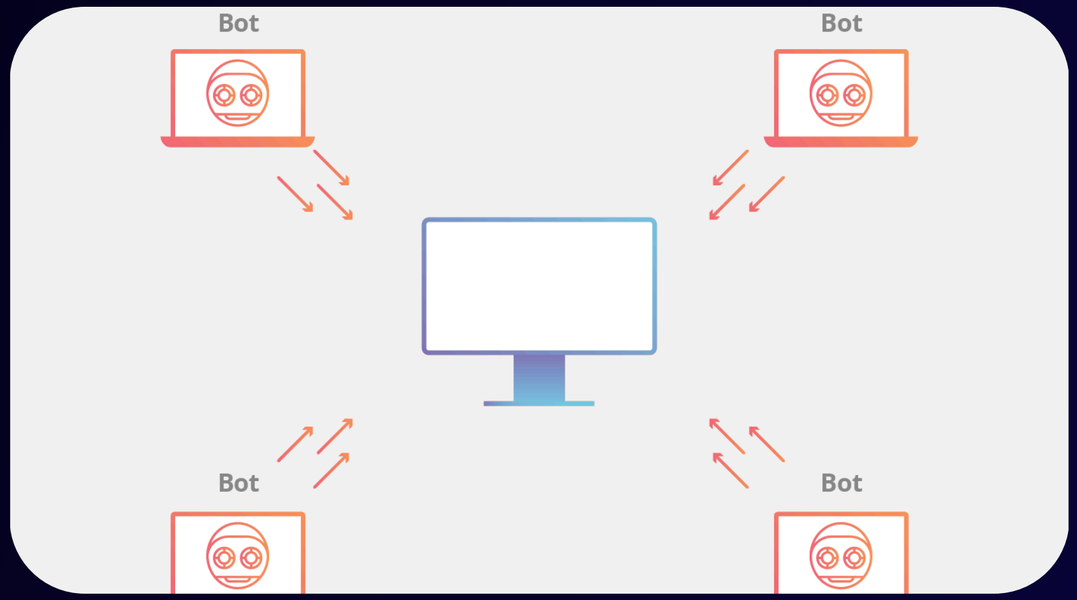
Ataques DDoS

Que es un ataque DDoS

Un **DDoS** es un ataque a un sistema de computadoras o red que **causa** que un **servicio** o recurso sea **inaccesible.**



Ej. Ataque a Instagram y se caen los servidores.

Sistemas O. Utilizados

Atacante vs Defensor

Utilizare **Kali,** para comprobar la **eficiencia de mi script** sobre un servidor Apache2 en **Ubuntu Server.**

Repositorio en GitHub

Key of the proyect

La parte importante de este proyecto es la de los scripts de automatización en bash los cuales están subidos a GitHub y se podran descargar desde ahí.

