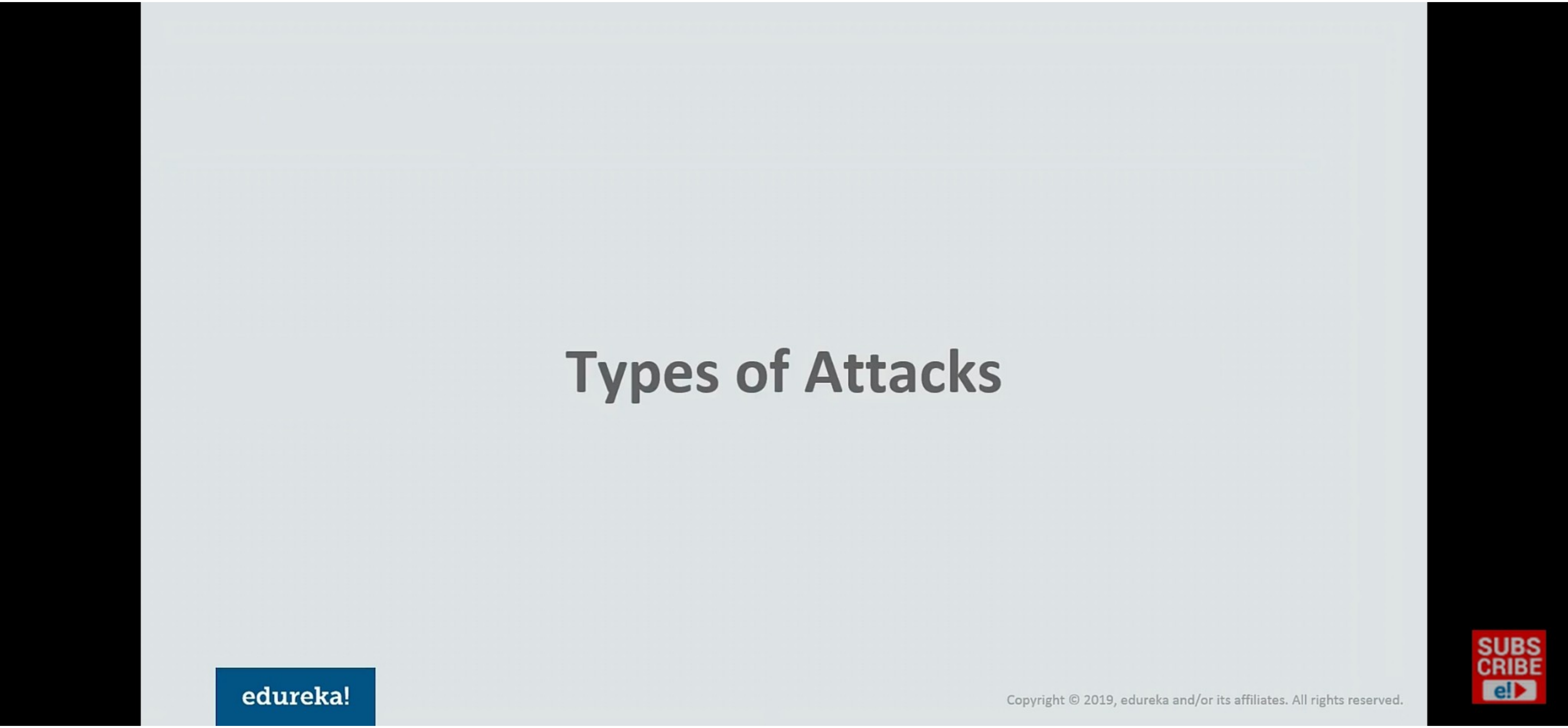
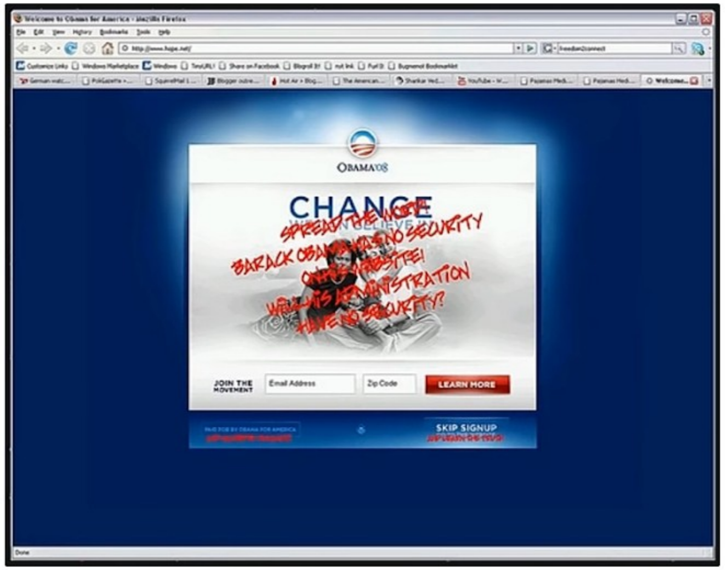


