ACTIVIDAD 5: LABORATORIO DDoS

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

KEVIN NICOLÁS SIERRA GONZÁLEZ 20182020151

LUIS MIGUEL POLO 20182020158

YEISON ALEXANDER FARFAN PERALTA 20201020138

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

INGENIERÍA DE SISTEMAS

TELEINFORMATICA I

ANDRES ALEXANDER RODRIGUEZ FONSECA

2024-III

Objetivos

- Implementar un escenario de Hacking ético.
- Implementar una red en GNS3 con equipos cisco y vulnerar un usuario de la red con Kali Linux.

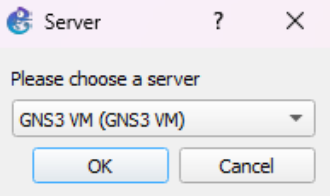
Materiales

- Computador personal con acceso a Internet
- GNS3 usando el servidor GNSVM, Kali Linux, Windows 7, IOS Cisco 2691, VirtualBox

Procedimiento

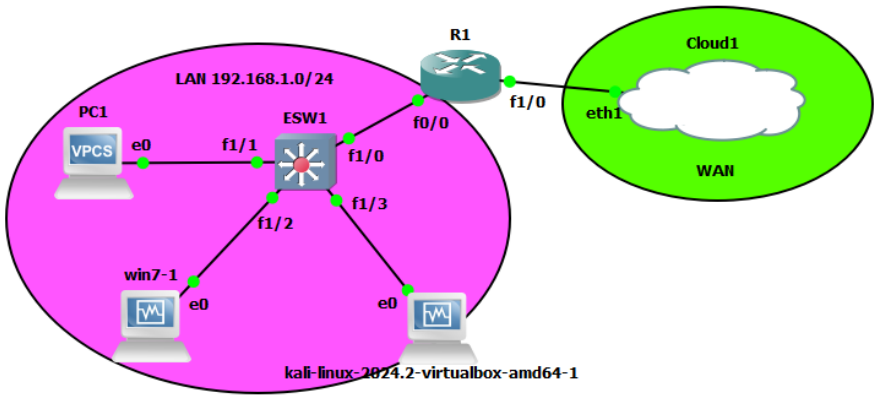
Selección de servidor para Cloud1

Se utiliza la máquina virtual GNS3 VM como un servidor



Montaje de topología de red

Se utiliza un router IOS c7200 y un swtich IOS c2691 que proporciona servicios de capa 3 (multiswtich), un cloud, la máquina virtual GNS3 VM, y tres hosts: la máquina virtual de kali Linux, la máquina virtual de windows 7 y un pc de tipo VPC que proporciona GNS3; y se conectan dentro de una red como se muestra a continuación:



Configuración de servicio dhcp en ESW1 con la red 192.168.1.0/24

Se configura un pool de direcciones en el EthernetSwitch para ofrecer servicio dhcp a los hosts

```
ESW1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ESW1(config)#interface vlan 1
ESW1(config-if)#ip add 192.168.1.2 255.255.255.0
ESW1(config-if)#no sh
ESW1(config-if)#
*Mar  1 00:06:23.151: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Mar  1 00:06:24.151: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
ESW1(config-if)#exit
ESW1(config)#service dhcp
ESW1(config)#ip dhcp pool myPOOL
ESW1(dhcp-config)#network 192.168.1.0 255.255.255.0
ESW1(dhcp-config)#default-router 192.168.1.1
ESW1(dhcp-config)#dns-server 8.8.8.8
ESW1(dhcp-config)#lease 0 7 20
ESW1(dhcp-config)#exit
ESW1(config)#ip dhcp excluded-
ESW1(config)#ip dhcp excluded-address 192.168.1.2 192.168.1.6
ESW1(config)#exit
ESW1#wr
Building configuration...
```