Link al Repositorio:
https://github.com/Malonsocabral/Proyecto_ASO_Marcos

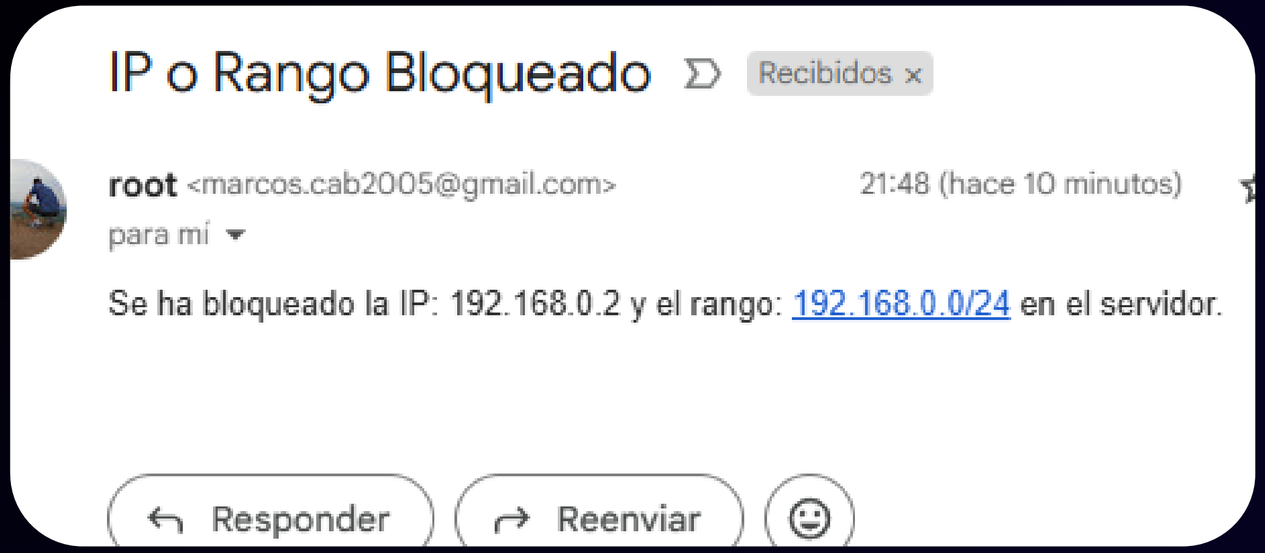
Scripts: Instalacion UbuntuS. – Mitigacion DDoS – Correo

Ejecucion de Prueba

```
marcos@pfmarcos:~$ sudo ./030_Script_Mitigacion-DDOS_Marcos.sh
Ejecutando como sudo!
Buscando patrón: sqlmap
Buscando patrón: nikto
Buscando patrón: nmap
Buscando patrón: hydra
Analizando conexiones excesivas...
IP con conexiones excesivas detectada: 192.168.0.2 - Conexiones: 12669
Bloqueando IP: 192.168.0.2
Como el rango de ips, es el 192.168.0.0/24 y engloba a este propio servidor, no sera bloqueado

Aun no es la hora en punto, por lo que no se vaciaran ni los logs de apache ni las iptables.

Proceso de mitigación completado.
```



