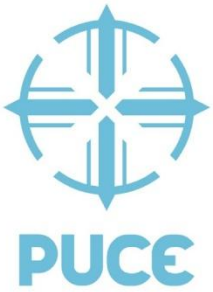
PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN



Trabajo de Titulación

TEMA: IMPLEMENTACIÓN DE UN ESCENARIO DE ATAQUE DNS EN UN ENTORNO CORPORATIVO SIMULADO UTILIZANDO GNS3

AUTOR

OMAR DANIEL VALAREZO LÓPEZ

DIRECTOR

MILTON NEPTALI ROMÁN CAÑIZARES

QUITO DM, 2024

DEDICATORIA

Este trabajo es el resultado de años de esfuerzo, dedicación y, sobre todo, del apoyo incondicional de muchas personas que han sido fundamentales en mi vida. Es dedicado para mi toda familia, en especial a mis padres y tíos que siempre me apoyaron de todas las formas posibles, fueron mi sustento para los momentos más dificiles que tuve que afrontar como estudiante, me dieron la motivación y la disciplina necesaria para seguir adelante.

A mis padres, por su amor incondicional, por ser mi fuente de fortaleza y por enseñarme el valor del esfuerzo y la perseverancia. Por creer en mí, incluso en los momentos más difíciles, y por ser mi ejemplo a seguir. Su apoyo ha sido un pilar fundamental en este camino.

A mis primos y hermanos, por su constante aliento y por estar siempre a mi lado. Sus palabras de ánimo y su compañía han sido esenciales para mantenerme firme en esta travesía.

A mis amigos, quienes han compartido risas, lágrimas y momentos inolvidables a lo largo de estos años. Gracias por ser mi refugio en los momentos de estrés y por celebrar conmigo cada pequeño logro.

A mis profesores y mentores, quienes con su sabiduría y paciencia me han guiado y motivado a lo largo de mi formación. Gracias por transmitir su conocimiento y por inspirarme a ser cada día mejor en mi área de estudio.

Finalmente, dedico este trabajo a mí mismo, por no rendirme, por superar los obstáculos y por tener la valentía de perseguir mis sueños. Este es solo el comienzo de una nueva etapa llena de desafíos y oportunidades.

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a todas las personas que, de una forma u otra, han sido parte fundamental en la realización de este trabajo y en mi formación académica y personal.

A mi familia, que a pesar de los problemas su fe en mí ha sido una fuente inagotable de motivación y fortaleza en cada paso de este camino.

A mis primos y hermanos, por su comprensión y ánimo en los momentos difíciles. Su confianza y apoyo me han acompañado a lo largo de este proceso y han sido fundamentales para superar los desafíos que se presentaron.

A mis amigos, por estar a mi lado en las buenas y en las malas, por su compañía, su aliento y sus palabras de ánimo. Gracias por hacer que este viaje académico sea más llevadero y lleno de momentos inolvidables.

Quiero agradecer a todos los que han sido parte de mi vida durante estos años de estudio. Cada uno de ustedes ha dejado una huella imborrable en mi camino y ha contribuido significativamente a que hoy pueda culminar esta etapa de mi vida con éxito.

ÍNDICE

1. CAPÍTULO I – INTRODUCCIÓN 8

1.1. TEMA 8

1.2. JUSTIFICACIÓN 8
1.3. PLANTEAMIENTO DEL PROBLEMA 8
1.4. OBJETIVOS 9
1.4.1. OBJETIVO GENERAL 9
1.4.2. OBJETIVOS ESPECÍFICOS 9
1.5. ALCANCE 10
2. CAPÍTULO II – MARCO TEÓRICO Y CONCEPTUAL 10
2.1. ANTECEDENTES 10
2.2. MARCO TEÓRICO 11
2.3. MARCO CONCEPTUAL 12
2.3.1. DNS (Domain Name System) 12
2.3.2. Tipos de consultas DNS 12
2.3.3. Vulnerabilidades en DNS 13
2.3.4. Tipos de Ataques DNS 13
2.3.5. Diferencia entre DNS Spoofing y DNS Poisoning 16
2.3.6. Tipos de Ataques en ciberseguridad más comunes 17
2.3.7. Análisis de Tráfico de Red 18
2.3.8. Simulación de Redes 19
2.3.9. Tipos de pruebas de pentesting 22
2.3.10. Herramienta para la Evaluación de la Seguridad en Redes 25
2.3.11. Ciberseguridad y mejores prácticas 26
2.3.12. Herramientas de ataque DNS 26
2.3.13. Herramientas para mitigar los ataques DNS. 28
3. CAPÍTULO III – METODOLOGÍA 29
3.1. Introducción a la Metodología 29
3.2. Descripción del entorno simulado en GNS3 30
3.2.1. Componentes del entorno corporativo simulado 30
3.3. Herramienta para el análisis de vulnerabilidades 30
3.3.1. Nessus 30
3.4. Herramienta para la explotación de vulnerabilidades 32
3.4.1. Burp Suite 32
3.4.2. Hydra 32

3.4.3. Aircrack-ng 32
3.4.4. Bettercap 33
3.5. Medidas para mitigar ataques DNS 33
3.5.1. DNSSEC (DNS Security Extensions) 33
4. CAPÍTULO IV – IMPLEMENTACIÓN 34
4.1. Topología de la Red 34
4.2. Configuración de dispositivos 35
4.2.1. Direccionamiento IP 35
4.2.2. Configuración de vlans 36
4.2.3. Zona DMZ 38
4.2.4. Zona LAN 39
4.2.5. Zona Servidores 40
4.2.6. Firewall 42
4.2.7. Configuración de la Máquina Atacante 45
4.3. Simulación del ataque DNS spoofing 46
4.3.1. Uso de la herramienta bettercap en Kali Linux 46
4.3.2. Análisis del ataque de envenenamiento DNS 47
5. CAPÍTULO V – MEDIDAS PARA MITIGAR ATAQUES DNS 49
5.1. Implementar DNSSEC (Domain Name System Security Extensions): ... 49
5.1.1. ¿Cómo Funciona DNSSEC? 49
5.1.2. Implementación de DNSSEC 50
5.1.3. Herramientas de Implementación y Verificación 50
5.2. Utilizar servidores DNS autorizados y confiables: 50
5.3. Configurar firewalls y filtros de DNS: 51
5.4. Realizar actualizaciones y parches regulares: 51
5.5. Monitorear el tráfico DNS: 51
5.6. Educación y capacitación del personal: 51
CONCLUSIONES 52
6. ANEXO A 57
7. Anexo B 60

Índice de Figuras

Figura 1 Interfaz de la Herramienta Nessus 31

Figura 2 Topología de red 35
Figura 3 Vlan 10 37
Figura 4 Vlan 20 37
Figura 5 Zona DMZ 38
Figura 6 Página Empresarial 39
Figura 7 Zona LAN 39
Figura 8 Máquina Atacante 40
Figura 9 Zona de Servidores 41
Figura 10 Administración DNS 41
Figura 11 Propiedades de Firewall 42
Figura 12 Ilustración del Fortigate 43
Figura 13 Información de puertos en el Fortigate 43
Figura 14 Configuración del Port2 44
Figura 15 Show system interface 44
Figura 16 Políticas en el Fortigate 45
Figura 17 Instalación de bettercap 45
Figura 18 Instalación de Apache 46
Figura 19 Comando net.probe on 46
Figura 20 Comando set arp.spoof targets 47
Figura 21 Comando arp.spoof on 47
Figura 22 Comando set dns.spoof.domains 47
Figura 23 Comando set dns.spoof.address 47
Figura 24 Comando dns.spoof.on 47
Figura 25 Página Empresarial 48
Figura 26 Página alterada 49

Índice de Tablas

Tabla 1 Diferencia entre DNS Poisoning y Spoofing..... 16
Tabla 2 Configuración DMZ..... 35
Tabla 3 Configuración LAN..... 35
Tabla 4 Configuración Servidores 36
Tabla 5 Configuración Vlans 36

1. CAPÍTULO I – INTRODUCCIÓN

1.1. TEMA

Implementación de un escenario de ataque DNS en un entorno corporativo simulado utilizando GNS3.

1.2. JUSTIFICACIÓN

El crecimiento acelerado de las TICs ha llevado a las grandes empresas a tener que adaptarse a las nuevas tecnologías. El siguiente proyecto, que se llevará a cabo, tiene como fin conocer los ataques cibernéticos y cómo combatirlos.

Es un hecho que la demanda tecnológica ha tenido un aumento imprescindible en todos los ámbitos laborales, al igual que un crecimiento de múltiples ataques cibernéticos. "El mayor ataque DDoS hasta la fecha ocurrió en septiembre de 2017. Su tamaño fue de 2,54 Tbps y se dirigió a los servicios de Google" (CloudFlare, 2024, párr. 2). Grandes corporaciones como Amazon AWS, GitHub, entre otras, han sido víctimas de ataques DNS, lo que les ha costado grandes sumas de dinero al igual que perdida de usuarios.

Por esta razón, es importante conocer la importancia de la seguridad informática y los riesgos a los que están expuestas las empresas. Este trabajo, se generará una simulación de un ataque en un ambiente controlado con el fin evidenciar las vulnerabilidades, conocer el proceso de la explotación de la vulnerabilidad y proponer medidas para proteger los sistemas ante estos sucesos.

El uso de internet, email, aplicaciones colaborativas, servicios en la nube, etc. dentro de las organizaciones, son necesarias y fundamentales en las actividades cotidianas. Las operaciones empresariales dependen del funcionamiento de determinados servicios de herramientas tecnológicas como los DNS, es decir, su interrupción o mal funcionamiento, podría significar afectaciones en la confidencialidad, integridad o disponibilidad de sus servicios o activos empresariales.

1.3. PLANTEAMIENTO DEL PROBLEMA

Actualmente, es un hecho que los delitos cibernéticos se han incrementado de forma acelerada, obligando a empresas u organizaciones a tener que generar planes de protección de su integridad. Para este proyecto, se plantea descubrir el proceso de

infiltración cibernética y conocer como contrarrestar estos sucesos, para poder mitigarlos y no volver a ser víctima de estos.

Muchas empresas han sido afectadas por los ciberdelitos que en muchos de los casos las han llevado a la quiebra. En el caso de un banco de Brasil, la filial brasileña de un banco fue víctima de un ataque phishing, donde el proveedor de seguridad en la nube detecto que el ataque era un envenenamiento a la caché DNS (Castro, 2011). Esto llevo a que se tenga una captura de datos críticos que puso en debilidad la seguridad del banco.

En este trabajo, se generará la simulación de un ataque DNS, a la red empresarial simulada en el entorno GNS3, utilizando herramientas apropiadas para la ejecución de análisis de vulnerabilidades, pruebas de pentesting y seguridad ofensiva. El ataque particular que se ejecuta es un ataque DNS spoofing, que hará que comprometa la integridad del sistema de nombres de dominio, lo que puede resultar en que las víctimas sean redirigidas a sitios web maliciosos o pierdan la conectividad con servicios legítimos, para así de esto modo, obtener los datos o credenciales de la víctima y poder ingresar a su plataforma o sistema.

Aunque existen numerosas soluciones de seguridad disponibles para mitigar este tipo de amenazas, la falta de comprensión y entrenamiento adecuado en el ámbito corporativo puede dar lugar a situaciones de alto riesgo.

1.4. OBJETIVOS

1.4.1. OBJETIVO GENERAL

Vulnerar la red corporativa de un entorno virtualizado mediante un ataque de DNS.

1.4.2. OBJETIVOS ESPECÍFICOS

- Establecer un entorno de red virtual que emule una infraestructura corporativa con servidores, estaciones de trabajo y un servidor DNS.
- Implementar una alternativa para simular un ataque de envenenamiento de DNS en el entorno corporativo.
- Analizar el proceso y resultados del ataque DNS a la red corporativa.
- Proponer medidas para mitigar los riesgos producidos por el ataque DNS.

1.5. ALCANCE

Definición del entorno corporativo simulado: Esto implica la creación de una red virtual que simula la infraestructura de red de una organización típica. Esto puede incluir servidores, estaciones de trabajo, dispositivos de red (como switches, routers, firewalls), y otros dispositivos relevantes.

Implementación del mecanismo de ataque DNS: Esto implica la creación y ejecución de un ataque DNS contra el servidor DNS configurado. El tipo de ataque DNS será la captura de este para poder ser envenenado.

Análisis los resultados mediante pruebas hacia páginas web que redireccione a sitios fraudulentos.

Desarrollo de estrategias de mitigación: Basándose en los resultados del análisis del ataque, se deben desarrollar y probar estrategias para mitigar este tipo de ataques DNS en el futuro.

2. CAPÍTULO II – MARCO TEÓRICO Y CONCEPTUAL

2.1. ANTECEDENTES

El incremento de la conectividad, la interacción y dependencia de las organizaciones en los sistemas de información, se ha visto reflejado en un incremento del desinterés de los ciber atacantes por vulnerar sus seguridades. Según (IBM, 2023), el costo promedio por filtraciones de datos por ataques cibernéticos para el año 2023 fue de 4.45 millones de dólares, lo que ha significado grandes pérdidas o incluso la quiebra de las empresas. Durante el año 2022, en todo el mundo se estima que se produjeron alrededor de 493 millones de ataques del tipo ransomare.

