TEST DE PENETRACIÓN PARA EL ESTUDIO DE VULNERABILIDADES A LOS CIBERATAQUES MEDIANTE TÉCNICAS DE HACKING ÉTICO EN REDES IPV4

(PENTESTING FOR THE STUDY OF VULNERABILITIES TO CYBER-ATTACKS USING ETHICAL HACKING TECHNIQUES IN IPV4 NETWORKS)

Ing. Luis Rincon
Zuliana de Plásticos C.A
luisgustavorincon@gmail.com
ORCID ID: 0000-0003-4550-9372

RESUMEN

El presente trabajo se inició estableciendo un objetivo de ataque en internet a la empresa “Zuliana de Plásticos C.A” realizando un test de penetración el cual tuvo como objetivo principal determinar si existen vulnerabilidades a nivel de arquitectura e infraestructura en las redes (IPv4), la misma se desarrolló implementando la metodología “NIST SP 800-115” la cual está fundamentada bajo el “Instituto Nacional de Normas y Tecnología de los Estados Unidos” para la etapa de identificación de vulnerabilidades. Las bases teóricas se sustentaron en diversos autores como: Palacios (2021), González (2021), Edison (2017), Montesino (2018), Cárdenas (2016), Guzmán (2016) y el Instituto Nacional de Normas y Tecnología “NIST” (2008), entre otros. La herramienta de software utilizada fue el sistema operativo Kali Linux 2022.v1 orientado a la seguridad informática, adicionalmente se utilizó la técnica de “footprinting” la cual es aplicada para la búsqueda de vulnerabilidades en sistemas informáticos como: puertos abiertos, información expuesta a internet, información relacionada a la infraestructura de IT y ciberataques en los sistemas informáticos. Luego fueron desarrolladas dos etapas del Pentesting con las herramientas y comandos de Kali Linux: Reconocimiento o recolección de información y escaneo o análisis de vulnerabilidades. El desarrollo del trabajo estuvo fundamentado bajo una investigación del tipo descriptiva, en la cual se describieron los procedimientos, metodologías y procesos para llevar a cabo el desarrollo del mismo. La población estuvo conformada por la intranet de la empresa Zuliana De Plásticos C.A, de la cual se tomó la muestra en las redes IPv4 de la organización. Se empleó como instrumento de recolección de datos la aplicación de pentesting a la organización. En los resultados se observa información confidencial de la organización la cual no fue revelada en su totalidad para incentivar el uso del “Hacking ético”. La información más relevante extraída y publicada del proceso fue la siguiente: usuarios, correos, geolocalización, números telefónicos, puertos abiertos, dominios y subdominios, entre otros. Para concluir los resultados fueron analizados con el propósito de demostrar el alcance del pentesting con sus herramientas, técnicas y metodologías implementadas, del mismo modo fue posible conocer las vulnerabilidades a las que se expone la organización.

Palabras clave: Pentesting, hacking ético y footprinting.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

ABSTRACT

The present work began by presenting an internet attack objective to the company "Zuliana de Plásticos C.A" carrying out a penetration test which had as its main objective to determine if there are vulnerabilities at the level of architecture and infrastructure in the networks (IPv4), the It was developed by implementing the "NIST SP 800-115" methodology, which is based on the "National Institute of Standards and Technology of the United States" for the vulnerability identification stage. The theoretical bases were based on various authors such as: Palacios (2021), González (2021), Edison (2017), Montesino (2018), Cárdenas (2016), Guzmán (2016) and the National Institute of Standards and Technology "NIST" (2008), among others. The software tool used was the Kali Linux 2022.v1 system oriented to computer security, in addition the "footprinting" technique was used, which is applied for the operational search for vulnerabilities in computer systems such as: open ports, information exposed to the Internet , information related to IT infrastructure and cyber-attacks on computer systems. Two stages of Pentesting were then developed with Kali Linux tools and commands: Reconnaissance or information gathering and vulnerability scanning or analysis. The development of the work was based on an investigation of the descriptive type, in which the procedures, methodologies and processes to carry out its development were described. The population was made up of the intranet of the company Zuliana De Plásticos C.A, from which the sample was taken in the organization's IPv4 networks. The application of Pentesting to the organization was used as a data collection instrument. In the results, confidential information of the organization is observed, which was not fully disclosed to encourage the use of "ethical hacking". The most relevant information extracted and published from the process was the following: users, emails, geolocation, telephone numbers, open ports, domains and subdomains, among others. To conclude, the results were analyzed with the purpose of demonstrating the scope of Pentesting with its tools, techniques and methodologies implemented, in the same way it was possible to know the vulnerabilities to which the organization is exposed.

Keywords: Pentesting, ethical hacking and footprinting.

INTRODUCCIÓN

En la actualidad existen diferentes herramientas automatizadas con las cuales se aplican diferentes tipos de pruebas en ataques informáticos reales, para luego tomar acciones. Algunas de estas herramientas están disponibles en internet de forma gratuita y se distribuyen de manera que sean accesibles para expertos, auditorias de ciberseguridad e incluso a personas que aplican las herramientas de manera delictiva. La seguridad informática que es transmitida en redes de datos es sumamente fundamental debido a que la aplicación de estas técnicas protege el

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

acceso delictivo de personas que atentan o atacan diariamente en contra de organizaciones.

