de escribir los correos y las paginas web daba la impresión de ser bastante legitima. Asimismo, para el análisis de contraseñas se tuvo que considerar no tener contraseñas reutilizadas o débiles (como sería el caso de contraseñas quen no poseen una gran variedad de caracteres).

C. Indique al menos dos soluciones de Awareness para phishing attacks e indique los principales beneficios o servicios de estas.

Una de las soluciones seria introducir datos personales o confidenciales únicamente en WEB seguras, las webs seguras han de empezar por 'https://' y debe aparecer en tu navegador el icono de un pequeño candado cerrado. [6]

La segunda solución podría ser aprender a identificar claramente los correos electrónicos sospechosos de ser Phising. Verifique los indicadores de seguridad del sitio web en el cual ingresará información personal. Si resulta indispensable realizar un trámite o proveer información personal a una organización a través del sitio de Internet, escriba entonces la dirección web usted mismo en el navegador y busque los indicadores de seguridad del sitio. Al hacerlo, deberá notar que la dirección web comienza con https://, donde la s indica que la transmisión de información es segura. Verifique también que en la parte inferior de su navegador aparezca un candado cerrado. Al hacer clic sobre este último, podrá comprobar la validez del certificado digital y obtener información sobre la identidad del sitio al que está accediendo. [7]

Hay aspectos que se deben tomar en cuenta para identificar ataques a través de correo electrónico que son: [6]

- Utilizan nombres y adoptan la imagen de empresas reales.
- Llevan como remitente el nombre de la empresa o el de un empleado real de la empresa.
- Incluyen webs que visualmente son iguales a las de empresas reales.
- Como gancho utilizan regalos o la perdida de la propia cuenta existente.

Otra solución que debe ser muy importante es reforzar la seguridad del ordenador con un buen antivirus que bloquee este tipo de ataques. Además, siempre debes tener actualizado tu sistema operativo y navegadores web.

D. Conclusiones

- Un servidor proxy puede ser fácilmente implementado dentro de un sistema operativo Linux con la ayuda de squid ya que, para añadir reglas nuevas, no se requiere más que escribir dentro del archivo de configuración de la aplicación.
- Un proxy puede ser usado tanto para regular la actividad de los empleados dentro de una organización, como para denegar el ingreso a sitios peligrosos que pueden abrir una vulnerabilidad en la red de la empresa.
- La estructura de proxy transparente se produce a través de la redirección de tráfico en el puerto 80 para el servicio interno del proxy, y hay muchos otros puertos que pueden utilizar el protocolo HTTP.

E. Recomendaciones

- Un servidor proxy debe ser configurado de manera que regule el tráfico de acuerdo a lo deseado, pero se debe tener cuidado de no limitar demasiado el uso del internet.
- El uso de un proxy transparente es más recomendado para organizaciones ya que a los clientes les cuesta más darse cuenta que su conexión esta siendo regulada por un servidor proxy.
- Las herramientas de gestión de contraseñas son recomendadas en caso de que se maneje un número considerable de contraseñas o se tenga dificultad en recordarlas, debido a que almacenan la información de inicio de sesión para todos los sitios web que se utilizan y mejoran el inicio de sesión en ellos.

REFERENCES

[1] "Proxy transparente, conozca sus beneficios y limitaciones" (2016). recueprado de:https://ostec.blog/es/seguridad-perimetral/proxy-transparente-beneficios-limitaciones/. accedido (11,Agos,2021).

[2] Prieto. R. "Cómo configurar proxy SQUID en modo transparente". Recuperado de: https://www.raulprietofernandez.net/blog/gnu-linux/como-configurar-proxy-squid-en-modo-transparente. Accedido (11,Agos,2021).

[3] Miguel. A.E. (2014). "Proyecto: Creación de un Proxy Transparente en Linux". Recuperado de: https://nanopdf.com/download/adobe-acrobat-5ae56c4aa4afd_pdf. Accedido (11, Agos, 2021).

[4] "Bitwarden Open Source Password Manager | Bitwarden". https://bitwarden.com/ (accedido ago. 12, 2021).

[5] "Securely Store, Manage & Autofill Passwords". https://nordpass.com/homepage/ (accedido ago. 12, 2021).

[6] "10 consejos para evitar ataques de Phishing " https://www.pandasecurity.com/es/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/. (accedido ago. 20, 2021).

[7] "Recomendaciones para evitar ser víctima del phishing". https://www.econo.unlp.edu.ar/detise/phishing-3923. (accedido ago. 20, 2021).