UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMA DE INFORMACIÓN

TEMA:

ANÁLISIS TÉCNICO COMPARATIVO DE HERRAMIENTAS DE ESCANEO DE PUERTOS DE REDES DE TELECOMUNICACIONES

ESTUDIANTE:

GEOVANNY GIUSSEPE VALENCIA MARTINEZ

TUTOR:

ING. FREDDY MAXIMILIANO JORDAN CORDONES

JUNIO 2023 - OCTUBRE 2023

Contenido

Resumen

Comparar herramientas como Nmap, Netcat y Unicornscan para ver cuáles son las más rápidas y fáciles de usar dentro de los escaneos en las redes de telecomunicaciones es útil, pero recuerda, usar estas herramientas de manera ética es muy importante, ya que el hacking ético es una práctica legal que ayuda a encontrar problemas en sistemas informáticos, como redes WiFi.

Cuando haces hacking ético, necesitas permiso del dueño de la red para evitar problemas legales, porque todas estas herramientas para nos ayudan a poder simular ataques reales y encontrar diversos problemas de seguridad, debido a que Nmap, Netcat y Unicornscan son útiles porque hacen esto de diferentes maneras.

Es vital mantener actualizadas y seguras las medidas de seguridad, ya que las amenazas informáticas cambian, por esta razón se debe estar al tanto de las últimas prácticas de seguridad y aplicarlas en un mundo donde los métodos de ataques evolucionan rápidamente y los hackers son cada vez más inteligentes.

Palabras claves: red wifi, vulnerabilidad, seguridad, hacking ético

Summary

Comparing tools such as Nmap, Netcat and Unicornscan to see which ones are the fastest and easiest to use for scanning telecommunication networks is useful, but remember, using these tools in an ethical way is very important, because ethical hacking is a legal practice that helps to find problems in computer systems, such as WiFi networks.

When you do ethical hacking, you need permission from the network owner to avoid legal problems, because all these tools help us to simulate real attacks and find various security problems, because Nmap, Netcat and Unicornscan are useful because they do this in different ways.

It is vital to keep your security measures up to date and secure, as computer threats change, so you need to be aware of the latest security practices and apply them in a world where attack methods are evolving rapidly and hackers are getting smarter and smarter.

Keywords: wifi network, vulnerability, security, ethical hacking

Planteamiento del Problema

La elección de la herramienta indicada para poder llevar a cabo el escaneo de puertos en las redes de un sistema es un gran desafío para quienes trabajan en el área de la seguridad de información ya que hoy en día existe una considerable falta de comparaciones técnicas que sean detalladas entre las diferentes alternativas existentes en el mercado gracias a la falta de directrices claras que les permitan a los expertos poder tomar decisiones actualizadas e informadas sobre las herramientas para el escaneo de puertos a las cuales se le deben emplear sus respectivas configuraciones ya que esto coloca a los técnicos en seguridad de redes en una posición difícil.

El problema aumenta por la falta de información actualizada sobre la eficacia y el rendimiento de las herramientas de escaneado de puertos disponibles, ya que esto limita la capacidad de los profesionales de la seguridad a llevar a cabo una evaluación exhaustiva de las características de cada herramienta, terminando así en la toma de decisiones de manera errónea y a la implantación de soluciones de escaneo de puertos ineficaces por lo que es aún más crucial llevar a cabo una evaluación precisa y actualizada de estas herramientas.

La necesidad de una evaluación actualizada y detallada de las diferentes herramientas de escaneo de puertos disponibles aumenta a medida que cambian las amenazas, por lo que elegir una buena herramienta para satisfacer la mayoría de los requisitos de seguridad de cada red resulta ser un reto importante pero no imposible, en gran parte porque no existen análisis comparativos técnicos que sean únicos y estén actualizados, es por esta razón que es necesario realizar un análisis técnico comparativo que proporcione a los profesionales de la seguridad de redes una base sólida sobre la que elegir y utilizar herramientas eficaces.

En esta evaluación comparativa es necesario abordar diferentes cuestiones esenciales como lo son la precisión del análisis, la velocidad de detección, la capacidad para identificar vulnerabilidades y la sencillez de uso de la herramienta, puesto que solo será posible tomar decisiones basadas un enfoque estratégico mediante un análisis basado en información precisa y datos pertinentes, incrementando significativamente la seguridad de las redes de telecomunicaciones.

Justificación

Se considera con el presente estudio la importancia de realizar un análisis técnico comparativo de las herramientas de escaneo de puertos de telecomunicaciones ya que gracias al aumento de ciberataques y otras diferentes amenazas la seguridad de las redes es un tema preocupante actualmente, por lo que es necesario abordar esta necesidad para así poder mejorar y solucionar estas inquietudes.

En este estudio de caso se realizará un análisis técnico comparativo de estas importantes herramientas dedicadas al escaneo de puertos de redes para evaluar sus características, ventajas y desventajas, su facilidad de uso, velocidad de escaneo, entre otras funciones, lo cual permitirá determinar cuál herramienta es la más adecuada para llevar a cabo operaciones de seguridad y así ayudar a los expertos en seguridad a tomar decisiones en cuanto a la elección de que herramienta de escaneo de puertos emplear para sus necesidades específicas.

Objetivos

Objetivo General

- Realizar un análisis comparativo de herramientas de escaneo de puertos para evaluar su eficacia, funcionalidad y precisión en la detección de puertos en una red.

Objetivos Especifico

- Analizar los resultados de cada prueba para determinar los puntos fuertes y débiles de cada herramienta en términos de eficacia y precisión de detección de puertos.
- Evaluar la facilidad de uso y la usabilidad de cada herramienta usando factores como su interfaz gráfica y el nivel de experiencia necesario para su manejo.
- Comparar los resultados de las diferentes herramientas para determinar cuál o cuáles ofrecen el mejor rendimiento y precisión en el escaneo de puertos.

Líneas de Investigación

Las líneas de investigación con los que se vincula este trabajo de investigación son "Sistemas de información y comunicación, emprendimiento e innovación" y "Redes y tecnologías inteligentes de software y hardware" ya que realizaremos un análisis comparativo exhaustivo de las herramientas de análisis de puertos más populares del sistema operativo Kali Linux, incluidos Nmap, Unicornscan y Netcat, destacando las ventajas y desventajas de cada herramienta, así como sus fortalezas y debilidades.

Desde un enfoque de ingeniería de sistemas, la seguridad cibernética es esencial ya que siempre queremos mantener un acceso seguro y confiable además de proteger la información del cliente, por lo que analizar estas herramientas contribuirá a la investigación de ciberseguridad al evaluar su efectividad y precisión para escanear puertos de sistemas de información en entornos en constante cambio.

Marco Conceptual

Red de Computadoras

Según Mendes (2020) indica que las redes informáticas son una forma estandarizada de interconectar ordenadores para compartir recursos físicos o lógicos, estos pueden incluir unidades de CD-ROM, directorios de disco duro, módems, GPON ONUs, impresoras, escáneres, unidades USB, etc. Por lo que resulta esencial que los profesionales de TI que busquen una buena posición en el mercado laboral sepan definir el tipo de red y de sistema operativo que deben utilizar, así como configurar este tipo de entorno.

Estas tecnologías web alcanzaron una etapa masiva cuando las computadoras comenzaron a extenderse en el mundo de los negocios y comenzaron a desarrollarse aplicaciones complejas multiusuario (navegación web, correo electrónico, bases de datos, redes sociales, blogs, Twitter, YouTube), gracias a que sus componentes comunes (hardware, software, infraestructura y accesorios) se pueden encontrar en cualquier tienda especializada en informática y los componentes provienen de decenas de fabricantes, es por esta razón que surgió un hecho interesante: la competencia entre fabricantes condujo a menores costos de componentes en la primera etapa, mientras que la competencia entre diferentes tiendas de informática condujo a un menor valor final. Además, los avances tecnológicos simplifican el proceso, facilitando el trabajo técnico y brindando más oportunidades, sin embargo, el costo y la compatibilidad de los equipos de red no siempre son económicos y flexibles para los administradores de red. (p.19)

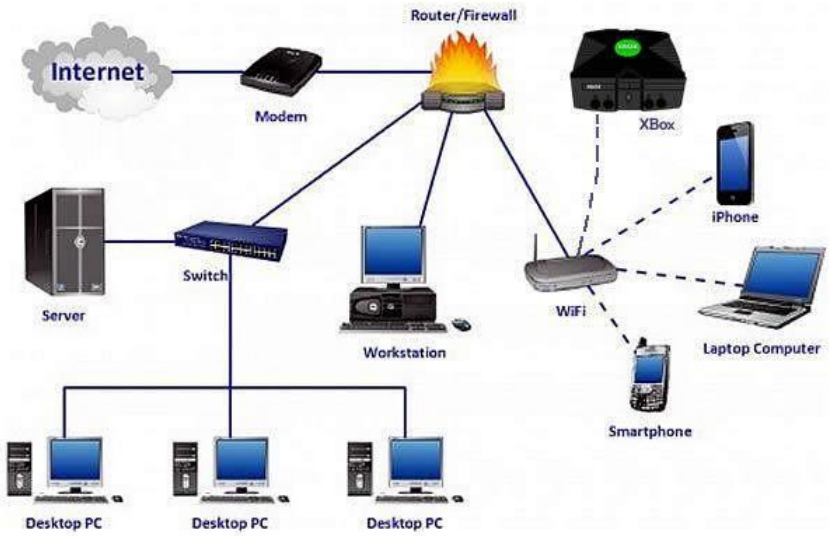


Figura 1. *Red de computadores doméstica*
Fuente: *Plotandesign*

Seguridad en Redes

Desde el punto de vista de Briceño (2021) se establece que podemos estar vulnerables a cualquier amenaza proveniente de diversos atacantes poniendo en peligro a alguna infraestructura o dispositivos de red mal configurado aunque la mayoría de la población mundial depende de las redes, la pérdida de conectividad de red y de los servicios proporcionados por dichas redes puede ser asfixiante en el mejor de los casos y devastadora para las empresas, por lo que han surgido varias formas de proteger la red y sus recursos frente a las diversas amenazas a las que se puede enfrentar, se puede aumentar la seguridad en términos de diseño de redes diseñando nuestras redes para que sean inherentemente más seguras y resistentes a ataques o fallas técnicas, a su vez es posible implementar diversos dispositivos en el borde (seguridad perimetral) y en la red, como firewalls y sistemas de detección de intrusos (IDS), para aumentar el nivel de seguridad.

