Alumno: Rodrigo Vila

Ejercicio número 1 - Unidad 3

Buscar en Internet alguna noticia de un incidente (ataque) informático (no importa el tipo de técnica de ataque) y hacer un análisis personal de cómo PIENSAN que sucedió y cómo habría que evitarlo de acuerdo a sus puntos de vista o conocimientos.

Fuente: https://haveibeenpwned.com/

"El hackeo de abril de 2021 a Facebook fue un incidente que afectó a más de 530 millones de usuarios de la plataforma. En este caso, los datos personales, incluidos números de teléfono, direcciones de correo electrónico, nombres y otros detalles, fueron extraídos de la plataforma y luego publicados en un foro de hacking. El conjunto de datos robados, que se vendía inicialmente en línea, fue filtrado de forma gratuita poco después, lo que aumentó la preocupación sobre la privacidad y la seguridad de los usuarios de Facebook en todo el mundo. La vulnerabilidad que permitió este hackeo implicaba la explotación de una falla en la función de importación de contactos de la plataforma, lo que permitió a los actores maliciosos recopilar grandes cantidades de información de usuarios."

Como bien describe la noticia, el hackeo se produjo aprovechando una vulnerabilidad en la funcion de importacion de contactos que tenia la plataforma. Mi pensamiento es que los atacantes utilizaron varios exploits y tecnicas para intentar colarse por la brecha, o bien intentaron por todos los medios hasta que encontraron poder filtrarse a traves de esa funcion de importacion de contactos.

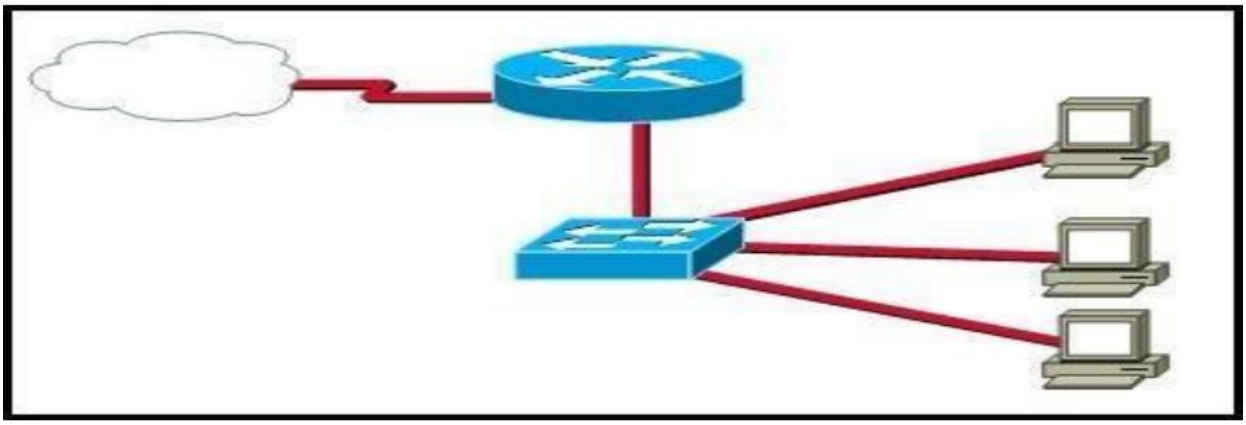
Mas alla de lo que pienso yo con mi limitado conocimiento sobre el tema, investigando un poco descubro que: "se cree que los hackers utilizaron técnicas de web scraping o raspado web para recopilar datos de perfiles públicos y luego los combinaron con los datos obtenidos a través de la vulnerabilidad en la función de importación de contactos."

Para poder evitarlo creo que la compañia deberia tener expertos en seguridad intentando hackear la plataforma constantemente, para asi identificar las brechas antes que lo hagan los ciberdelincuentes y asi poder parchearlas, por medio de auditorias de seguridad regulares.

Tambien los datos personales de los usuarios deberian estar encriptados, por si son robados o extraidos por los atacantes, no puedan ser interpretados y no quede al descubierto la informacion sensible de los usuarios.

Ejercicio número 2 - Unidad 3

Completar con direccionamiento y puertos, utilizando el protocolo PAT.