Configuración de puerto para recepción de dchp a través de Cloud

Se solicita servicio dhcp desde el router (R1) que proporciona el cloud

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#inter f1/0
R1(config-if)#ip address dhcp
R1(config-if)#no sh
R1(config-if)#
*Oct  6 18:12:07.091: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Oct  6 18:12:08.091: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R1(config-if)#end
R1#
*Oct  6 18:12:11.023: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]
R1#
*Oct  6 18:12:16.779: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet1/0 assigned DHCP address 10.0.3.16, mask
 255.255.255.0, hostname R1

R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
FastEthernet1/0            10.0.3.16       YES DHCP   up                    up
Serial2/0                  unassigned      YES unset  administratively down down
```

Solicitud de dhcp y prueba de conectividad en PC1

Se solicita servicio dhcp desde el PC1

```
PC1> ip dhcp
DDDO
Can't find dhcp server

PC1> ip dhcp
DORA IP 192.168.1.7/24 GW 192.168.1.1

PC1> show ip

NAME        : PC1[1]
IP/MASK     : 192.168.1.7/24
GATEWAY     : 192.168.1.1
DNS         : 8.8.8.8
DHCP SERVER : 192.168.1.2
DHCP LEASE  : 26390, 26400/13200/23100
MAC         : 00:50:79:66:68:00
LPORT       : 20002
RHOST:PORT  : 127.0.0.1:20003
MTU         : 1500

PC1> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=116 time=41.371 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=116 time=25.769 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=116 time=32.531 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=116 time=27.627 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=116 time=25.026 ms
```

Prueba de conectividad desde enrutador

Se hace una prueba de conectividad desde el router (R1) hacia el servidor DNS que en este caso es google.com (8.8.8.8) y la dirección 172.217.28.100

```
R1#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/19/24 ms
R1#ping www.google.com

Translating "www.google.com"
% Unrecognized host or address, or protocol not running.