IP o Rango Bloqueado Recibidos ×

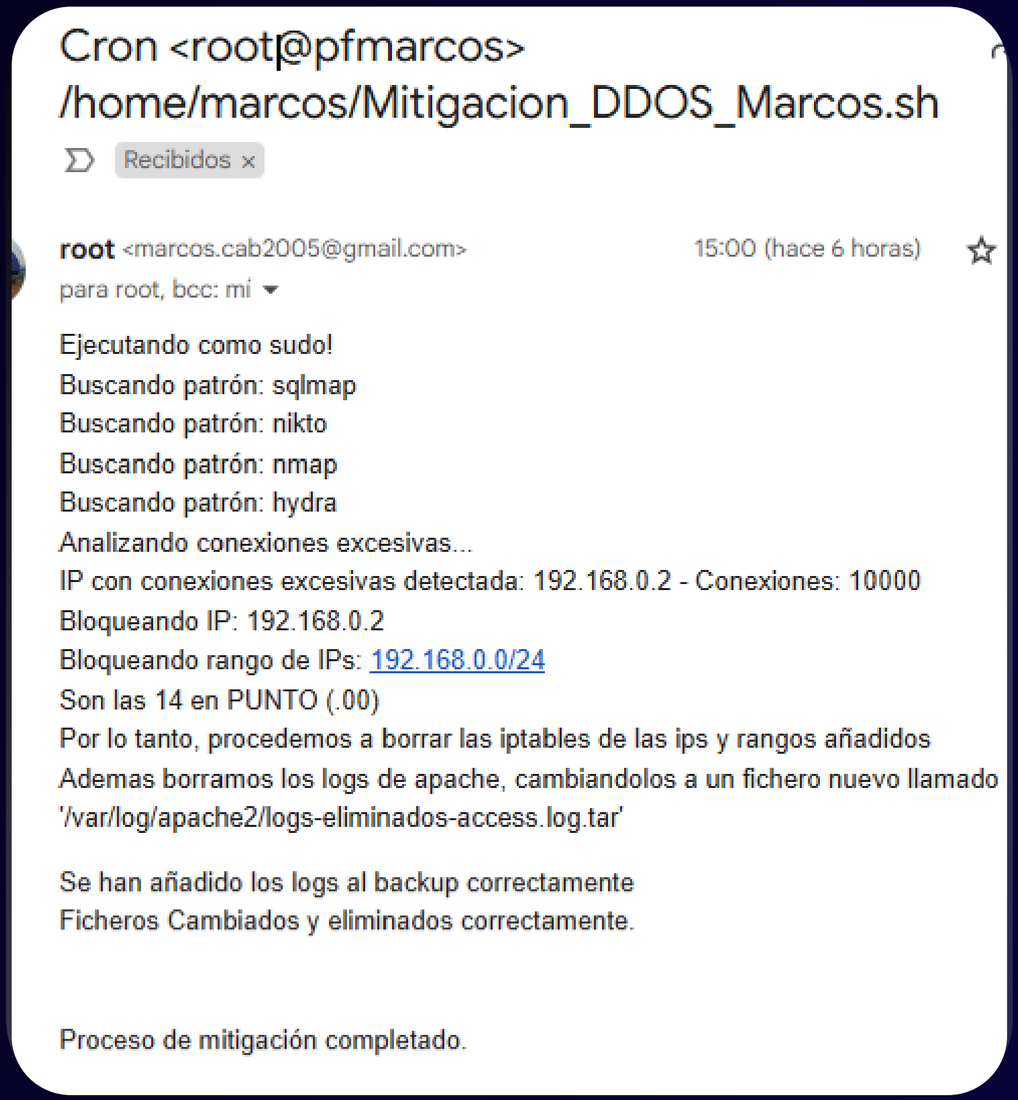
root <marcos.cab2005@gmail.com> 21:48 (hace 10 minutos)

para mí

Se ha bloqueado la IP: 192.168.0.2 y el rango: 192.168.0.0/24 en el servidor.

Responder Reenviar

Ejemplos de Correos



Cron <root@pfmarcos> /home/marcos/Mitigacion_DDOS_Marcos.sh

Recibidos ×

root <marcos.cab2005@gmail.com> 15:00 (hace 6 horas)

para root, bcc: mí

Ejecutando como sudo!
Buscando patrón: sqlmap
Buscando patrón: nikto
Buscando patrón: nmap
Buscando patrón: hydra
Analizando conexiones excesivas...
IP con conexiones excesivas detectada: 192.168.0.2 - Conexiones: 10000
Bloqueando IP: 192.168.0.2
Bloqueando rango de IPs: 192.168.0.0/24
Son las 14 en PUNTO (.00)
Por lo tanto, procedemos a borrar las iptables de las ips y rangos añadidos
Ademas borramos los logs de apache, cambiandolos a un fichero nuevo llamado '/var/log/apache2/logs-eliminados-access.log.tar'

Se han añadido los logs al backup correctamente
Ficheros Cambiados y eliminados correctamente.

Proceso de mitigación completado.

Comparación con otras aplicaciones

Fail2ban y Cloudflare

Casi todas las aplicaciones de DDoS **afectan a más capas** (OSI) y tienen **herramientas más avanzadas** (comparado con mi script).

FAIL2BAN

CLOUDFLARE

Aprendizajes:
Iptables,
github,
automatización,
funcionamiento
DDoS...

Conclusión
del Proyecto

Aunque es una **solución creativa** y efectiva para entornos pequeños, **carece** de la **escalabilidad y precisión** comparado con otros servicios y/o aplicaciones.

Muchas gracias