IP Pública: 200.168.50.100

PC1:

IP Privada: 192.168.0.10

Servicio HTTP, puerto 80

Direccionamiento: 192.168.0.10:80

Redireccionamiento PAT: 200.168.50.100:5001

PC2:

IP Privada: 192.168.0.20

Servicio FTP, puerto 21

Direccionamiento: 192.168.0.10:21

Redireccionamiento PAT: 200.168.50.100:5002

PC3:

IP Privada: 192.168.0.30

Servicio MySQL, puerto 3306

Direccionamiento: 192.168.0.10:3306

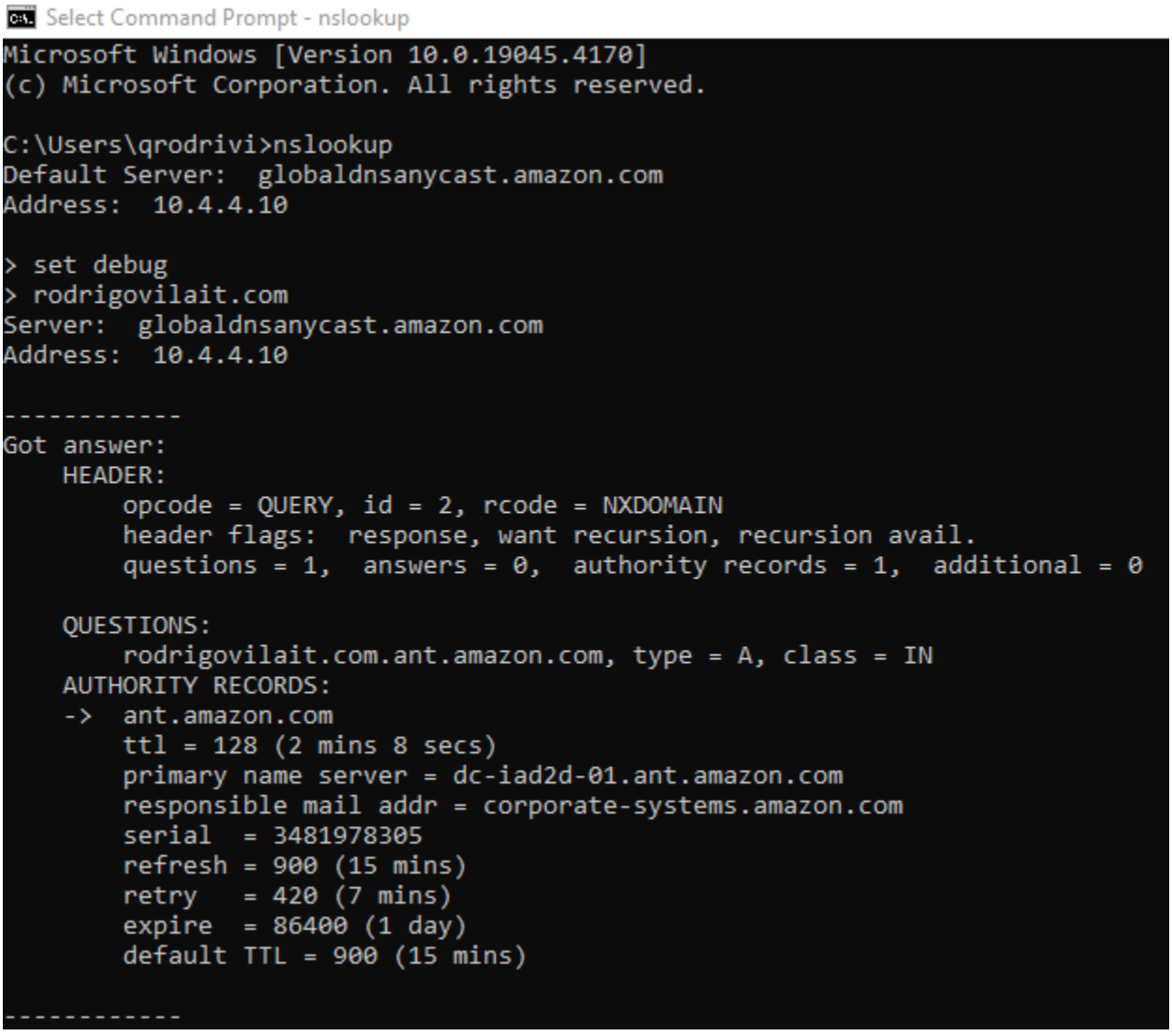
Redireccionamiento PAT: 200.168.50.100:5003

Ejercicio número 3 - Unidad 3

Utilizar y probar el comando "nslookup", usar como guía el help del mismo comando. Buscar 3 direcciones IP y resolverlas a través del mismo comando.

