Fuga de Información a través del Sistema de Nombres de Dominio (DNS)

Dennis Edson Vargas Peña
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
dennis.edson@gmail.com

***Resumen*—La fuga de información se produce, cuando la información que es considerada como confidencial pierde esta característica, dándose a conocer a terceras partes no autorizadas. El objetivo del presente artículo es demostrar cómo puede realizarse la fuga de información, dentro de redes corporativas LAN (Red de Área Local), mediante técnicas que emplean el Sistema de Nombres de Dominio – (DNS, del inglés Domain Name System), como un canal de comunicación encubierto para la transferencia de información a través de este protocolo.**

Palabras clave—canal encubierto, fuga de información, dns.

I. INTRODUCCIÓN

La información es un conjunto de datos procesados y organizados, siendo este en la actualidad el activo más importante en cualquier organización, institución o empresa; la información, por ejemplo: datos de clientes, estados financieros, propiedad intelectual, entre otros; cuya información es crítica según el tipo de empresa y la clasificación de información que posea. La información de las empresas, puede llegar a ser de gran importancia para el negocio, por lo que el riesgo de que ésta pueda filtrarse a terceras partes no autorizadas, como la competencia u otros interesados, puede dar lugar a que la información filtrada sea utilizada con fines comerciales para su venta, divulgación o emplearla contra a la empresa e incluso contra sus clientes. Siendo el impacto por fuga de información perjudicial, llegando a ocasionar desde daños a la imagen, reputación, pérdidas económicas, sanciones, multas, consecuencias legales, pérdida de clientes e incluso en casos más serios el cierre de la empresa. Sólo en la gestión 2019 como ejemplos de referencia se tuvieron los siguientes incidentes de fuga de información:

TABLA I. EJEMPLOS DE CASOS DE FUGA DE INFORMACIÓN EN 2019

2019	HECHO
MAR	Robo de información de millones de clientes de Toyota [1].
ABR	Expuestos 540 millones de registros de usuarios de Facebook [2].
JUL	Se filtra información privada de millones de ciudadanos del ministerio de hacienda de Bulgaria [3].
JUL	Expuestos 7.5TB datos de la agencia de inteligencia rusa [4].
AGO	Registro del 80% de votantes Chile, expuesto en Internet [5].
AGO	Fuga de información Cloud Web Application Firewall de Imperva [6].
SEP	Filtración masiva de datos de ciudadanos en Ecuador [7].

La fuga de información puede llegar a darse por organizaciones criminales, ciberdelincuentes externos que, tras vulnerar algún punto de la infraestructura tecnológica de su objetivo, buscan información sensible para poder filtrarla (extraerla); incluso la fuga de información también puede darse por personal interno de las empresas quien de forma deliberaba puede extraer información sensible aprovechando su privilegio de acceso a este tipo de información.

De acuerdo al estudio realizado por INCIBE (2017), las formas más comunes por las que se da la fuga de información son las siguientes [8]:

- Mediante portátiles, móviles y otros dispositivos externos como discos duros, CD/DVD o USB que se extravían o se usan para «sacar» información.
- A través del correo electrónico corporativo y cuentas de correo gratuitas se envía información como consecuencia de un engaño o de forma «voluntaria».
- Cuando se utilizan redes inalámbricas desprotegidas, como la de los aeropuertos o los hoteles, por trabajadores de viaje sin tener en cuenta que transmiten y quién puede estar escuchando.
- Utilizando aplicaciones no controladas por la empresa, por ejemplo, para almacenamiento en la nube (Dropbox, Google Drive, Mega) o herramientas de colaboración, mensajería instantánea o multiconferencia (Skype, Hangouts, Line) y otras para compartir archivos en P2P (eMule, uTorrent).
- Publicando en redes sociales información de forma inadecuada o algo que no debería publicarse, y cuando se responde a usuarios sin control.
- Si resultamos infectados por malware que roba datos (troyanos, spyware, keyloggers, stealers y ransomware) nuestra información «abandonará» nuestras instalaciones o dejará de estar disponible muchas veces sin que nos demos cuenta.