Una de estas herramientas es Kali del sistema operativo Linux la cual es una distribución basada en Debian GNU/Linux diseñada principalmente para auditorias y seguridad informática en general, este software cuenta con una multitud de herramientas tanto en modo grafico como por comandos, lo que lo convierte en un sistema muy completo, bien sea para defensores que buscan sistemas más seguros o para atacantes que buscan datos valiosos como cuentas, contraseñas y demás datos personales. Entre todo lo que se puede realizar con Kali Linux, los aspectos más resaltantes son: Recopilación de información, análisis de vulnerabilidad, ataques inalámbricos, aplicaciones web, herramientas forenses, ataques con contraseña, hacking de hardware, entre otras cosas.

METODOLOGÍA

El desarrollo del trabajo estuvo fundamentado bajo una investigación del tipo descriptiva, según Hernández, R. Fernández, C. y Baptista, M. (2014), la investigación consiste en llegar a conocer situaciones y actitudes predominantes de un objeto de estudio a través de la descripción exacta de las actividades, objetos, procesos a llevar a cabo la investigación. El objetivo no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables. Los investigadores no son tabuladores, sino que recopilan los datos sobre la base de una hipótesis o teoría, exponen y resumen la información de manera cuidadosa y luego analizan minuciosamente los resultados.

ANALISIS DE LOS RESULTADOS

Para dar respuesta a los objetivos planteados en la presente investigación, el desarrollo del artículo consta de dos (02) fases, una de ellas se basa en recopilar la mayor cantidad de información de la organización seleccionada como objetivo de ataque mediante las herramientas del pentesting, seguidamente se realizó un escaneo online en los sistemas detectados de la fase anterior mediante herramientas disponibles en la web que serán descritas en el transcurso del trabajo y finalmente se realizan las conclusiones en torno a los resultados de la investigación.

Fase I. Recopilación de Información

1. Dominio de la organización

Para iniciar el proceso de recopilación de la información, fue realizada una investigación profunda en internet, sobre la organización en cuestión. Como resultados obtenidos luego de una investigación informática, no fue posible localizar ningunos enlaces pertenecientes de forma directa a la empresa, del mismo modo tampoco fue posible localizar dominios de ingreso a la intranet de la organización. Desde la página www.netcraft.com se realizó un análisis al enlace utilizado por la

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

empresa para su página comercial, lo cual permitió “indagar” sobre si el dominio comercial, es el dominio usado a nivel industrial.

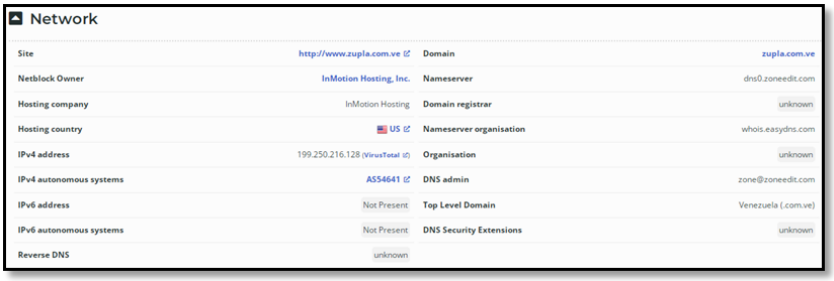

Figura 1. Análisis del enlace comercial de Zuliana de Plásticos C.A
Fuente: Elaboración Propia (2022).

Una vez, agotada la información conseguida en los motores de búsqueda, se procedió a utilizar herramientas en “Kali Linux” la cual consistió en una distribución de Linux basada en Debian, específicamente diseñada para temas de seguridad muy variados, como análisis en redes, ataques inalámbricos, análisis forense, entre otros. En esta oportunidad se utilizó para conseguir más información sobre la organización, para ello se implementó el comando “Sublist3r” mostrado en la figura 2, el cual permite mostrar si existen dominios y subdominios en la organización.

Figura 2. Herramienta Sublist3r, Kali Linux.
Fuente: Elaboración Propia (2022).

Realizando una pequeña conclusión luego de utilizar la herramienta “Sublist3r”, el programa indico que no fue posible encontrar algún resultado referente a los subdominios, adicionalmente se agregó el API de “virus total” para evitar errores de “requests” e igual el resultado no mostro variación alguna. Indagando con otras herramientas para obtener más resultados, se obtuvo que mediante la web www.nmmapper.com ilustrada en la figura 3, para la página www.zupla.com.ve fue posible localizar los siguientes subdominios:

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

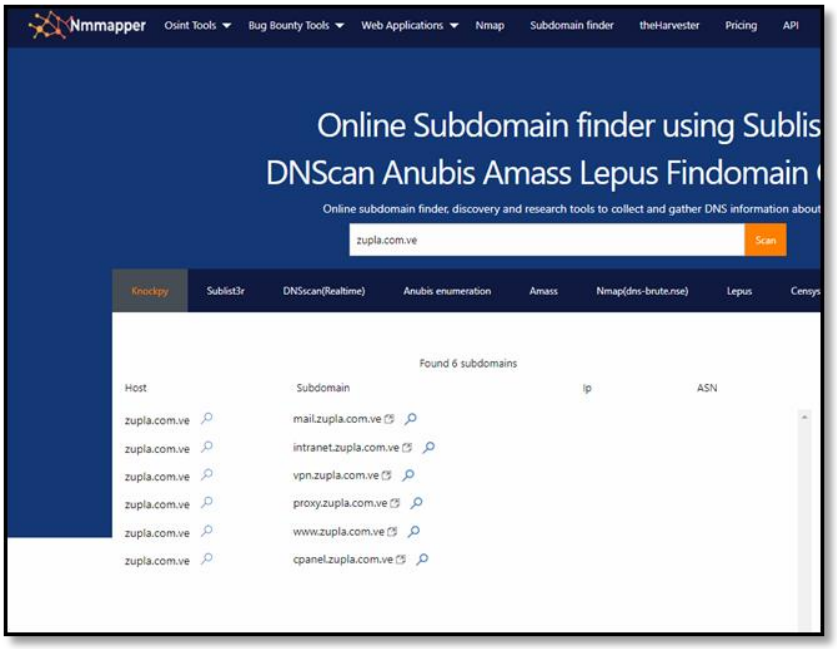

Figura 3. Subdominios, Nmmapper.
Fuente: Elaboración Propia (2022).

Seguidamente se procedió a utilizar como herramienta el paquete “Amass” en Kali, Linux en el cual se realizó de forma satisfactoria el mapeo de la red en las superficies de ataque, del mismo modo se efectuó el descubrimiento de los activos externos utilizando técnicas de reconocimiento activo y recopilación de información de fuente abierta. Para ello se utilizó el comando a continuación: “Amass enum -v -passive -o domains.txt -d zupla.com.ve”, de esta forma se recopilaron los subdominios mostrados en la figura 4.

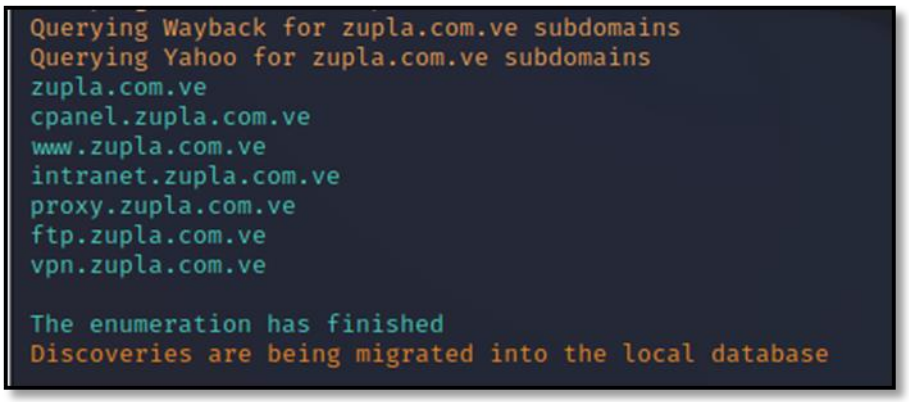

Figura 4. Subdominios. Kali, Linux.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

Fuente: Elaboración Propia (2022).

2. Usuarios y Trabajadores.

Para iniciar se realizó una búsqueda mediante la red social LinkedIn en la cual una gran cantidad de usuarios cuelgan sus currículos online y entablan relaciones comerciales, donde buscan u ofrecen trabajo de forma libre sin seguridad alguna, expuestos a cualquier amenaza. Luego de realizar la búsqueda en la mencionada red social, se encuentra que existen al menos más de 33 trabajadores que pertenecen a la organización, esto se puede observar en la figura 5.

Figura 5. Cantidad de empleados aproximada, LinkedIn.
Fuente: Elaboración Propia (2022).

a) Emails

Para realizar una búsqueda de los correos electrónicos de algunos trabajadores de le organización se utilizó la herramienta “crosslinked” en Kali, Linux mostrada en la figura 6, se obtuvo como resultado una gran lista de correos electrónicos pertenecientes a los posibles empleados activos de la organización, permitiendo desde este punto, seguir planificando un ciberataque direccionado con la información obtenida mediante esta herramienta.

Figura 6. Crosslinked / Correos electrónicos. Kali, Linux

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

Fuente: Elaboración Propia (2022).

3. Geolocalización

Para realizar una búsqueda de forma sencilla se implementó el buscador de geolocalización más utilizado en la actualidad llamado “Google Maps” ilustrado en la figura 7, en el cual se obtuvo una clara y precisa dirección de las instalaciones, donde se deja en evidencia diversas fotografías de las instalaciones exteriores e interiores, adicionalmente se consigue observar cómo es la infraestructura dentro de una de las plantas de producción llamada polipropileno II.