R1#ping 172.217.28.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.217.28.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/22/28 ms
R1#
```

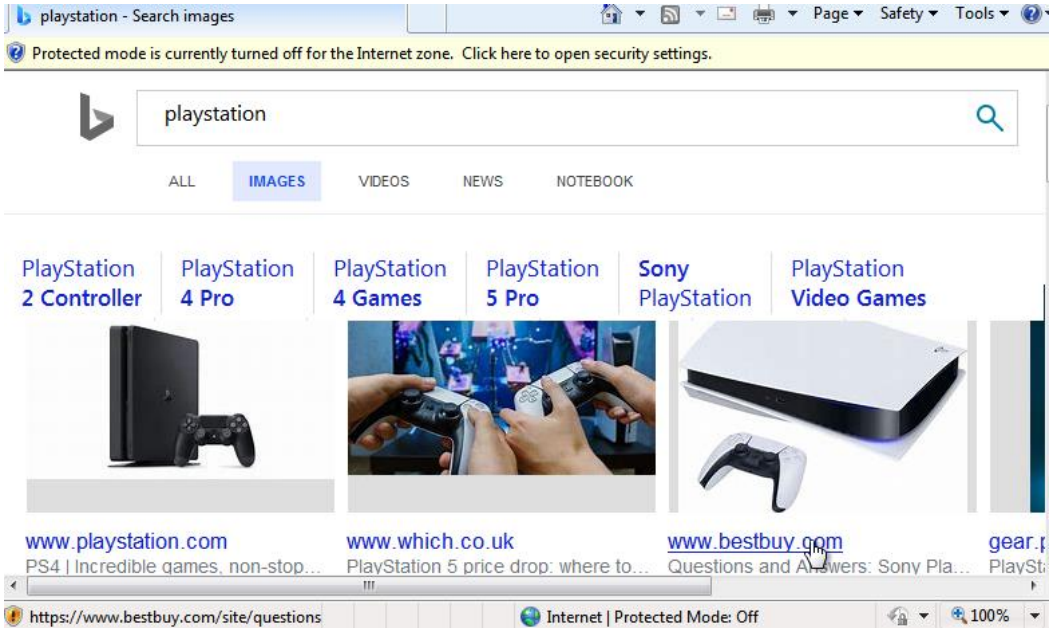
Configuración interfaz f0/0 enrutador

Se asigna una dirección IP al router dentro de la red 192.168.1.0/24 en la interfaz f0/0 y se muestra las direcciones IP de cada una de las interfaces del router.

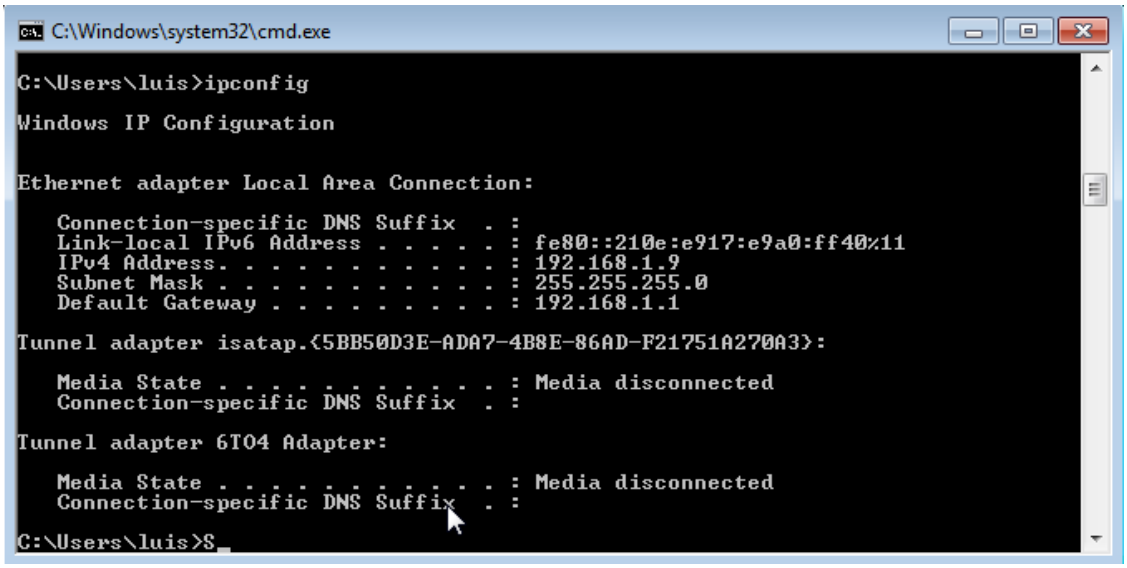
```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#
*Oct  6 18:33:12.179: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Oct  6 18:33:13.179: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#end
R1#
*Oct  6 18:33:15.291: %SYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.1.1     YES manual up                    up
FastEthernet1/0            10.0.3.16       YES DHCP   up                    up
```

Prueba de conectividad desde windows 7 (acceso a internet)

Se verifica que hay acceso a internet desde la máquina virtual de windows 7, digitando en el buscador del navegador predeterminado “playstation”



Con el comando ipconfig se verifica la dirección recibida por dhcp

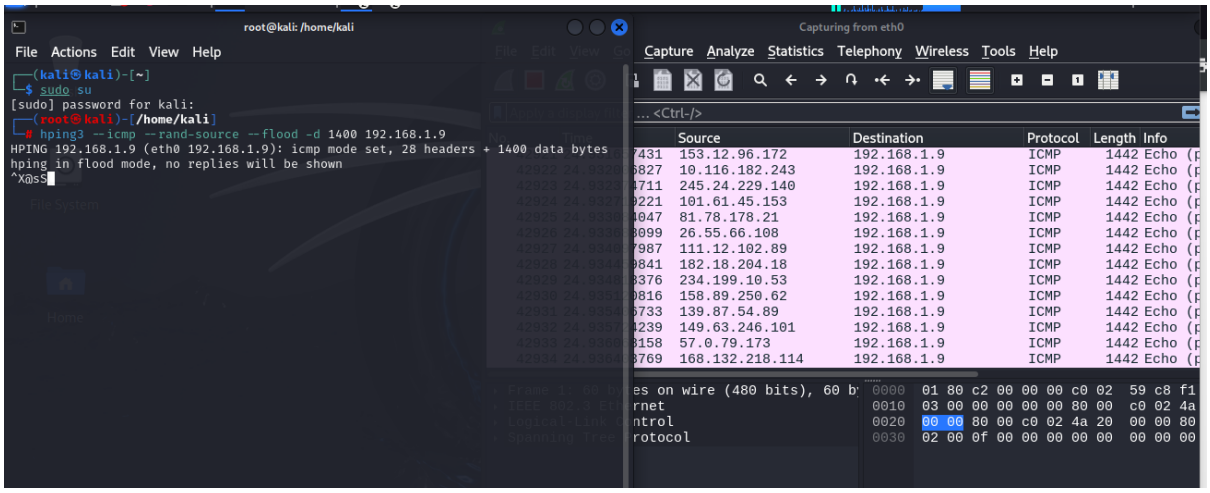


Ataque DDoS desde Kali Linux hacia Windows 7

Desde Kali Linux se inicia el ataque abriendo el analizador de tráfico Wireshark

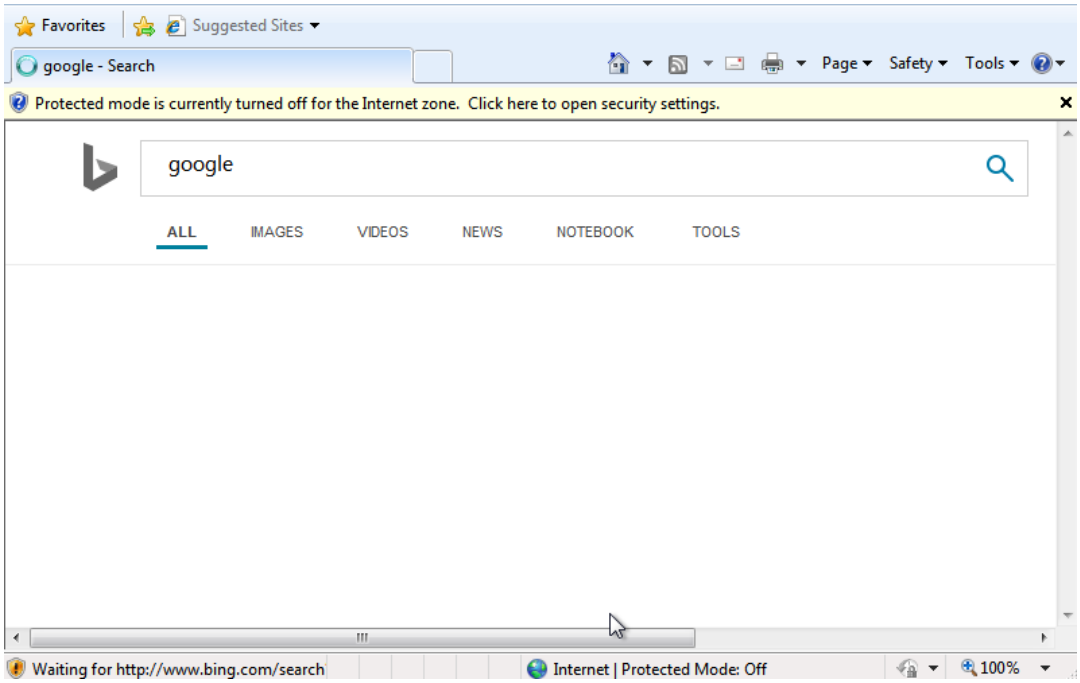
Y en una terminal de Kali se digita el siguiente comando para inciar el ataque de inundación de pings a través del protocolo ICMP, utilizando la herramienta hping3 y --rand-source --flood hacia la dirección ip de la máquina virtual de windows 7

$sudo su #hping3 --icmp --rand-source --flood -d 1400 192.168.1.9



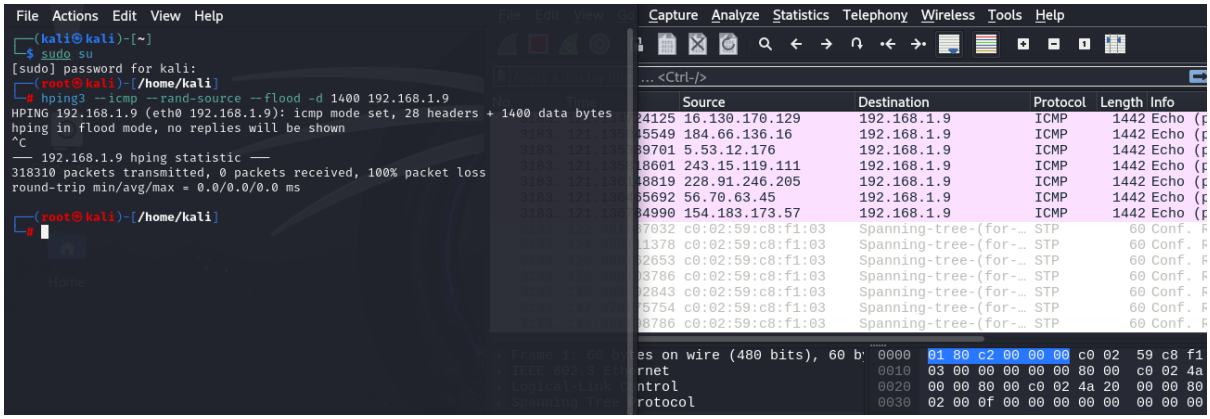
Comprobación de Denegación de Servicio (DoS)

Se intenta acceder a google desde el buscador del navegador y no funciona



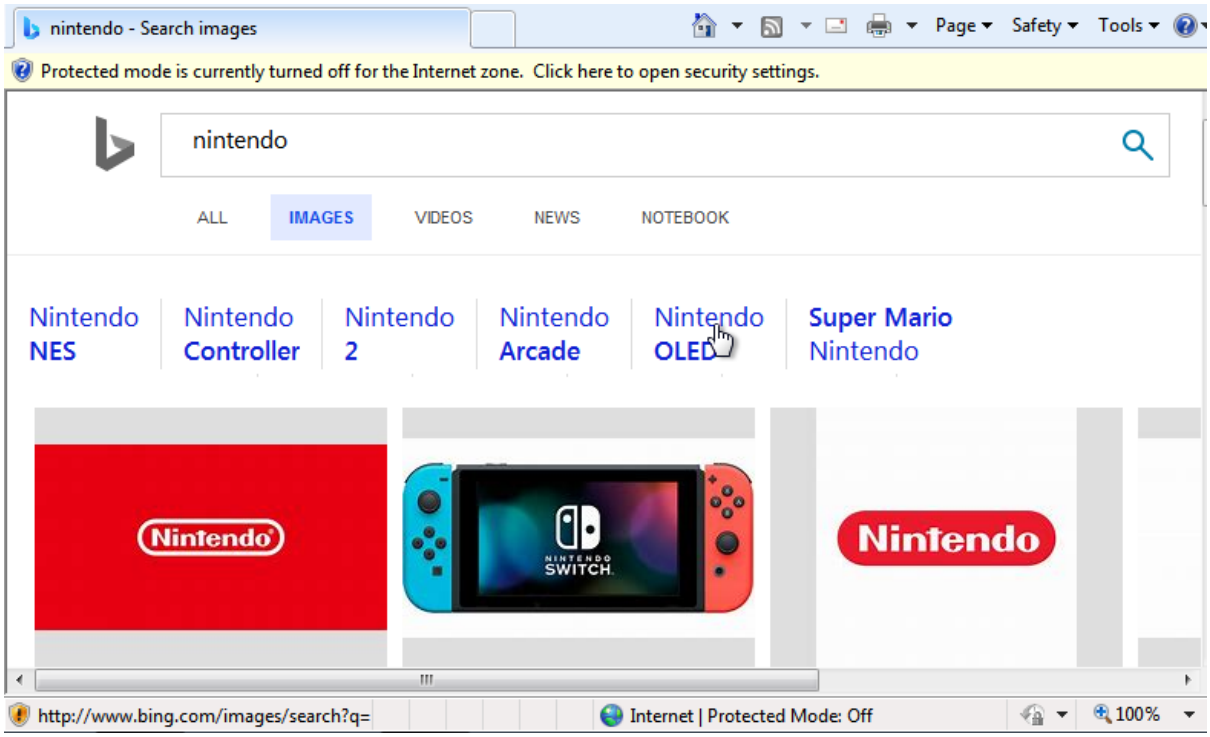
Desactivación del ataque