La segmentación de la red puede reducir significativamente el impacto de dichos ataques, debido a que cuando segmentamos una red, la dividimos en varias redes más pequeñas, cada una

de las cuales actúa como su propia pequeña red llamada subred por lo que es posible controlar el tráfico entre subredes, permitir o denegar el tráfico en función de diversos factores e incluso bloquear el tráfico por completo si es necesario, ya que una red adecuadamente segmentada puede mejorar el rendimiento de la red al incluir parte del tráfico que realmente necesita ver partes de la red y puede ayudar a identificar problemas técnicos de la red. Además, la segmentación de la red evita que el tráfico de red no autorizado o los ataques lleguen a partes de la red que queremos evitar y facilita mucho la monitorización del tráfico de la red.

La mayoria de los firewalls que se utilizan hoy en día se basan en el concepto de inspeccionar los paquetes de datos a medida que pasan a través de la red, este análisis determina lo que se debe permitir entrar y salir, y esto puede basarse en varios factores y depende en gran medida de la complejidad del firewall. Por ejemplo, podemos permitir o bloquear el tráfico según el protocolo utilizado, permitiendo el paso del tráfico web y de correo electrónico pero bloqueando el resto del tráfico. (p.79)

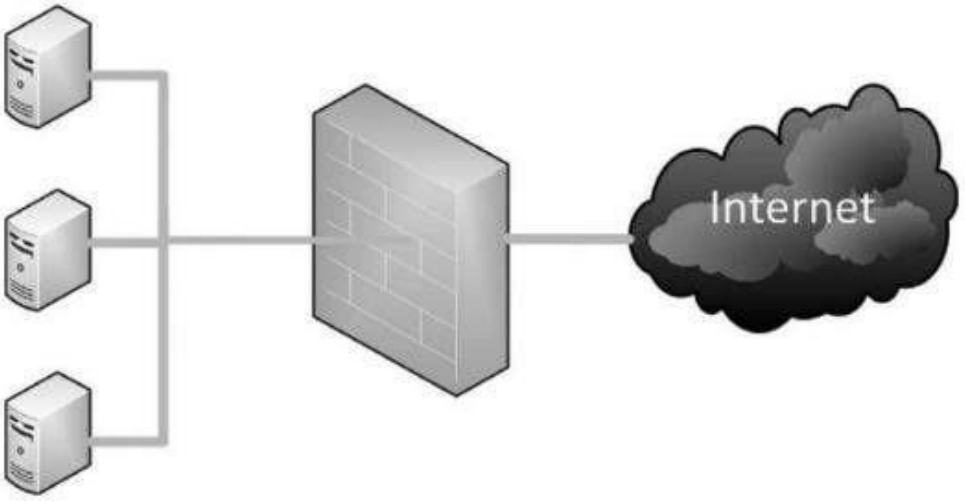


Figura 2. *Topología de Red con Firewall*
Fuente: *Researchgate*

Monitoreo de redes

La detección de errores a través del monitoreo de la red es primordial para poder brindar un buen servicio a los usuarios internos de una organización, por esta razón existe la necesidad de contar con un sistema de monitoreo de red, el cual se encarga de notificar fallas de la red, mostrar el rendimiento de la red mediante la recopilación y el análisis de datos que son puntos críticos para la detección temprana y la toma de decisiones.

Para ello, Villafuerte et al (2021) detallan que es imposible crear una red de telecomunicaciones óptima sin conocer la información sobre el tráfico que cruza la red, qué enlace satura el ancho de banda o qué servicio sobrecarga el servidor, porque el servidor o dispositivo puede caer en cualquier momento y detener los servicios indispensables para la comunicación de una organización o empresa, además especifican que la detección temprana de errores y el seguimiento de los elementos que componen la red informática son indispensables para dar un buen servicio a los usuarios, debido a que es importante contar con herramientas que puedan reportar fallas en la red y detectar su comportamiento a través del análisis y agregación del tráfico. (p.15)

Escaneo de Puertos

Como señala Hernández et al (2019) el escaneo de puertos es una técnica de prueba que intenta conocer qué servicios ofrece una red o servidor, analizando conexiones o intentando conectarse a diferentes puertos de la víctima, ya sea TCP o UDP, esperando respuesta de uno o más puertos y averiguando que servicio está escuchando en algún puerto, todo esto se da a través de una metodología de ataque que consta de seis fases: reconocimiento, escaneo, inventario, explotación, mantenimiento de acceso y eliminación de rastros, organizadas de tal manera que el

éxito de una fase garantiza un mejor escenario para la siguiente fase. Todas las herramientas, métodos y tiempo necesarios para completar cada tarea son muy importantes.

La fase de escaneo tiene cuatro objetivos principales: encontrar hosts activos, puertos abiertos, versiones de aplicaciones y sistemas operativos y otras vulnerabilidades de la red en caso de un ataque, es por este motivo que se recomiendan los sistemas proxy móviles para enriquecer el proceso de protección de puertas lógicas, al tratarse de sistemas heterogéneos muy extendidos que permiten la creación, interpretación, ejecución, transmisión y terminación de proxys.

Estos sistemas incluyen dos conceptos básicos: un servidor de recursos que puede tener uno o más sistemas de agentes, que a su vez pueden contener una o más ubicaciones, y los agentes pueden implementarse en una o más ubicaciones y tener capacidades de roaming para visitar sus recursos o comunicarse con otros agentes, también encontramos la movilidad de agentes, es decir su capacidad para migrar de una ubicación a otra es un diferenciador clave entre este enfoque y otras alternativas de desarrollo de sistemas distribuidos existentes, como la llamada a procedimiento remoto (RPC) o la evaluación remota (p.6).

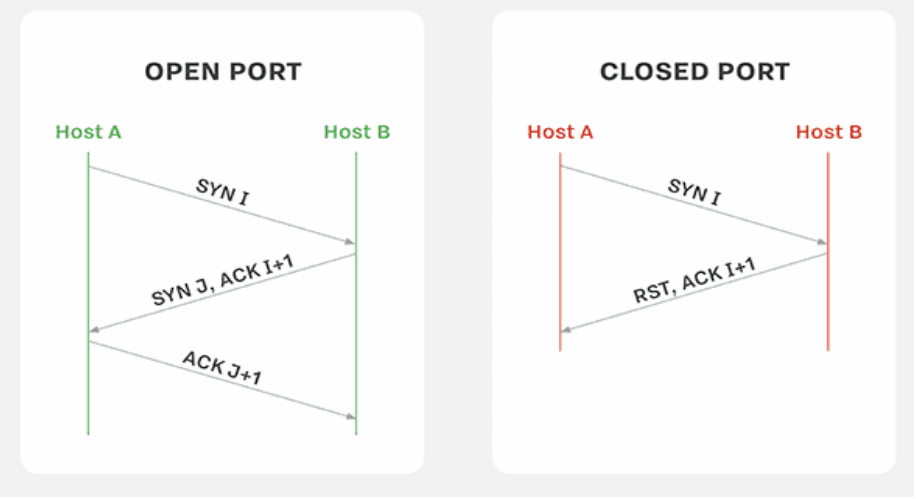


Figura 3. *Tecnicas de Escaneo de Puertos*
Fuente: *Techtarget*

Firewall

Teniendo en cuenta a Anwar et al (2021) los firewalls cumplen con una función primordial dentro de la seguridad y el acceso a los registros electrónicos, tanto dentro como fuera de la red y estos servicios están disponibles a través de la nube, debido a que los cortafuegos han sido durante mucho tiempo la primera línea de defensa en la seguridad de los sistemas, ya que un buen firewall siempre debe actuar como filtro entre el tráfico proveniente de la red interna (tráfico saliente) y el tráfico generado (tráfico entrante) desde redes externas y a menudo menos seguras (tráfico entrante) para proteger la red de ataques y riesgos externos, evitando así ataques a la red. (p. 9183)

Los Firewalls son fundamentales dentro de la seguridad de cualquier red, estos pueden ser de dos tipos: los cortafuegos de red los cuales se encargan de proporcionar seguridad entre redes y se ejecutan en el hardware de la red o los cortafuegos basados en host que son los que ayudan a filtrar el tráfico hacia los dispositivos finales o los hosts.

Desde el punto de vista de Mukkamala & Rajendran (2020) es importante conocer que anteriormente los cortafuegos funcionaban a partir de reglas que se configuraban estáticamente, como las listas de políticas de acceso, gracias al incremento de amenazas estas han tenido que evolucionar dinámicamente y reaccionar ante los diferentes peligros de la red, es por esta razón que distintos tipos de tecnologías Firework trabajan en diferentes capas del modelo TCP/IP (p.363)

Hacking Ético

Teniendo en cuenta a Avila (2019) el hacking ético es la capacidad de una persona de verificar la existencia de una brecha y se responsabiliza de la seguridad de los datos de una empresa para poder informar sobre la situación de seguridad de la empresa tras un análisis

completo, detectando así cuando se ha producido alguna brecha de seguridad y así poder proporcionar una rápida solución a la organización ante cualquier situación para proteger la información delicada de la empresa ante los actores maliciosos.

Una persona se considera un hacker ético si ayuda a mantener segura la empresa, tomándose muy en serio la protección de toda la información de la organización, evaluando la seguridad e identificando las vulnerabilidades en sistemas o infraestructuras de red, incluida la búsqueda y explotación de vulnerabilidades específicas para determinar si se ha producido un acceso no autorizado u otra actividad maliciosa. (p.2)

Figura 3. *Clasificación de sujetos que realizan las pruebas de penetración*
Fuente: *Revista Seguridad Unam*

De acuerdo con Llerena (2020) esto es lo que puede hacer un hacker:

Reconocimiento: los piratas informáticos realizan un reconocimiento pasivo antes de cualquier ataque y recopilan información sobre el objetivo del ataque para obtener información.

Escaneo: El escaneo puede realizar ataques de varias maneras, como por ejemplo redes, pero esto ya se hace usando la información del paso anterior.

Obtener acceso: Obtener acceso se refiere al ataque en sí, como explotar un error o una vulnerabilidad para obtener acceso a una contraseña.

Acceso de mantenimiento: Se refiere al mantenimiento continuo de los privilegios adquiridos.