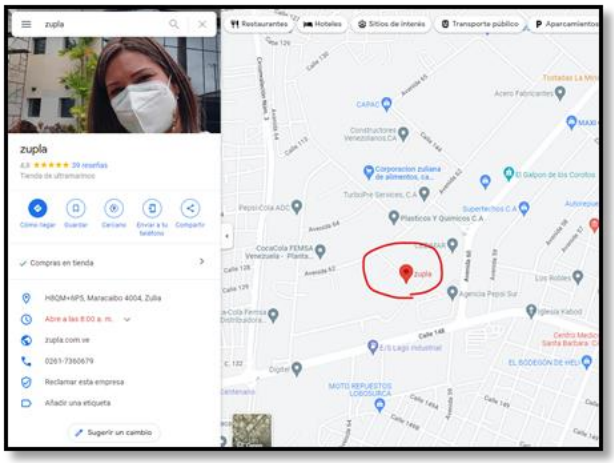

Figura 7. Ubicación. Google, Maps.
Fuente: Elaboración Propia (2022).

4. Información sensible expuesta en Internet

Luego de una búsqueda exhaustiva en internet para tratar de recopilar información de alta confiabilidad se consiguió que la única información sensible expuesta en internet fue el número telefónico personal de un empleado de alto rango de la organización, el cual no será revelado en este artículo por prácticas éticas, el mismo se encontraba listado en una página web externa a la empresa, con información adicional de la misma.

5. Rangos de red y sistemas autónomos.

Para visualizar los rangos de red en el sistema se puede observar la imagen 8, donde se utilizaron las herramientas de “Netcraft”, los cuales son una compañía de servicios de seguridad en Internet, incluyendo servicios contra el fraude y phishing, evaluación de aplicaciones y escaneo PCI. A su vez permiten analizar varios aspectos de Internet, incluyendo el mercado de servidores web, sistemas operativos, proveedores de hosting y autoridades de certificados SSL. De igual forma “Netcraft” proporciona una herramienta que permite capturar información

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

sobre las tecnologías utilizadas en un sitio web. Del mismo modo permite obtener una lista de subdominios asociados con cualquier sitio web que “Netcraft” conozca.

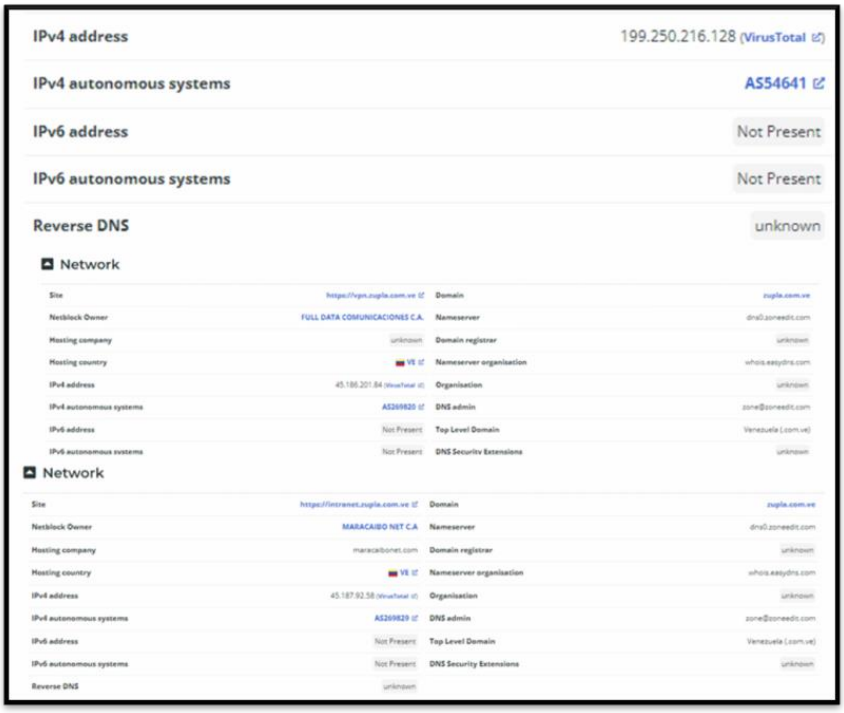

Figura 8. Rangos de red para (zupla.com.ve. / vpn.zupla.com.ve./intranet.zupla.com.ve.) Netcraft. Fuente: Elaboración Propia (2022).

Una vez obtenido el reporte generado por la página de www.netcraft.com fue posible visualizar todos los rangos de red en los diferentes dominios y subdominios de la organización, por consiguiente se llegó a la conclusión que para el dominio www.zupla.com.ve se direcciona a una IP utilizada para una web de forma comercial, mientras que para los siguientes subdominios www.intranet.zupla.com.ve y www.vpn.zupla.com.ve se direccionan a dos IP utilizadas de forma local, ambas pertenecientes a la red de la organización Zuliana De Plásticos C.A.

6. Identificación y clasificación de los diferentes tipos de sistemas encontrados mediante buscadores Shodan, ZoomEye, oShada y Censys.