Se desactiva o se detiene el ataque desde la máquina virtual de Kali Linux en la terminal con el comando Ctrl+C



Restauración del servicio de navegación en windows 7

Después de detener el ataque se restaura nuevamente el servicio, y ya se puede realizar búsquedas nuevamente.



Análisis y Discusión:

- ¿Qué función cumple la opción --rand-source en el comando hping3 y cómo afecta al ataque de denegación de servicio?

  Hping3 es una herramienta de red capaz de enviar paquetes como lo hace el protocolo ICMP también funciona con TCP y UDP estos pueden ser personalizados y mostrar respuestas como lo hace ping. Con hping3 se puede

probar reglas de firewall, realizar escaneos de puertos (falsos), probar el rendimiento de la red con diferentes protocolos, realizar descubrimientos MTU de ruta, traceroute, entre otras funciones.

--rand-source utilizado dentro hping3 permite habilitar el modo de fuente aleatoria, es decir, hping enviará paquetes con una dirección de origen aleatoria con el fín de saturar la tabla de estado del firewall y otras tablas dinámicas por IP dentro de la pila de protocolos TCP/IP y el sofware del firewall.

Con esta opción la generación de direcciones origen falsas son inmensas saturando así la tabla de estado del firewall, hasta llegar al colapso y esto implica que no pueda procesar nuevas solicitudes de conexiones activas y puede incluso bloquear tráfico legitimo.

- ¿Qué tipos de ataques de denegación de servicio existen y cuáles son las diferencias principales entre ellos?

Tipos de denegación de servicio (DoS):

Ataque de goteo

Impide que el servidor vuelva a ensamblar los paquetes de datos fragmentados. El servidor se ve inundado de paquetes fragmentados, que se superponen entre sí y dificultan que el servidor vuelva a compilar los datos originales. Esto hace que el servidor se bloquee.

Ataque de inundación ICMP