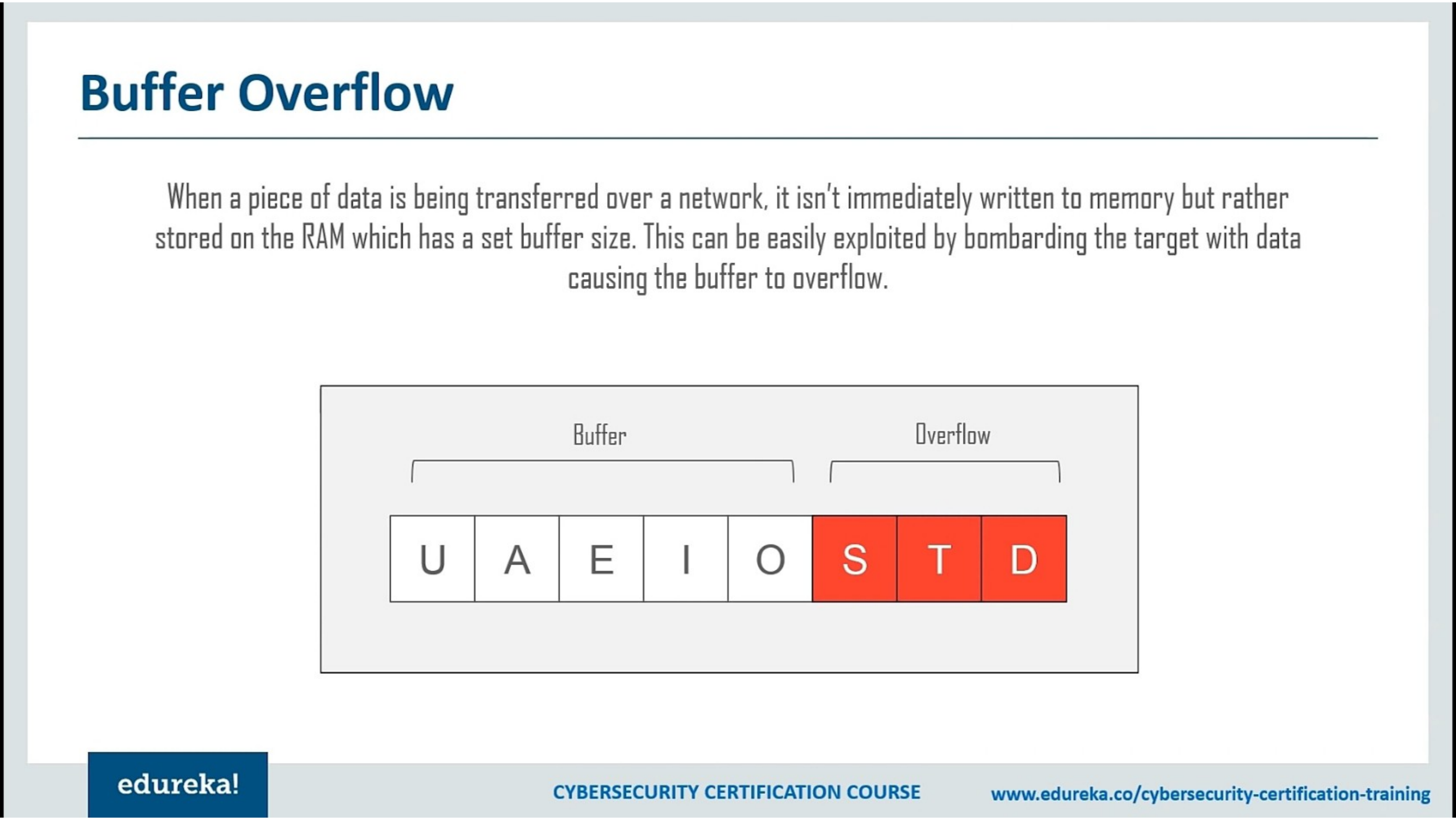
Types of Attacks

edureka!