ZoomEye es un motor de búsqueda para el ciberespacio, que contiene información sobre dispositivos, sitios web y servicios o componentes utilizados en el espacio de Internet. ZoomEye tiene dos motores de detección principales: “Xmap” y “Wmap”, que identifican respectivamente los servicios y componentes utilizados por los dispositivos y sitios web de Internet a través de la detección e identificación

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

ininterrumpida de 24 horas para dispositivos y sitios web en el ciberespacio. Los investigadores pueden comprender fácilmente la tasa de penetración de los componentes y el alcance de la vulnerabilidad a través de “ZoomEye”. Usando el buscador “ZoomEye” mediante el siguiente filtro de búsqueda “zupla +country:"VE" +port:"443" +service:"https"” se obtienen los siguientes resultados ilustrados en la figura 9:

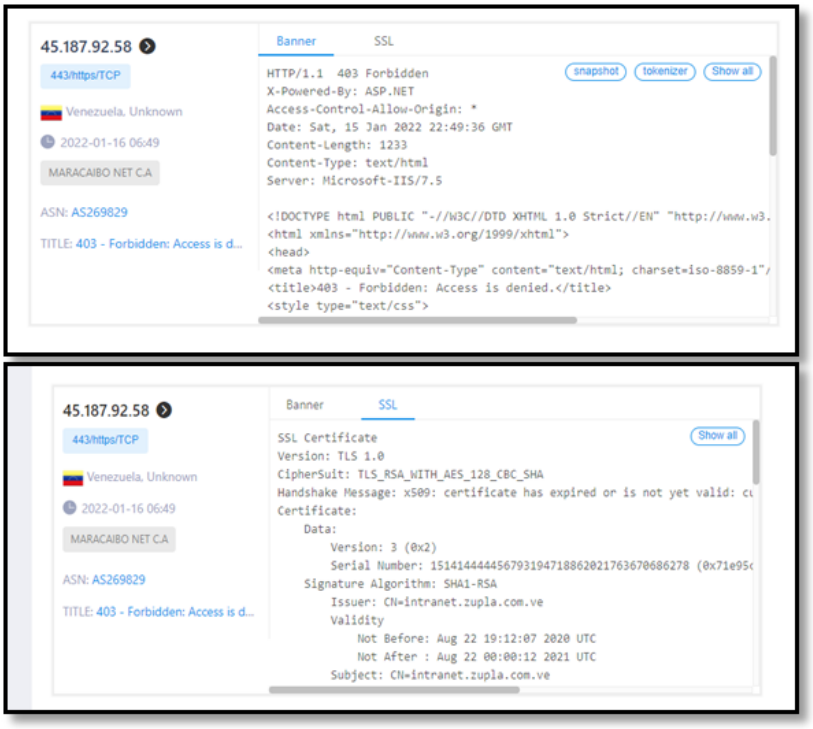

Figura 9. Motor de búsqueda y Certificado SSL. ZoomEye.
Fuente: Elaboración Propia (2022).

Una vez fue descrita la aplicación o el funcionamiento del motor de búsqueda ZoomEye, se realizó la búsqueda del sistema para la empresa en cuestión mediante filtros de búsqueda para optimizar el proceso, en los resultados obtenidos, se observó en la figura 9 que se trata de una entrada a la intranet de la organización mediante el puerto TCP/443, del cual se pudo obtener que el servidor intranet está alojado en un servidor de Microsoft usando IIS/7.5 basado en ASP.NET. Del mismo modo que se explicó la definición y se observó el funcionamiento de las herramientas del motor de búsqueda se procedió a utilizar otro buscador llamado “Shodan.io” lo cual es más reconocido y antiguo que el anterior, en el mismo se aplicaron los siguientes filtros de búsqueda “Net: 45.187.92.58 http” y “net: 45.187.92.58 vpn” mostrados en la figura 10:

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

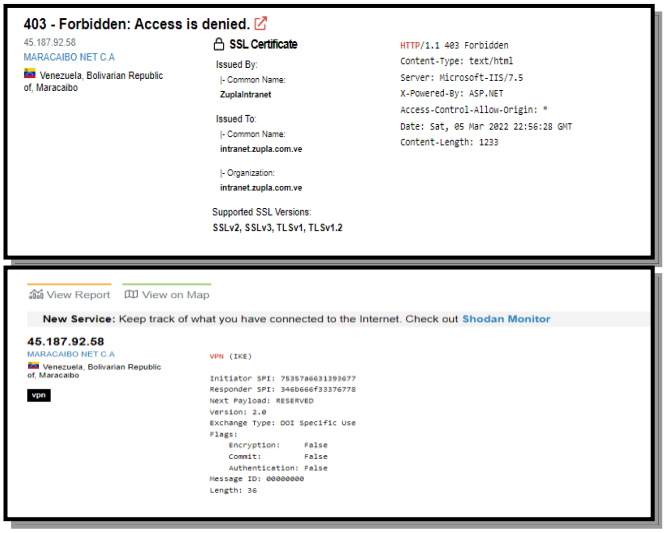

Figura 10. Motor de búsqueda "Http y Vpn". Shodan.io.
Fuente: Elaboración Propia (2022).