Eliminación de pruebas: Eliminación de pruebas con lo que se puede descubrir. (p.119)

Figura 4. *Metodología completa del Hacking Etico*
Fuente: *Researchgate*

Herramientas de Escaneo de Puertos

Nmap

Según Calderon (2021) Nmap es una herramienta de auditoría de seguridad y descubrimiento de redes gratuita y de código abierto, la cual resulta muy útil a muchos administradores de sistemas y redes para tareas complejas como la supervisión del tiempo de actividad de hosts o servicios, la gestión de programas de actualización de servicios y el inventario de redes.

Debido a que Nmap emplea paquetes IP sin procesar este ofrece novedosas formas para determinar qué hosts están disponibles en la red o qué servicios ofrecen esos hosts, qué sistemas operativos y versiones de SO se están ejecutando, también qué tipo de filtros de paquetes o firewalls se utilizan, además de muchas otras características, por esta razón es importante aclarar que es capaz de escanear rápidamente grandes redes y funciona bien contra hosts específicos. (p.36)

Teniendo en cuenta a Sunny & Christy (2022) la GUI oficial del escáner de seguridad NMAP se llama Zenmap la cual es una herramienta gratuita y de código abierto diseñada para que NMAP sea fácil de usar para los principiantes, siendo compatible con la gran mayoria de sistemas operativos como Linux, Windows, Mac OS X. Zenmap proporciona una amplia funcionalidad para los expertos en mapeo de redes, ademas permite la reutiliacion de codigo gracias a que se pueden guardar como archivos de configuración los diversos análisis realizados. (p.921)

Escaneo de una web nmap	www.google.com
Escaneo de un rango de IPs nmap	192.168.0.1-100
Escanear toda una subnet nmap	192.168.0.1/24
Escáner desde un fichero de texto nmap	-iL fichero.txt
Escanear un rango de puertos nmap	-p 201-300 192.168.0.1
Escanear los puertos más utilizados nmap	-F 192.168.0.1
Escanear los 65535 puertos	-p 192.168.0.1

Tabla 1. *Principales usos de NMAP*
Fuente: *Elaboración Propia*

Unicornscan

Como opina Moniruzzaman et al (2019) Unicornscan es una herramienta que tiene como objetivo escanear grandes cantidades de redes proporcionando una eficiencia y velocidad bastante alta, debido a que es capaz de procesar escaneos simultáneos de puertos y protocolos de sitios web, lo que permite identificar servicios que se ejecutan en algún puerto específico, además de que no solo eso, sino que también puede procesar solicitudes Ping, SYN y otros tipos de exploración UDP, logrando realizar exploraciones de forma inesperada, lo que abre la posibilidad de comprobar la seguridad de la red sin usar la detección del cortafuegos.

El escaneo de puertos implica enviar paquetes a portadores abiertos y verificar la respuesta a las solicitudes SYN, lo que puede ser considerado como actividad sospechosa, esto también se considerará la posibilidad de un ataque de atacante durante este proceso de escaneo, ya que el atacante puede enviar datos cambiando el puerto utilizado para ejecutar el script. (p.6)

Escaneo de Puertos TCP	unicornscan -mT 192.168.0.1
Escaneo de Puertos UDP	unicornscan -mU 192.168.0.1
Detección de Servicios	unicornscan -mT -Iv 192.168.0.1:8080
Personalización Avanzada	unicornscan -mU -Iv -p 53,80,443 192.168.0.1
Escaneo de Rango IP	unicornscan 192.168.0.0/24

Tabla 2. *Principales usos de UnicornScan*
Fuente: *Elaboración Propia*

Netcat

De acuerdo con Kimosop (2021) Netcat es Instrumento empleado en la seguridad cibernética haciendo uso de líneas de códigos para poder enviar/recibir datos a través de una red, también es empleada generalmente por especialistas en el área de seguridad y por otras personas

como atacantes informáticos para realizar trabajos como el análisis del tráfico y otras características de la red, por esto es considera por muchos la navaja suiza de la tecnología de la información debido a que es una herramienta que dispone de una gran capacidad de utilidades que dan paso a la creación de casi cualquier tipo de conexión de red.

Netcat en sus inicios fue creado simplemente para diseñar y abrir una conexión ya sea de tipo UDP/TCP entre dos ordenadores desde cualquier puerto deseado sin ningún inconveniente, pero debido al gran avance del tiempo y la repentina aparición de nuevas herramientas con muchas funcionalidades similares se vio obligado a incluir nuevas características y funciones como lo son el escaneo de puertos, el reenvío de puertos o la transferencia de archivos y control remoto.

Netcat también se puede emplearse como un dispositivo backend que otros programas o scripts pueden utilizar o administrar sin ningún inconveniente, ya que, al ser una herramienta imprescindible para los probadores de penetración, esta es esencial para la investigación y la resolución de problemas de la red.

Transferencia de Datos	- En el servidor: nc -l -p 12345 - En el cliente: nc 192.168.0.100 12345
Escaneo de Puertos	nc -vz 192.168.0.200 80
Establecimiento de Conexiones	- TCP: nc -v 192.168.0.150 8080 - UDP: nc -u -v 192.168.0.175 514
Chat de Red	- En el servidor: nc -l -p 7777 - En el cliente: nc 192.168.0.50 7777
Escucha de Puertos	nc -l -p 9999

Tabla 3. *Principales usos de NetCat*
Fuente: *Elaboración Propia*

Técnicas de Escaneo

Escaneo TCP SYN

Como señalan Sunny & Christy (2022) esta técnica de escaneo consiste en simular una apertura activa al enviar un segmento SYN a un puerto específico de la máquina destino, si esta obtiene una respuesta de tipo RST (bit utilizado para reiniciar la conexión) esto quiere decir que el puerto objetivo está realmente a la escucha; caso contrario, si recibe un segmento SYN | ACK, el puerto de destino se cierra y se revisa algún nuevo puerto para comprobar si está programado, para esto se envía de vuelta al objetivo un segmento RST para poder finalizar el establecimiento de la conexión, por esta razón es que se conoce a esta técnica como "escaneo medio abierto" porque no se establecen conexiones completas durante el escaneo SYN.

Aunque para algunos loggers como tcplogger esta técnica puede ser reconocida y detectada, la principal ventaja del escaneo SYN es que las conexiones incompletas se registran con más frecuencia que los intentos de conexión SYN, mientras que la contrapartida de esto es que el remitente debe construir a medida todo el paquete IP, lo cual muchas veces requiere del acceso de superusuario del sistema para así poder generar estos paquetes SYN a medida. (p.922)

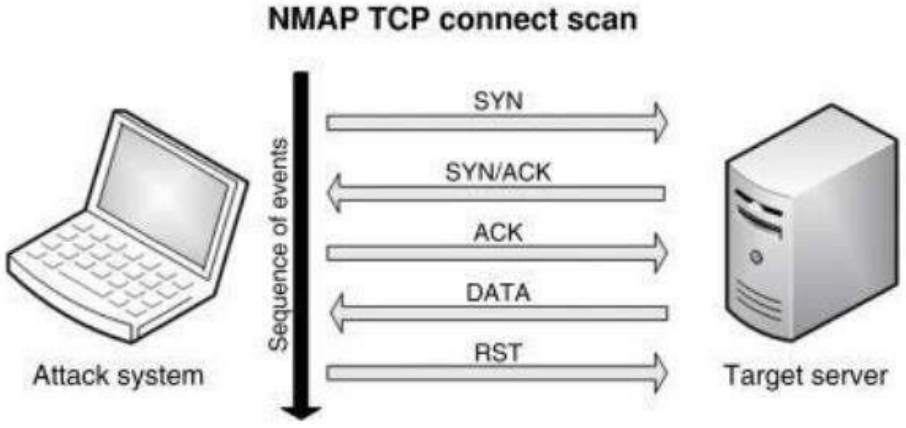


Figura 5. *Escaneo de conexión TCP NMAP*
Fuente: *Journal of Pharmaceutical Negative Results*

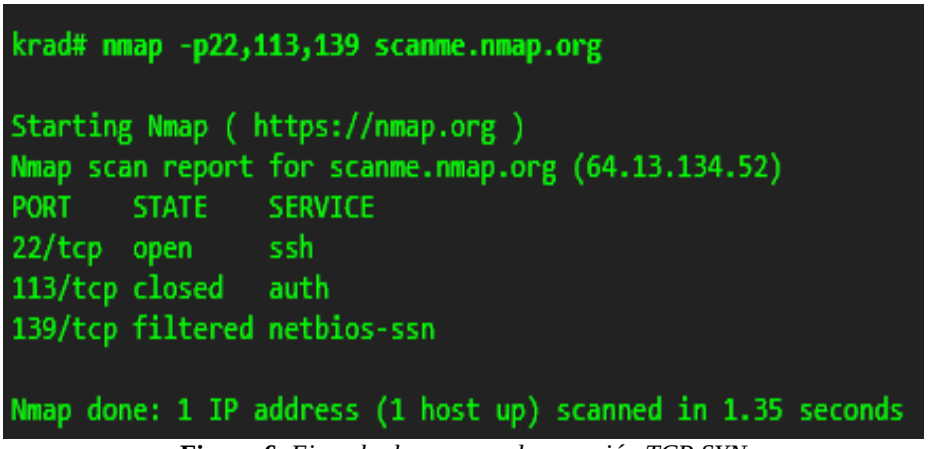


Figura 6. *Ejemplo de escaneo de conexión TCP SYN*
Fuente: *Nmap*

Escaneo no sigiloso (TCP Connect)

De acuerdo con Upadhya & Srinivas (2020) un escaneo no sigiloso emplea el método de conexión TCP, el cual realiza un protocolo de enlace completo de tres vías (three way handshake) con el host, por lo que cuando un cliente requiere realizar una conexión con un servidor, este primero envía un paquete TCP con el numero indicador de secuencia síncrono (SYN), si el puerto del servidor está abierto, este devuelve un paquete TCP con todos los indicadores SYN y ACK también conocidos como indicadores de confirmación o envía un paquete de reinicio si el puerto está cerrado.

El escaneo de puertos TCP se puede hacer con diferentes herramientas, como Nmap y hping2 las cuales utilizan el método TCP connect(), que se encarga de establecer una conexión con el host de destino. El método connect() hace una llamada proporcionada por el sistema operativo para abrir una conexión con un host remoto donde la ventaja de este método es que no requiere muchos permisos especiales del sistema, pero la desventaja es que la actividad de escaneo es muy visible para los administradores. (p.3018)

```
krad~> nmap -T4 -sT scanme.nmap.org

Starting Nmap ( https://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Not shown: 994 filtered ports
PORT    STATE  SERVICE
22/tcp  open   ssh
25/tcp  closed smtp
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http
113/tcp closed auth

Nmap done: 1 IP address (1 host up) scanned in 4.74 seconds
```

Figura 7. *Ejemplo de escaneo TCP Connect*
Fuente: *Nmap*

Escaneo UDP

Como señala Aliaga (2021) aunque la mayoría de los servicios más populares de Internet funcionan a través del protocolo TCP, los servicios UDP están muy extendidos, puesto a que el escaneo UDP es generalmente más lento y más difícil que el TCP, algunos auditores de seguridad ignoran estos puertos, pero esto se considera un error, debido a que los servicios UDP explotables son bastante comunes y los atacantes ciertamente no ignoran todo el protocolo.