- Realizando un "*nslookup"* desde un equipo en la red corporativa de Amazon descubro que la IP del servidor DNS en la que estoy consultando es 10.4.4.10 y el dominio del servidor es: globaldnsanycast.amazon.com
- Utilizo el comando *"set debug"* para extraer toda la información que pueda sobre los dominios.

Consulto sobre el dominio *"rodrigovilait.com":*



```
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 8, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        rodrigovilait.com, type = A, class = IN
    ANSWERS:
    ->  rodrigovilait.com
        internet address = 144.217.139.54
        ttl = 14254 (3 hours 57 mins 34 secs)

------------
Non-authoritative answer:
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 9, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 0,  authority records = 1,  additional = 0

    QUESTIONS:
        rodrigovilait.com, type = AAAA, class = IN
    AUTHORITY RECORDS:
    ->  rodrigovilait.com
        ttl = 454 (7 mins 34 secs)
        primary name server = ns1.dns-parking.com
        responsible mail addr = dns.hostinger.com
        serial  = 2024032801
        refresh = 10000 (2 hours 46 mins 40 secs)
        retry   = 2400 (40 mins)
        expire  = 604800 (7 days)
        default TTL = 600 (10 mins)

------------
Name:    rodrigovilait.com
Address:  144.217.139.54

>
```

<u>Datos relevantes que consigo:</u>

Dominio: rodrigovilait.com

IP: 144.217.139.54

DNS Server: dns.hostinger.com

Nameserver: ns1.dns-parking.com

Por deducción descubro que el dominio esta administrado a través de la empresa Hostinger.

Consulto sobre el dominio *“hostinger.com”:*

```
------------
Non-authoritative answer:
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 17, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 2,  authority records = 0,  additional = 0

    QUESTIONS:
        hostinger.com, type = AAAA, class = IN
    ANSWERS:
    ->  hostinger.com
        AAAA IPv6 address = 2606:4700::6810:936c
        ttl = 194 (3 mins 14 secs)
    ->  hostinger.com
        AAAA IPv6 address = 2606:4700::6810:926c
        ttl = 194 (3 mins 14 secs)

------------
Name:    hostinger.com
Addresses:  2606:4700::6810:936c
          2606:4700::6810:926c
          104.16.147.108
          104.16.146.108
```

<u>Datos relevantes que consigo:</u>

Dominio: hostinger.com

IPv4: 104.16.147.108

IPv4: 104.16.146.108

IPv6: 2606:4700::6810:936c

IPv6: 2606:4700::6810:926c

(2 IP relacionadas al mismo dominio)

Consulto sobre el dominio *“mercadolibre.com”:*

```
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 24, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 4,  authority records = 0,  additional = 0

    QUESTIONS:
        mercadolibre.com, type = A, class = IN
    ANSWERS:
    ->  mercadolibre.com
        internet address = 108.139.166.103
        ttl = 60 (1 min)
    ->  mercadolibre.com
        internet address = 108.139.166.101
        ttl = 60 (1 min)
    ->  mercadolibre.com
        internet address = 108.139.166.10
        ttl = 60 (1 min)
    ->  mercadolibre.com
        internet address = 108.139.166.119
        ttl = 60 (1 min)
```

Descubro 4 IPs relacionadas al dominio:

108.139.166.103

108.139.166.101

108.139.166.10

108.139.166.119

```
------------
Non-authoritative answer:
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 25, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 0,  authority records = 1,  additional = 0

    QUESTIONS:
        mercadolibre.com, type = AAAA, class = IN
    AUTHORITY RECORDS:
    ->  mercadolibre.com
        ttl = 300 (5 mins)
        primary name server = ns-368.awsdns-46.com
        responsible mail addr = awsdns-hostmaster.amazon.com
        serial  = 1
        refresh = 7200 (2 hours)
        retry   = 900 (15 mins)
        expire  = 1209600 (14 days)
        default TTL = 86400 (1 day)

------------
Name:    mercadolibre.com
Addresses:  108.139.166.103
          108.139.166.101
          108.139.166.10
          108.139.166.119
```

Nameserver: ns-368.awsdns-46.com

Deduzco que la plataforma de Mercadolibre.com esta montada en servidores de la empresa Amazon Web Services. O por lo menos parte de la gestión del dominio utiliza los servicios de AWS.

Nota: Cambiando el servidor dns con el comando “server 8.8.8.8” al server dns de Google no conseguí resultados. Creo que se debe a las configuraciones restrictivas dentro de la red corporativa. Mismo con otros comandos como “ls”, etc. Siendo “set debug” lo mas completo que pude utilizar para extraer información de estos dominios/IPs.

Adjunto imágenes:

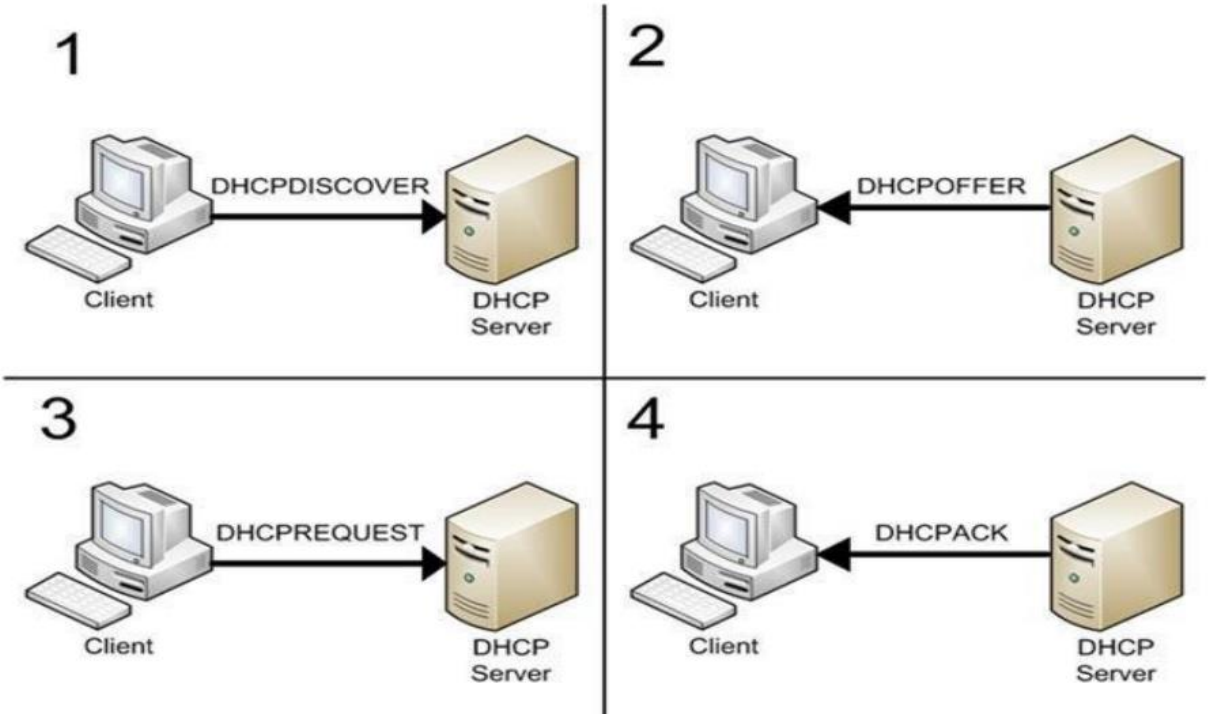
Command Prompt - nslookup

```
(c) Microsoft Corporation. All rights reserved.

C:\Users\qrodrivi>nslookup
Default Server:  globaldnsanycast.amazon.com
Address:  10.4.4.10

> server 8.8.8.8
Default Server:  dns.google
Address:  8.8.8.8

> set debug
> rodrigovilait.com
Server:  dns.google
Address:  8.8.8.8

DNS request timed out.
    timeout was 2 seconds.
timeout (2 secs)
DNS request timed out.
    timeout was 2 seconds.
timeout (2 secs)
DNS request timed out.
    timeout was 2 seconds.
timeout (2 secs)
DNS request timed out.
    timeout was 2 seconds.
timeout (2 secs)
*** Request to dns.google timed-out
>
```

```
> ls rodrigovilait.com
[globaldnsanycast.amazon.com]
*** Can't list domain rodrigovilait.com: BAD ERROR VALUE
The DNS server refused to transfer the zone rodrigovilait.com to your computer. If this
is incorrect, check the zone transfer security settings for rodrigovilait.com on the DNS
server at IP address 10.4.4.10.
```