Es así que a razón de los diferentes vectores de fuga de información, existen en el mercado soluciones que ofrecen protección ante este tipo de fuga, como las soluciones para dispositivos móviles MDM (*Mobile Device Management*), soluciones DLP (*Data Loss Prevention*), soluciones Antispam avanzado con DLP, Firewalls para el control del tráfico de red, soluciones Proxy para el control del tráfico de Internet, Antivirus y Antimalware para mitigar infecciones por malware, entre otras

Para referenciar este artículo (IEEE):
[N] D. Vargas, «Fuga de Información a través del Sistema de Nombres de Dominio (DNS)», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 18-22, 2020.

soluciones que sirvan de control. Sin embargo, si bien estas soluciones disponibles en el mercado actual cubren una gran parte de los vectores para la fuga de información, aún quedan puntos débiles por cubrir, como el uso del protocolo del Sistema de Nombres de Dominio–DNS, empleándolo como un canal encubierto para la filtración de información.

DNS es un sistema ampliamente utilizado en la resolución de nombres de dominio a direcciones IP, facilitando la comunicación entre los sistemas y entre los usuarios con los sistemas; los nombres de dominio en general constan de las siguientes partes:

Fig. 1. Partes de un nombre de dominio.
Fuente: elaboración propia.

En la figura.1 se puede apreciar el dominio de primer nivel conocido como TLD (*Top Level Domain*), de acuerdo a la ICANN (*Internet Corporation for Assigned Names and Numbers*), se tienen los siguientes tipos de TLD [9]:

- gTLD (*Generic Top Level Domain*). - Son los dominios de primer nivel genéricos, cuya gestión está a cargo de la ICANN, por ejemplo: ".com", ".net", ".org".
- ccTLD (*Country Code Top Level Domain*). - Son los dominios de primer nivel de código de país, lo que quiere decir que cada país tiene asignado un dominio de primer nivel, y cada país es responsable de su gestión, dominios de este tipo por ejemplo son: Bolivia ".bo", Argentina ".ar", Perú ".pe".

Es relevante conocer estos tipos de dominios gTLD y ccTLD, porque al tener gestiones distintas, cada una tiene sus propias políticas para otorgar nombres de dominio, siendo incluso algunos nombres de dominio otorgados de manera gratuita como por ejemplo dominios: ".tk", ".ml", ".ga". Para la resolución de nombres de dominio se la realiza de la siguiente manera, como se muestra a continuación:

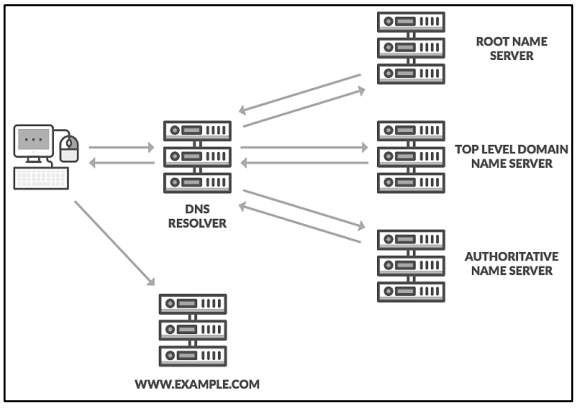

Fig. 2. Resolución de nombres de dominio.
Fuente: https://www.appneta.com/dns/

De la figura.2 la comunicación que se realiza entre la PC y el Servidor DNS, utiliza el protocolo UDP (*User Datagram Protocol*) en el puerto 53, el cual se encuentra definido en las especificaciones RFC-1035 de la IETF (*Internet Engineering Task Force*) [10]. Considerando este esquema de comunicación, las solicitudes de resolución de nombres de dominio de los clientes (PCs), son enviadas al Servidor DNS corporativo, sin embargo, el cliente puede configurar otros servidores DNS, ajenos a los DNS corporativos dentro su infraestructura tecnológica, para realizar la resolución de nombres de dominio, como por ejemplo empleando servicios DNS gratuitos de Google, CloudFlare, OpenDNS, entre otros.

Es en este contexto, es donde surge la siguiente pregunta de investigación ¿Es posible la fuga de información a través del protocolo DNS?, por lo que el objetivo de la investigación es demostrar la fuga de información, utilizando el protocolo DNS.

