

**CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E
INGENIERÍAS DEPARTAMENTO DE CIENCIAS
COMPUTACIONALES**



Seguridad

SECCIÓN D04

INTEGRANTES DE EQUIPO:

Gildo López Miguel Ángel

González Ramírez Alen Leonardo

Montejano Paredes Diego Fernando

PROFESOR: Vazquez Curiel Armida Griselda

11/04/2023

Actividad 3.3 Seguridad en Comunicaciones de datos

Los riesgos en una comunicación de red son una preocupación cada vez mayor para los usuarios de Internet. La red nos ofrece muchas formas de comunicación, como correo electrónico, redes sociales, chats y videoconferencias. Estas formas de comunicación pueden ser muy útiles para compartir información, pero también pueden ser una vía para la violación de nuestra privacidad.

Los usuarios de Internet pueden ser vulnerables a una variedad de amenazas, como el robo de información personal, el uso indebido de nuestros datos, el phishing, el malware y el ransomware. Estas amenazas pueden causar daños a nuestros dispositivos, invadir nuestra privacidad y robar nuestra información personal.

Por otro lado, también hay amenazas relacionadas con la seguridad de la red. Estas amenazas pueden incluir ataques de denegación de servicio, ataques de fuerza bruta y la explotación de vulnerabilidades de la red. Estos ataques pueden ser muy dañinos para las empresas, las instituciones gubernamentales y los usuarios individuales.

Es importante tener en cuenta que los riesgos de la comunicación de red no se limitan a la privacidad o seguridad de la red. Existen riesgos relacionados con la seguridad de la información, como el encriptado de la información, el control de acceso a los datos y la protección contra el uso indebido de la información. Para protegernos de los riesgos en una comunicación de red, debemos tomar precauciones para mantener nuestra información segura. Esto incluye el uso de contraseñas seguras, el mantenimiento de sistemas de seguridad actualizados y la comprensión de los riesgos relacionados con la comunicación de red. Es importante recordar que nuestra privacidad y seguridad deben ser nuestra principal prioridad.

A continuación algunos de los ataques más comunes a una red:

Spoofing: Estos ataques se realizan para ocultar la verdadera dirección IP del atacante. El atacante puede enviar mensajes con una dirección IP falsa para engañar a la víctima y obtener acceso no autorizado a la red.

- **Ataque:** Un atacante envía un paquete con una dirección IP falsa para engañar a la víctima y obtener acceso no autorizado a la red.
- **Defensa:** El destinatario verificará la dirección IP del remitente y, si es sospechosa, bloqueará el paquete. Además, el destinatario también podría usar un sistema de autenticación de dos factores para verificar la identidad del remitente antes de permitir el acceso a la red.

Denegación de Servicio (DoS): Estos ataques se realizan para sobrecargar un sistema con solicitudes y hacer que la aplicación o el equipo deje de funcionar. El atacante puede utilizar técnicas como el envío de muchos paquetes de datos o la modificación de cabeceras de paquete.

- **Ataque:** El atacante envía una gran cantidad de paquetes de datos al sistema para sobrecargarlo.
- **Defensa:** El destinatario usará técnicas como el filtrado de direcciones IP y el filtrado de contenido para bloquear los paquetes de datos no deseados. El destinatario también podría usar un sistema de detección y prevención de intrusiones para detectar y bloquear los ataques DoS antes de que tengan éxito.

Suplantación de identidad: Estos ataques se realizan para usurpar la identidad de alguien más, generalmente para obtener acceso no autorizado a una red. El atacante puede usar técnicas como el phishing para obtener información de la víctima.

- **Ataque:** El atacante utiliza técnicas como el phishing para obtener información de la víctima y obtener acceso no autorizado a la red.
- **Defensa:** El destinatario usará un sistema de autenticación de dos factores para verificar la identidad del remitente antes de permitir el acceso a la red. El destinatario también podría usar filtros de contenido para bloquear cualquier correo electrónico sospechoso y páginas web maliciosas.


A continuación una demostración práctica de ataque y defensa usando **Denegación de servicio**.

Para esta demostración haremos uso de una red LOCAL (Con fines de demostración) y dos computadoras conectadas a dicha red, una cuenta con el sistema operativo Windows 10 la cuál actuará de defensor/víctima, por otro lado la otra computadora cuenta con el sistema operativo Lubuntu 22.04 LTS la cuál actuará de atacante.