Ejercicio número 4 - Unidad 3

Explicar el proceso de DHCP (con sus palabras o sea que comprendieron) en el dibujo, y especificar cómo sería el direccionamiento IP que ofrecería a los dispositivos (la máscara es 255.255.255.0 o podría ser la 255.255.0.0)



El dispositivo a conectar envia una peticion al servidor DHCP “DHCPDISCOVER”, el servidor DHCP le ofrece una configuración “DHCPOFFER”, el dispositivo le solicita al servidor dicha configuración “DHCPREQUEST” y por ultimo el Servidor DHCP carga la configuración en el dispositivo asignándole una IP que este dentro del rango seleccionado para DHCP “DHCPACK”.

En la configuración del DHCP uno puede elegir que rangos de IPs se asignaran a los dispositivos que quieran conectarse. Por ejemplo, uno puede setear que sea entre las ip: 192.168.0.50 a 192.168.0.100,

Y se asignarían en orden a medida que se vayan conectando los dispositivos las ip .50, .51, .52, y asi sucesivamente hasta la .100. A menos que este guardada o especificada la MAC de un dispositivo designada a cierta IP especifica dentro del rango seleccionado del DHCP.

Entregable: Estrategias de Mitigación de Ataques a Servicios y Protocolos de Red

Potenciales formas de mitigar ataques a dos servicios o protocolos de red comunes: DNS y SSH.

Ataque: Ataque de Amplificación DNS (DNS Amplification Attack)

Servicio/Protocolo Atacado: Servidores DNS

Descripción del Ataque: En un ataque de amplificación DNS, los atacantes explotan servidores DNS abiertos para amplificar el tráfico hacia un objetivo, inundando la red del objetivo con paquetes DNS.

Formas de Mitigación:

Restricción de Zonas Abiertas: Configurar los servidores DNS para restringir las consultas solo a las zonas que administran puede ayudar a mitigar el riesgo de amplificación. Esto impide que los atacantes utilicen el servidor como amplificador.

Implementación de Rate Limiting: Configurar límites de tasa en los servidores DNS puede limitar la cantidad de respuestas que un servidor puede enviar en un período de tiempo determinado, lo que reduce la efectividad de un ataque de amplificación.

Ataque: Fuerza Bruta a SSH (SSH Brute Force Attack)

Servicio/Protocolo Atacado: SSH (Secure Shell)

Descripción del Ataque: En un ataque de fuerza bruta a SSH, los atacantes intentan adivinar las credenciales de autenticación SSH de un sistema mediante la prueba de múltiples combinaciones de nombres de usuario y contraseñas.

Formas de Mitigación:

Implementación de Políticas de Contraseñas Fuertes: Promover el uso de contraseñas largas y complejas puede dificultar que los atacantes adivinen las credenciales mediante fuerza bruta.

Uso de Autenticación de Dos Factores (2FA): Habilitar la autenticación de dos factores en SSH agrega una capa adicional de seguridad, ya que incluso si un atacante obtiene las credenciales, todavía necesitaría el segundo factor de autenticación para acceder al sistema.

Configuración de Listas Blancas de IP: Limitar el acceso SSH solo a direcciones IP específicas mediante el uso de listas blancas puede reducir el riesgo de ataques de fuerza bruta al restringir el acceso solo a ubicaciones confiables.

