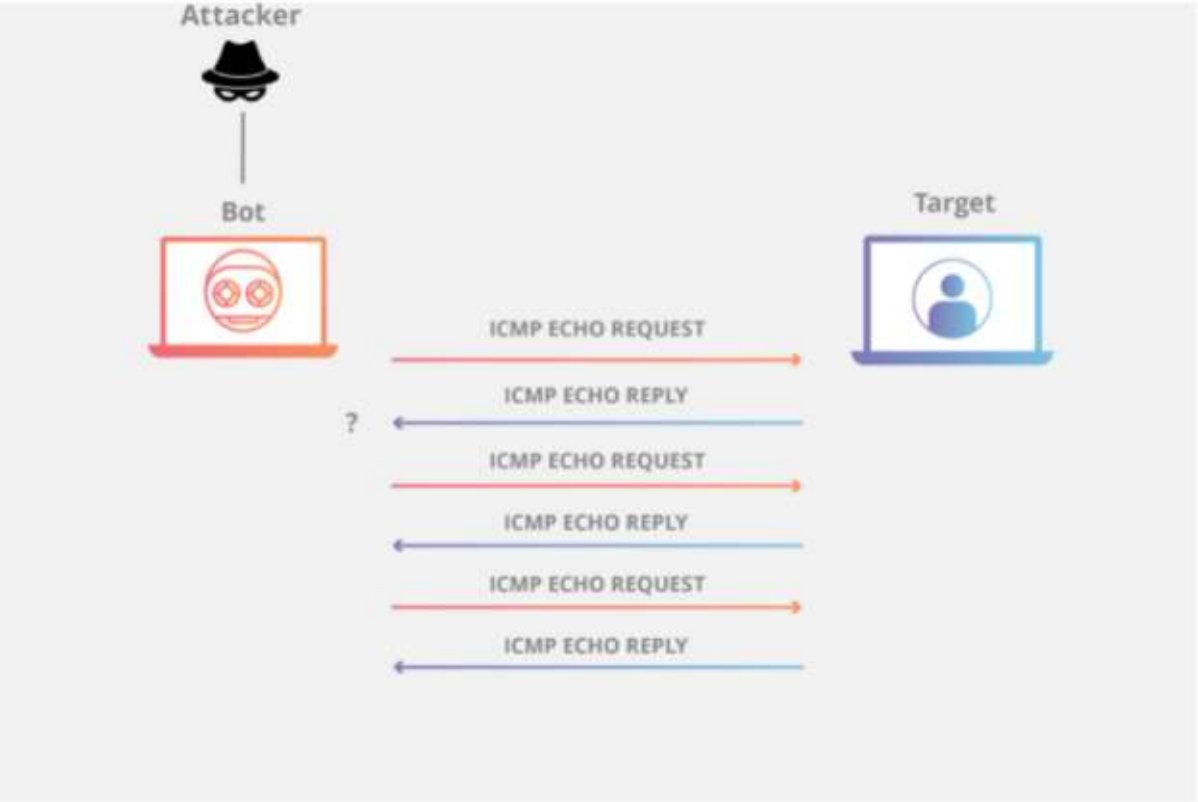
Verification of end-to-end network path operation is through the use of the Internet Control Message Protocol(ICMP) ping, by sending an ICMP echo request packet to the target network node with the expectation of an ICMP echo reply to verify network connectivity between the sender and receiver (Gunnam and Kumar, 2017). In a ping flood attack, the ICMP echo command functionality gets abused by sending a flood on ping requests to the targeted host with the intention to over utilise the network interface resources to the point of depletion, thereby achieving a successful denial of service(DoS) (Manna, 2012).



Pentest-Tools.com

ICMP Ping Echo Request Report (Light)

✔ google.co.za

Scan results

```
PING google.co.za (172.217.169.35) 56(84) bytes of data.

64 bytes from lhr48s08-in-f3.1e100.net (172.217.169.35): icmp_seq=1 ttl=120 time=1.41 ms
64 bytes from lhr48s08-in-f3.1e100.net (172.217.169.35): icmp_seq=2 ttl=120 time=1.48 ms
64 bytes from lhr48s08-in-f3.1e100.net (172.217.169.35): icmp_seq=3 ttl=120 time=1.50 ms

--- google.co.za ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
```