Defacing



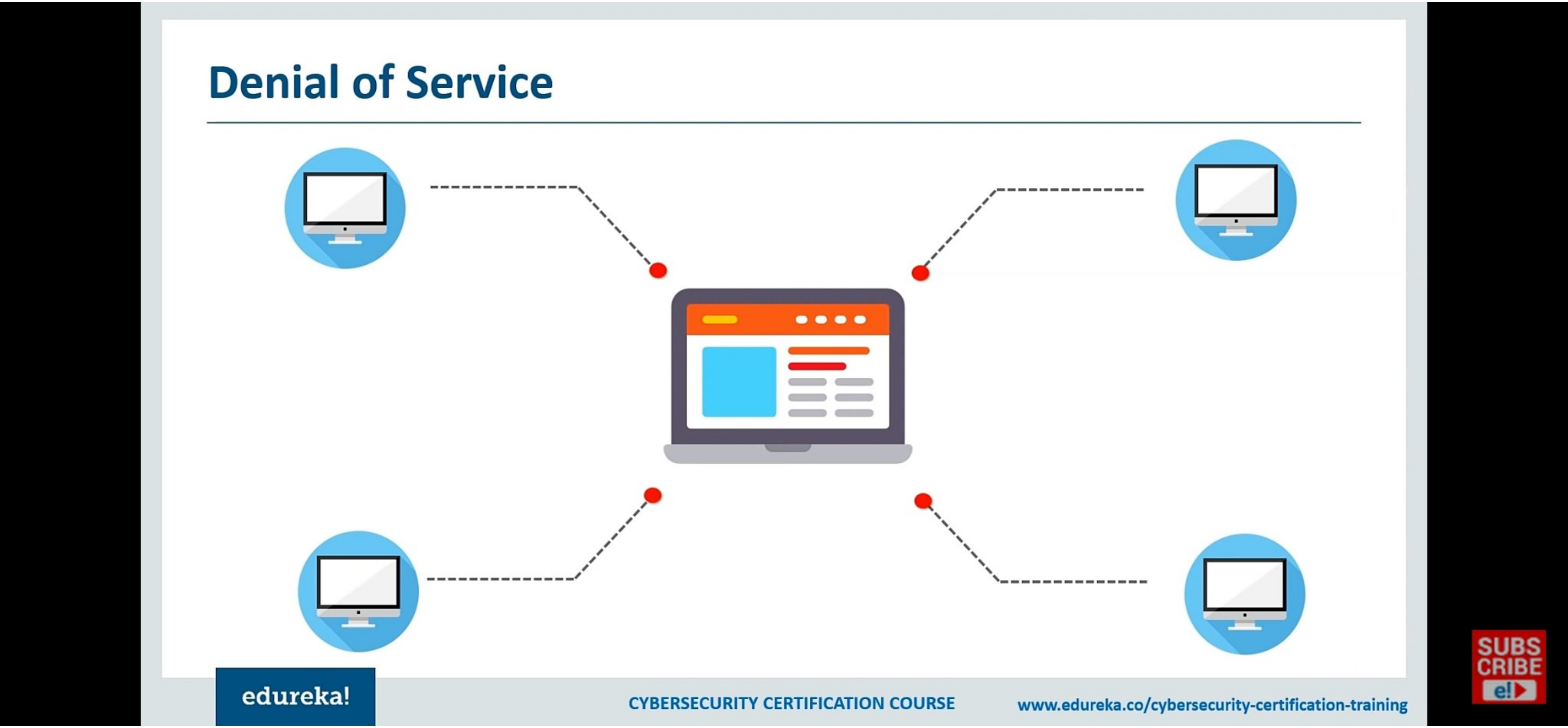
A **website defacement** is an attack on a **website** that changes the visual appearance of the site or a **webpage**. These are typically the work of system crackers, who break into a web server and replace the hosted **website** with one of their own.