Dependiendo del uso, este escaneo funciona enviando un paquete vacío o un paquete diferente por puerto, en el caso de que el puerto está cerrado, se recibe una respuesta, en cambio, si el puerto está abierto o filtrado, no se envía ninguna respuesta al emisor (p.25)

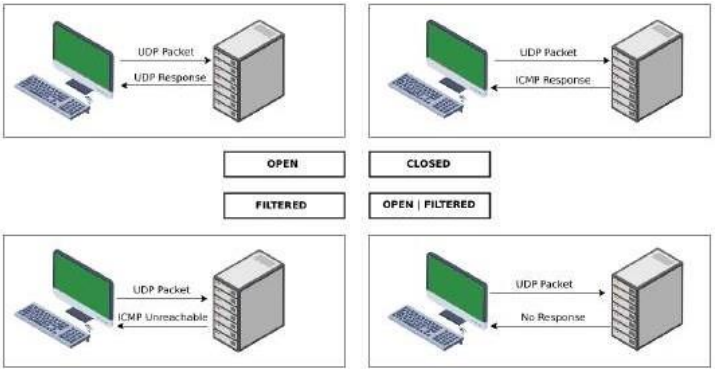


Figura 8. *Funcionamiento del escaneo UDP*
Fuente: *Geeksforgeeks*

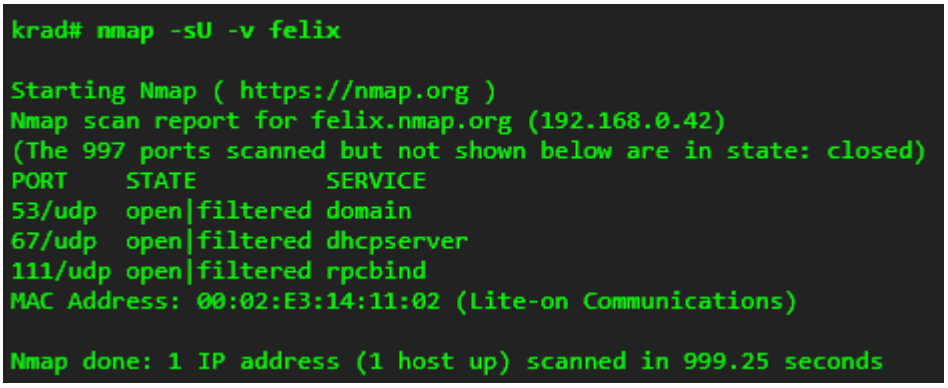


Figura 9. *Ejemplo de escaneo UDP*
Fuente: *Nmap*

Banner Grabbing

Según Khan et al (2020) banner Grabbing es el método que recopila información textual sobre dispositivos móviles y computadoras, el uso de este también puede compartir información sobre la red y los puertos abiertos con los que se conecta el dispositivo, por lo que se la puede utilizar para obtener la lista de todos los dispositivos conectados a una red específica ya sea para hacer un inventario o para comprobar los recursos y servicios de la red que utilizan, además de eso esta técnica se puede utilizar para obtener información sobre los hosts, el uso de protocolos, los puertos abiertos, el sistema operativo que se ejecuta en el host, la versión y los detalles de las aplicaciones.

Los protocolos de capa de aplicación, que incluyen HTTPS, FTP y SMTP en los puertos 80, 20 y 25, se utilizan para recopilar información sobre las aplicaciones y su versión, así como los detalles del sistema operativo, la captura de banners de dispositivos se puede realizar con herramientas como Nmap, telnet, zmap y netcat, que generalmente funcionan en el entorno Linux (p.5)

Marco Metodológico

Se utilizará un enfoque de investigación exploratorio y descriptivo debido a que, al realizar un análisis técnico comparativo de diferentes herramientas de escaneo de puertos en redes de telecomunicaciones, es necesario realizar una revisión integral de diversos textos relacionados con este campo. como trabajos de investigación, libros, revistas científicas o estudios de casos, también se utilizarán métodos de investigación cualitativos donde se realizarán una serie de entrevistas a diversos expertos en el área de la red para enriquecer el contenido del trabajo de investigación.

La comprensión de diversos textos que están estrechamente relacionados con el contenido del análisis establecerá una base sólida de conocimiento teórico y contextual sobre el tema, que luego producirá una variedad de ejemplos sobre cómo implementar estas herramientas (Nmap, UnicornScan y Netcat) y probado en redes de telecomunicaciones con el objetivo de aportar a la investigación información útil sobre la aplicación y uso de estas herramientas en problemas de la vida real.

Además se realizarán una serie de entrevistas a especialistas en el área o personal que previamente conoce y ha ocupado estas herramientas en sus lugares de trabajo puesto que las diferentes percepciones y experiencias de estos especialistas sobre la eficacia, la facilidad de uso y las diversas limitaciones de estas herramientas serán analizadas en estas entrevistas, identificando así patrones de la información recopiladas en la revisión bibliográfica, empleando diversas técnicas para organizar y analizar los datos recopilados de manera eficiente.

Resultados

Después de realizar un análisis comparativo de las herramientas de escaneo de puertos de redes de telecomunicaciones Nmap, UnicornScan y Netcat respectivamente, se obtuvieron varios resultados según diferentes criterios, como facilidad de uso, funciones adicionales o precisión del análisis. Estos resultados se presentan a continuación en la siguiente sección.

Criterios	Nmap	UnicornScan	Netcat
Precisión en la detección de puertos	Alta	Alta	Media
Velocidad de escaneo	Media-Alta	Alta	Media-Alta
Detección de vulnerabilidades	Sí	Sí	No
Facilidad de uso	Media	Media	Alta
Funcionalidades adicionales	Amplia variedad de funciones.	Algunas características adicionales.	Transmisión de datos.
Capacidad de escaneo de puertos	Escaneo completo y personalizado.	Escaneo completo y detección de servicios.	Escaneo básico de puertos.
Integración con otras herramientas	Sí	No	Sí

Tabla 4. *Diferentes Criterios de Evaluación de las herramientas de Escaneo*
Fuente: *Elaboración Propia*

Se descubrió que en términos de velocidad de escaneo, Nmap y UnicornScan son las alternativas rápidas, siendo UnicornScan especialmente la más rápida, pero esta velocidad de escaneo puede afectar un poco la precisión de la detección porque, de hecho, UnicornScan comenzó a omitir algunos servicios y esto se debió a que basado en análisis de paquetes, mientras que Nmap identificó servicios y puertos con alta precisión, incluso en modo sigiloso, lo que demuestra el equilibrio entre velocidad y precisión.

Herramienta	Tiempo promedio de escaneo (segundos)	Detección de servicios (%)
Nmap	83.05	95
UnicornScan	60.12	80
Netcat	273.21	70

Tabla 5. *Velocidad de Escaneo*
Fuente: *Elaboración Propia*

Herramienta	Falsos Positivos (%)	Falsos Negativos (%)
Nmap	5	3
UnicornScan	10	8
Netcat	8	12

Tabla 6. *Precisión de Detección*
Fuente: *Elaboración Propia*

También se encontró que Nmap puede requerir un mayor nivel de comprensión que otras herramientas para aprovechar al máximo sus características, ya que ofrece muchas opciones en términos de configuración y formato de resultados, al igual que UnicornScan requiere mayores conocimientos para una configuración correcta y finalmente, aunque Netcat es más fácil de usar, carece de muchas características de otras herramientas, ya que Nmap se destaca por muchas técnicas de análisis, flexibilidad y funcionalidad mientras que UnicornScan se enfoca en escaneos rápidos sin ofrecer muchas opciones de personalización.

Herramienta	Nivel de dificultad	Flexibilidad	Funcionalidades clave
Nmap	Moderado	Alta	Escaneo completo, detección de servicios, scripting
UnicornScan	Fácil	Media	Escaneo rápido, análisis de topología

Netcat	Difícil	Baja	Escaneo básico, conectividad de puertos

Tabla 7. *Facilidad de Uso y Funcionalidades*
Fuente: *Elaboración Propia*

Cuando se busca un equilibrio entre velocidad y precisión en auditorías de seguridad, Nmap resulta ser la opción preferida en cuanto a su utilización en los escenarios de uso recomendados, después, aunque puede perder un poco de precisión UnicornScan resulta ser útil en situaciones donde la velocidad es fundamental, mientras que Netcat carece de las capacidades avanzadas de las otras herramientas, pero es útil en tareas básicas de transferencia de datos y pruebas de conectividad, es por esta razón que muchos de los profesionales de seguridad y redes deben considerar el contexto y los objetivos específicos al elegir la herramienta más adecuada para un análisis de escaneo de puertos en redes de telecomunicaciones.

Escenario de Uso	**Herramienta Recomendada**
Escenario 1	Nmap
Escenario 2	UnicornScan
Escenario 3	Netcat

Tabla 8. *Escenarios de Uso Recomendados*
Fuente: *Elaboración Propia*

Discusión de Resultados

Este análisis técnico comparativo de herramientas de escaneo de puertos como Nmap, UnicornScan y Netcat se puede realizar con precisión, arrojando resultados muy interesantes y claros que efectivamente se alinean con los conceptos previamente especificados en el marco conceptual, ya que se pueden encontrar diferentes conceptos. coincidencias y diferencias significativas al comparar los resultados obtenidos con las expectativas establecidas en el marco conceptual.

En primer lugar, se ha demostrado y comprobado que la velocidad de escaneo es un factor clave e importante en la evaluación de estas herramientas, pues según el marco conceptual, la velocidad de escaneo es el punto básico para encontrar potenciales vulnerabilidades en tiempo real y así asegurar una respuesta rápida ante sospechas, es por esta razón que los resultados del análisis son consistentes con esta premisa porque en comparación con UnicornScan y Netcat, Nmap, es conocido por sus excelentes y completas capacidades de análisis, como lo demostró en la prueba donde mostró una velocidad de reacción menor que el tiempo promedio de escaneo, lo que confirma la importancia de considerar la velocidad al seleccionar el motor de escaneo.