La suplantación de DNS es uno de los ataques muy comunes. Este tipo de ataque permite a los atacantes redirigir el tráfico de red de las víctimas a servidores maliciosos sin su conocimiento, lo que puede conducir a la captura de credenciales, el robo de información y la distribución de software malicioso.

El engaño DNS se basa en alterar las respuestas DNS para dirigir a los usuarios a sitios web falsos. Esto se hace simulando la respuesta de un servidor DNS legítimo. Al recibir una respuesta DNS manipulada, la víctima se dirige a un servidor controlado por el atacante en lugar del servidor legítimo al que intentaba acceder. Esta

estrategia se ha utilizado en varios ciberataques que han afectado a personas y grandes organizaciones.

En este contexto, la simulación de ataques DNS en un entorno controlado emerge como una herramienta valiosa para comprender mejor estas amenazas y desarrollar estrategias de mitigación adecuadas. Plataformas de simulación de redes como GNS3 permiten a expertos e investigadores recrear escenarios realistas y seguros para analizar estos ataques.

Por tanto, la creación de un escenario de ataque DNS en un entorno corporativo simulado mediante GNS3 representa un paso significativo para profundizar en la comprensión de estos ataques y cómo contrarrestarlos. Este proyecto se enfoca en explorar este aspecto de la ciberseguridad y contribuir a la defensa contra los ataques DNS.

2.2. MARCO TEÓRICO

El DNS funciona mediante la resolución de nombres de dominio a direcciones IP a través de consultas y respuestas entre clientes y servidores DNS. Este proceso implica la comunicación entre distintos componentes, incluyendo clientes, servidores autorizados y servidores raíz, que colaboran para proporcionar la información requerida.

La mayoría de los dispositivos conectados a Internet, que van desde los teléfonos inteligentes y computadoras portátiles hasta los servidores que alojan los sitios web de comercio masivo, su comunicación entre ellos se lleva a cabo mediante identificadores numéricos llamados direcciones IP. Estas direcciones son esenciales para que los dispositivos se encuentren y se comuniquen entre sí en la red. Sin embargo, para los usuarios finales, recordar y utilizar estos números largos resultaría poco práctico. Por ello, cuando ingresamos a un sitio web a través de un navegador, no necesitamos introducir una secuencia numérica extensa; en su lugar, simplemente escribimos un nombre de dominio, como ejemplo.com, lo que nos permite acceder al sitio correcto de manera intuitiva y sencilla.

Ahora, estos DNS pueden ser factores críticos para una empresa o usuario, dando paso a múltiples ataques a su infraestructura para generar problemas a la organización. La suplantación y el envenenamiento del Sistema de Nombres de Dominio son formas

de ciberataques que se aprovechan de las debilidades presentes en los servidores DNS para redirigir el tráfico desde los servidores auténticos hacia servidores falsificados.

Las amenazas más destacadas son dos:

Suplantación de DNS, el cual trata de una amenaza emergente que replica los destinos de servidores auténticos con el fin de desviar el tráfico de un dominio. Los usuarios que no están alerta pueden ser dirigidos a sitios web maliciosos, siendo este el propósito perseguido mediante diversas técnicas de suplantación de DNS.

También tenemos el Envenenamiento de caché de DNS, es una técnica de suplantación de DNS dirigida al usuario final, en la cual el sistema guarda la dirección IP falsa en su caché local. Esto provoca que el DNS redirija al usuario hacia el sitio malicioso, incluso después de que el problema haya sido resuelto o si dicho sitio nunca estuvo registrado en el servidor.

2.3. MARCO CONCEPTUAL

En el siguiente capítulo toparemos los fundamentos teóricos y conceptuales inevitables para entender los ataques DNS y la simulación de redes. Se presentará una explicación minuciosa del funcionamiento del DNS, los diferentes tipos de ataques más frecuentes, y una introducción a las herramientas utilizadas en la simulación.

2.3.1. DNS (Domain Name System)

El DNS es un sistema jerárquico y descentralizado que se usa para traducir nombres de dominio legibles por humanos en direcciones IP. Este sistema es esencial para el funcionamiento de Internet porque facilita la localización de recursos y servicios en la red (Cloudflare, 2024).

- **Funcionamiento del DNS:** Se realiza una consulta DNS cuando un usuario ingresa un nombre de dominio en su navegador. Esta consulta pasa por varios servidores (resolvers, servidores raíz, servidores TLD y servidores autoritativos) hasta obtener la dirección IP adecuada.

2.3.2. Tipos de consultas DNS

- **Recursivas:** El resolvedor ejecuta todas las consultas necesarias para alcanzar una respuesta definitiva.

- **Iterativas:** El servidor DNS proporciona la respuesta más efectiva (con frecuencia con una referencia a otro servidor) y permite que el resolver realice consultas adicionales.

2.3.3. Vulnerabilidades en DNS

Al ser un protocolo importante y ampliamente utilizado, el DNS también es un objetivo usual para ataques. Las principales amenazas incluyen:

- **Falta de Autenticación:** El protocolo DNS original carecía de autenticación, lo que permitía que las respuestas fueran falsas.
- **Cache Poisoning:** Manejo de la caché de un servidor DNS para almacenar respuestas erróneas.

2.3.4. Tipos de Ataques DNS

- **DNS Spoofing**

El engaño DNS es un método para que la potencial víctima cambie las direcciones de los servidores DNS y pueda controlar las consultas que se realizan.

Según (We Live Security, 2012), muchos atacantes se benefician de este nodo dentro de la ruta de comunicación cuando se consulta un sitio web, aprovechando esta dependencia con los servidores de nombres de dominio. Por decirlo de otra manera, cambian las direcciones IP de los servidores DNS de la víctima para que apunten a servidores maliciosos.

- **DNS Poisoning**

El ataque Poisoning o conocido como envenenamiento de caché de DNS, consiste en agregar información falsa a una caché DNS, lo que hace que las consultas de DNS devuelvan una respuesta incorrecta y lleve a los usuarios a sitios web incorrectos.

Las direcciones IP son los "números de teléfono" de Internet y permiten que el tráfico llegue a los lugares correctos. Los directorios de números telefónicos contienen cachés de resolución DNS, y cuando almacenan información errónea, el tráfico se dirige a sitios equivocados hasta que se corrige la información de caché (Cloudflare, 2024).

- **Amplificación de DNS**

Un tipo de ataque DDoS conocido como amplificación de DNS utiliza servidores DNS abiertos o mal configurados para amplificar el tráfico hacia un objetivo deseado. El atacante envía consultas DNS falsas utilizando la dirección IP de la víctima como dirección de origen, lo que provoca que los servidores DNS generen respuestas DNS extensas que limitan la capacidad de la red de la víctima (Arguelles, 2024).

- **DNS Phishing**

El phishing DNS es un método en el que los atacantes engañan a los usuarios para que visiten sitios web falsos que son similares a los reales, con el fin de sustraer información personal como credenciales de inicio de sesión, información bancaria, etc. (Cloudflare, 2024).

- **Túnel DNS**

Este método de ataque implica el uso de diversos protocolos para enviar consultas y respuestas DNS mediante un túnel. Mediante SSH, TCP o HTTP, los atacantes pueden transmitir malware o datos robados a través de consultas DNS, eludiendo la detección de la mayoría de los firewalls (Cloudflare, 2024).

- **Secuestro DNS**

El secuestro de DNS, también conocido como robo de dominio, implica alterar la configuración de DNS de manera no autorizada para redirigir el tráfico de un sitio web legítimo hacia sitios web malintencionados. El compromiso de los servidores DNS, la interceptación de las consultas DNS o el uso de fallas en los sistemas de nombres de dominio pueden lograr esto. El secuestro de DNS puede utilizarse para robar datos confidenciales o para realizar otros tipos de ataques con el nombre del dominio (Arguelles, 2024).

- **Ataque NXDOMAIN**

Se trata de un tipo de ataque de inundación de DNS en el cual un servidor DNS es sobrecargado por un atacante con registros falsos, con el objetivo de interrumpir el servicio del tráfico legítimo. Este método puede implementarse utilizando herramientas de ataque avanzadas que tienen la capacidad de generar subdominios únicos para cada solicitud. Los ataques NXDOMAIN también pueden estar dirigidos

hacia un solucionador recursivo con el propósito de saturar su caché con solicitudes innecesarias (Cloudflare, 2024).

- **Ataque de dominio fantasma**

Este tipo de ataque se realiza mediante la creación de servidores DNS ficticios que no responden o lo hacen de manera extremadamente lenta, lo que interfiere con la comunicación normal.

Cuando un servidor DNS no puede resolver una dirección IP, el proceso recursivo implica buscarla en otros servidores DNS conectados. Los ataques de dominio ficticio buscan obstaculizar este proceso. La saturación de los servidores de resolución DNS resulta en una denegación de servicio (Arguelles, 2024).

- **Ataque de bloqueo de dominio**

Los perpetradores de este tipo de ataque planifican su estrategia configurando solucionadores y dominios específicos para establecer conexiones TCP con otros solucionadores legítimos. Los dominios responden enviando flujos de paquetes aleatorios a una velocidad lenta cuando los solucionadores atacados envían solicitudes, lo que resulta en la inutilización de los recursos del solucionador (Cloudflare, 2024).

- **Ataque CPE basado en red de robots (botnet)**

Estos ataques son ejecutados utilizando dispositivos CPE, que son equipos locales de los clientes y hardware suministrado por los proveedores de servicios, como módems, enrutadores y cajas de cables. Los CPE son comprometidos y los dispositivos se incorporan a una red de robots, conocida como botnet, que se emplea para llevar a cabo ataques de subdominios aleatorios contra sitios web o dominios específicos (Cloudflare, 2024).

2.3.5. Diferencia entre DNS Spoofing y DNS Poisoning

Tabla 1 Diferencia entre DNS Poisoning y Spoofing

	DNS Poisoning	*DNS Spoofing*
Definición	Técnica que implica la inyección de datos falsos en la caché de un servidor DNS.	Técnica que implica la falsificación de respuestas DNS para redirigir el tráfico a sitios maliciosos.
Método de Ataque	Manipula la caché DNS para almacenar registros falsos, redirigiendo el tráfico a destinos maliciosos.	Envía respuestas DNS falsas a una víctima antes de que llegue la respuesta legítima del servidor DNS.
Objetivo	Comprometer la caché de un servidor DNS, afectando a múltiples usuarios.	Engañar a un usuario o dispositivo específico para que se comunique con un servidor malicioso.
Alcance	Afecta a cualquier usuario que utilice el servidor DNS comprometido.	Principalmente afecta a la víctima que recibe la respuesta DNS falsificada.
Impacto	Puede afectar a un gran número de usuarios y sistemas durante un período prolongado.	Generalmente afecta a un único usuario o grupo de usuarios por un corto período de tiempo.
Persistencia del Ataque	Los registros falsos permanecen en la caché hasta que se vacíen o se actualicen.	La redirección dura solo mientras la respuesta falsificada está en la caché de la víctima o hasta que se actualice la resolución DNS.
Facilidad de Detección	Más difícil de detectar ya que afecta la caché DNS y	Relativamente más fácil de detectar mediante la

	puede parecer como tráfico legítimo.	comparación de respuestas DNS y análisis de tráfico.
Vector de Ataque	Vulnerabilidades en el software de servidor DNS, configuración incorrecta o ataques man-in-the-middle.	Respuestas DNS falsas, posibles ataques man-in-the-middle o comprometimiento del canal de comunicación.
Prevención	Implementación de DNSSEC, uso de caché y configuraciones seguros de servidores DNS.	Uso de DNSSEC, autenticación de respuestas DNS y monitoreo del tráfico de red.
Ejemplo Común	Un atacante manipula la caché DNS de un servidor ISP para redirigir a los usuarios de un banco a un sitio web de phishing.	Un atacante envía respuestas DNS falsificadas a un usuario para redirigirlo a un servidor de control y comando malicioso.

2.3.6. Tipos de Ataques en ciberseguridad más comunes

Malware:

Se refiere a los programas intrusivos diseñados para explotar dispositivos a expensas del usuario y en beneficio del atacante. Existen varios tipos de malware, pero todos usan técnicas diseñadas no solo para engañar a los usuarios, sino también para burlar los controles de seguridad.

Ataques de denegación de servicio distribuidos (DDoS):

Los ataques de red distribuida, comúnmente conocidos como DDoS (Denegación Distribuida de Servicio), explotan los límites de capacidad específicos impuestos a cualquier recurso de red, como la infraestructura que sostiene el sitio web de una empresa. Este tipo de ataque implica el envío masivo de solicitudes al recurso web objetivo, con el objetivo de sobrecargar su capacidad y así impedir su correcto funcionamiento (latam.kaspersky.com, 2024).

Phishing:

Los ataques de phishing emplean correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web falsos con el propósito de engañar a las personas y conseguir que divulguen información confidencial, descarguen malware o se expongan de alguna otra manera a actividades delictivas en línea (Kosinski, 2024).