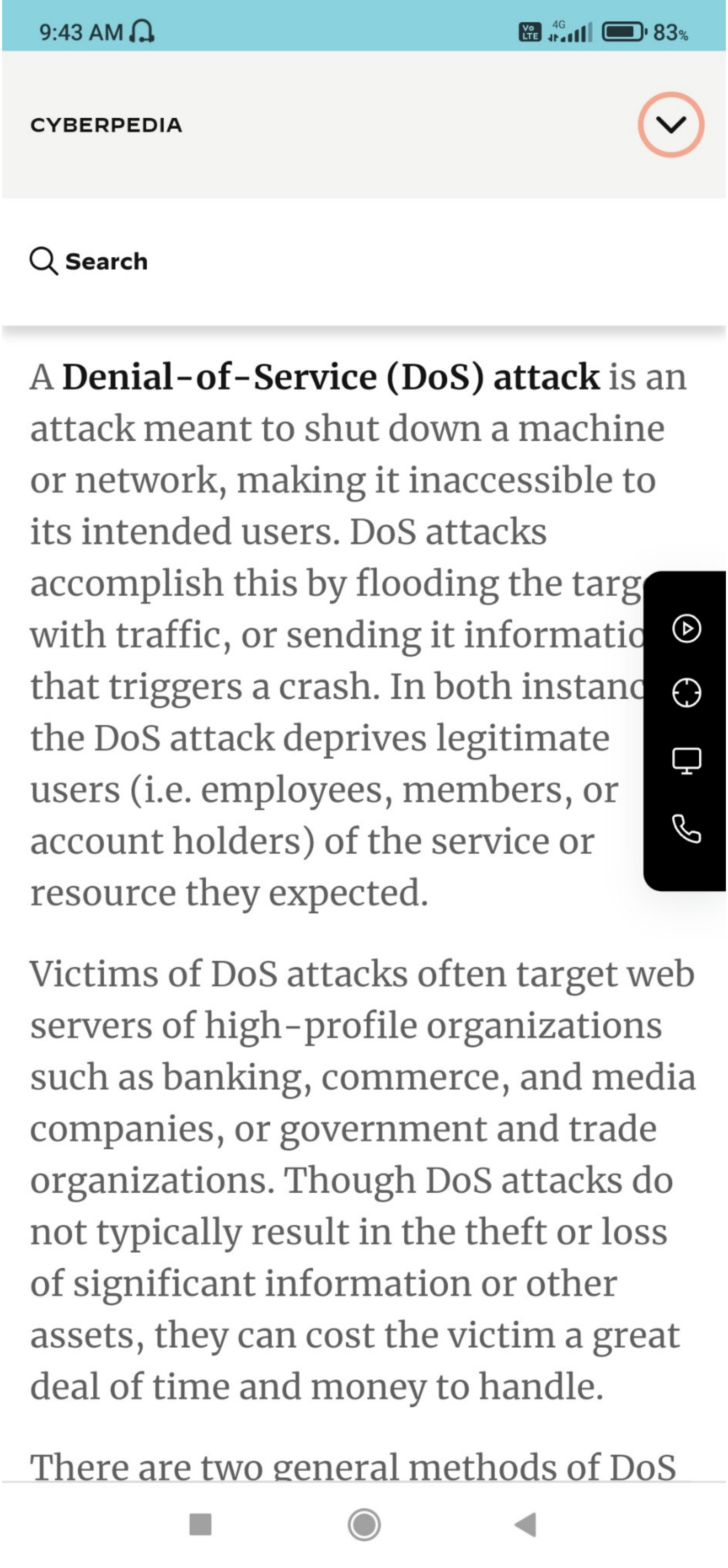
Buffer Overflow

When a piece of data is being transferred over a network, it isn't immediately written to memory but rather stored on the RAM which has a set buffer size. This can be easily exploited by bombarding the target with data causing the buffer to overflow.