En términos de precisión en el descubrimiento de servicios, esto cumple con las expectativas del marco conceptual, ya que en la comparación actual con UnicornScan y Netcat, Nmap muestra nuevamente una tasa de detección más alta debido a su enfoque en la detección ya que la detección precisa es esencial para identificar eficazmente diversas vulnerabilidades y tomar decisiones para mejorar la ciberseguridad.

Aun así, todavía surgen dudas en cuanto al aspecto de facilidad de uso y diversas funcionalidades, ya que en el marco conceptual se enfatizó que las herramientas analíticas deben

ser fáciles de usar y flexibles, aunque Nmap tiene tantas características, los resultados muestran su dificultad para usuarios con poca experiencia en el campo. Por otro lado, UnicornScan destaca por su facilidad de uso, pero en comparación con otras herramientas, algunas de sus características son menos adaptables al entorno. Estos resultados muestran que, si bien la funcionalidad es importante al utilizar herramientas, también se debe considerar la facilidad de uso en función de las habilidades y necesidades del usuario.

Conclusiones

El análisis técnico comparativo de las diferentes herramientas de escaneo de puertos como Nmap, UnicornScan y Netcat mostraron resultados que destacan su importancia de considerar una variedad de factores al elegir la herramienta adecuada para realizar una evaluación de seguridad de las redes de telecomunicaciones, puesto que factores como la velocidad de escaneo, la precisión de detección y la facilidad de uso juegan un papel fundamental en la toma de decisiones.

Nmap demostró ser una herramienta rápida y eficiente en los términos de velocidad de escaneo y esto coincide con la necesidad de identificar vulnerabilidades en tiempo real para mantener la seguridad e integridad de las redes, pero es importante tener en cuenta que aunque Nmap es poderoso y variado, esto juega un papel negativo debido a que su interfaz puede resultar complicada de usar para usuarios menos experimentados, por otro lado UnicornScan resaltó su facilidad de uso aunque algunas de sus funciones avanzadas pueden ser algo limitadas, mientras que la velocidad de escaneo de Netcat fue comparable a la de Nmap, pero su enfoque en las pruebas de conectividad podría no ser tan completo en aspecto de la detección de servicios.

Debido a su enfoque principal está basado en la realización de esta tarea, Nmap se benefició de la precisión en la detección de servicios, puesto que es un aspecto crucial para identificar posibles vulnerabilidades, aunque UnicornScan y Netcat mostraron habilidades de detección aceptables, lo que indica que la elección de la herramienta debe basarse en las necesidades específicas de la red y la profundidad del análisis.

Recomendaciones

Nmap se recomienda para ser utilizado en entornos donde la identificación rápida de vulnerabilidades sea un aspecto fundamental como en redes críticas o redes de alta demanda, ya que destaca por su velocidad de escaneo, sin embargo, para evitar posibles inconvenientes también es importante tener en cuenta los efectos en el rendimiento de la red para así poder ajustar la configuración de Nmap según sea necesario.

UnicornScan es la herramienta ideal para realizar los diferentes análisis preliminares o para ser utilizado en redes menos complejas debido a que es simple y rápido, sin embargo, se recomienda que los usuarios con menos experiencia en el área reciban una formación básica sobre la funcionalidad y diversos aspectos de la herramienta para que así puedan aprovechar todo el provecho a su funcionalidad.

Se recomienda utilizar la herramienta Nmap en escenarios donde los análisis requieran una exploración completa de la red, además de una identificación precisa de vulnerabilidades, ya que demostró tener una mayor precisión en la detección de servicios, pero para obtener un panorama aún más completo y asegurarse de no pasar por alto posibles puntos de riesgo, se recomienda combinar esta herramienta con otras soluciones.

Referencias

Aliaga, L. J. (2021). *Modelo para la detección de escaneo de puertos de la computadora en una red Wlan*. Obtenido de Universidad Mayor De San Andrés Facultad De Ciencias Puras Y Naturales Carrera De Informática: https://repositorio.umsa.bo/bitstream/handle/123456789/29646/T-3864.pdf?sequence=1&isAllowed=y

Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall Best Practices for Securing Smart Healthcare Environment: A Review. *Applied Sciences*, 9183.

Arteaga, S., Martínez, J., Mura, J., & Fernández, M. (Octubre de 2018). Seguridad en Redes. Naguanagua, Venezuela.

Avila, M. A. (2019). Hacking ético: impacto en la sociedad. *Universidad Piloto de Colombia*, 9.

Briceño, E. V. (2021). *Seguridad de la información.* 3Ciencias.

Calderon, P. (2021). *Nmap Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips.* Packt Publishing Ltd.

ElectrónicaOnline. (17 de Junio de 2020). *Telecomunicación es comunicación a distancia utilizando señales eléctricas u ondas electromagnéticas*. Obtenido de ElectrónicaOnline: https://electronicaonline.net/telecomunicaciones/redes-y-sistemas-de-telecomunicaciones/

Grupo Atico34. (Julio de 2021). *Escaneo de puertos. ¿Para qué se hace?* Obtenido de https://protecciondatos-lopd.com/empresas/escaneo-de-puertos/#Que_es_el_escaneo_de_puertos

Hernández, J. A., Cobos, R. A., & Wanumen, L. F. (2019). Arquitectura para escaneo de puertos usando agentes móviles. *Visión Electrónica, algo más que un estado sólido*, 23.

Khan, A., Chen, Y., Ahmad, W., Javed, K., & Khan, A. (2020). Monitoring and Detection of Security Events through IoT Device Identification Using Application Layer Protocols. *International Journal of Hybrid Information Technology*, 1–16.

Kimosop, M. (21 de Octubre de 2021). *Introduction to NetCat*. Obtenido de Section: https://www.section.io/engineering-education/introduction-to-netcat/

Kurose, J. (2017). *Computer Networking: A Top-Down Approach (7th ed.).* Pearson.

Llerena, A. E. (2020). Herramientas fundamentales para el hacking ético. *Revista Cubana de Informática Médica*, 116-131.

Mendes, D. R. (2020). *Redes de Computadores: Teoria e Prática.* Novatec Editora.

Moniruzzaman, M., Chowdhury, F., & Ferdous, M. S. (2019). Measuring Vulnerabilities of Bangladeshi Websites. *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, 1-7.

Mukkamala, P. P., & Rajendran, S. (2020). A Survey On The Different Firewall Technologies. *International Journal of Engineering Applied Sciences and Technology*, 363-365.

Pinheiro, . N., Oliveira, J. P., & Vieira, P. R. (2018). *NMAP*. Obtenido de FACULDADE SENAC GOIÁS CURSO DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO FUNDAMENTOS DE TECNOLOGIA DA INFORMAÇÃO: https://jpjoaonasc.github.io/files/modulo1/Mapeamento.pdf

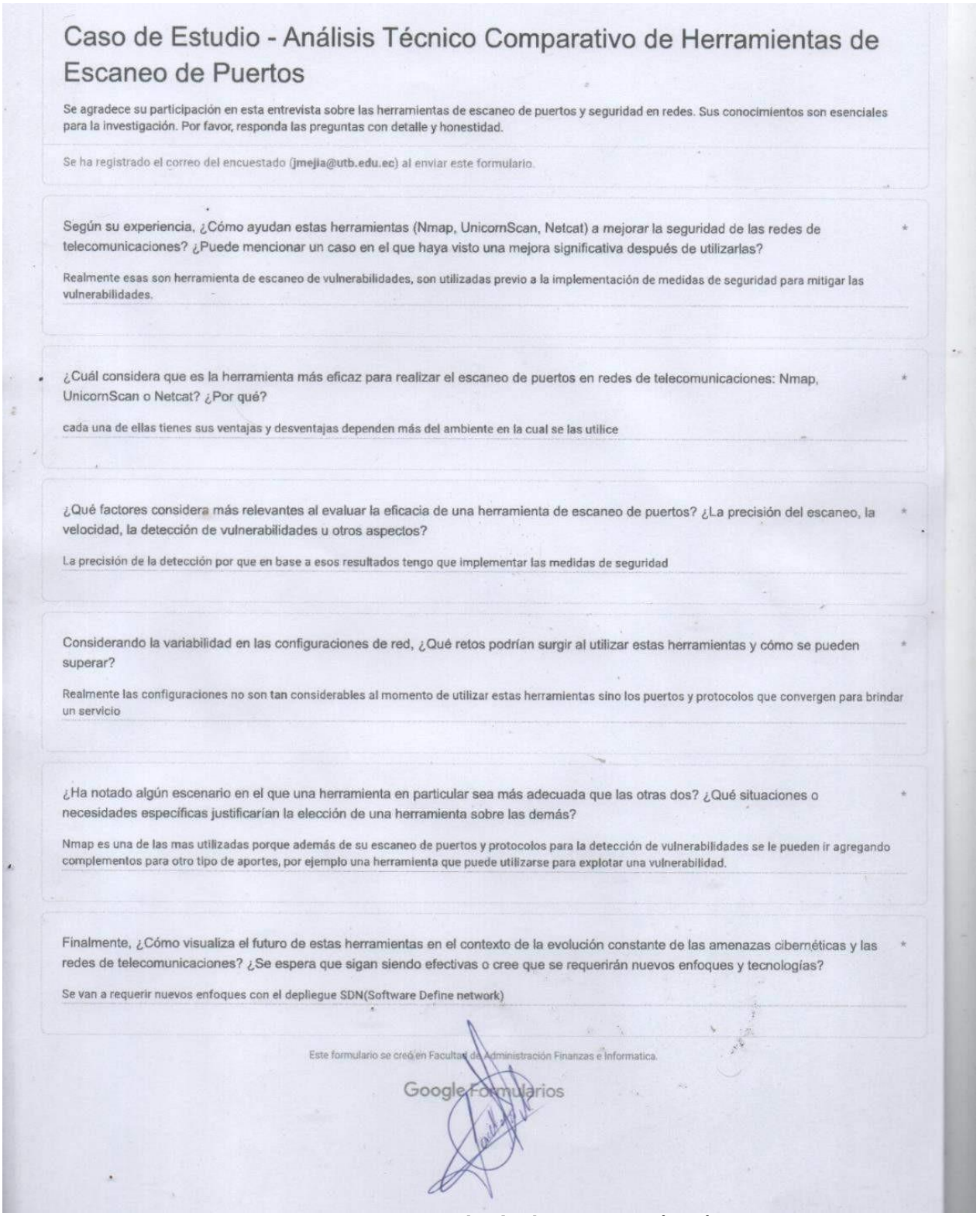
Soriano, A. G. (2018). *Hacking ético: mitos y realidades*. Obtenido de Revista .Seguridad: https://revista.seguridad.unam.mx/numero-12/hacking-%C3%A9tico-mitos-y-realidades

Sunny, S., & Christy, A. G. (2022). Comparison of TCP scanning techniques using nmap. *Journal of Pharmaceutical Negative Results*, 919-925.