2.3.7. Análisis de Tráfico de Red

El análisis de tráfico de red es fundamental para detectar y prevenir ataques, existen tres herramientas más comunes y conocidas por todos los usuarios para el análisis del tráfico de red, entre estas están:

- **Wireshark**

Se trata de una herramienta de análisis de tráfico de red que permite a los usuarios capturar, visualizar y examinar el flujo de datos a través de una red de computadoras. Esta herramienta resulta invaluable para administradores de redes y expertos en seguridad informática, ya que ofrece una visión detallada del tráfico en tiempo real, facilitando la detección de problemas y el análisis de la seguridad de la red (OpenWebinars.net, 2022).

- **Tcpdump**

Es una herramienta de software diseñada para capturar y analizar el tráfico de red, permitiendo a los usuarios examinar los paquetes de datos que circulan por una red de computadoras. Tcpdump opera desde la línea de comandos, proporcionando una gran flexibilidad para filtrar y mostrar información específica, lo que resulta valioso

para administradores de redes y especialistas en seguridad al momento de detectar problemas y auditar la actividad de la red (De Luz, 2024).

- **IDS/IPS (Sistemas de Detección/Prevención de Intrusiones)**

Los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) desempeñan roles críticos en la seguridad de las redes informáticas. El IDS tiene la función de identificar y alertar sobre actividades potencialmente sospechosas o no autorizadas en la red. Por otro lado, el IPS no solo detecta estas actividades, sino que también las bloquea activamente para prevenir posibles ataques. Estos sistemas son esenciales para garantizar la seguridad y proteger la información en redes de computadoras (INCIBE, 2020).

2.3.8. Simulación de Redes

La creación de un entorno simulado de red es beneficioso para la creación de diferentes topologías de red complejas en un entorno controlado, brindándonos seguridad sin tener que afectar los sistemas reales.

Importancia de la simulación en ciberseguridad:

- ✓ Comprobar vulnerabilidades y ataques sin dañar los sistemas o equipos reales.
- ✓ Analizar la certeza de las medidas de seguridad.
- ✓ Tener las debidas precauciones ante incidentes imprevistos de seguridad.

Herramientas de simulación de redes

- **GNS3**

GNS3 es una plataforma de simulación de redes que permite la creación y configuración de redes virtuales con dispositivos de red como ruteadores, switches entre otros. Es considerablemente utilizado en la industria para la formación en redes (GNS3, s.f.).

Características de GNS3:

- ✓ Permite la vinculación con diferentes máquinas virtuales.
- ✓ Facilita la captura y análisis del tráfico de red mediante la herramienta de Wireshark.
- ✓ Es capaz de admitir imágenes de IOS de cisco y otros sistemas de red.

Ventajas:

- ✓ Simulación Completa: Permite la simulación de redes completas con equipos reales, como routers y switches, lo que proporciona un entorno de pruebas cercano a la realidad.
- ✓ Compatibilidad con Software Real: Puedes usar imágenes de sistemas operativos de red reales (por ejemplo, Cisco IOS), lo que facilita la práctica y el aprendizaje en un entorno auténtico.

Desventajas:

- ✓ Curva de Aprendizaje: Puede tener una curva de aprendizaje pronunciada debido a la necesidad de configurar varios componentes y dispositivos de red.
- ✓ Dependencia de Imágenes: Depende de imágenes de sistemas operativos reales, lo que puede ser complicado de obtener y configurar para dispositivos específicos.

- **NS-3 (Network Simulator 3)**

NS-3 es una herramienta de simulación de redes de código abierto utilizada ampliamente en la investigación académica y en la industria (Nsnam, s.f.).

Característica:

- ✓ Soporta simulaciones detalladas de redes con protocolos avanzados, ofrece un modelado preciso del comportamiento de la red y permite la simulación de grandes topologías de red.

Ventajas:

- ✓ Muy detallado y preciso.
- ✓ Gran comunidad de usuarios y desarrolladores.
- ✓ Extensible y personalizable.

Desventajas:

- ✓ Curva de aprendizaje empinada.
- ✓ Requiere conocimientos en programación (C++ y Python).

- **OMNeT++**

Es una plataforma de simulación extensible y modular, ideal para la simulación de redes de comunicación, redes inalámbricas y sistemas distribuidos (OMNeT++, s.f.).

Característica:

✓ Proporciona una interfaz gráfica de usuario para la configuración y visualización de simulaciones.

Ventajas:

✓ Interfaz gráfica amigable.
✓ Flexibilidad y modularidad.
✓ Soporta múltiples tipos de redes.

Desventajas:

✓ Requiere conocimientos en C++ para simulaciones avanzadas.
✓ Menos detallado que NS-3 en algunos aspectos.

- **Cisco Packet Tracer**

Es una herramienta de simulación de redes desarrollada por Cisco, destinada principalmente para la enseñanza y el aprendizaje de redes (Networking Academy, 2024).

Característica:

✓ Permite la simulación de redes Cisco y la práctica de configuraciones de red.

Ventajas:

✓ Interfaz intuitiva y fácil de usar.
✓ Ideal para estudiantes y principiantes en redes.
✓ Gratis para estudiantes y usuarios educativos.

Desventajas:

- ✓ Limitado a dispositivos y tecnologías Cisco.
- ✓ Menos flexible para simulaciones avanzadas o no relacionadas con Cisco.

2.3.9. Tipos de pruebas de pentesting

Las pruebas de pentesting se clasifican en tres tipos: White Box, Black Box y Gray Box.

La White Box, Black Box y Gray Box son tres enfoques metodológicos que se utilizan en la evaluación de software y sistemas, y cada uno de ellos se caracteriza por sus propias ventajas y desventajas.

- **White Box**

La prueba de caja blanca, también conocida como prueba estructural, es una técnica de prueba de software que permite al evaluador tener acceso completo al código fuente y la estructura interna del sistema. Como resultado, se concentra en verificar el flujo de datos, la lógica y las estructuras internas de la aplicación (Nowak, 2024).

Características:

- ✓ Acceso Completo: El probador puede ver el código fuente y entender su estructura y lógica.
- ✓ Pruebas Detalladas: Se pueden probar caminos específicos del código, condiciones de lógica, y estructuras de datos.
- ✓ Cobertura: Se busca una cobertura completa del código, incluyendo sentencias, ramas y condiciones.

Ventajas:

- ✓ Detección de Defectos Internos: Permite identificar errores internos del sistema que no se pueden detectar mediante pruebas externas.
- ✓ Optimización de Código: Facilita la optimización del código y la identificación de ineficiencias.

- ✓ Cobertura Completa: Asegura que todas las partes del código sean examinadas.

Desventajas:

- ✓ Requiere Conocimiento Técnico: Es necesario tener un conocimiento profundo del código y de la arquitectura del sistema.
- ✓ Tiempo y Recursos: Puede ser costosa en términos de tiempo y recursos necesarios para realizarla.
- ✓ No Detecta Problemas de Uso: No es eficaz para identificar problemas de usabilidad o experiencia del usuario.

- **Black Box**

La prueba de caja negra, también conocida como prueba funcional, se realiza sin conocer el código fuente interno. Los probadores examinan las entradas y salidas del sistema para determinar si las funciones del software cumplen con los requisitos (Nowak, 2024).

Características:

- ✓ Orientada a Funcionalidad: Evalúa la funcionalidad del software según los requisitos.
- ✓ Sin Conocimiento Interno: Los probadores no necesitan conocer la estructura interna o el código.
- ✓ Pruebas Externas: Se enfocan en probar la interfaz del sistema y su comportamiento bajo diferentes condiciones de entrada.

Ventajas:

- ✓ Simplicidad: No requiere conocimientos técnicos profundos sobre el código.
- ✓ Orientación al Usuario: Evaluación desde la perspectiva del usuario final.
- ✓ Eficiencia en la Identificación de Fallos: Puede detectar errores que afectan la funcionalidad del sistema.

Desventajas:

- ✓ Cobertura Limitada: No proporciona una cobertura completa del código interno.
- ✓ Dependencia de la Documentación: La calidad de la prueba depende de la calidad de los casos de prueba y la documentación de requisitos.
- ✓ Puede No Detectar Errores Internos: No es efectiva para identificar errores en la lógica interna o la estructura del código.

- **Gray Box**

La prueba de caja gris combina las pruebas de caja blanca y negra. El probador puede crear casos de prueba más efectivos porque conoce parcialmente la estructura interna del sistema. Este método equilibra la necesidad de realizar pruebas de funcionalidad y lógica interna del sistema (Nowak, 2024).

Características:

- ✓ Conocimiento Parcial: El probador tiene acceso limitado al conocimiento del código o la arquitectura interna.
- ✓ Equilibrio: Combina la verificación de la funcionalidad externa y algunos aspectos internos.
- ✓ Flexibilidad: Permite pruebas más detalladas que la caja negra y menos intrusivas que la caja blanca.

Ventajas:

- ✓ Cobertura Ampliada: Proporciona una mayor cobertura que las pruebas de caja negra sin la complejidad total de las pruebas de caja blanca.
- ✓ Detección de Fallos: Puede identificar errores en la funcionalidad y en la lógica interna del sistema.
- ✓ Optimización del Proceso de Prueba: Permite una evaluación más completa y eficaz con menos tiempo y recursos que las pruebas de caja blanca.

Desventajas:

- ✓ Conocimiento Técnico Requerido: Aunque no tan exhaustivo como la caja blanca, requiere una comprensión básica del sistema interno.

- ✓ Complejidad de Configuración: Puede ser más complicado de configurar que las pruebas de caja negra.
- ✓ Cobertura No Completa: No proporciona la misma profundidad de cobertura que la prueba de caja blanca.

2.3.10. Herramienta para la Evaluación de la Seguridad en Redes

- **OpenVAS (Open Vulnerability Assessment System)**

OpenVAS es un conjunto de herramientas que se encuentran en el código abierto y se utilizan para analizar y escanear vulnerabilidades de seguridad. Ofrece una solución integral para la evaluación de vulnerabilidades en redes y sistemas (OpenWebinars.net, s.f.).

Características:

- ✓ Escaneo de Vulnerabilidades: Realiza escaneos completos para detectar vulnerabilidades conocidas.
- ✓ Informes Personalizados: Permite la generación de informes adaptados a las necesidades específicas.
- ✓ Actualizaciones Frecuentes: Se actualiza regularmente con nuevas firmas de vulnerabilidades.

Ventajas:

- ✓ Gratuito y de Código Abierto: Accesible para organizaciones de todos los tamaños.
- ✓ Escalabilidad: Adecuado para redes de cualquier tamaño.
- ✓ Personalización: Permite la creación de escaneos personalizados y la integración con otras herramientas.

2.3.11. Ciberseguridad y mejores prácticas

- Autenticación y control de acceso

Sirve para asegurarse de que solo los usuarios autorizados puedan acceder a los recursos de la red.

- Encriptación de datos

El uso de técnicas criptográficas para proteger la confidencialidad y la integridad de los datos.

- Monitoreo Continuo

Esta práctica nos aporta el control de la red para detectar actividades sospechosas o maliciosas.

2.3.12. Herramientas de ataque DNS

- **Bettercap**

Es una herramienta extensible y versátil para pruebas de penetración y análisis de redes. El descubrimiento de redes, la suplantación de ARP, la manipulación de paquetes y otras tareas son ejemplos de tareas que se pueden realizar con Ruby. Estos son algunos de los aspectos principales de Bettercap:

Ataques de hombre en el medio (MITM): Bettercap es particularmente útil para los ataques MITM porque permite a los piratas informáticos éticos interceptar y manipular el tráfico de red entre dos partes sin su conocimiento.

Secuencias de comandos integradas: Bettercap ofrece un motor de secuencias de comandos que permite a los usuarios crear secuencias de comandos automatizadas y módulos personalizados para una variedad de tareas de red.

Escaneo pasivo y activo: Puede escanear activamente para encontrar dispositivos y servicios o monitorear pasivamente el tráfico de la red, lo que ayuda a identificar objetivos potenciales.

Sistema de complementos: El sistema de complementos de Bettercap lo hace extremadamente extensible, ya que permite el desarrollo e integración de más funciones y protocolos.

Secuestro de sesión: Puede secuestrar inicios de sesión para obtener acceso no autorizado a las aplicaciones web.

- **Ettercap**

Ettercap es otra herramienta comúnmente utilizada en el contexto de la piratería ética. El enfoque principal es el análisis de redes y los ataques MITM. Sigue siendo una buena opción para la exploración de redes, aunque no tiene tantas funciones como Bettercap. Ettercap tiene las siguientes características principales:

Rastreo de paquetes: Ettercap puede capturar y analizar paquetes en la red para determinar el tráfico de datos y las vulnerabilidades potenciales.

Ataques MITM: Pueden realizar ataques MITM interceptando, alterando o inyectando paquetes en el flujo de la red, lo que puede ser útil para probar la seguridad de la red.

Compatibilidad con complementos: Lo hace adecuado para varios escenarios de pruebas de penetración de red, ya que cuenta con una amplia gama de complementos que se pueden utilizar para mejorar su funcionalidad.