Al enviar una cantidad excesiva de pings ICMP, el servidor de destino no responde a todas las solicitudes con los recursos disponibles. Esto, en última instancia, hace que el servidor no responda, lo que da como resultado una condición de denegación de servicio.

Ataque de desbordamiento de buffer

El ataque intenta almacenar más datos que el búfer de memoria asignado, lo que sobrescribe las ubicaciones de búfer de memoria adyacentes. Esto hace que la pila de memoria almacene datos de error dañados y sobrescritos, lo que hace que el servidor se bloquee o no pueda evitar la ejecución de código malicioso. Los

intentos repetidos de dañar estos búferes provocan una condición de denegación de servicio en el servidor.

Ataque DoS no intencionado

No todos los ataques DoS surgen como una actividad maliciosa. Un servicio web que no puede manejar adecuadamente un aumento temporal del tráfico web orgánico, como el Black Friday en los EE. UU., también puede colapsar y entrar en un estado similar a la denegación de servicio.

Diferencias

En el primer caso (ataque de goteo) el servidor no puede con la sobrecarga de fragmentos de paquetes de datos, es decir es una cantidad considerable lo que implica que el servidor no pueda computarlos y se bloquee, en el segundo caso (inundación ICMP) la cantidad exagerada de pings hacia el servidor provoca que el servidor no pueda responderlos de manera efectiva, en los dos casos se aprovechó de su vulnerabilidad, en el tercer caso (desbordamiento de buffer), va más allá ya que puede comprometer la seguridad del servidor, inyectándole código malicioso al sobrescribir y desbordar el buffer, en el cuarto caso no es grave, no se compromete ni la vulnerabilidad ni seguridad del servidor, en este caso las múltiples peticiones hacia el servidor por una cantidad inmensa de usuarios conlleva a que el servidor esté limitado a responder dichas peticiones debido a su capacidad.

- ¿Qué medidas de mitigación se pueden implementar para proteger una red contra ataques de denegación de servicio?