Investigaciones como la de Zimba y Chishimba (2017), titulado *"Exploitation of DNS Tunneling for Optimization of Data Exfiltration in Malware-free APT Intrusions"*, indican que "El hecho de que muchos Firewall e IDS no inspeccionan el tráfico DNS, motiva a los atacantes a explotar el DNS como un túnel de red para conducir el tráfico con una muy pequeña detección de cualquiera de estos" [11] [15]. Siendo factible el uso del DNS tunneling como una técnica de exfiltración de datos, ya que cualquier comunicación de los computadores locales a internet depende del servicio de DNS, como se describe en el trabajo de investigación de Nadler, Aminov, Shabtai (2018) titulado *"Detection of Malicious and Low Throughput Data Exfiltration Over the DNS Protocol"*. Por esa razón, restringir la comunicación DNS puede resultar en la desconexión de servicios remotos legítimos [12].

El objetivo del presente artículo es demostrar cómo puede realizarse la fuga de información, dentro de redes corporativas LAN (Red de Área Local), mediante técnicas que emplean el Sistema de Nombres de Dominio – (DNS, del inglés *Domain Name System*), como un canal de comunicación encubierto para la transferencia de información a través de este protocolo.

II. MATERIAL

Para demostrar que es posible realizar la fuga de información a través del protocolo DNS se preparó un entorno de laboratorio, el cual consta de un equipo que simulará la PC de un usuario, y otro equipo que servirá como Servidor DNS Autoritativo para el dominio dennisedson.tk, en el siguiente diagrama se puede apreciar una representación de este entorno de laboratorio:

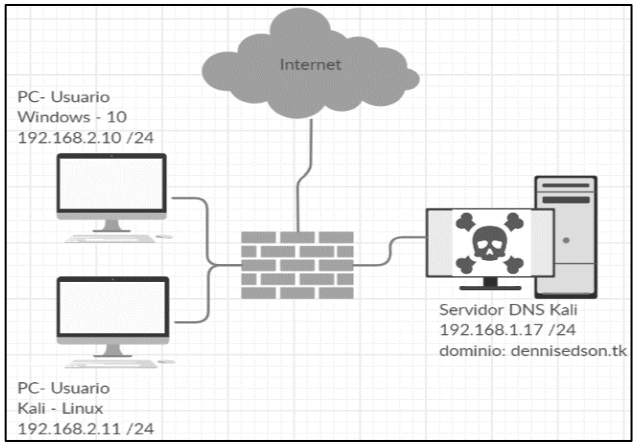

Fig. 3. Diagrama de red – Entorno de laboratorio.
Fuente: Elaboración propia.

Para llevar a cabo la demostración, se tiene en cuenta la siguiente consideración, los equipos PC de usuario tanto Linux, como Windows-10, no cuentan con salida directa a internet, siendo este tráfico es bloqueado, sin embargo, ambos equipos si

pueden realizar consultas DNS a servidores externos (maliciosos) fuera del DNS oficial configurado para la red, como se ve en la Fig.3 el servidor 192.168.1.17 ha sido configurado como un servidor DNS malicioso. El objetivo de la demostración es sacar información confidencial de las PCs de usuario, por lo que, para este laboratorio, se definieron los siguientes archivos como información confidencial en cada PC de usuario:

- PC Windows 10 (usuario)

  Archivo confidencial.xlsx, el cual puede contener desde contraseñas, cuentas de clientes, entre otros datos.

- PC Kali Linux (usuario)

  Archivo /etc/passwd, este archivo contiene información de los usuarios locales del equipo, el cual es necesario cuando para el crackeo de contraseñas de usuarios Linux.

Aprovechando herramientas que están pre instaladas en las PC de usuario, no hubo la necesidad de instalar ningún tipo de software adicional en estos equipos, las herramientas preinstaladas que se utilizaron fueron:

- PC Windows 10 (usuario)

  Powershell v5.0 que está disponible por defecto en el sistema operativo.

- PC Kali Linux (usuario)

  Python 3.7, disponible por defecto en la versión del sistema operativo Kali 2019.

A diferencia de las PC de usuario, en el servidor si requiere la instalación de diferente herramientas y librerías, que permitieron transferir información a través desde las PC de usuario al Servidor DNS malicioso, empleando el protocolo DNS como un canal encubierto, a continuación, se indican estas herramientas y librerías: Librerías tweepy, pysocks, dnslib, pycrypto, slackclient, bitstring, dpkt>=1.9.1, pyftpdlib, email==6.0.0.a1, scapy, pygithub.