Upadhya, A., & Srinivas, B. K. (2020). A Survey on different Port Scanning Methods and the Tools used to perform them. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 3018-3024.

Villafuerte, C. J., Vélez, G. M., & Tapia, J. H. (2021). Herramientas de código abierto para el monitoreo de redes LAN. *Revista Científica de Informática ENCRIPTAR*, 26-39.

Anexos



Caso de Estudio - Análisis Técnico Comparativo de Herramientas de Escaneo de Puertos

Se agradece su participación en esta entrevista sobre las herramientas de escaneo de puertos y seguridad en redes. Sus conocimientos son esenciales para la investigación. Por favor, responda las preguntas con detalle y honestidad.

Se ha registrado el correo del encuestado (**jmejia@utb.edu.ec**) al enviar este formulario.

Según su experiencia, ¿Cómo ayudan estas herramientas (Nmap, UnicornScan, Netcat) a mejorar la seguridad de las redes de telecomunicaciones? ¿Puede mencionar un caso en el que haya visto una mejora significativa después de utilizarlas? *

Realmente esas son herramienta de escaneo de vulnerabilidades, son utilizadas previo a la implementación de medidas de seguridad para mitigar las vulnerabilidades.

¿Cuál considera que es la herramienta más eficaz para realizar el escaneo de puertos en redes de telecomunicaciones: Nmap, UnicornScan o Netcat? ¿Por qué? *

cada una de ellas tienes sus ventajas y desventajas dependen más del ambiente en la cual se las utilice

¿Qué factores considera más relevantes al evaluar la eficacia de una herramienta de escaneo de puertos? ¿La precisión del escaneo, la velocidad, la detección de vulnerabilidades u otros aspectos? *

La precisión de la detección por que en base a esos resultados tengo que implementar las medidas de seguridad

Considerando la variabilidad en las configuraciones de red, ¿Qué retos podrían surgir al utilizar estas herramientas y cómo se pueden superar? *

Realmente las configuraciones no son tan considerables al momento de utilizar estas herramientas sino los puertos y protocolos que convergen para brindar un servicio

¿Ha notado algún escenario en el que una herramienta en particular sea más adecuada que las otras dos? ¿Qué situaciones o necesidades específicas justificarían la elección de una herramienta sobre las demás? *

Nmap es una de las mas utilizadas porque además de su escaneo de puertos y protocolos para la detección de vulnerabilidades se le pueden ir agregando complementos para otro tipo de aportes, por ejemplo una herramienta que puede utilizarse para explotar una vulnerabilidad.

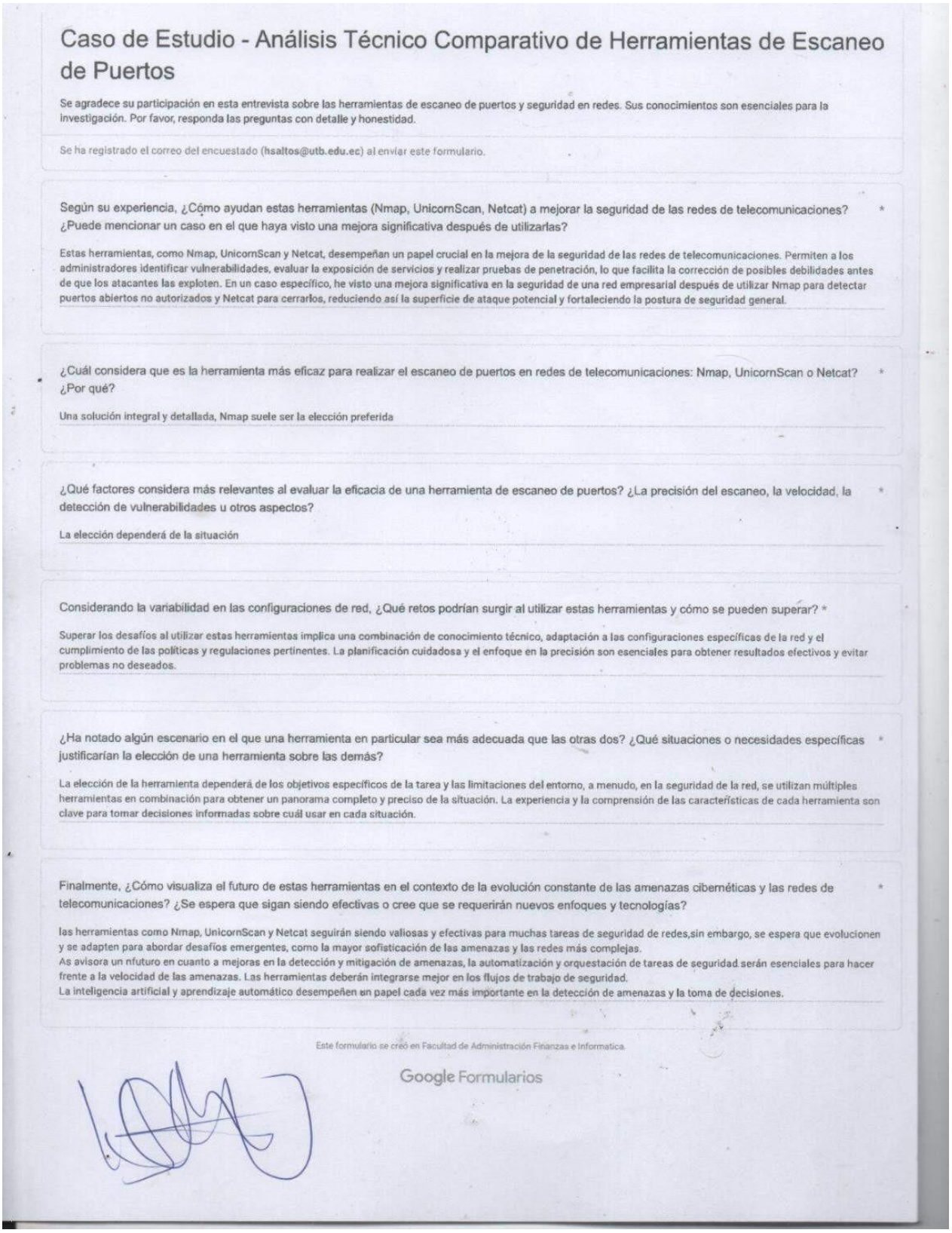
Finalmente, ¿Cómo visualiza el futuro de estas herramientas en el contexto de la evolución constante de las amenazas cibernéticas y las redes de telecomunicaciones? ¿Se espera que sigan siendo efectivas o cree que se requerirán nuevos enfoques y tecnologías? *

Se van a requerir nuevos enfoques con el depliegue SDN(Software Define network)

Este formulario se creó en Facultad de Administración Finanzas e Informatica.

Google Formularios

Anexo 1. *Entrevista Realizada al Ingeniero José Mejía*
Fuente: *Elaboración Propia*



Caso de Estudio - Análisis Técnico Comparativo de Herramientas de Escaneo de Puertos

Se agradece su participación en esta entrevista sobre las herramientas de escaneo de puertos y seguridad en redes. Sus conocimientos son esenciales para la investigación. Por favor, responda las preguntas con detalle y honestidad.

Se ha registrado el correo del encuestado (**hsaltos@utb.edu.ec**) al enviar este formulario.

Según su experiencia, ¿Cómo ayudan estas herramientas (Nmap, UnicornScan, Netcat) a mejorar la seguridad de las redes de telecomunicaciones? ¿Puede mencionar un caso en el que haya visto una mejora significativa después de utilizarlas? *

Estas herramientas, como Nmap, UnicornScan y Netcat, desempeñan un papel crucial en la mejora de la seguridad de las redes de telecomunicaciones. Permiten a los administradores identificar vulnerabilidades, evaluar la exposición de servicios y realizar pruebas de penetración, lo que facilita la corrección de posibles debilidades antes de que los atacantes las exploten. En un caso específico, he visto una mejora significativa en la seguridad de una red empresarial después de utilizar Nmap para detectar puertos abiertos no autorizados y Netcat para cerrarlos, reduciendo así la superficie de ataque potencial y fortaleciendo la postura de seguridad general.

¿Cuál considera que es la herramienta más eficaz para realizar el escaneo de puertos en redes de telecomunicaciones: Nmap, UnicornScan o Netcat? ¿Por qué? *

Una solución integral y detallada, Nmap suele ser la elección preferida

¿Qué factores considera más relevantes al evaluar la eficacia de una herramienta de escaneo de puertos? ¿La precisión del escaneo, la velocidad, la detección de vulnerabilidades u otros aspectos? *

La elección dependerá de la situación

Considerando la variabilidad en las configuraciones de red, ¿Qué retos podrían surgir al utilizar estas herramientas y cómo se pueden superar? *

Superar los desafíos al utilizar estas herramientas implica una combinación de conocimiento técnico, adaptación a las configuraciones específicas de la red y el cumplimiento de las políticas y regulaciones pertinentes. La planificación cuidadosa y el enfoque en la precisión son esenciales para obtener resultados efectivos y evitar problemas no deseados.

¿Ha notado algún escenario en el que una herramienta en particular sea más adecuada que las otras dos? ¿Qué situaciones o necesidades específicas justificarían la elección de una herramienta sobre las demás? *

La elección de la herramienta dependerá de los objetivos específicos de la tarea y las limitaciones del entorno, a menudo, en la seguridad de la red, se utilizan múltiples herramientas en combinación para obtener un panorama completo y preciso de la situación. La experiencia y la comprensión de las características de cada herramienta son clave para tomar decisiones informadas sobre cuál usar en cada situación.