Scan parameters

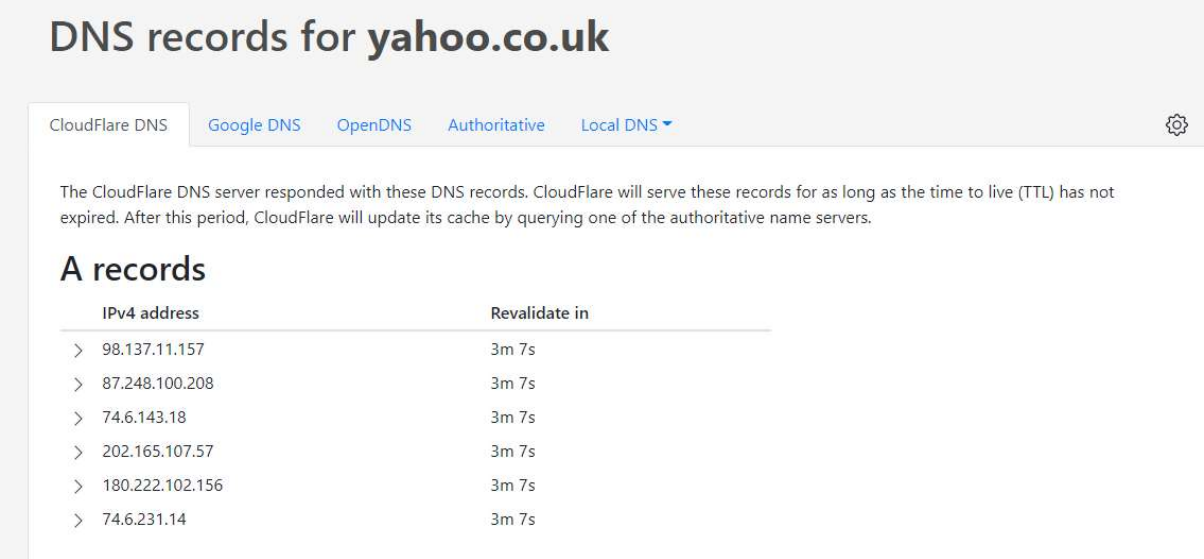
Target:	google.co.za

Scan information

Start time:	2021-06-01 19:29:17 UTC+03
Finish time:	2021-06-01 19:29:20 UTC+03
Scan duration:	3 sec
Scan status:	Finished

Preventing an ICMP flood attack is accomplished by disabling ICMP functionality through a host-based firewall or an access control list (ACL) on the targeted network node. However, disabling ICMP also disables other related services such as traceroute requests (CloudFlare, 2021)

As an essential element for the internet, a domain name system (DNS) constitutes a mapping of a fully qualified domain name (FQDN.i.e google.com) to the internet protocol(IP) address. Using another component of TCP/IP, name server lookup(nslookup), the mapping can be used to provide resolution from FQDN to IP address (forward lookup) and (reverse lookup) IP to FQDN (Alharbi et al., 2019).



Securing DNS is critical to the security of the internet. Threats to the availability and integrity of the DNS include DNS poisoning(injection of malicious entries on the mapping with the intent of redirecting client hosts to a malicious destination or denial of service by redirecting the client hosts to a destination that does not exist) (Alharbi et al., 2019).

Constantin (2020) states that the Domain Name System Security Extensions (DNSSEC) is a set of specifications that extend the DNS protocol by adding cryptographic authentication for responses received from authoritative DNS servers. Its goal is to defend against techniques that hackers use to direct computers to rogue websites and servers.

References:

Alharbi, F. *et al.* (2019) 'Collaborative Client-Side DNS Cache Poisoning Attack', *Proceedings - IEEE INFOCOM*, 2019-April(February), pp. 1153–1161. doi: 10.1109/INFOCOM.2019.8737514.

CloudFlare (2021) *Ping (ICMP) flood DDoS attack | Cloudflare*. Available at: https://www.cloudflare.com/learning/ddos/ping-icmp-flood-ddos-attack/ [Accessed: 1 June 2021].

Constantin, L. (2020) *What is DNSSEC? And how it prevents redirection to rogue websites | CSO Online*. Available at: https://www.csoonline.com/article/3569277/dnssec-explained-why-you-might-want-to-implement-it-on-your-domain.html [Accessed: 1 June 2021].

Gunnam, G. R. and Kumar, S. (2017) 'Do ICMP Security Attacks Have Same Impact on Servers?', *Journal of Information Security*, 08(03), pp. 274–283. doi:

10.4236/jis.2017.83018.

Manna, M. E. (2012) ‘Review Of Syn-Flooding Attack Detection Mechanism’, *International Journal of Distributed and Parallel systems*, 3(1), pp. 99–117. doi: 10.5121/ijdps.2012.3108.

.