Implementación de Bloqueo de IP: Configurar un mecanismo que bloquee temporalmente direcciones IP después de un número determinado de intentos fallidos de inicio de sesión puede ayudar a mitigar los ataques de fuerza bruta al disuadir a los atacantes y evitar accesos no autorizados.

Agrego dos ataque más. El flood por ping que se usaba mucho en mi época, desconozco si es popular en la actualidad. Y el famoso ataque distribuido de denegación de servicios DDoS realizado por botnets que dependiendo el tamaño pueden sobrecargar casi cualquier servidor.

Ataque: Ataque de Flood por Ping (Ping Flood Attack)

Servicio/Protocolo Atacado: Protocolo ICMP (Internet Control Message Protocol)

Descripción del Ataque: En un ataque de flood por ping, los atacantes inundan la red de destino con una gran cantidad de solicitudes de eco ICMP (ping), lo que puede saturar el ancho de banda de la red y agotar los recursos del sistema objetivo.

Formas de Mitigación:

Configuración de Listas de Control de Acceso (ACL): Implementar ACL en los dispositivos de red para limitar o bloquear el tráfico ICMP entrante puede ayudar a mitigar el impacto de un ataque de flood por ping al filtrar o reducir la cantidad de solicitudes ICMP que llegan al sistema objetivo.

Configuración de Rate Limiting en Routers y Firewalls: Configurar límites de velocidad en los dispositivos de red para el tráfico ICMP puede ayudar a prevenir la saturación de la red y a mitigar los efectos de un ataque de flood por ping al limitar la cantidad de paquetes ICMP que un dispositivo puede procesar en un período de tiempo dado.

Implementación de Sistemas de Detección y Prevención de Intrusiones (IDS/IPS): Utilizar IDS/IPS para monitorear el tráfico de red en busca de patrones de comportamiento anormales asociados con ataques de flood por ping y tomar medidas automáticas para mitigar el impacto del ataque, como bloquear el tráfico malicioso o alertar al administrador de red.

Configuración de Protección Anti-DDoS en el Proveedor de Servicios de Internet (ISP): Trabajar con el proveedor de servicios de Internet para implementar protecciones anti-DDoS a nivel de red puede ayudar a mitigar el impacto de un ataque de flood por ping antes de que alcance la infraestructura interna de la organización, reduciendo así el impacto del ataque.

Ataque: Ataque Distribuido de Denegación de Servicio (DDoS)

Servicio/Protocolo Atacado: Varios servicios y protocolos, incluyendo HTTP, DNS, SSH, entre otros.

Descripción del Ataque: En un ataque DDoS, un gran número de sistemas comprometidos, conocidos como botnets, son utilizados para inundar un objetivo con tráfico malicioso, sobrecargando así los recursos de red, sistema o aplicación y causando una interrupción del servicio para los usuarios legítimos.

Formas de Mitigación:

Implementación de Firewalls de Aplicaciones Web (WAF): Utilizar un WAF puede ayudar a filtrar el tráfico malicioso antes de que llegue a la aplicación web, mitigando así los efectos de un ataque DDoS dirigido a través del protocolo HTTP.

Configuración de Servicios de Mitigación de DDoS: Contratar servicios de mitigación de DDoS ofrecidos

por proveedores especializados puede ayudar a detectar y mitigar ataques DDoS de manera proactiva, redirigiendo el tráfico malicioso lejos del objetivo y manteniendo la disponibilidad del servicio.

Implementación de Análisis de Comportamiento de Red (NBA): Utilizar NBA para monitorear el tráfico de red en busca de patrones de comportamiento anormales puede ayudar a detectar y mitigar ataques DDoS en tiempo real, permitiendo la implementación de contramedidas automáticas para proteger los recursos del sistema.

Configuración de Balanceadores de Carga y Clustering: Implementar balanceadores de carga y clustering puede distribuir la carga de tráfico entre múltiples servidores y redundancias, lo que ayuda a mitigar el impacto de un ataque DDoS al distribuir el tráfico malicioso y mantener la disponibilidad del servicio.

Rodrigo Vila.-