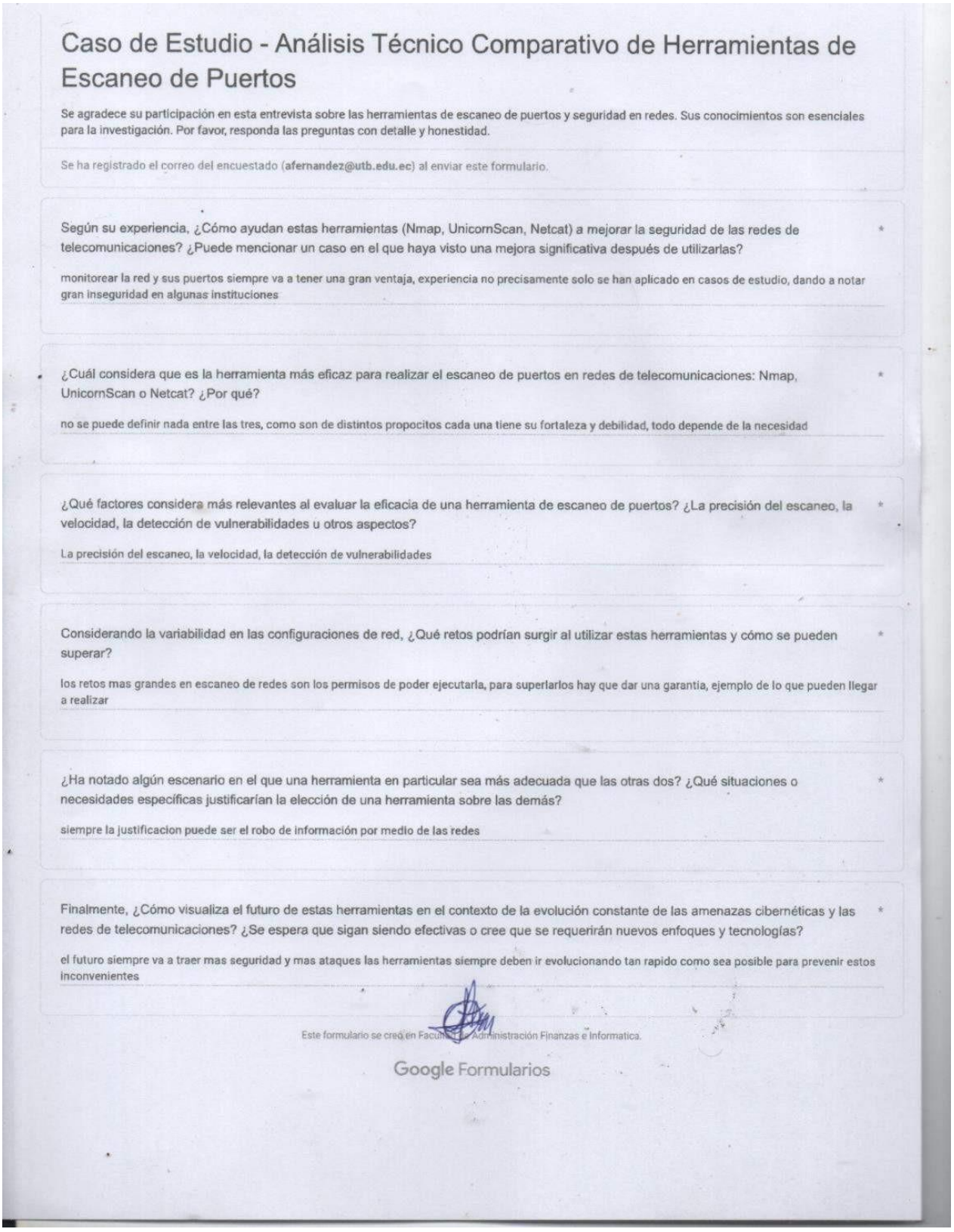
Finalmente, ¿Cómo visualiza el futuro de estas herramientas en el contexto de la evolución constante de las amenazas cibernéticas y las redes de telecomunicaciones? ¿Se espera que sigan siendo efectivas o cree que se requerirán nuevos enfoques y tecnologías? *

las herramientas como Nmap, UnicornScan y Netcat seguirán siendo valiosas y efectivas para muchas tareas de seguridad de redes,sin embargo, se espera que evolucionen y se adapten para abordar desafíos emergentes, como la mayor sofisticación de las amenazas y las redes más complejas.
As avisora un nfuturo en cuanto a mejoras en la detección y mitigación de amenazas, la automatización y orquestación de tareas de seguridad serán esenciales para hacer frente a la velocidad de las amenazas. Las herramientas deberán integrarse mejor en los flujos de trabajo de seguridad.
La inteligencia artificial y aprendizaje automático desempeñen un papel cada vez más importante en la detección de amenazas y la toma de decisiones.

Este formulario se creó en Facultad de Administración Finanzas e Informatica.

Google Formularios

Anexo 2. *Entrevista Realizada al Ingeniero Harry Saltos*
Fuente: *Elaboración Propia*



Caso de Estudio - Análisis Técnico Comparativo de Herramientas de Escaneo de Puertos

Se agradece su participación en esta entrevista sobre las herramientas de escaneo de puertos y seguridad en redes. Sus conocimientos son esenciales para la investigación. Por favor, responda las preguntas con detalle y honestidad.

Se ha registrado el correo del encuestado (**afernandez@utb.edu.ec**) al enviar este formulario.

Según su experiencia, ¿Cómo ayudan estas herramientas (Nmap, UnicornScan, Netcat) a mejorar la seguridad de las redes de telecomunicaciones? ¿Puede mencionar un caso en el que haya visto una mejora significativa después de utilizarlas? *

monitorear la red y sus puertos siempre va a tener una gran ventaja, experiencia no precisamente solo se han aplicado en casos de estudio, dando a notar gran inseguridad en algunas instituciones

¿Cuál considera que es la herramienta más eficaz para realizar el escaneo de puertos en redes de telecomunicaciones: Nmap, UnicornScan o Netcat? ¿Por qué? *

no se puede definir nada entre las tres, como son de distintos propocitos cada una tiene su fortaleza y debilidad, todo depende de la necesidad

¿Qué factores considera más relevantes al evaluar la eficacia de una herramienta de escaneo de puertos? ¿La precisión del escaneo, la velocidad, la detección de vulnerabilidades u otros aspectos? *

La precisión del escaneo, la velocidad, la detección de vulnerabilidades

Considerando la variabilidad en las configuraciones de red, ¿Qué retos podrían surgir al utilizar estas herramientas y cómo se pueden superar? *

los retos mas grandes en escaneo de redes son los permisos de poder ejecutarla, para superlarlos hay que dar una garantia, ejemplo de lo que pueden llegar a realizar

¿Ha notado algún escenario en el que una herramienta en particular sea más adecuada que las otras dos? ¿Qué situaciones o necesidades específicas justificarían la elección de una herramienta sobre las demás? *

siempre la justificacion puede ser el robo de información por medio de las redes

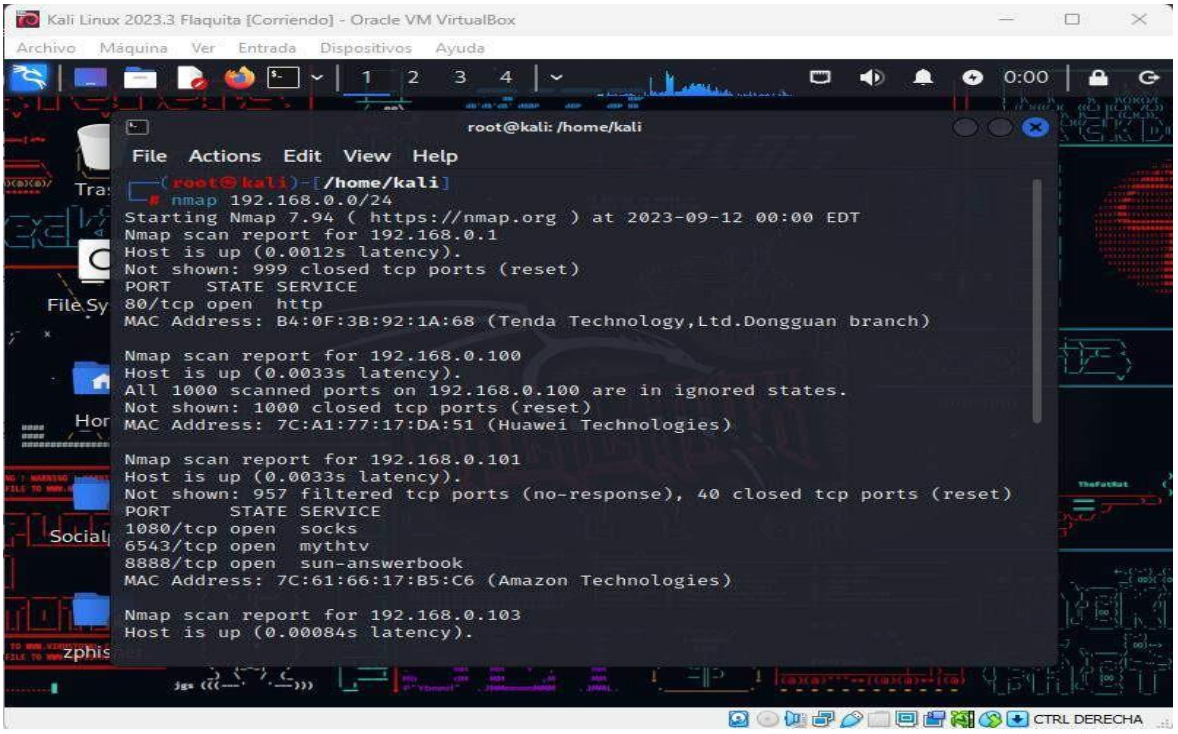
Finalmente, ¿Cómo visualiza el futuro de estas herramientas en el contexto de la evolución constante de las amenazas cibernéticas y las redes de telecomunicaciones? ¿Se espera que sigan siendo efectivas o cree que se requerirán nuevos enfoques y tecnologías? *

el futuro siempre va a traer mas seguridad y mas ataques las herramientas siempre deben ir evolucionando tan rapido como sea posible para prevenir estos inconvenientes