Buffer					Overflow		
U	A	E	I	O	S	T	D



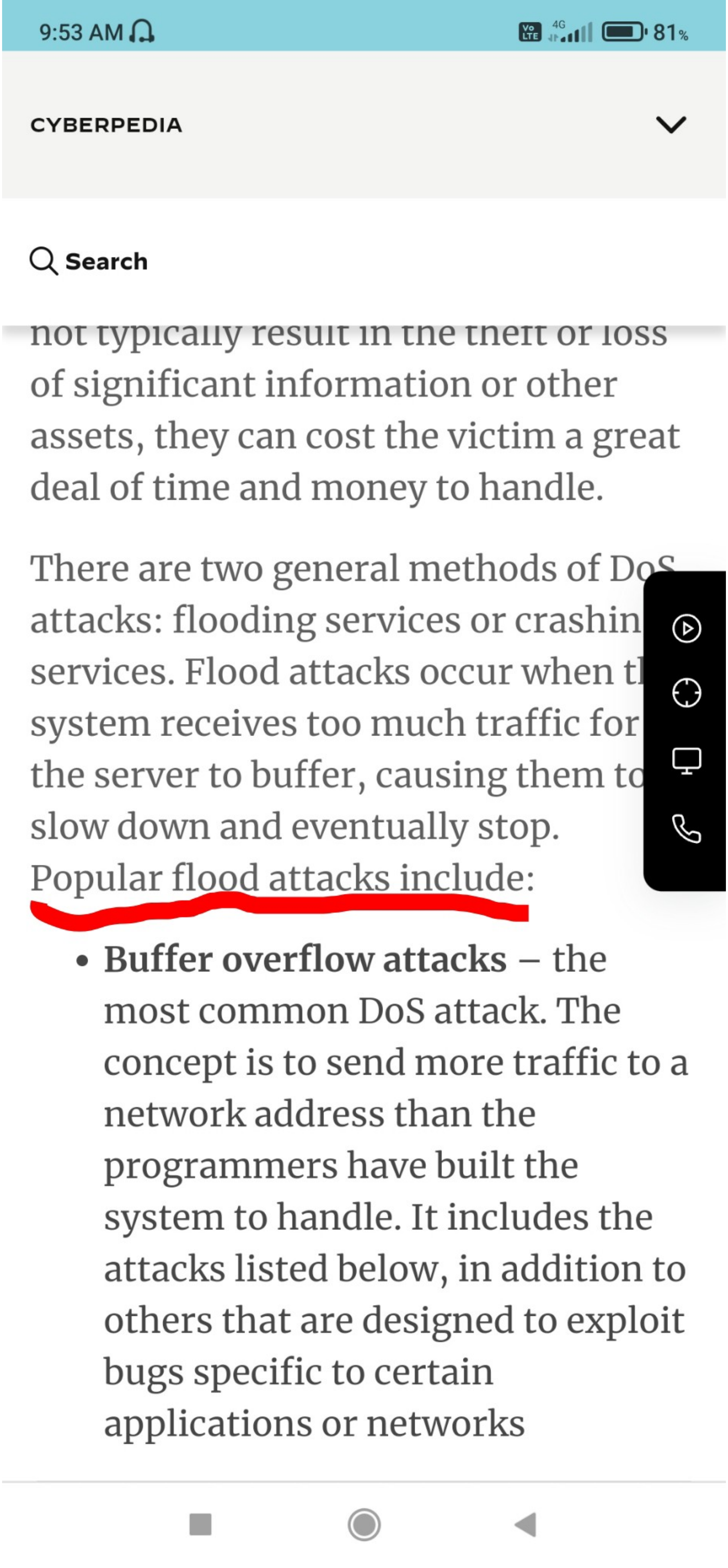
Denial of Service



A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the targ with traffic, or sending it informatio that triggers a crash. In both instanc the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