- **Dnsenum**

Es una herramienta de enumeración DNS que puede obtener detalles sobre la infraestructura DNS de un dominio objetivo.

Características:

- ✓ Enumeración Completa: Realiza una enumeración completa de registros DNS.
- ✓ Detección de Subdominios: Identifica subdominios y otros registros relacionados.
- ✓ Verificación de Transferencia de Zona: Comprueba la posibilidad de realizar una transferencia de zona DNS.

- **Scapy**

Es una herramienta poderosa para la manipulación de paquetes que le permite crear, enviar y recibir paquetes de red personalizados. Es extremadamente versátil y se puede utilizar para realizar una variedad de ataques DNS.

Características:

- ✓ Manipulación de Paquetes: Capacidad para crear y modificar paquetes de red.
- ✓ Soporte Multiplataforma: Funciona en varios sistemas operativos.
- ✓ Extensibilidad: Permite la creación de scripts personalizados para ataques específicos.

2.3.13. Herramientas para mitigar los ataques DNS.

- **DNSSEC (DNS Security Extensions)**

DNSSEC es una colección de extensiones de seguridad DNS que permiten la autenticación de respuestas DNS mediante firmas digitales. proporciona autenticidad e integridad a los datos DNS, lo que evita manipulaciones maliciosas (INCIBE, 2020).

Características:

- ✓ Firmas Digitales: Las respuestas DNS están firmadas digitalmente para asegurar su autenticidad.
- ✓ Validación de Respuestas: Los clientes pueden validar la autenticidad de las respuestas DNS.
- ✓ Compatibilidad: Puede integrarse con sistemas DNS existentes.

- **DNSCrypt**

DNSCrypt es un protocolo que protege contra ataques de interceptación y manipulación de consultas DNS al cifrar el tráfico entre el cliente y el resolver DNS.

Características:

- ✓ Cifrado de Consultas DNS: Protege la privacidad y la integridad de las consultas DNS.
- ✓ Autenticación de Resolutores: Verifica la autenticidad del servidor DNS.

- **Split-Horizon DNS**

La técnica Split-Horizon DNS limita la exposición de información DNS al devolver diferentes respuestas DNS dependiendo del origen de la consulta.

Características:

- ✓ Separación de Respuestas: Diferentes respuestas para usuarios internos y externos.
- ✓ Reducción de Riesgos: Menor exposición a datos sensibles para usuarios externos.

- **Cloud-based DNS Services**

Los servicios DNS basados en la nube ofrecen protección adicional contra ataques mediante filtrado de tráfico, redundancia y soporte para tecnologías como DNSSEC.

Características:

- ✓ Filtrado de Tráfico: Protección contra ataques DDoS y otras amenazas.
- ✓ Alta Disponibilidad: Redundancia y escalabilidad para garantizar la continuidad del servicio.
- ✓ Soporte para DNSSEC: Implementación y gestión simplificada de DNSSEC.

3. CAPÍTULO III – METODOLOGÍA

3.1. Introducción a la Metodología

Para abordar un escenario de ataque DNS en un entorno corporativo simulado utilizando GNS3, se utilizará una metodología experimental cualitativa con la cual se integra métodos de simulación y pruebas. Esto proporcionará una base sólida para la exploración y análisis de las vulnerabilidades de DNS y la eficacia de las contramedidas de seguridad.

Se generará la suplantación de la página principal de la empresa para poder capturar el DNS y ejecutar la redirección, por lo cual se hace la solicitud a nuestra máquina virtual atacante. Mediante la herramienta bettercap, se realiza la suplantación

del DNS para poder capturar el tráfico de la red, de este modo, si el usuario intenta acceder a la página de la empresa, será enviado a una página falsa donde se presentará cualquier información que el atacante desee.

Una vez que se detecta un ataque es fundamental implementar políticas de seguridad sólidas utilizando FortiGat para prevenir futuros incidentes. Este nos permite configurar controles avanzados que verifiquen que las URLs a las que los empleados intentan acceder son auténticas. Para garantizar que todas las conexiones sean legítimas, estas políticas de seguridad pueden incluir inspecciones de contenido en tiempo real, filtraciones de sitios web sospechosos y autenticación de tráfico. De esta manera, se reduce significativamente el riesgo de compromisos de seguridad al asegurar que los usuarios solo accedan a sitios web seguros y confiables.

3.2. Descripción del entorno simulado en GNS3

3.2.1. Componentes del entorno corporativo simulado

Para la simulación del ataque DNS, se utilizarán los siguientes componentes:

- **Servidor DNS:** Un servidor DNS configurado para realizar la suplantación de una página en el entorno simulado.
- **Usuario:** Se encargará en el uso de varias máquinas virtuales que actuarán como clientes que ejecutarán las debidas consultas al servidor DNS.
- **Atacante:** Se usará una máquina virtual con Kali Linux la cual tendrá las herramientas para establecer el ataque DNS.
- **Infraestructura de Red:** Uso de un switch simulados en GNS3 para la conexión de los dispositivos.
- **Firewall:** Uso del software Fortigate con el cual se aplicarán las políticas necesarias.

3.3. Herramienta para el análisis de vulnerabilidades

3.3.1. Nessus

Nessus es una herramienta de seguridad que busca vulnerabilidades en los sistemas informáticos y las redes. Busca y analiza fallas de seguridad en sistemas

operativos, aplicaciones y dispositivos de red. Es capaz de escanear varios tipos de dispositivos, incluidos servidores, teléfonos, enrutadores y filtros (Sepulveda, 2023).

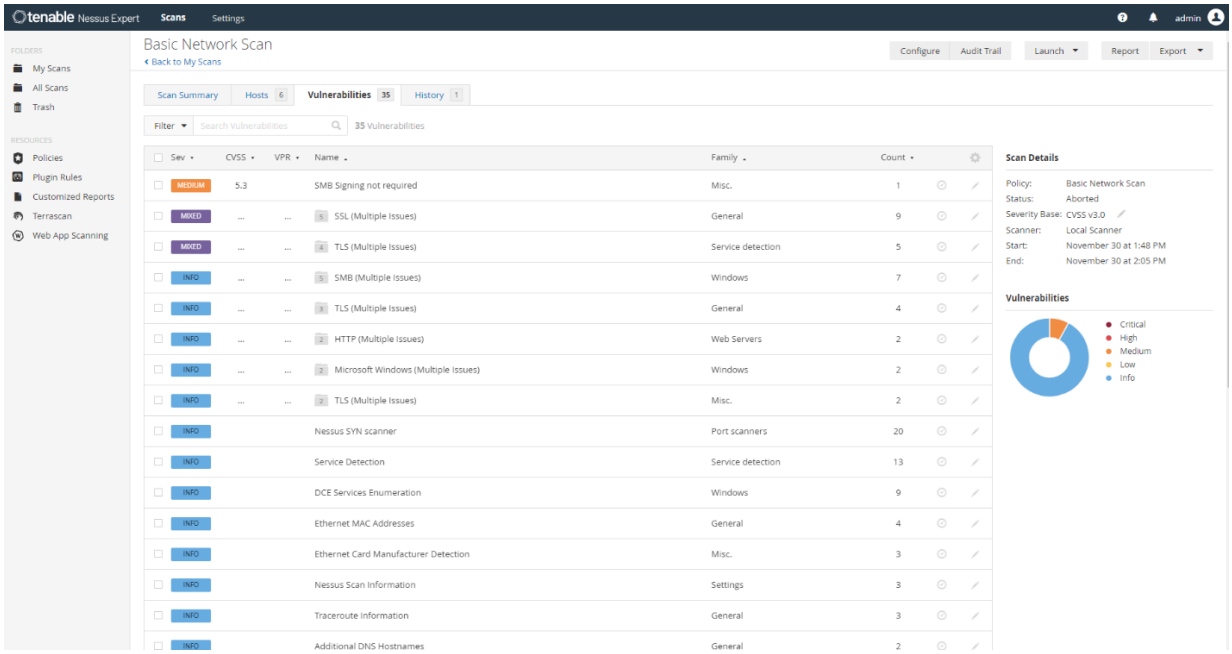
Características:

- ✓ Escaneo de Vulnerabilidades: Identifica vulnerabilidades conocidas en sistemas y redes.
- ✓ Informes Detallados: Genera informes exhaustivos con descripciones de vulnerabilidades y recomendaciones.
- ✓ Base de Datos Actualizada: Se actualiza regularmente con nuevas firmas de vulnerabilidades.

Ventajas:

- ✓ Cobertura Amplia: Soporta una amplia variedad de sistemas y aplicaciones.
- ✓ Detección Precisa: Identifica vulnerabilidades con alta precisión.
- ✓ Facilidad de Uso: Interfaz amigable y fácil de usar.

Figura 1 Interfaz de la Herramienta Nessus



Nota. - Interfaz de usuario tomado de (Tenable®, 2024).

3.4. Herramienta para la explotación de vulnerabilidades

3.4.1. Burp Suite

Burp Suite es una plataforma de pruebas de seguridad para aplicaciones web que contiene herramientas para la explotación de vulnerabilidades como inyecciones SQL y XSS.

Características:

- ✓ Intercepción de Tráfico: Permite interceptar y modificar tráfico HTTP/HTTPS.
- ✓ Explotación de Vulnerabilidades Web: Herramientas específicas para detectar y explotar vulnerabilidades en aplicaciones web.
- ✓ Extensibilidad: Soporta la creación de extensiones para ampliar sus capacidades.

3.4.2. Hydra

Hydra es una herramienta de fuerza bruta que puede atacar servicios de red como FTP, SSH e HTTP, utilizando credenciales débiles.

Características:

- ✓ Ataques de Fuerza Bruta: Realiza ataques de fuerza bruta contra diversos servicios de red.
- ✓ Compatibilidad con Múltiples Protocolos: Soporta una amplia gama de protocolos de red.
- ✓ Extensibilidad: Permite la creación de módulos personalizados para nuevos servicios.

3.4.3. Aircrack-ng

Aircrack-ng es un conjunto de herramientas que permite la explotación de vulnerabilidades en redes inalámbricas auditando y atacando estas redes.

Características:

- ✓ Captura de Tráfico Wi-Fi: Permite capturar y analizar tráfico de redes inalámbricas.

- ✓ Ataques de Fuerza Bruta: Realiza ataques de fuerza bruta para descifrar claves de Wi-Fi.
- ✓ Compatibilidad con Múltiples Protocolos Wi-Fi: Soporta WPA, WPA2, y WEP.

3.4.4. Bettercap

Es una herramienta de seguridad de red de código abierto utilizada para descubrir y aprovechar vulnerabilidades en sistemas mediante análisis de red, pruebas de seguridad y monitoreo de redes.

Puede realizar ataques de MITM (Man-In-The-Middle), descifrar el tráfico HTTPS, interceptar el tráfico de red y manipular los paquetes de red.

Características:

- ✓ Monitoreo en Tiempo Real: Permite el monitoreo en tiempo real del tráfico de red, lo que es crucial para la identificación de amenazas y la recolección de datos de seguridad.
- ✓ Ataques Man-in-the-Middle (MitM): Bettercap es especialmente conocido por su capacidad para realizar ataques MitM, permitiendo la interceptación, modificación y redirección del tráfico de red.
- ✓ Manipulación de Tráfico: Capaz de manipular el tráfico de red en tiempo real, incluyendo la inyección de código, redirección de tráfico, y otros tipos de manipulación.
- ✓ Captura de Credenciales: Puede capturar credenciales y datos sensibles de varios servicios y protocolos, proporcionando información crucial para la evaluación de la seguridad.
- ✓ Automatización de Ataques: Permite la automatización de diversos tipos de ataques, facilitando la ejecución de pruebas de seguridad complejas de manera eficiente.

3.5. Medidas para mitigar ataques DNS

3.5.1. DNSSEC (DNS Security Extensions)

El sistema de nombres de dominio (DNS) utiliza una serie de especificaciones llamadas DNSSEC para agregar una capa de seguridad al sistema de nombres de

dominio. El objetivo principal de DNSSEC es proteger a los usuarios de ataques de envenenamiento de caché y otros tipos de manipulaciones de DNS, asegurando la autenticidad e integridad de la información DNS que reciben (INCIBE, 2020).