  Las aplicaciones y servicios deben restringir el tráfico web en un solo nodo y en su lugar distribuir el servicio desde múltiples nodos ubicados en ubicaciones distintas. El uso redes de distribución de contenido y servicios en la nube puede ayudar a lograr estos objetivos.

  Utilizar un mecanismo sólido de gestión e identidad de acceso para garantizar que solo el tráfico autorizado y legítimo pueda acceder a sitios web: considerar controles de acceso basados en políticas, para servicios que requieren iniciar sesión y ACLs (listas de acceso) para dispositivos de red.

  Utilizar cortafuegos para evitar ataques como la inyección SQL y la falsificación entre sitios. Mantener la red actualizada con parches que solucionen vulnerabilidades conocidas.

Diseñar y gestionar aplicaciones e infraestructura de TI de modo que pueda satisfacer las demandas de tráfico web escalables.

- ¿Cómo puede afectar un ataque de denegación de servicio a la disponibilidad y operación de un servicio en línea?
  Un ataque de denegación de servicio (DoS) afecta la disponibilidad de un servicio en línea al sobrecargar sus recursos, haciéndolos incapaces de responder a solicitudes legítimas. Esto implica que los usuarios que intenten acceder al servicio experimentarán retrasos, interrupciones o la imposibilidad de utilizar el servicio. La operación del servicio se ve comprometida ya que la infraestructura, como servidores, redes y firewalls, no puede manejar el tráfico excesivo. Por ejemplo, en un ataque de inundación ICMP, la cantidad de solicitudes ICMP satura el servidor, impidiéndole responder de manera efectiva a las peticiones legítimas, lo que provoca su inoperancia
- ¿Qué otras herramientas, además de hping3, se pueden utilizar para realizar pruebas de resistencia contra ataques de denegación de servicio y qué características ofrecen?

  Además de **hping3**, existen varias herramientas que se pueden utilizar para realizar pruebas de resistencia contra ataques DoS:

  1. **LOIC (Low Orbit Ion Cannon)**: Es una herramienta fácil de usar que permite realizar ataques de denegación de servicio al enviar múltiples solicitudes a un servidor objetivo, saturando su capacidad de respuesta. Se utiliza principalmente para ataques de inundación HTTP y UDP.
  2. **HOIC (High Orbit Ion Cannon)**: Similar a LOIC, pero con capacidades mejoradas, HOIC puede realizar ataques masivos de HTTP, permitiendo un mayor volumen de tráfico de ataque. Además, permite la personalización de los encabezados de las solicitudes para evitar medidas de mitigación básicas.
  3. **Slowloris**: Este tipo de ataque DoS se centra en mantener abiertas tantas conexiones como sea posible al enviar solicitudes HTTP incompletas, lo que agota los recursos del servidor objetivo. Es particularmente efectivo contra servidores que dependen de conexiones persistentes.
  4. **SYNFlood**: Herramienta que explota el proceso de establecimiento de conexiones TCP. Al enviar múltiples solicitudes SYN sin completar el proceso de conexión, los recursos del servidor se saturan, impidiendo nuevas conexiones.
  5. **Metasploit**: Aunque es más conocido por su uso en pruebas de penetración, Metasploit también incluye módulos para realizar ataques DoS de manera controlada, probando la resistencia de los sistemas ante diferentes vectores de ataque.

Estas herramientas, junto con hping3, permiten evaluar la robustez de los sistemas ante diferentes tipos de ataques DoS, probando no solo la infraestructura, sino también los mecanismos de defensa implementados

Referencias

hping3 | Kali Linux Tools. (s. f.). Kali Linux. https://www.kali.org/tools/hping3/#hping3

hping3 - manual page | send (almost) arbitrary TCP/IP . . .. (s. f.).

https://www.venea.net/man/hping3(8)

Denial-of-Service Attacks: History, Techniques & Prevention | Splunk. (s. f.). Splunk.

https://www.splunk.com/en_us/blog/learn/dos-denial-of-service-attacks.html