Todas estas herramientas y librerías detalladas, están basadas en software libre, haciendo que estas puedan ser utilizadas por cualquier persona, sin la necesidad de comprar o pagar por una licencia de uso. Es importante señalar este punto para tener en cuenta que estas herramientas se encuentran disponibles en internet para quien desee utilizarlas.

III. MÉTODOS

A. *Diseño y tipo de estudio*

Experimental, considerando las siguientes variables:

- Variable Dependiente: Fuga de Datos.
- Variable Independiente: Técnicas de canal encubierto para el protocolo DNS.

B. *Población de estudio*

Archivos que contienen información sensible.

C. *Unidades de observación*

Para la realización del experimento se tomaron dos archivos de muestra, que contienen información sensible.

- Para el cliente con sistema operativo GNU Linux, el archivo "*/etc/passwd"*, que contiene información de los usuarios de este sistema operativo.
- Para el cliente con sistema operativo Windows 10, un archivo Excel *"confidencial.xlsx"*, que contiene información confidencial.

D. *Variables a medir.*

Para la medición de la variable dependiente se obtuvo el porcentaje de archivos transferidos exitosamente empleando el canal encubierto a través del protocolo DNS.

Para la medición de la variable independiente se seleccionaron los siguientes indicadores a partir de los nombres dominio:

TABLA II. VARIABLE INDEPENDIENTE

INDICADOR	DESCRIPCIÓN	UNIDAD DE MEDIDA
Tamaño	Tamaño del archivo.	KB - KiloBytes
Longitud	Longitud del nombre de dominio	N° caracteres.
MD5	Hash del archivo	Valor en MD5 del archivo

E. *Experimento – Instrumentos – Cliente GNU Linux*

Para proceder con el experimento se realizó la adquisición del dominio dennisedson.tk, el cual es un dominio de tipo ccTLD de nivel superior geográfico para el archipiélago neozelandés de Tokelau, de registro gratuito.

Empleando la herramienta DET (*Data Exfiltration Toolkit*), basada en Python, se procedió a su instalación en el servidor DNS Linux [13], este Servidor se encarga de recibir las solicitudes de resolución del dominio dennisedson.tk, para procesar los datos recibidos por el canal encubierto y almacenarlos localmente, configurando en el servidor el archivo config-server.json de la siguiente manera:

```
"dns": {
    "key": "dennisedson.tk",
    "target": "192.168.1.17",
    "port": 53
},
```

Fig. 4. Configuración del Servidor.
Fuente: Elaboración propia.

Para poner en funcionamiento el servidor se hizo correr el programa con Python:

```
op/DET$ sudo python det.py -L -c config-server.json -p dns
nn:
CTRL+C to kill DET
[dns] Waiting for DNS packets for domain dennisedson.tk
```

Fig. 5. Servidor de DNS para exfiltración en funcionamiento.
Fuente: Elaboración propia.

A partir del cliente con GNU-Linux instalado, se procedió a utilizar de igual manera la herramienta DET, configurado como cliente mediante el archivo config-client.json de la siguiente manera (desde el lado del Cliente):

```
"dns": {
    "key": "dennisedson.tk",
    "target": "192.168.1.17",
    "port": 53
},
```

Fig. 6. Configuración del Cliente.
Fuente: Elaboración propia.

Para realizar la transferencia del archivo /etc/passwd desde el cliente Linux, al servidor DNS, se lo realizó de la siguiente manera:

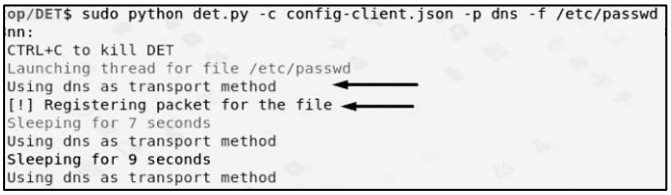

Fig. 7. Inicio de transferencia del archivo /etc/passwd.
Fuente: Elaboración propia.