Realizando una breve conclusión, luego de los procesos anteriormente desarrollados con los motores de búsqueda "ZoomEye" y "Shodan.io", fue posible visualizar que los resultados obtenidos por el motor de búsqueda "Shodan.io" fueron en gran parte resultados muy similares a los obtenidos mediante el proceso de búsqueda con "ZoomEye". De igual forma fue implementado como una tercera opción, el motor de búsqueda llamado "Censys", en el cual se realizó la búsqueda del host "Intranet.zupla.com.ve" ilustrado en la figura 11.

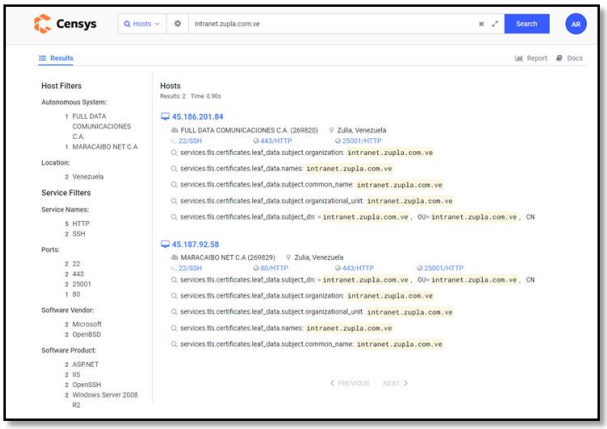

Figura 11. Motor de búsqueda "Censys".
Fuente: Elaboración Propia (2022).

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

Luego de los resultados obtenidos mediante el tercer motor de búsqueda "Censys" implementado en el proceso anterior, se pudo observar en la figura 11, la versión del servidor donde se está alojando la intranet de la organización, siendo su sistema operativo Windows Server 2008 R2, adicionalmente se observó que los servicios de "HTTP" y "SSH" están habilitados, permitiendo realizar investigaciones sobre las vulnerabilidades que nunca fueron solventadas para ese sistema operativo.

Fase II. Escaneo online sobre los sistemas detectados.

1. **Identificación pasiva de posibles vulnerabilidades**

Para realizar la identificación de vulnerabilidades se utilizó la herramienta suministrada por www.nmap.online.com para realizar un escaneo de los dominios ingresados y observar si estos poseen puertos abiertos. Mediante el escaneo realizado se obtuvo como resultado que para el host "intranet.zupla.com.ve" y vpn.zupla.com.ve fueron localizados diversos puertos abiertos que se muestran a continuación en la figura 12:

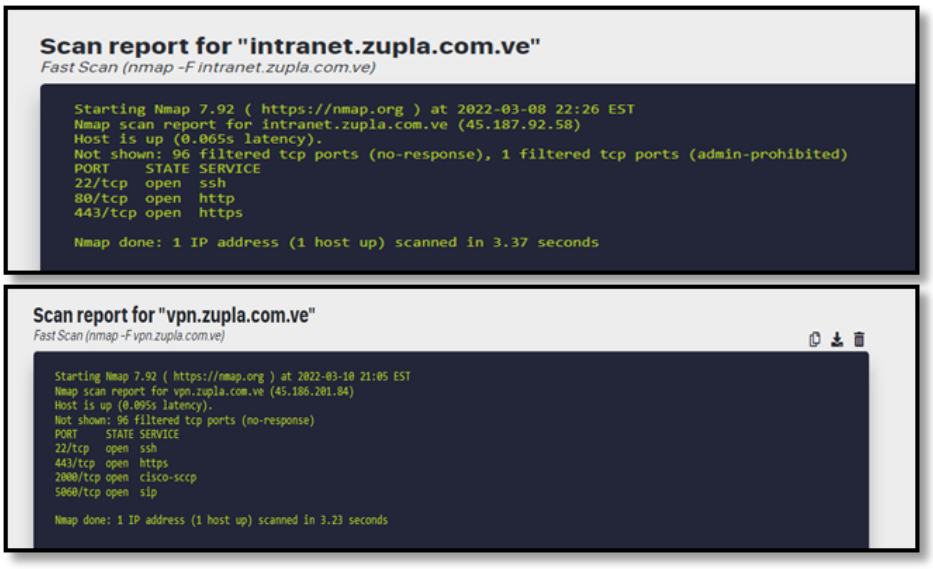

Figura 12. Rastreo de puertos (Intranet), Nmap.
Fuente: Elaboración Propia (2022).

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

2. Análisis de dominios

En esta etapa fue necesario seleccionar los dominios principales de la organización y extraer mediante aplicaciones como “DNSdumpster” y “CRT.sh” los subdominios para luego analizar si estos subdominios se encuentran en infraestructura del cliente o en proveedores. Usando la web www.DNSdumpster.com, es posible encontrar resultados muy parecidos a los obtenidos con otras herramientas haciendo uso del dominio principal “zupla.com.ve”, esto se puede observar en la figura 13.