Características:

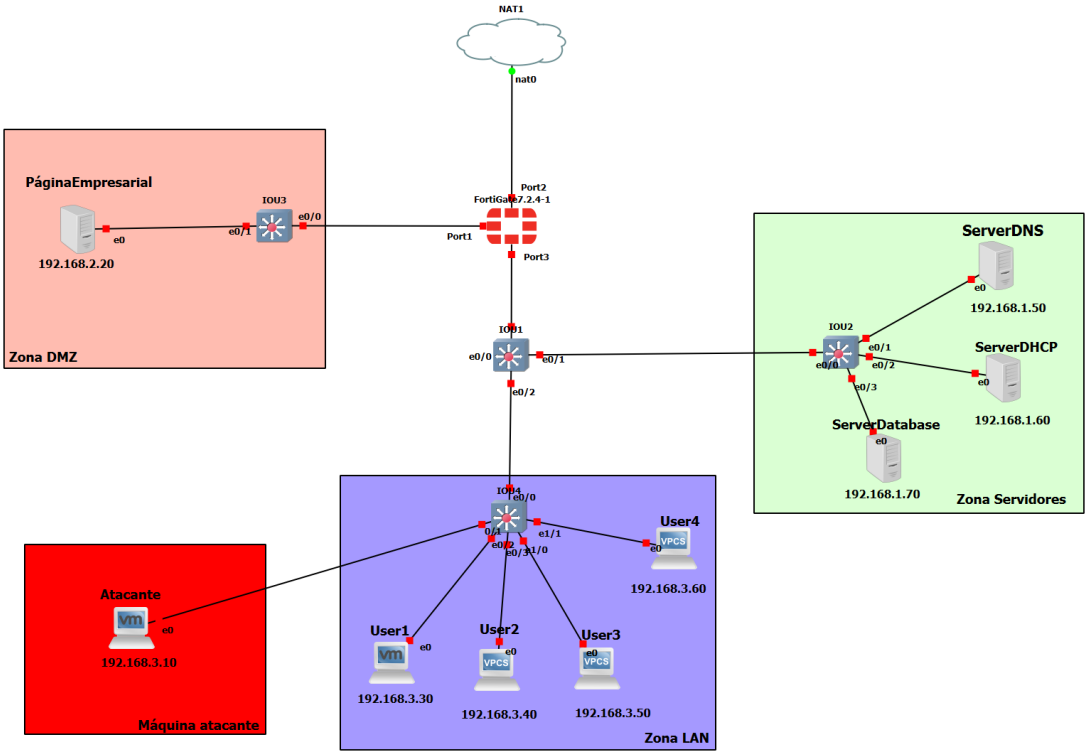
- ✓ Autenticidad de Datos: DNSSEC verifica que la información recibida proviene del propietario autorizado del dominio y no de una fuente maliciosa.
- ✓ Integridad de Datos: Garantiza que la información del DNS no ha sido alterada entre el servidor y el usuario final.
- ✓ Resistencia a Ataques de Envenenamiento de Caché: Protege contra ataques en los que un atacante intenta insertar información falsa en el caché de un servidor DNS.
- ✓ Uso de Firmas Digitales: Utiliza criptografía de clave pública para firmar las respuestas del DNS, lo que permite a los resolvers verificar la autenticidad e integridad de los datos.
- ✓ Compatibilidad con DNS Tradicional: DNSSEC es compatible con el protocolo DNS tradicional, lo que permite una implementación gradual sin interrupciones significativas.

4. CAPÍTULO IV – IMPLEMENTACIÓN

4.1. Topología de la Red

Se recreará un escenario real usando un software el cual nos permitirá simular el caso de estudio que deseamos generar. Haciendo uso de varias máquinas virtuales para conformar la arquitectura de red y de esto modo lograr la obtención del caso.

Figura 2 Topología de red



Nota. - Simulación de una red corporativa.

4.2. Configuración de dispositivos

4.2.1. Direccionamiento IP

Zona DMZ:

Tabla 2 Configuración DMZ

Dirección IP – Página Empresarial	*192.168.2.254*
Gateway	192.168.2.1
DNS	192.168.1.50

Zona LAN:

Tabla 3 Configuración LAN

Dirección IP – User1	192.168.3.30
Dirección IP – User2	192.168.3.40

Dirección IP – User3	192.168.3.50
Dirección IP – User4	192.168.3.60
Dirección IP – Máquina atacante	192.168.3.10
Gateway	192.168.3.1
DNS	192.168.1.50

Zona Servidores:

Tabla 4 Configuración Servidores

Dirección IP - Server DNS	192.168.1.50
Dirección IP - Server Dhcp	192.168.1.60
Dirección IP - Server Database	192.168.1.70
Gateway	192.168.1.1
DNS	192.168.1.50

Vlans:

Tabla 5 Configuración Vlans

VLAN 10 – Zona LAN	192.168.3.1
VLAN 20 – Zona Servidores	192.168.1.1

4.2.2. Configuración de vlans

La figura 3 muestra la configuración de la VLAN 10, con su respectivo procedimiento y comandos, para la Zona LAN:

Figura 3 Vlan 10

```
IOU4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IOU4(config)#vlan 10
IOU4(config-vlan)#name Zona LAN
IOU4(config-vlan)#int
IOU4(config-vlan)#inte
IOU4(config-vlan)#interfac
IOU4(config-vlan)#exit
IOU4(config)#in
IOU4(config)#interface ra
IOU4(config)#interface range e0/1-3, e1/0-1
IOU4(config-if-range)#sw
IOU4(config-if-range)#switchport mode
IOU4(config-if-range)#switchport mode ac
IOU4(config-if-range)#switchport mode access
IOU4(config-if-range)#sw
IOU4(config-if-range)#switchport ac
IOU4(config-if-range)#switchport access vlan 10
```

Luego, se configuró la vlan 20 para la zona servidores, con su respectivo direccionamiento IP, como se muestra en la figura 4:

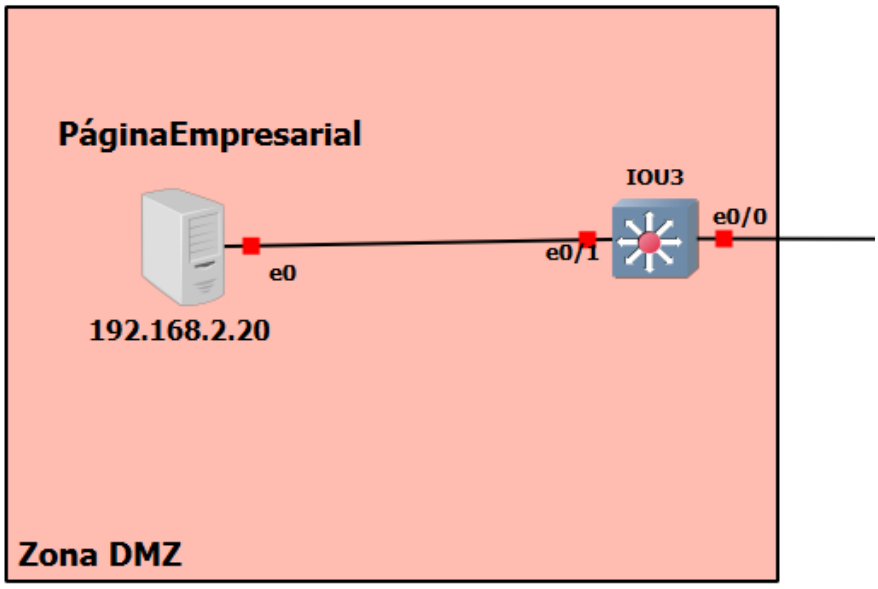
Figura 4 Vlan 20

```
IOU2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IOU2(config)#vlan 20
IOU2(config-vlan)#name Zona Servidores
IOU2(config-vlan)#interface range e0/1
IOU2(config-vlan)#interface range e0/1-3
IOU2(config-if-range)#sw
IOU2(config-if-range)#switchport mode ac
IOU2(config-if-range)#switchport mode access
IOU2(config-if-range)#sw
IOU2(config-if-range)#switchport ac
IOU2(config-if-range)#switchport access vlan 20
```

4.2.3. Zona DMZ

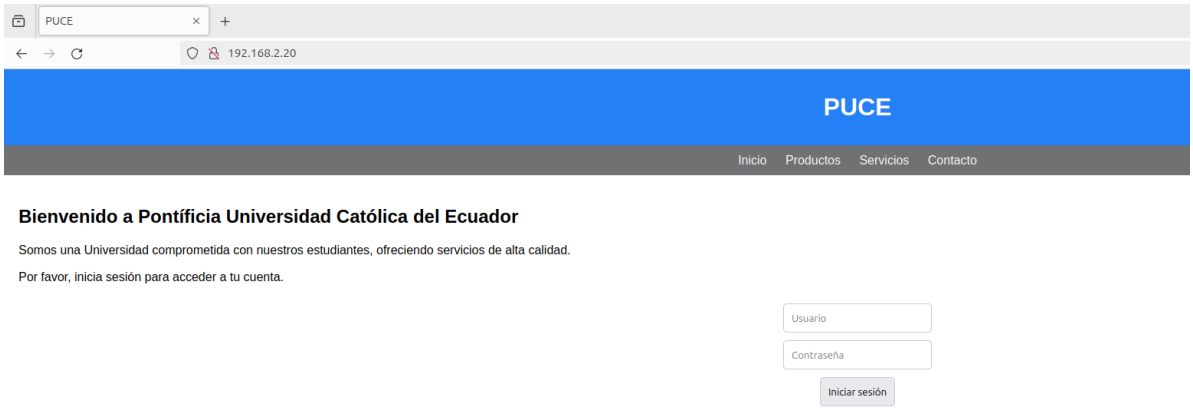
Para la siguiente zona, se utilizó una máquina virtual con Ubuntu, en la cual se aloja la página principal de la empresa en Apache2. En este servidor se encuentra la página web de la empresa, a la que los usuarios pueden acceder tanto desde dentro de la organización, como desde el internet, como se muestra en la figura 3.

Figura 5 Zona DMZ



Dentro de la máquina virtual con Ubuntu Server, donde se encuentra almacenada la página empresarial, se puede observar la interfaz de dicha página, como se muestra en la figura 4:

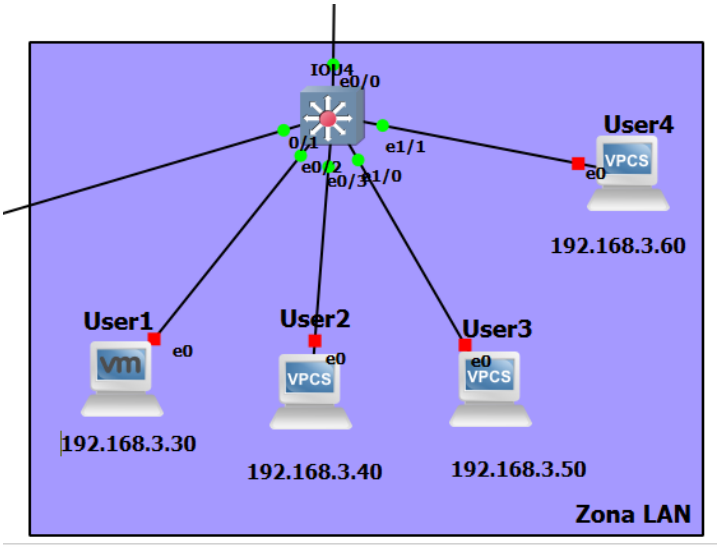
Figura 6 Página Empresarial



4.2.4. Zona LAN

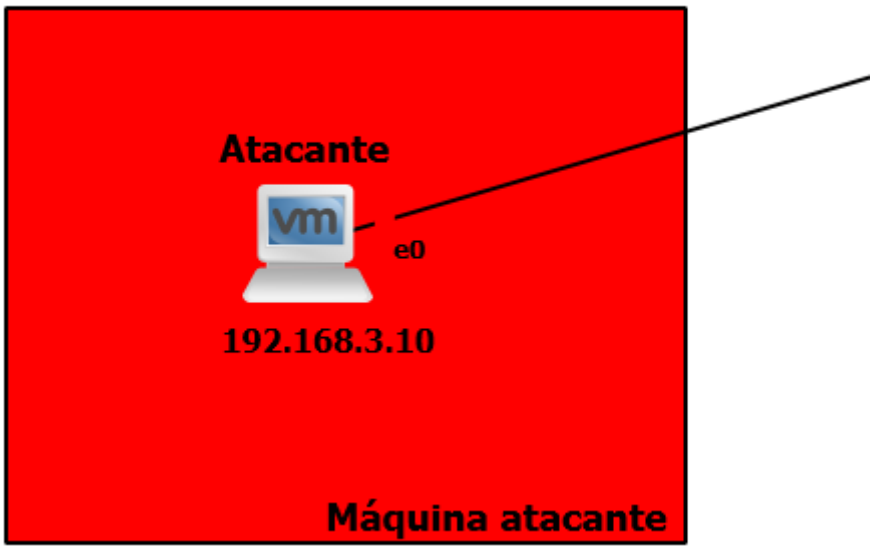
Dentro de esta zona, se ha realizado una simulación del entorno empresarial, recreando la red de los trabajadores. En esta simulación se cuenta con cuatro máquinas que representan a los usuarios empleados, como se muestra en la figura 5:

Figura 7 Zona LAN



También dentro de esta zona, se conectará la máquina virtual del atacante con el sistema operativo Kali Linux, desde la cual se generará el ataque y se obtendrá la información deseada, como se muestra en la figura 6:

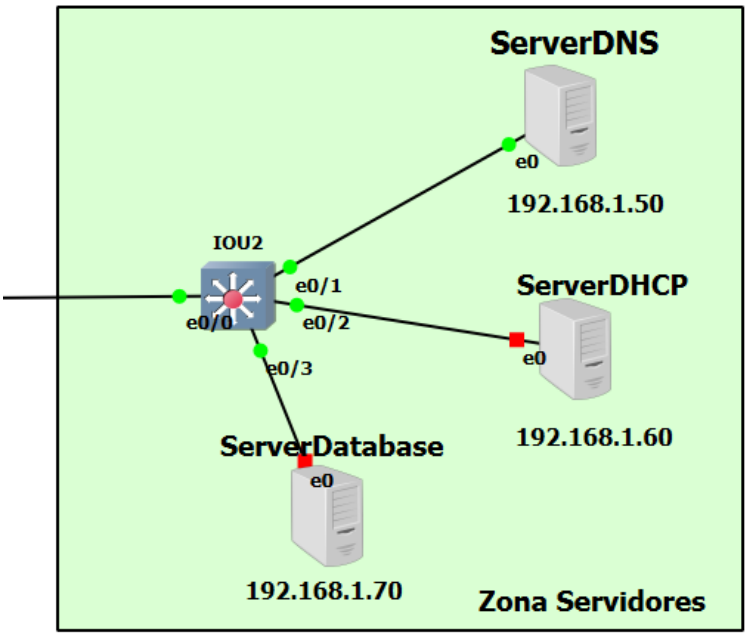
Figura 8 Máquina Atacante



4.2.5. Zona Servidores

Para esta zona, se cuenta con tres servidores, cada uno con una función específica. El primer servidor es el Servidor DNS, el segundo es el Servidor DHCP y, por último, el tercero es el Servidor de Base de Datos, como se muestra en la figura 7:

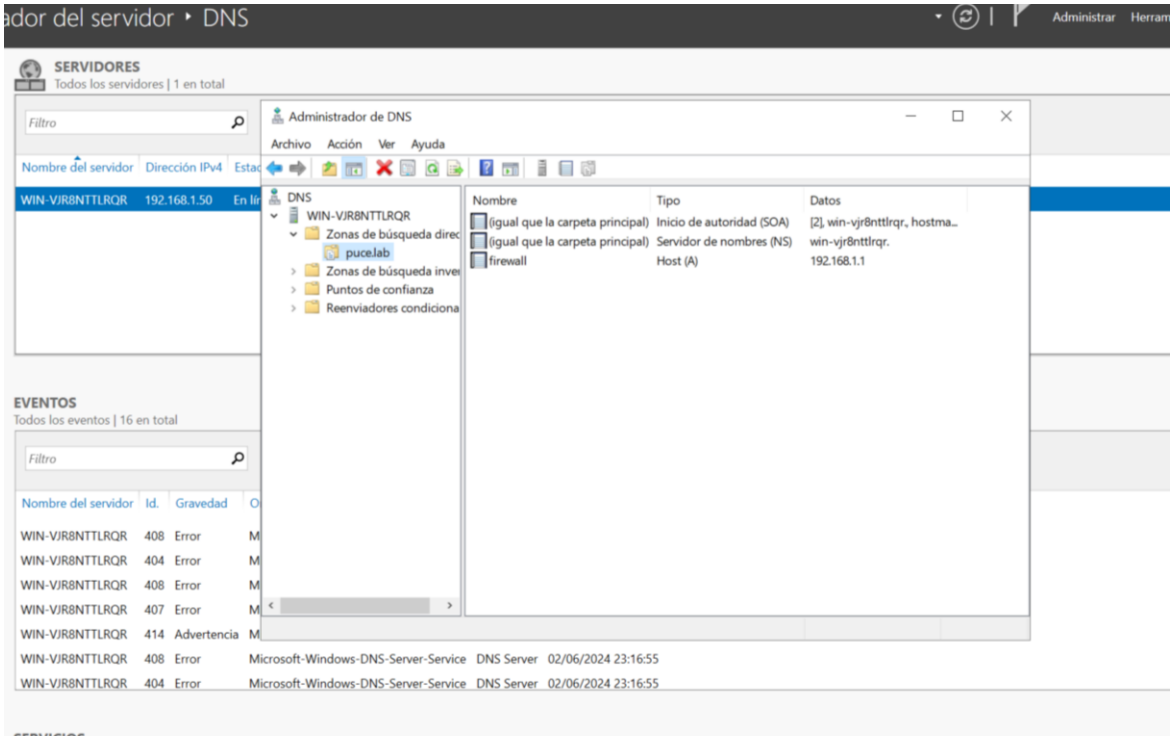
Figura 9 Zona de Servidores



Configuración del Servidor DNS

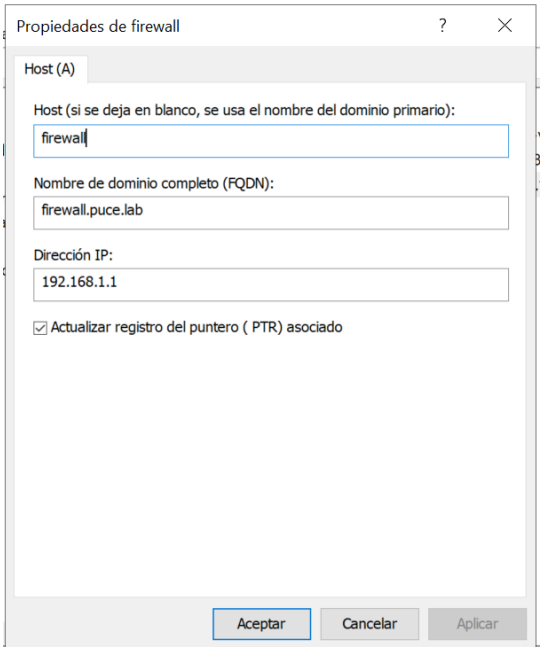
El servidor DNS se ha configurado en un sistema operativo Windows Server 2022. A continuación, se describen los pasos principales para su configuración:

Figura 10 Administración DNS



Se ha configurado el DNS en Windows Server 2022, donde se creó una zona de búsqueda directa con el dominio puce.lab, como se muestra en la figura 9:

Figura 11 Propiedades de Firewall



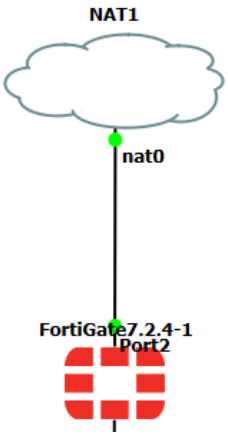
Luego, se configuro el firewall con el dominio completo firewall.puce.lab y la dirección IP del Gateway 192.168.1.1.

Todo esto para lograr la resolución de DNS que está conectada al fortigate que tiene salida a la NAT.

4.2.6. Firewall

Para este caso, se ha configurado un Fortigate, con el cual se crean las políticas correspondientes para la empresa, permitiendo así evitar ataques cibernéticos. Además, este dispositivo proporciona acceso a Internet, como se muestra en la figura 10:

Figura 12 Ilustración del Fortigate



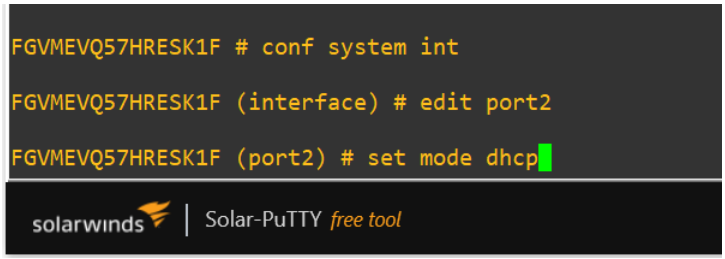
Configuración del Fortigate:

Primero es necesario conocer la dirección IP a la que nos conectaremos para acceder a la interfaz y configurar la conexión NAT. Para obtener información sobre los diferentes puertos, ingresamos el comando **show system interface.**

Figura 13 Información de puertos en el Fortigate

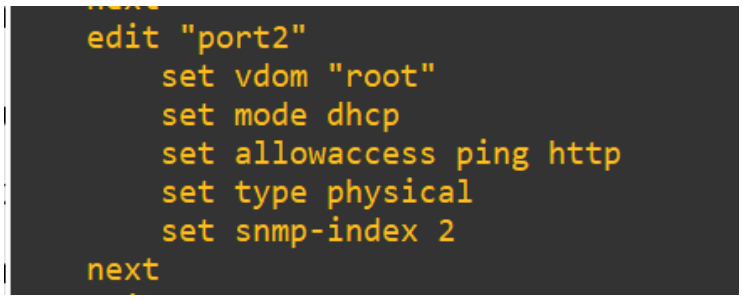
Se accede a la configuración mediante el comando **conf system interface** y luego se selecciona el puerto que se va a configurar, en este caso el Port2, con el comando **edit port2**. A continuación, se utiliza el comando **set mode dhcp** para asignar la dirección por DHCP en el Port2, el cual está conectado a la NAT.

Figura 14 Configuración del Port2



Se ejecuta el comando **show system interface** para visualizar la configuración realizada, como se muestra en la figura 13:

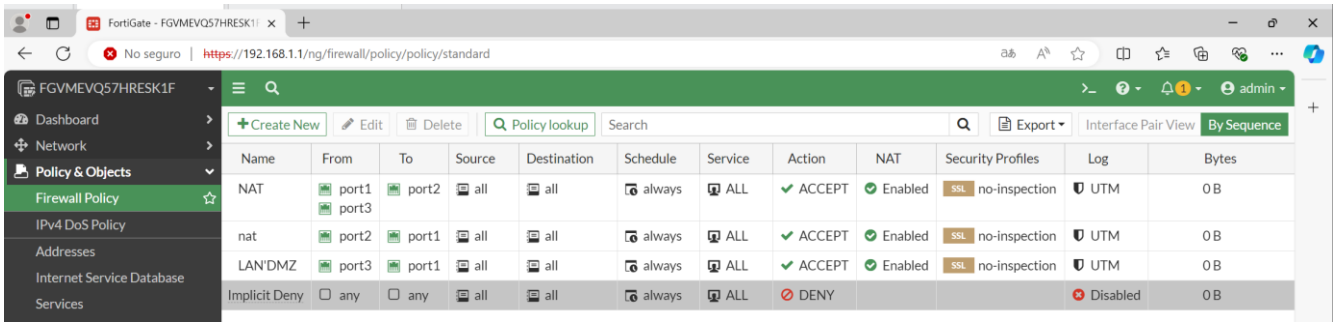
Figura 15 Show system interface



Una vez realizadas las configuraciones necesarias, procedemos a acceder a la interfaz de Fortigate para establecer las políticas requeridas para la red.

Se han configurado distintas políticas para los tres puertos habilitados en Fortigate, estableciendo conexiones entre las diversas zonas. Se excluyó la zona DMZ, permitiendo únicamente el acceso a dicha zona y bloqueando el tráfico saliente desde esa misma zona hacia el exterior.

Figura 16 Políticas en el Fortigate



4.2.7. Configuración de la Máquina Atacante

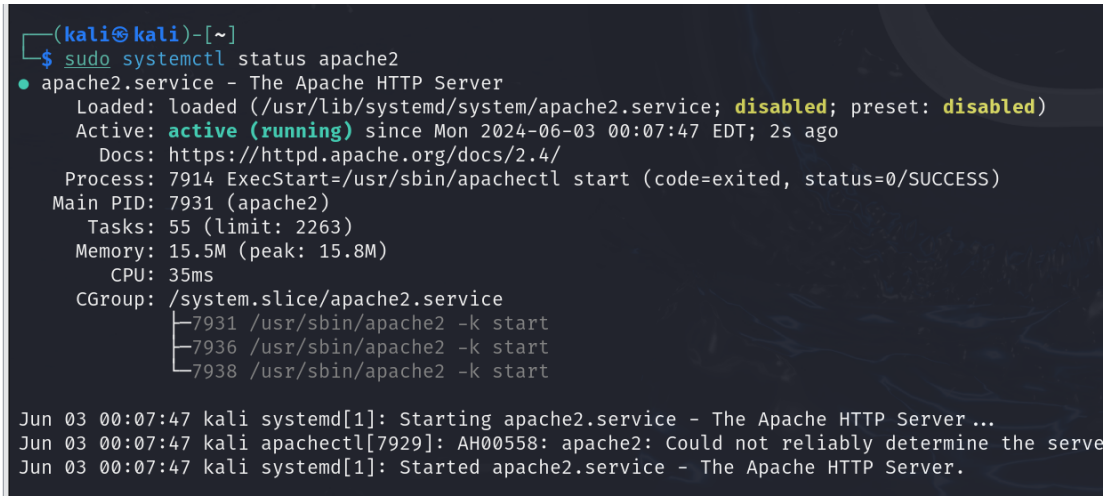
- Se utilizará la máquina virtual de Kali Linux, con el cual usaremos las respectivas herramientas para realizar el ataque.
- La máquina atacante se ha configurado para ejecutar herramientas específicas de ataque DNS, como bettercap.
- La herramienta bettercap no viene instalada en Kali Linux, por lo que tenemos que instalar manualmente, usando el comando **sudo apt install bettercap,** de esta manera se instalará y podremos hacer uso de la herramienta.