Iniciada la transferencia del archivo, se puede ver como los datos son enviados como una solicitud de resolución de subdominio del dominio dennisedson.tk:

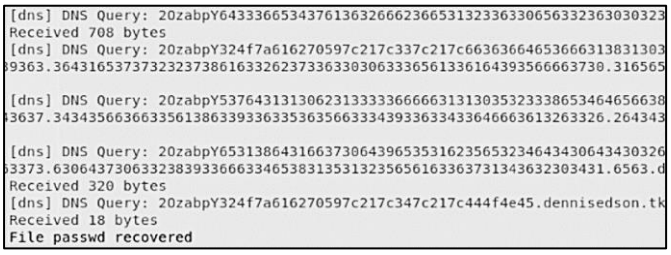

Fig. 8. Solicitudes de resolución de subdominio.
Fuente: Elaboración propia.

Concluida la transferencia del archivo se verifica en el servidor que efectivamente el archivo se transfirió exitosamente:

Fig. 9. Archivo transferido.
Fuente: Elaboración propia.

Para el experimento desde un cliente con sistema operativo Windows 10, se empleó un script basado en powershell DNSExfiltrator [14], el archivo a ser filtrado al servidor DNS es "confidencial.xlsx" cuyo contenido dentro el equipo Windows 10, es el siguiente:

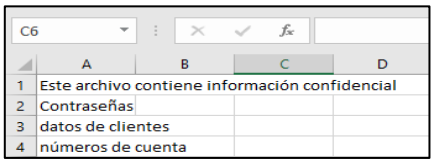

Fig. 10. Contenido del archivo confidencial.xlsx
Fuente: Elaboración propia.

Desde una consola Powershell, en la PC del Cliente con Windows 10, se procedió a verificar los archivos requeridos para la fuga de información (el script, y el archivo a ser filtrado):

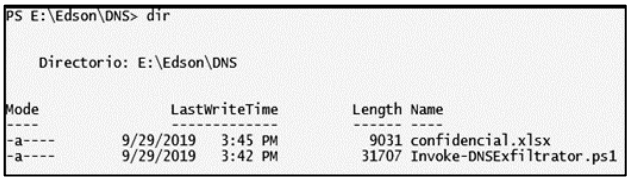

Fig. 11. Script powershell y archivo confidencial.xlsx.
Fuente: Elaboración propia.

Tras la ejecución del Script, se procedió a transferir el archivo "confidencial.xlsx", con el comando:

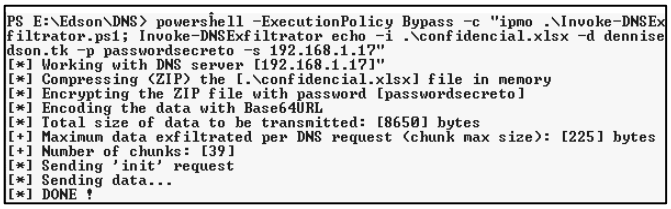

Fig. 12. Transferencia del archivo.
Fuente: Elaboración propia.

Revisando del lado del servidor, se puede ver el archivo transferido:

Fig. 13. Verificación del archivo transferido.
Fuente: Elaboración propia.

Realizando la verificación de los archivos, tanto el archivo original como el transferido estos poseen el mismo HASH en MD5 CC76DDAF5CF5F48FCB5B6AB8581641E8. Lo cual indica que la información se transfirió de manera íntegra.

IV. Resultados

El experimento realizado pudo comprobar la factibilidad de filtrar información (fuga de información), empleando el protocolo DNS como un canal encubierto (UDP puerto 53), pasando por este canal la información de manera íntegra como si se tratasen solicitudes de resoluciones DNS, a manera de subdominios para el dominio configurado.

V. Discusión

El presente trabajo demostró como información puede ser filtrada a través de un canal encubierto con el protocolo DNS, por lo que la información y técnicas descritas, se las presentó con fines académicos para demostrar el riesgo existente y generar conciencia para su protección; por lo que ni el autor del artículo, ni la revista se responsabilizan por el mal uso que se pueda hacer de ello.

Este protocolo suele ser pocas veces filtrado y monitoreado por las empresas u organizaciones, ya que incluso algunas empresas carecen de servidores propios DNS en su infraestructura tecnológica, dando lugar a utilizar servidores DNS externos disponibles en internet, exponiendo de esta manera a los riesgos concernientes con el protocolo DNS; por lo que el reto se encuentra en la detección de esta actividad, analizando el tráfico de red para estas solicitudes de DNS que utilizan el protocolo UDP en puerto 53, porque la información se transfiere en la porción del subdominio.