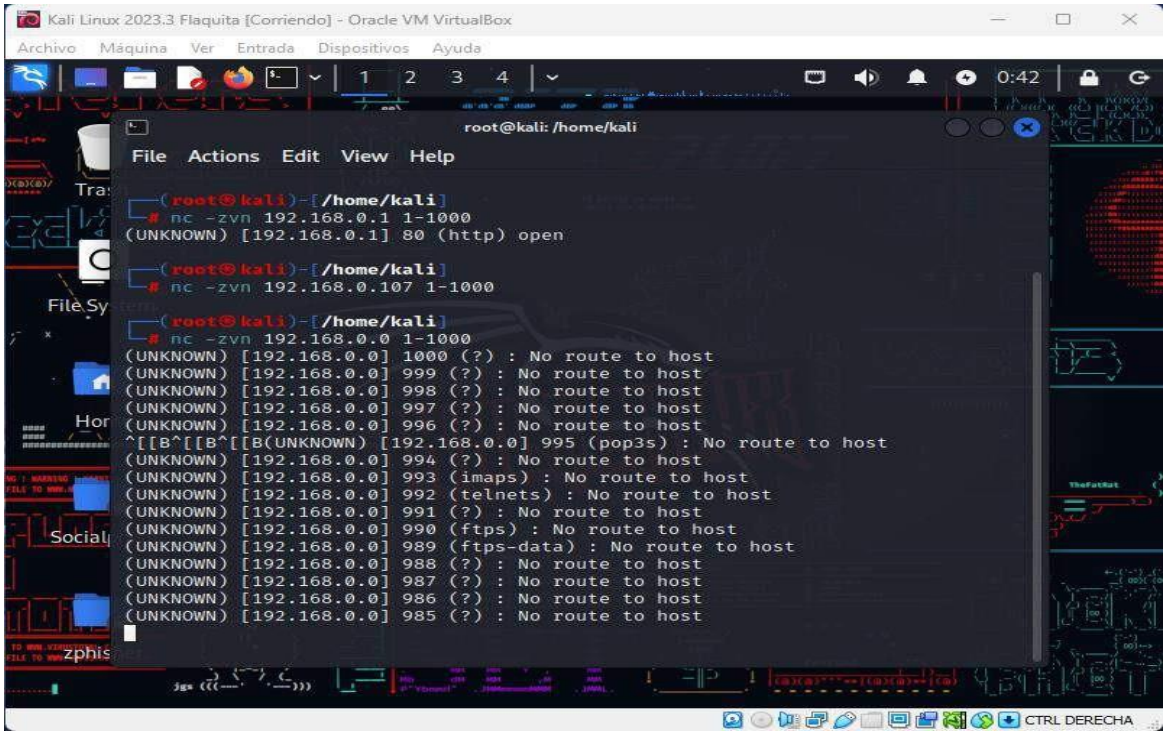
Este formulario se creó en Facultad de Administración Finanzas e Informatica.

Google Formularios

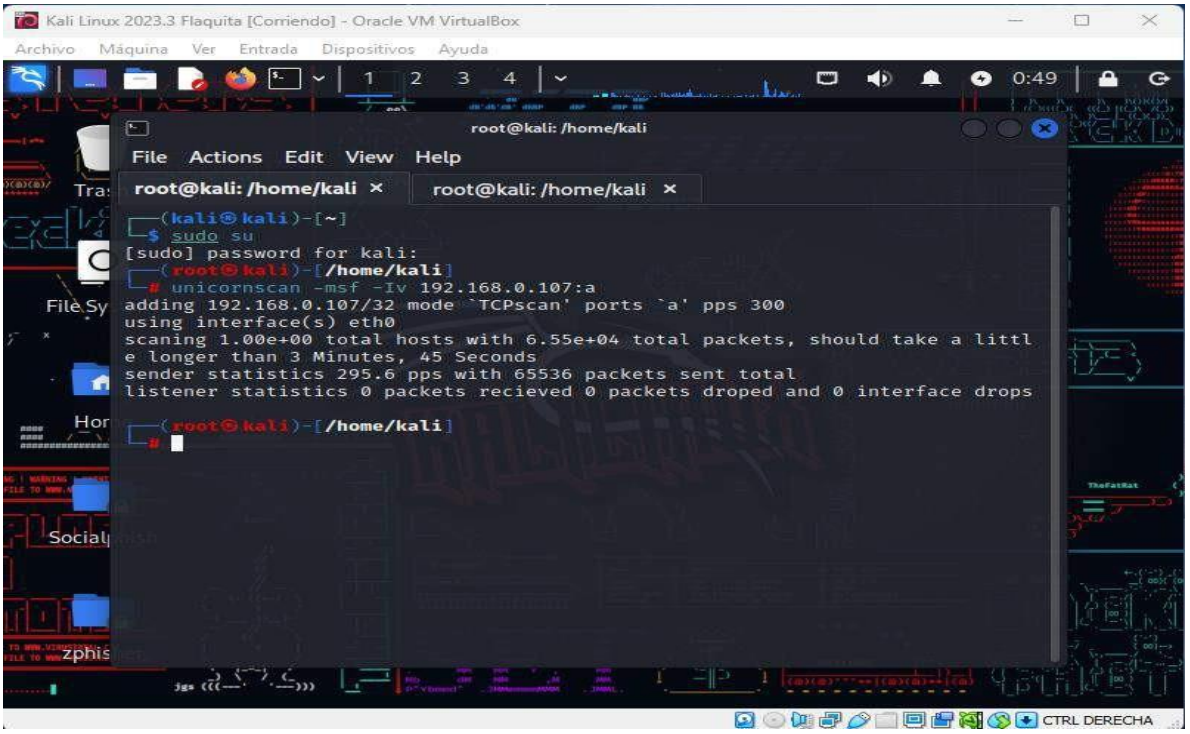
Anexo 3. *Entrevista Realizada a la Ingeniera Ana Fernández*
Fuente: *Elaboración Propia*



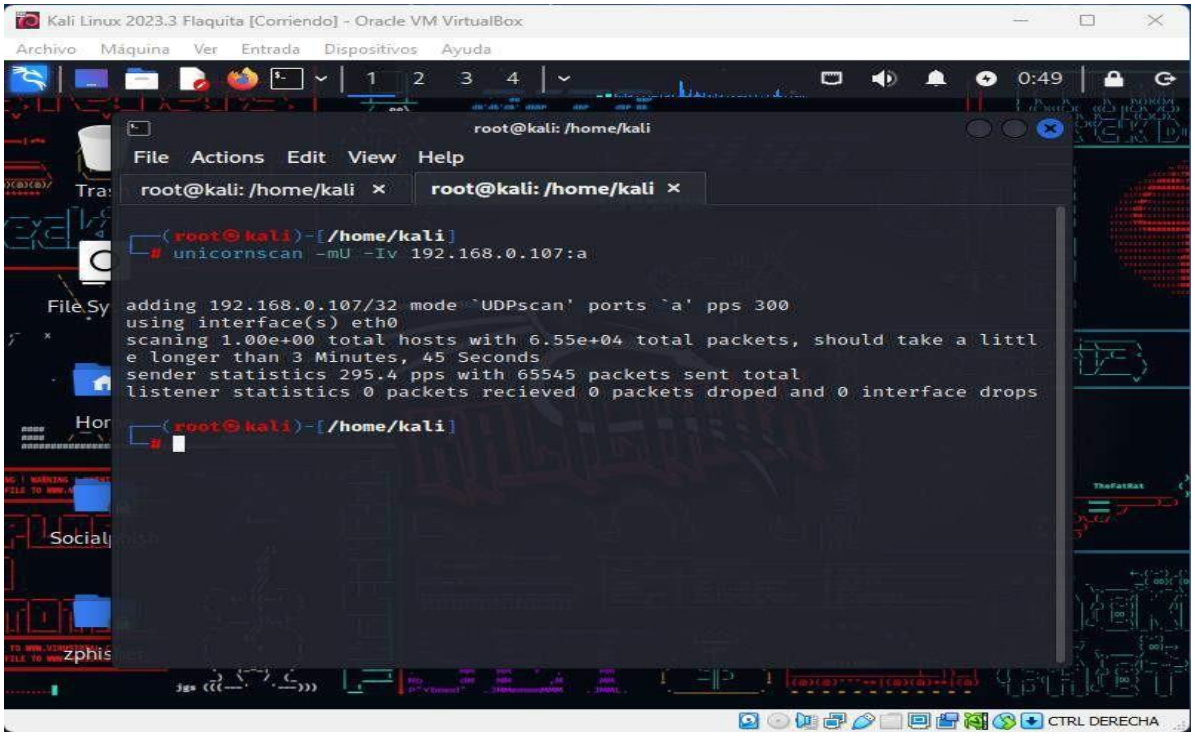
Anexo 4. *Escaneo de Puertos Realizado en Nmap*
Fuente: *Elaboración Propia*



Anexo 5. *Escaneo de Puertos Realizado en Netcat*
Fuente: *Elaboración Propia*



Anexo 6. *Escaneo de Puertos por modo TCP en UnicornScan*
Fuente: *Elaboración Propia*



Anexo 7. *Escaneo de Puertos por modo UDP en UnicornScan*
Fuente: *Elaboración Propia*

CERTIFICADO DE ANÁLISIS
magister

ANÁLISIS TÉCNICO COMPARATIVO DE HERRAMIENTAS DE ESCANEO DE PUERTOS DE REDES DE TELECOMUNICACIONES

< 1% Similitudes

< 1% Texto entre comillas
< 1% similitudes entre comillas
< 1% Idioma no reconocido

Nombre del documento: Caso de Estudio-Geovanny Valencia.docx
ID del documento: 17c7d8a4c96e8b2f146115c231519d2efbb67d28
Tamaño del documento original: 405,39 kB
Autor: Geovanny Valencia Martínez

Depositante: Geovanny Valencia Martínez
Fecha de depósito: 15/9/2023
Tipo de carga: url_submission
fecha de fin de análisis: 15/9/2023

Número de palabras: 5849
Número de caracteres: 37.733

Ubicación de las similitudes en el documento:

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	www.solvetic.com | Ejemplos de comandos NMAP para sistemas Linux - Solvetic https://www.solvetic.com/tutoriales/article/5000-ejemplos-comandos-nmap-para-sistemas-linux/	< 1%		Palabras idénticas: < 1% (18 palabras)
2	dspace.utb.edu.ec | Análisis de los problemas de seguridad y redes en la empresa... http://dspace.utb.edu.ec/bitstream/49000/11881/3/E-UTB-FAFI-SIST_INF-000039.pdf.txt	< 1%		Palabras idénticas: < 1% (15 palabras)
3	nmap.org | Técnicas de sondeo de puertos | Guía de referencia de Nmap (Página ... https://nmap.org/man/es/man-port-scanning-techniques.html	< 1%		Palabras idénticas: < 1% (17 palabras)

Anexo 8. *Certificado de Análisis de Detección de Plagio*
Fuente: *Compilatio*