Atacante

Para el lado del atacante, se hizo uso del siguiente software: <https://github.com/Black-Hell-Team/Power-DoS.git>

La cual es una herramienta que nos permitirá mandar una cantidad muy grande de solicitudes/paquetes con el fin de reducir el rendimiento de la red de la victura. El programa luce de la siguiente manera:



```

  POWER DOSS
  Version: 1.3      Coded by Leonardo Sasaki
  Xernoboy hacked FBI

[>] Enter the target ip » |

[>] Enter the target ip » 192.168.1.75
[>] Enter the target port » 4321
[>] Enter the packet size » 512
[>] Enter how many threads to use » 2|
```

Lo primero que hacemos es ingresar la IP a la cual deseamos enviar solicitudes. Posteriormente ingresamos el puerto a usar, el tamaño del paquete y cuantos hilos de

nuestra CPU deseamos usar, si hacemos uso de más hilos aumentará la cantidad de paquetes que enviamos por segundo.

Si pulsamos enter el programa empezará a funcionar:

```
[THREAD 1] » 512 bytes sent to 192.168.1.75
[THREAD 0] » 512 bytes sent to 192.168.1.75
[THREAD 1] » 512 bytes sent to 192.168.1.75
[THREAD 0] » 512 bytes sent to 192.168.1.75
[THREAD 1] » 512 bytes sent to 192.168.1.75
[THREAD 0] » 512 bytes sent to 192.168.1.75
[THREAD 1] » 512 bytes sent to 192.168.1.75
[THREAD 0] » 512 bytes sent to 192.168.1.75
[THREAD 1] » 512 bytes sent to 192.168.1.75
```

Defensa

Por parte del defensor. si observamos los paquetes entrantes a través de una herramienta como wireshark se observa lo siguiente:

No.	Time	Source	Destination	Protocol	Length	Info
79853	15.462098	192.168.1.79	192.168.1.75	UDP	170	51822 → 4321 Len=128
79854	15.462098	192.168.1.79	192.168.1.75	UDP	170	59970 → 4321 Len=128
79855	15.462340	192.168.1.79	192.168.1.75	UDP	170	51822 → 4321 Len=128
79856	15.462340	192.168.1.79	192.168.1.75	UDP	170	51822 → 4321 Len=128
79857	15.462340	192.168.1.79	192.168.1.75	UDP	170	59970 → 4321 Len=128
79858	15.462340	192.168.1.79	192.168.1.75	UDP	170	59970 → 4321 Len=128
79859	15.462340	192.168.1.79	192.168.1.75	UDP	170	51822 → 4321 Len=128
79860	15.462584	192.168.1.79	192.168.1.75	UDP	170	59970 → 4321 Len=128
79861	15.462820	192.168.1.79	192.168.1.75	UDP	170	51822 → 4321 Len=128
79862	15.463059	192.168.1.79	192.168.1.75	UDP	170	51822 → 4321 Len=128
79863	15.463059	192.168.1.79	192.168.1.75	UDP	170	59970 → 4321 Len=128
79864	15.463296	192.168.1.79	192.168.1.75	UDP	170	51822 → 4321 Len=128
79865	15.463530	192.168.1.79	192.168.1.75	UDP	170	59970 → 4321 Len=128
79866	15.463530	192.168.1.79	192.168.1.75	UDP	170	59970 → 4321 Len=128
79867	15.463769	192.168.1.79	192.168.1.75	UDP	170	59970 → 4321 Len=128
79868	15.463769	192.168.1.79	192.168.1.75	UDP	170	51822 → 4321 Len=128
79869	15.464005	192.168.1.79	192.168.1.75	UDP	170	59970 → 4321 Len=128
79870	15.464250	192.168.1.79	192.168.1.75	UDP	170	51822 → 4321 Len=128
79871	15.464250	192.168.1.79	192.168.1.75	UDP	170	51822 → 4321 Len=128
79872	15.464497	192.168.1.79	192.168.1.75	UDP	170	51822 → 4321 Len=128
79873	15.464702	192.168.1.79	192.168.1.75	UDP	170	59970 → 4321 Len=128
79874	15.464702	192.168.1.79	192.168.1.75	UDP	170	59970 → 4321 Len=128
79875	15.464940	192.168.1.79	192.168.1.75	UDP	170	59970 → 4321 Len=128
79876	15.465189	192.168.1.79	192.168.1.75	UDP	170	59970 → 4321 Len=128
79877	15.465189	192.168.1.79	192.168.1.75	UDP	170	51822 → 4321 Len=128