VI. Conclusiones

El uso de técnicas avanzadas para la fuga de información usando canales encubiertos en la red como el protocolo DNS, es una técnica exitosa, cuando se carecen de controles y monitoreo del tráfico de red en muchas organizaciones. Por lo que se sugiere como buena práctica la implementación de controles y

monitoreo de la red en general que coadyuven en su oportuna detección y mitigación de riesgos.

REFERENCIAS

[1] Pinedo E. (2019). Una brecha de seguridad en Toyota. Recuperado el 03/02/2020, de https://hipertextual.com/2019/03/brecha-seguridad-toyota

[2] Arán, J. (2019). 540 millones de registros de usuarios de Facebook expuestos. Recuperado el 03/02/2020, de https://www.welivesecurity.com/la-es/2019/04/04/millones-registros-usuarios-facebook-expuestos/

[3] INCIBE-CERT. (2019). Filtrada información de millones de ciudadanos de Bulgaria. Recuperado el 03/02/2020, de https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/filtrada-informacion-millones-ciudadanos-bulgaria

[4] Pérez, E. (2019). Expuestos 7.5TB de datos con proyectos de la agencia de inteligencia rusa. Recuperado el 03/02/2020, de https://www.xataka.com/seguridad/expuestos-7-5tb-datos-proyectos-agencia-inteligencia-rusa-como-desanonimizar-trafico-tor-vulnerar-redes-p2p

[5] Cimpanu, C., Williams, C. (2019). Registro de votantes de 80% de la población de Chile queda expuesto en Internet. Recuperado el 03/02/2020, de https://blog.segu-info.com.ar/2019/08/registro-de-votantes-de-80-de-la.html?m=0

[6] Wang, W. (2019). Imperva Breach Exposes WAF Customers' Data, Including SSL Certs, API Keys. Recuperado el 03/02/2020, de https://thehackernews.com/2019/08/imperva-waf-breach.html

[7] BBC News Mundo. (2019). Filtración de datos en Ecuador. Recuperado el 03/02/2020, de https://www.bbc.com/mundo/noticias-america-latina-49721456

[8] INCIBE. (2017). Estás preparado para hacer frente a una fuga de datos. Recuperado el 04/02/2020, de https://www.incibe.es/protege-tu-empresa/blog/estas-preparado-hacer-frente-fuga-datos

[9] ICANN. (2012). Top-Level Domains (gTLDs). Recuperado el 04/02/2020, de http://archive.icann.org/en/tlds/

[10] Mockapetris, P. (1987). Domain Names - Implementation And Specification. Recuperado el 05/02/2020, de https://www.ietf.org/rfc/rfc1035.txt

[11] Zimba, A., Chishimba, M. (2017). Exploitation of DNS Tunneling for Optimization of Data Exfiltration in Malware-free APT Intrusions. *Zambia Information Communication Technology (ICT) Journal, 1*(1), 51-56.

[12] Nadler, A., Aminov, A., Shabtai, A. (2018). Detection of Malicious and Low Throughput Data Exfiltration Over the DNS Protocol. *arXiv:1709.08395 [cs.CR]*.

[13] PaulSec. (2019). DET (extensible) Data Exfiltration Toolkit. Recuperado el 06/02/2020, de https://github.com/PaulSec/DET

[14] Arno0x. (2018). DNSExfiltrator. Recuperado el 06/02/2020, de https://github.com/Arno0x/DNSExfiltrator.

[15] Bromberger, S. (2011). DNS as a Covert Channel Within Protected Networks. *Department of Energy under Award Number DE-OE0000516 [WP2011-01-01]*.

Breve CV del autor

Dennis Edson Vargas Peña es Licenciado en Informática, mención en Ingeniería de Sistemas, graduado por Excelencia en la Universidad Mayor de San Andrés, La Paz. Diplomado en Educación Superior, CEPIES-UMSA. Actualmente realiza la Maestría en Informática Forense, Auditoria Informática y Seguridad de la Información en el Postgrado en Informática UMSA. Tiene certificaciones Cisco CCNA Security, CCDA y CCNA Routing & Switching, CEH Practical y Master de EC-Council. Ejerció laboralmente en entidades financieras y en el sector público en áreas de infraestructura tecnológica, seguridad informática y seguridad de la información. Email: dennis.edson@gmail.com.