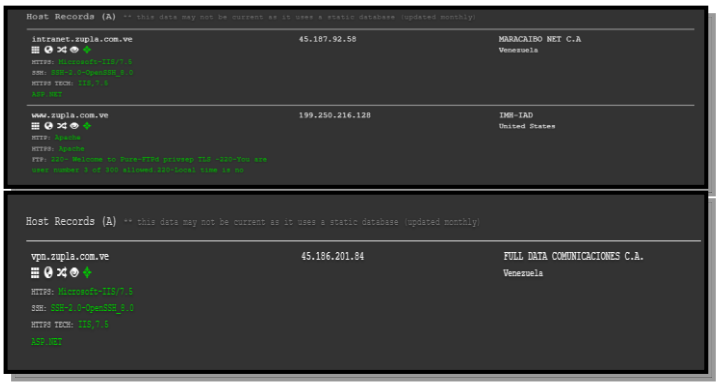

Figura 13. Análisis de dominio (intranet.zupla.com.ve / vpn.zupla.com.ve), DNSdumpster.
Fuente: Elaboración Propia (2022).

Luego de haber realizado la búsqueda de ambos dominios se puede concluir que debido a la geolocalización de las direcciones IP, los subdominios “intranet.zupla.com.ve” y “vpn.zupla.com.ve” se encuentran a nivel de infraestructura del cliente, mientras que www.zupla.com.ve se encuentra a nivel de proveedor externo. Del mismo modo se realizó la búsqueda utilizando la herramienta disponible en la web https://crt.sh/ “CRT.sh” se obtuvo:

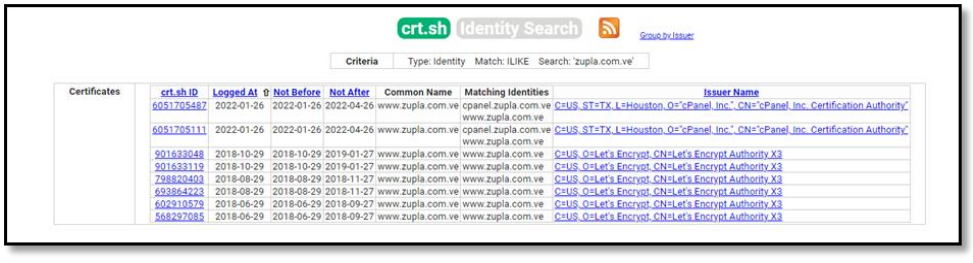

Figura 14. Análisis de dominio (zupla.com.ve), crt.sh.
Fuente: Elaboración Propia (2022).

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

Al observar la figura 14, se evidencia que el dominio principal de la organización llamado “zupla.com.ve” se encuentra a nivel de proveedor externo. Ahora bien, para realizar un escaneo de los puertos para el dominio “intranet.zupla.com.” y “vpn.zupla.com.ve” fue necesario utilizar la herramienta “Nmap” disponible en Kali Linux. Como resultado de lo anteriormente descrito se encontraron diversos puertos abiertos, mostrados en la figura 15, los cuales representan un riesgo la seguridad de le empresa.

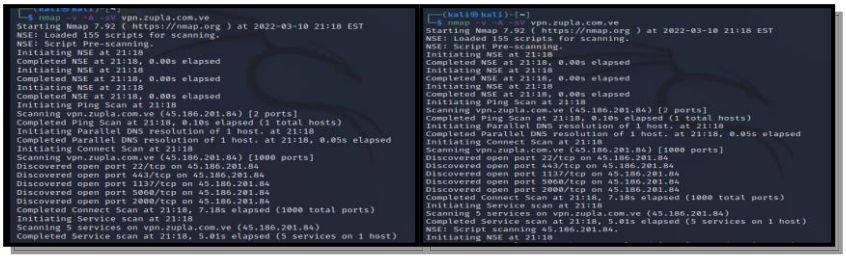

Figura 15. Análisis de puertos (intranet.zupla.com.ve/ vpn.zupla.com.ve), Nmap.
Fuente: Elaboración Propia (2022).

3. Detección de servidores virtuales o “Vhost”

Para iniciar la búsqueda o detección de algún servidor virtual fue necesario seleccionar algún determinado dominio o subdominio de la organización que permita realizar la búsqueda en el mismo sistema, esto se puede realizar mediante la siguiente herramienta “vhosts-sieve” en Kali, Linux. Para comenzar a utilizar la herramienta antes mencionada se escribió el siguiente código: “python3 vhosts-sieve.py -d /home/kali/domains.txt -o vhosts.txt”

Figura 16. Detección de Vhost. Kali, Linux.
Fuente: Elaboración Propia (2022).

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

Una vez ejecutado el código se observó en la figura 16 que mediante la herramienta "vhosts-sieve" en Kali, Linux, no se consiguieron servidores virtuales o mejor dicho "Vhosts". Al no conseguir respuesta por la herramienta antes mencionada, se realizó la búsqueda mediante la siguiente página www.pentest-tools.com utilizando la herramienta "information-gathering" Se encontró que para el dominio "intranet.zupla.com.ve", existe un virtual host.