Figura 17 Instalación de bettercap

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install bettercap
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
bettercap is already the newest version (2.32.0+git20240107.924ff57-1~exp1).
0 upgraded, 0 newly installed, 0 to remove and 1579 not upgraded.
```

- Dentro de la misma máquina, debemos tener el instalado el servidor Apache2 donde tendremos una página falsa para el ataque.
- Procedemos a instalar el servidor Apache2, con el comando **sudo apt install Apache2.**

Figura 18 Instalación de Apache



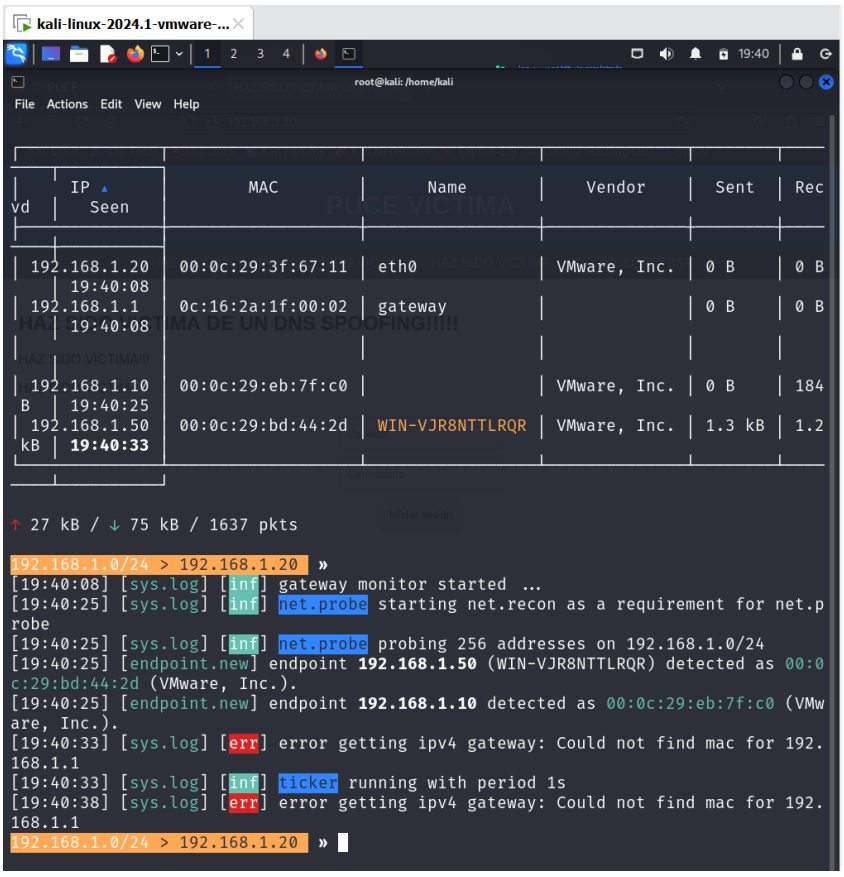
4.3. Simulación del ataque DNS spoofing

4.3.1. Uso de la herramienta bettercap en Kali Linux

Ingresamos como administrador a la herramienta bettercap, donde ejecutaremos los dos siguientes comandos:

- net.probe on: para detectar los dispositivos que están conectados a la red.

Figura 19 Comando net.probe on



- Luego, ejecutamos el comando set arp.spoof targets <ip victima>, con este comando suplantamos la ip del Gateway.

Figura 20 Comando set arp.spoof targets

- Seguido de esto, realizamos el comando arp.spoof on para que esta suplantación se active.

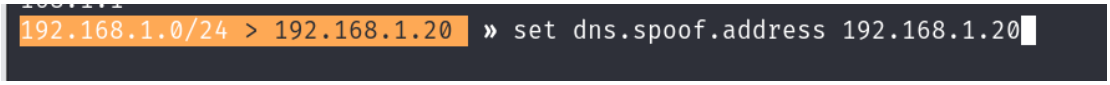
Figura 21 Comando arp.spoof on

- El siguiente comando nos ayudará para suplantar el dominio que queramos cuando la víctima quiera ingresar, set dns.spoof.domains <nombre del dominio>.

Figura 22 Comando set dns.spoof.domains

- A continuación, se ejecuta el comando set dns.spoof.address <ip del servidor donde está la página falsa>, con esto redirigiremos a la víctima a nuestra página web suplantada.

Figura 23 Comando set dns.spoof.address



- Por último, el comando dns.spoof on, para que de esta manera el envenenamiento DNS se active.

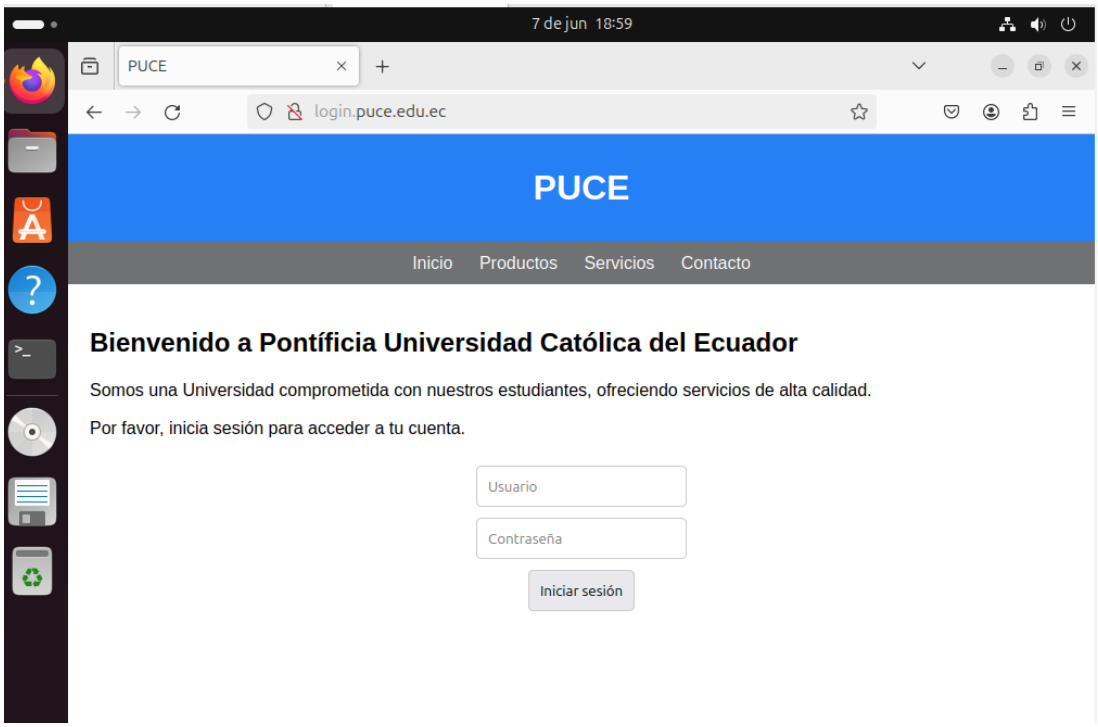
Figura 24 Comando dns.spoof.on

4.3.2. Análisis del ataque de envenenamiento DNS

El usuario está navegando normalmente por Internet, pero cuando el atacante ejecuta el envenenamiento del DNS, el dominio que ha sido infectado cambiará.

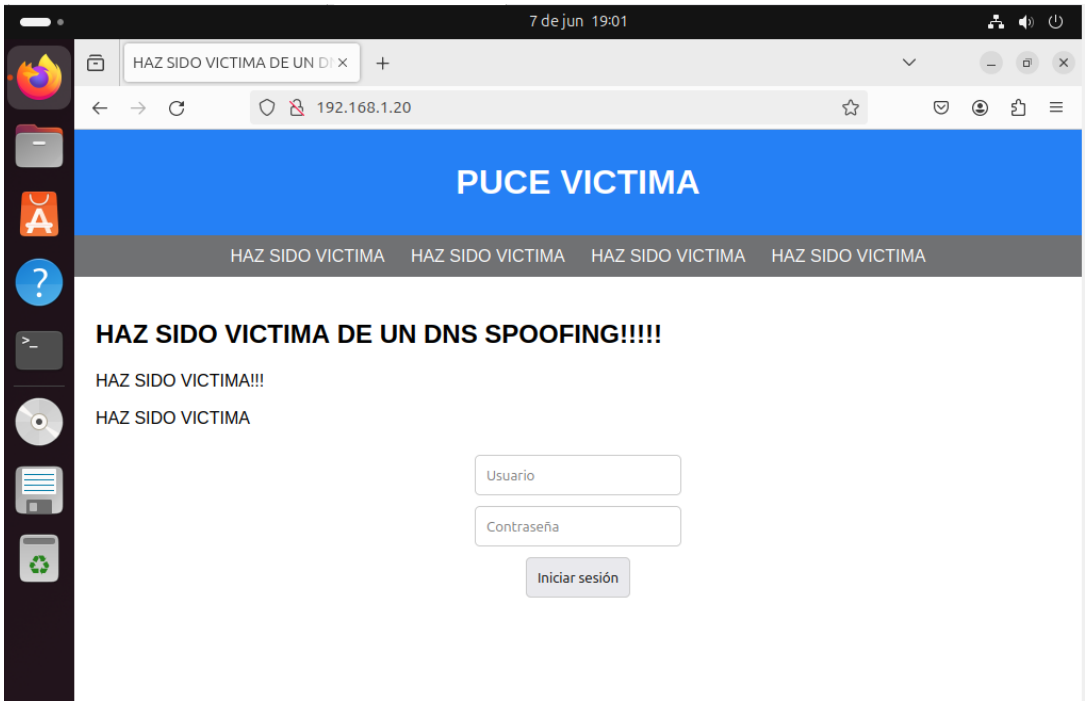
- Primero, se observará cómo el usuario accede al dominio http://login.puce.edu.ec/, el cual será infectado por el atacante.

Figura 25 Página Empresarial



- Cuando el ataque es activado, en el momento en que el usuario víctima intenta acceder a ese dominio, este puede aparecer corrompido y mostrar algo diferente o alterado.

Figura 26 Página alterada



- En este caso podemos observar que el sitio web a sido manipulado, y que lo que queramos hacer no podrá ser posible.

5. CAPÍTULO V – MEDIDAS PARA MITIGAR ATAQUES DNS

5.1. Implementar DNSSEC (Domain Name System Security Extensions):

DNSSEC es una extensión del protocolo DNS que proporciona protección a las consultas DNS. Al establecer DNSSEC, la información DNS se firma digitalmente, lo que ayuda a prevenir la manipulación de datos y garantiza la autenticidad de las respuestas DNS.

5.1.1. ¿Cómo Funciona DNSSEC?

Proceso de Firma y Verificación:

Firma de Zonas: El administrador de la zona DNS utiliza su clave privada para firmar digitalmente cada zona DNS. La clave pública adecuada se publica en DNS para que los resolvers puedan verificar las firmas.

Publicación de Claves: Las claves públicas se publican en los registros DNSKEY como registros de recursos.

Verificación de Firmas: Un resolver de DNS verifica la firma digital con la clave pública publicada cuando recibe una respuesta firmada. Si la firma es válida, se considera que la respuesta es auténtica.

Cadenas de Confianza: DNSSEC utiliza una cadena de confianza que comienza en la zona raíz del DNS y se propaga a través de los niveles del dominio para garantizar que la clave pública del servidor es auténtica.

5.1.2. Implementación de DNSSEC

- Generar Claves Criptográficas: Generar las claves públicas y privadas necesarias para firmar las zonas DNS.
- Firmar la Zona: Firmar la zona DNS con la clave privada para crear los registros RRSIG.
- Publicar Claves Públicas: Publicar la clave pública en la zona DNS para permitir la verificación de las firmas.
- Configurar DS Records: Configurar los registros DS para crear una cadena de confianza hacia la zona raíz.
- Verificar Configuración: Verificar la configuración y la funcionalidad de DNSSEC utilizando herramientas de prueba para asegurar que las firmas y la validación funcionan correctamente.

5.1.3. Herramientas de Implementación y Verificación

- BIND: Un servidor DNS ampliamente utilizado que soporta la implementación de DNSSEC.
- NSD: Otro servidor DNS que proporciona soporte para DNSSEC.
- Unbound: Un resolver de DNS que soporta la validación de DNSSEC.
- DNSViz: Una herramienta en línea para visualizar y diagnosticar problemas de configuración de DNSSEC.
- dnsviz.net: Un sitio web para la validación y prueba de configuraciones DNSSEC.

5.2. Utilizar servidores DNS autorizados y confiables:

Asegurarse de que los servidores DNS que se utilizan en la red corporativa sean confiables y estén configurados correctamente. Evite usar servidores DNS públicos y solo permitir que servidores autorizados realicen consultas DNS en la red.

5.3. Configurar firewalls y filtros de DNS:

Configure filtros y firewalls DNS para evitar consultas DNS maliciosas y filtrar paquetes DNS sospechosos. Esto puede ayudar a evitar ataques de envenenamiento DNS y proteger la integridad de las consultas DNS en la red corporativa.

5.4. Realizar actualizaciones y parches regulares:

Mantener los sistemas y software actualizados con los parches de seguridad más recientes es crucial para protegerse de vulnerabilidades conocidas que podrían ser utilizadas para ataques de envenenamiento DNS y otras amenazas de seguridad.

5.5. Monitorear el tráfico DNS:

Implementar herramientas de monitoreo de tráfico DNS para detectar actividades sospechosas y analizar los registros de DNS para encontrar signos de envenenamiento DNS u otros ataques. El monitoreo constante del tráfico DNS puede ayudar a detectar y reducir los ataques de manera proactiva.

5.6. Educación y capacitación del personal:

Los ataques de envenenamiento DNS causados por ingeniería social o errores humanos pueden prevenirse capacitando al personal en ciberseguridad y concientizándolos sobre las prácticas de seguridad en línea. Enseñar a los empleados a verificar la autenticidad de las fuentes antes de hacer clic en enlaces o descargar archivos puede reducir el riesgo de compromiso de seguridad.

CONCLUSIONES

- Se logró crear un entorno de red virtual que reproduce fielmente la infraestructura de una red corporativa, incluyendo servidores, estaciones de trabajo y un servidor DNS. Esta configuración permitió replicar condiciones reales de operación y experimentar con diversas técnicas de ataque y defensa, proporcionando una base sólida para los siguientes objetivos del proyecto.
- Se implementó exitosamente una simulación de ataque de envenenamiento de DNS en la red virtual corporativa. Esta simulación permitió identificar vulnerabilidades específicas dentro de la infraestructura DNS y proporcionó un escenario práctico para observar los efectos y las técnicas utilizadas por los atacantes para comprometer la resolución de nombres de dominio.
- El análisis del ataque de DNS reveló varias debilidades críticas en la configuración de la red y en las prácticas de seguridad DNS. Los resultados del ataque mostraron cómo los atacantes pueden redirigir el tráfico a destinos maliciosos, comprometiendo la integridad y la confidencialidad de los datos. Este análisis fue esencial para comprender la magnitud del riesgo y la efectividad de las técnicas de ataque.
- Se propusieron y evaluaron una serie de medidas de mitigación para contrarrestar los riesgos asociados con el ataque de DNS. Entre estas medidas se incluyeron la implementación de DNSSEC, la configuración adecuada de los servidores DNS, y la adopción de prácticas de monitoreo y respuesta ante incidentes. Estas recomendaciones buscan fortalecer la seguridad de la infraestructura DNS y reducir la probabilidad de futuros ataques exitosos.

RECOMENDACIONES

- Programar auditorías de seguridad y pruebas de penetración periódicas en el entorno DNS les permite identificar vulnerabilidades y áreas de mejora en la infraestructura. Estas pruebas deben incluir simulaciones de ataques DNS para evaluar la eficacia de las medidas de seguridad implementadas y para mantener un sistema robusto y seguro.
- Implementar un sistema de monitoreo de tráfico DNS y configurar reglas de filtrado adecuadas les ayuda a detectar actividades sospechosas y a prevenir ataques de envenenamiento de DNS. El monitoreo continuo puede identificar patrones inusuales y alertar a los administradores de red sobre posibles amenazas, permitiendo una respuesta rápida.
- Mejorar la seguridad de la red mediante la implementación de firewalls, sistemas de detección y prevención de intrusiones y segmentación de redes les permite reducir la superficie de ataque y dificultar el éxito de los ataques DNS.

BIBLIOGRAFÍAS

Arguelles, G. T. (13 de 06 de 2024). *Acces Quality*. Obtenido de https://www.accessq.com.mx/tipos-de-ataques-dns/

Brown, S. (2019). *"Power Quality in Electrical Systems."*. Obtenido de McGraw-Hill Education.

Case, J. F. (1990). *"RFC 1157: A Simple Network Management Protocol (SNMP)."* . Obtenido de Internet Engineering Task Force (IETF).

Cheswick, W. R. (2003). *"Firewalls y Seguridad en Internet: Repensando la Arquitectura de Red."* . Obtenido de Addison-Wesley.

Ching, F. D. (2014). *"Diseño y Dibujo Arquitectónico." (Versión PDF)*. Obtenido de Editorial Gustavo Gili.

Cisco Systems, Inc. (2011). *"Cisco Networking Academy Program: CCNA Discovery 1."*. Obtenido de Cisco Press.

Cloudflare. (2024). Obtenido de https://www.cloudflare.com/es-es/learning/dns/what-is-dns/

Cloudflare. (2024). *Cloudflare*. Obtenido de https://www.cloudflare.com/es-es/learning/dns/dns-security/

Comer, D. (2017). *"Redes de Computadoras y TCP/IP."*. Obtenido de Pearson Educación.

De Luz, S. (27 de 05 de 2024). *RedesZone*. Obtenido de https://www.redeszone.net/tutoriales/servidores/tcpdump-capturar-trafico-red-linux/

Forouzan, B. A. (2017). *"Redes de Computadoras: Un Enfoque Descendente."*. Obtenido de McGraw-Hill Interamericana.

GNS3. (s.f.). Obtenido de https://docs.gns3.com/docs/

IBM, S. (2023). *Cost of a Data Breach Report*. Obtenido de Data breach: https://www.ibm.com/reports/data-breach

INCIBE. (08 de 10 de 2020). Obtenido de https://www.incibe.es/empresas/blog/son-y-sirven-los-siem-ids-e-ips

Kosinski, M. (17 de 05 de 2024). *IBM*. Obtenido de https://www.ibm.com/es-es/topics/phishing

latam.kaspersky.com. (28 de 05 de 2024). Obtenido de https://latam.kaspersky.com/resource-center/threats/ddos-attacks

Laudon, K. C. (2016). *"Sistemas de Información Gerencial: Administración de la Empresa Digital." (Versión PDF)*. Obtenido de Pearson Educación.:

https://www.economicas.unsa.edu.ar/sigeco/archivos/sig_material/Capitulo%20Base%20de%20Datos%20..%20Laudon%20y%20Laudon%202013.pdf

Lemon, T. (1997). *"RFC 2131: Dynamic Host Configuration Protocol."*. Obtenido de Internet Engineering Task Force (IETF).

Montaña, J. (2009). *"Diseño Arquitectónico: Fundamentos, Herramientas y Estrategias." (Versión PDF)*. Obtenido de Editorial Gustavo Gili.

Networking Academy. (5 de 05 de 2024). Obtenido de https://www.netacad.com/es/courses/packet-tracer

Nowak, S. (08 de 03 de 2024). *Nuclio Digital School*. Obtenido de https://nuclio.school/blog/que-es-el-pentesting/

OMNeT++. (s.f.). Obtenido de https://omnetpp.org/intro/

OpenWebinars.net. (s.f.). Obtenido de https://openwebinars.net/blog/que-es-openvas/

OpenWebinars.net. (07 de 01 de 2022). Obtenido de https://openwebinars.net/blog/wireshark-que-es-y-ejemplos-de-uso/

Patterson, D. A. (2017). *"Arquitectura de Computadoras: Fundamentos de los procesadores superescalares."*. Obtenido de McGraw-Hill Interamericana.

Ramachandran, A. (2017). *"Cloud Computing: Concepts, Technology & Architecture."*. Obtenido de MK Publications.

Sepulveda, M. (23 de 02 de 2023). *Ciberseguridad Club*. Obtenido de https://ciberseguridad.club/que-es-nessus-y-como-utilizarlo/

Sl, S. (s.f.). *DonDominio*. Obtenido de https://www.dondominio.com/es/help/266/dnssec-que-es-y-como-funciona/

Solberg, J. K. (2011). *"Sistemas Informáticos: Diseño e Implementación."* . Obtenido de Prentice Hall.

Tanenbaum, A. S. (2007). *"Sistemas Operativos Distribuidos."*. Obtenido de Pearson Educación.Servicios de alojamiento y sincronización.

Tanenbaum, A. S. (2011). *"Redes de Computadoras."*. Obtenido de Pearson Educación.

Tenable®. (27 de 06 de 2024). Obtenido de Escáner de vulnerabilidades Nessus:Solución de seguridad en la red: https://es-la.tenable.com/products/nessus

Turban, E. P. (2018). *"Gestión de la tecnología de la información: Perspectiva estratégica."*. Obtenido de Pearson Educación.

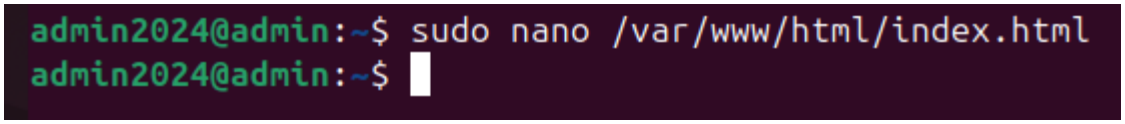
We Live Security. (18 de 06 de 2012). Obtenido de https://www.welivesecurity.com/la-es/2012/06/18/dns-spoofing/

6. ANEXO A

Código HTML

Se muestra el directorio donde se almacena el código de la página empresarial, como se ilustra en la figura 27:

Anexo A Directorio HTML



- A continuación, se presenta el código HTML que se utilizó para construir la página empresarial:

```
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>PUCE</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            margin: 0;
            padding: 0;
        }
        header {
            background-color: #2580F5;
            color: #fff;
```

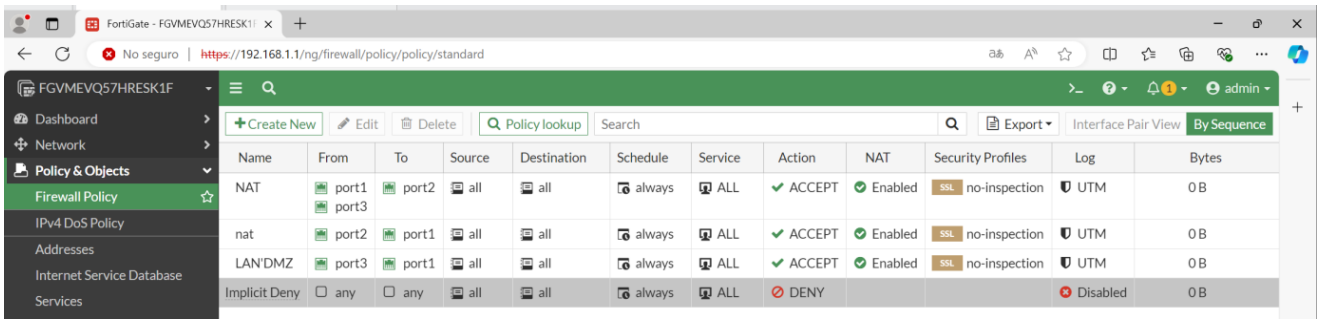
```
    padding: 10px 0;
    text-align: center;
}
nav {
    background-color: #707173;
    color: #fff;
    padding: 10px 0;
    text-align: center;
}
nav a {
    color: #fff;
    text-decoration: none;
    margin: 0 10px;
}
section {
    padding: 20px;
}
footer {
    background-color: #333;
    color: #fff;
    padding: 10px 0;
    text-align: center;
    position: fixed;
    bottom: 0;
```

```
            width: 100%;
        }
        .login-container {
            text-align: center;
            margin-top: 20px;
        }
        input[type="text"],
        input[type="password"],
        input[type="submit"] {
            padding: 10px;
            margin: 5px;
            border-radius: 5px;
            border: 1px solid #ccc;
        }
    </style>
</head>
<body>
    <header>
        <h1>PUCE</h1>
    </header>
    <nav>
        <a href="#">Inicio</a>
        <a href="#">Productos</a>
        <a href="#">Servicios</a>
```

```
            <a href="#">Contacto</a>
        </nav>
        <section>
            <h2>Bienvenido a Pontífica Universidad Católica del Ecuador</h2>
            <p>Somos una Universidad comprometida con nuestros estudiantes, ofreciendo servicios de alta calidad.</p>
            <p>Por favor, inicia sesión para acceder a tu cuenta.</p>
            <div class="login-container">
                <form action="login.php" method="post">
                    <input type="text" name="username" placeholder="Usuario" required><br>
                    <input type="password" name="password" placeholder="Contraseña" required><br>
                    <input type="submit" value="Iniciar sesión">
                </form>
            </div>
        </section>
        <footer>
            <p>&copy; 2024 PUCE. Todos los derechos reservados.</p>
        </footer>
    </body>
    </html>
```

7. Anexo B

Anexo B Políticas en Fortigate


FortiGate - FGVMEVQ57HRESK1F
No seguro | https://192.168.1.1/ng/firewall/policy/policy/standard
FGVMEVQ57HRESK1F
admin
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Create New
Edit
Delete
Policy lookup
Search
Export
Interface Pair View
By Sequence
Name
From
To
Source
Destination
Schedule
Service
Action
NAT
Security Profiles
Log
Bytes
NAT
port1
port3
port2
all
all
always
ALL
ACCEPT
Enabled
no-inspection
UTM
0 B
nat
port2
port1
all
all
always
ALL
ACCEPT
Enabled
no-inspection
UTM
0 B
LAN'DMZ
port3
port1
all
all
always
ALL
ACCEPT
Enabled
no-inspection
UTM
0 B
Implicit Deny
any
any
all
all
always
ALL
DENY
Disabled
0 B