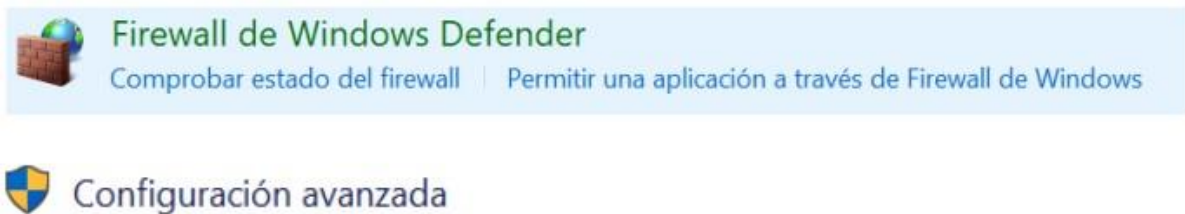
Como se puede observar, la cantidad de paquetes entrantes es inmensa, a pesar de ser solo una computadora la que está enviando las solicitudes. En un ataque real donde se hacen uso de miles de computadoras las cuales atacan al mismo tiempo, esto crecerá exponencialmente, tirando la red o saturando a tal punto de tumbarla.

Bloquear una IP con el Firewall de Windows

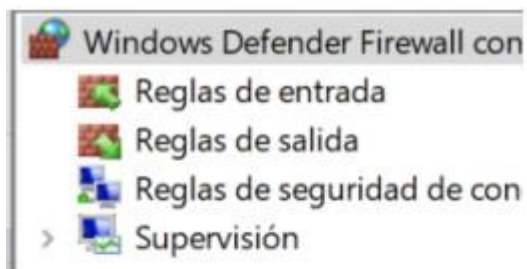
Para bloquear una dirección IP a través del Firewall de Windows, sigue estos pasos: 1. Abre el Panel de control de Windows y selecciona "Sistema y seguridad".



Selecciona "Firewall de Windows". Haz clic en "Configuración avanzada" en el panel izquierdo.



Selecciona "Reglas de entrada" en el panel izquierdo y haz clic en "Nueva regla" en el panel derecho.



Selecciona "Personalizada" y haz clic en "Siguiente"



Selecciona "Todos los programas" y haz clic en "Siguiente".

¿Se aplica esta regla a todos los programas o a uno específico?

☒ **Todos los programas**
La regla se aplica a todas las conexiones en el equipo que coinciden con otras propiedades de reglas.

☐ **Esta ruta de acceso del programa:**

Examinar...

Ejemplo: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Servicios
Especifique los servicios a los que se aplica esta regla.

Personalizar...

< Atrás **Siguiente >** Cancelar

En el campo "Protocolos y puertos", selecciona "TCP" o "UDP", dependiendo del protocolo que quieras bloquear, y escribe el número de puerto o rango de puertos que deseas bloquear.

¿A qué puertos y protocolos se aplica esta regla?

Tipo de protocolo:

Número de protocolo:

Puerto local:

Puerto remoto:

Configuración ICMP:

Cualquiera
Personalizado
HOPOPT
ICMPv4
IGMP
TCP
UDP
IPv6
Ruta-IPv6
IPv6-Frag
GRE
ICMPv6
IPv6-NoNxt
IPv6-Opts
VRRP
PGM
L2TP

< Atrás **Siguiente >** Cancelar

En el campo "Ámbito", selecciona "Estas direcciones IP" y agrega la dirección IP que deseas bloquear.

¿A qué direcciones IP locales se aplica esta regla?

☐ Cualquier dirección IP

☒ Estas direcciones IP:

Dirección IP

Especifique las direcciones IP coincidentes:

☒ Esta dirección IP o subred:

Ejemplos: 192.168.0.12
192.168.1.0/24
2002:9d3b:1a31:4:208:74ff:fe39:6c43
2002:9d3b:1a31:4:208:74ff:fe39:0/112

☐ Este intervalo de direcciones IP:

De:

A:

Aceptar **Cancelar**

Agregar...
Editar...
Quitar
Personalizar...
Agregar...
Editar...
Quitar
Siguiente > **Cancelar**

En el campo "Acción", selecciona "Bloquear la conexión" y haz clic en "Siguiente".

¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?

☐ **Permitir la conexión**
Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

☐ **Permitir la conexión si es segura**
Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

Personalizar...

☒ **Bloquear la conexión**

< Atrás **Siguiente >** **Cancelar**

Selecciona las opciones de perfil adecuadas y haz clic en "Siguiente". Asigna un nombre a la regla y escribe una descripción opcional.

¿Cuándo se aplica esta regla?

☒ **Dominio**
Se aplica cuando un equipo está conectado a su dominio corporativo.