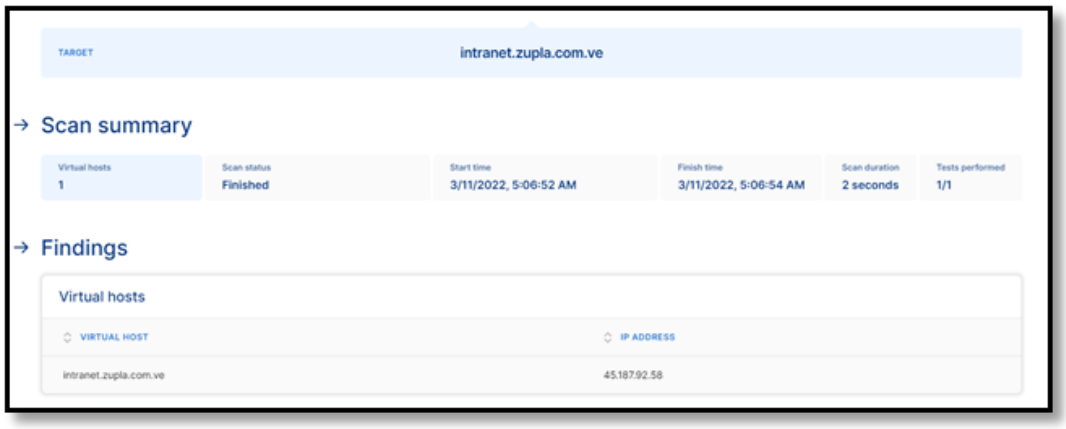

Figura 17. Detección de Vhost (intranet.zupla.com.ve).
Fuente: Elaboración Propia (2022).

Como se pudo observar en la figura 17, luego del escaneo se encontró que para el dominio "intranet.zupla.com.ve", existe un virtual host. Del mismo modo se realizó el escaneo utilizando otra página web llamada "scantrics" la cual está de forma gratuita en internet con la siguiente dirección www.scantrics.io.com haciendo uso de su herramienta llamada "virtual-host-scanner" se permitió determinar como resultado final que para el dominio "vpn.zupla.com.ve" también existe un virtual host, ilustrado en la figura 18.

Figura 18. Detección de Vhost (vpn.zupla.com.ve).
Fuente: Elaboración Propia (2022).

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

CONCLUSIÓN

Las pruebas de penetración constituyen un proceso importante para evaluar la seguridad de las redes informáticas, pero existen diversos riesgos que se deben tener en cuenta. En función de ello, en el presente artículo se definieron varios riesgos que pueden afectar la seguridad de la organización y la integridad de sus empleados. Para nadie es un secreto que con el constante aumento de las redes de computación la inseguridad informática ha aumentado de forma exponencial, a diario se buscan formas de estar más seguros informáticamente, pero al mismo tiempo, algunos hackers, encuentran vulnerabilidades o debilidades.

El pentesting o "prueba de penetración" juega un rol muy importante en la seguridad informática, por lo tanto, el profesional que es dedicado a esta área debe ser lo más ético posible para brindar asesoría a las empresas que soliciten su servicio como auditor. En efecto de los resultados obtenidos en el presente artículo se observó un aproximado de la cantidad de trabajadores de la organización, a su vez, la geolocalización de la empresa donde se mostró una de sus plantas de producción, del mismo modo fue posible localizar algunos correos electrónicos, números de teléfono, perfiles en LinkedIn con información personal de los trabajadores y la vulnerabilidad de más alto impacto consistió en el fácil acceso a la intranet de la organización mediante sus puertos abiertos.

REFERENCIAS BIBLIOGRÁFICAS

Cárdenas, M. (2016). Pentesting empleando técnicas de ethical hacking en redes IPv6. Ocaña, Colombia.

Edison, J. (2017). Prueba de penetración para la identificación de vulnerabilidades en la red de computadoras en la alcaldía del municipio de cantón del san pablo, departamento de choco. Quibdó, Colombia.

González, B. (2021). Riesgos de seguridad en las pruebas de penetración de aplicaciones web. Revista cubana de transformación digital, unión de informáticos de Cuba, Cuba.

Guzmán, I. (2016). Ética hacker, seguridad y vigilancia. Ediciones Universidad Claustro De Sor Juana. Ciudad de México - México.

Hernández, R. Fernández, C. y Baptista, M. (2014). Metodología de la investigación. Sexta edición McGraw-Hill/Interamericana Editores, S.A. de C.V. México.

Montesino, R. (2018). Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web. La Habana, Cuba.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021

National Institute of Standards and Technology, NIST. (2008). Technical Guide to Information Security Testing and Assessment. Gaithersburg, Maryland, USA.

Palacios, M. (2021). Aplicación de pentesting en el análisis de vulnerabilidades del sistema web de gestión administrativa de la empresa DEVHUAYRA SAC. Huancayo, Perú.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 20 Edición No .2 – Año 2021