☒ **Privado**
Se aplica cuando un equipo está conectado a una ubicación de red privada, como una red doméstica o del lugar de trabajo.

☒ **Público**
Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

< Atrás Siguiente > Cancelar

Haz clic en "Finalizar".

Nombre:
Bloqueo de ip

Descripción (opcional):

< Atrás Finalizar Cancelar

Una vez que hayas creado la regla, el Firewall de Windows bloqueará cualquier tráfico entrante de la dirección IP que especificaste.

Usamos la siguiente regla para bloquear la ip que nos está atacando:

Protocol type: UDP

Protocol number: 17

Local port: Specific Ports

 Example: 80, 443, 5000-5010

Remote port: Specific Ports

 Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings: Customize...

Which local IP addresses does this rule apply to?

☐ Any IP address

☒ These IP addresses:

Add...
Edit...
Remove

Customize the interface types to which this rule applies: Customize...

Which remote IP addresses does this rule apply to?

☐ Any IP address

☒ These IP addresses:

Add...
Edit...
Remove

1	0.000000	2806:102e:13:3189:a5de:de5e:405:ed9a	2600:1901:1:c36::	UDP	124	53040 → 443	Len=62
2	0.000113	2806:102e:13:3189:a5de:de5e:405:ed9a	2600:1901:1:c36::	UDP	124	53040 → 443	Len=62
3	0.010161	2600:1901:1:c36::	2806:102e:13:3189:a5de:de5e:405:ed9a	UDP	90	443 → 53040	Len=28
4	0.010161	2600:1901:1:c36::	2806:102e:13:3189:a5de:de5e:405:ed9a	UDP	87	443 → 53040	Len=25
5	0.010161	2600:1901:1:c36::	2806:102e:13:3189:a5de:de5e:405:ed9a	UDP	87	443 → 53040	Len=25
6	0.010390	2806:102e:13:3189:a5de:de5e:405:ed9a	2600:1901:1:c36::	UDP	95	53040 → 443	Len=33
7	0.056167	2600:1901:1:c36::	2806:102e:13:3189:a5de:de5e:405:ed9a	UDP	321	443 → 53040	Len=259
8	0.056420	2806:102e:13:3189:a5de:de5e:405:ed9a	2600:1901:1:c36::	UDP	98	53040 → 443	Len=36

Si volvemos a abrir wireshark, observaremos que esos paquetes ya no están entrando

Conclusiones

Conclusio:

Protegerse en las comunicaciones de red, se ha convertido en una necesidad absoluta para cualquier negocio o usuario de internet. El aumento de amenazas de seguridad en línea significa que todos deben estar conscientes de los riesgos y tomar medidas para asegurar su red. Esto incluye el uso de herramientas de seguridad como firewalls, antivirus y filtros de contenido para prevenir el acceso no deseado y proteger los datos importantes. Además, es importante realizar copias de seguridad regulares para minimizar la pérdida de datos. La protección de la red es la única forma de garantizar una comunicación segura entre usuarios y sistemas.

La seguridad en comunicaciones de datos es crítica en el intercambio de información digital debido a las amenazas cada vez más sofisticadas. Es importante implementar medidas efectivas, incluyendo tecnologías de cifrado, autenticación y control de acceso, así como políticas y procedimientos de seguridad. La seguridad de los datos debe ser un proceso continuo y actualizado regularmente para hacer frente a las amenazas emergentes.

Referencias

- Axarnet (2019) ¿Cómo bloquear una ip desde firewall de windows?【pasos】, Axarnet; Hosting web, VPS España y Backup en España. Available at: <https://axarnet.es/blog/bloquear-ip-firewall-windows> (Accessed: February 22, 2023).
- Mazara, K. (2021) Videotutorial ¿Qué son los ataques basados en red? - ataques, amenazas y vulnerabilidades de Ciberseguridad (Comptia security+ sy0-601): LinkedIn learning, Antes Lynda.com, LinkedIn. Available at: <https://es.linkedin.com/learning/ataques-amenazas-y-vulnerabilidades-de-ciberseguridad-comptia-security-plus-sy0-601/que-son-los-ataques-basados-en-red#:~:text=Un%20ataque%20basado%20en%20la,o%20realizar%20otra%20actividad%20maliciosa>. (Accessed: February 22, 2023).
- Kaspersky (2021) ¿Qué son los ataques ddos?, latam.kaspersky.com. Available at: <https://latam.kaspersky.com/resource-center/threats/ddos-attacks> (Accessed: February 22, 2023).