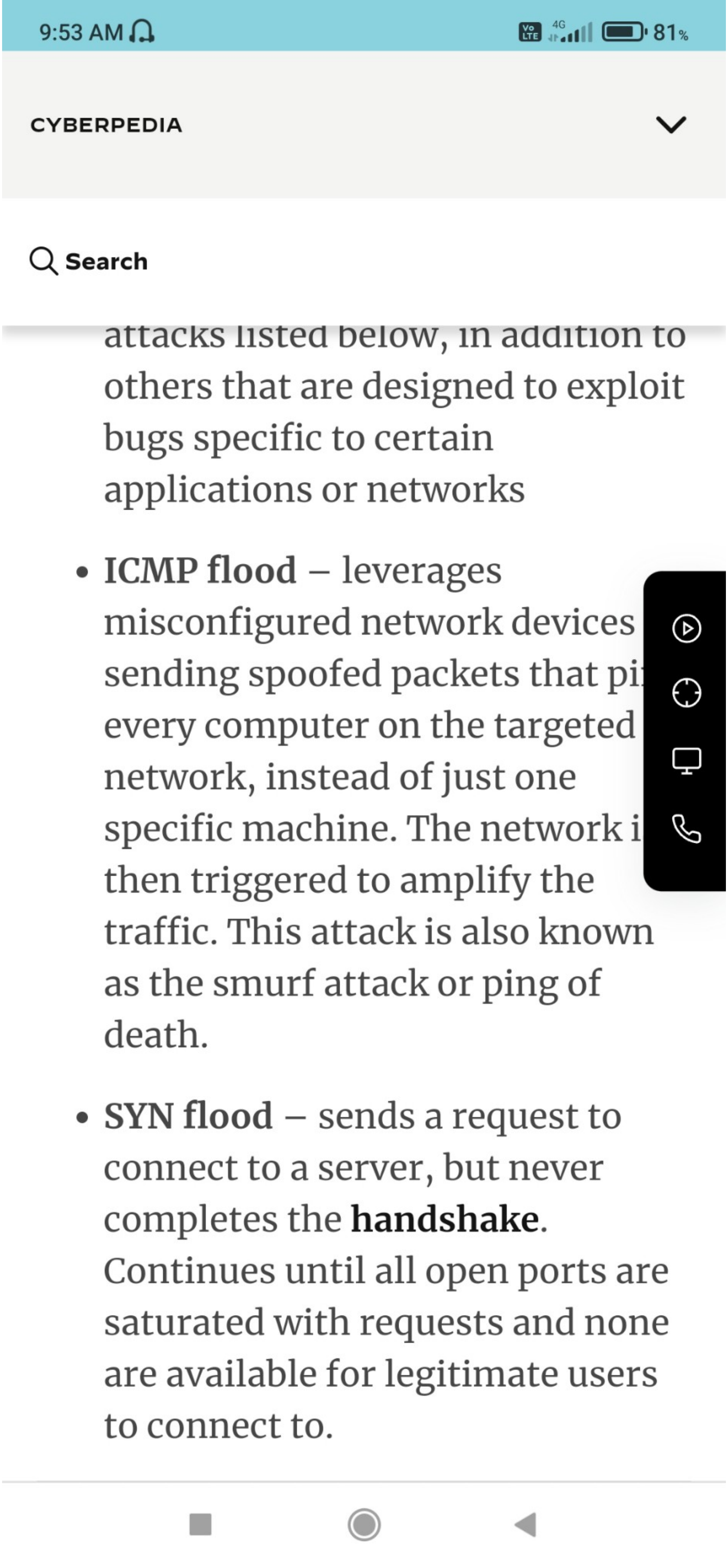
There are two general methods of DoS



not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

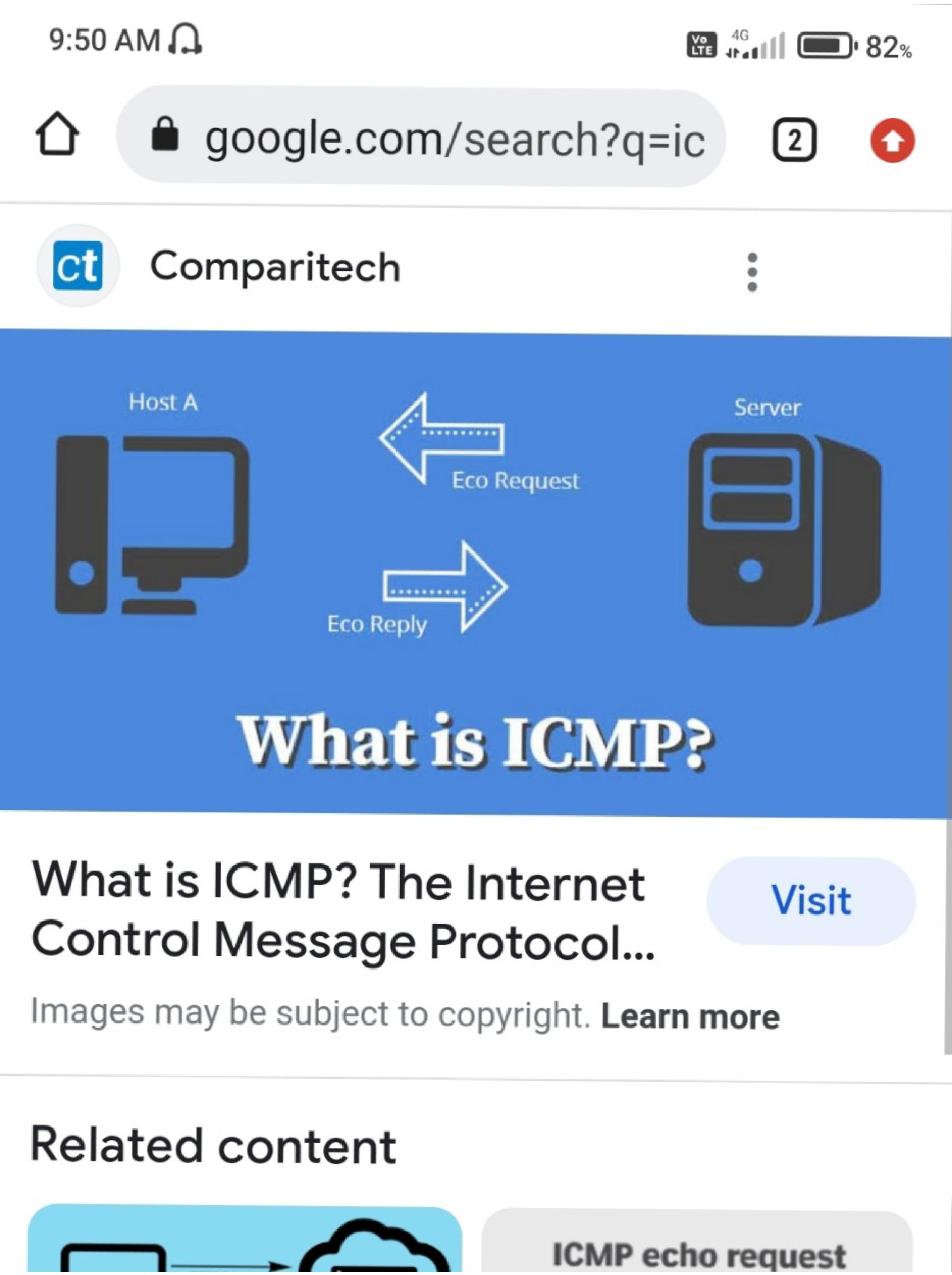
There are two general methods of DoS attacks: flooding services or crashin services. Flood attacks occur when t system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

- **Buffer overflow attacks** – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks



attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks

- **ICMP flood** – leverages misconfigured network devices sending spoofed packets that pi every computer on the targeted network, instead of just one specific machine. The network i then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.
- **SYN flood** – sends a request to connect to a server, but never completes the **handshake**. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.



What is ICMP?

What is ICMP? The Internet Control Message Protocol...

Images may be subject to copyright. **Learn more**

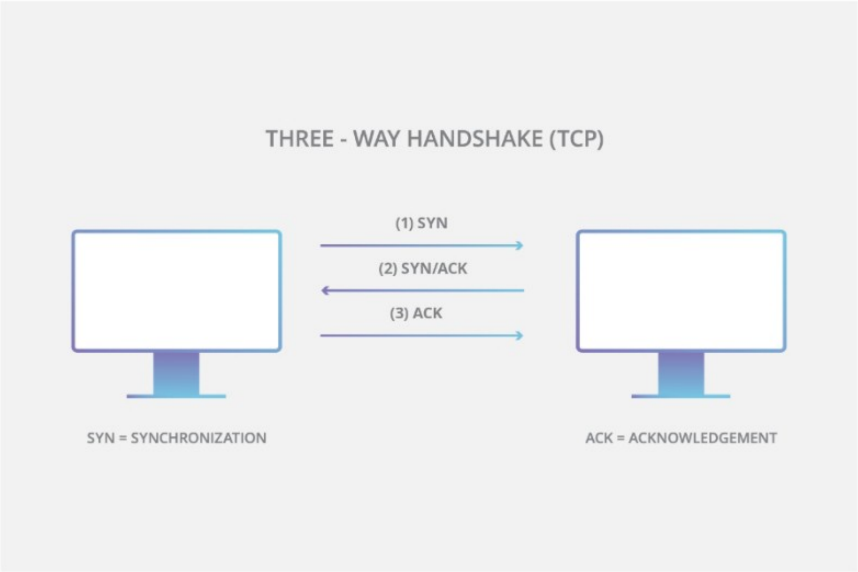
Related content

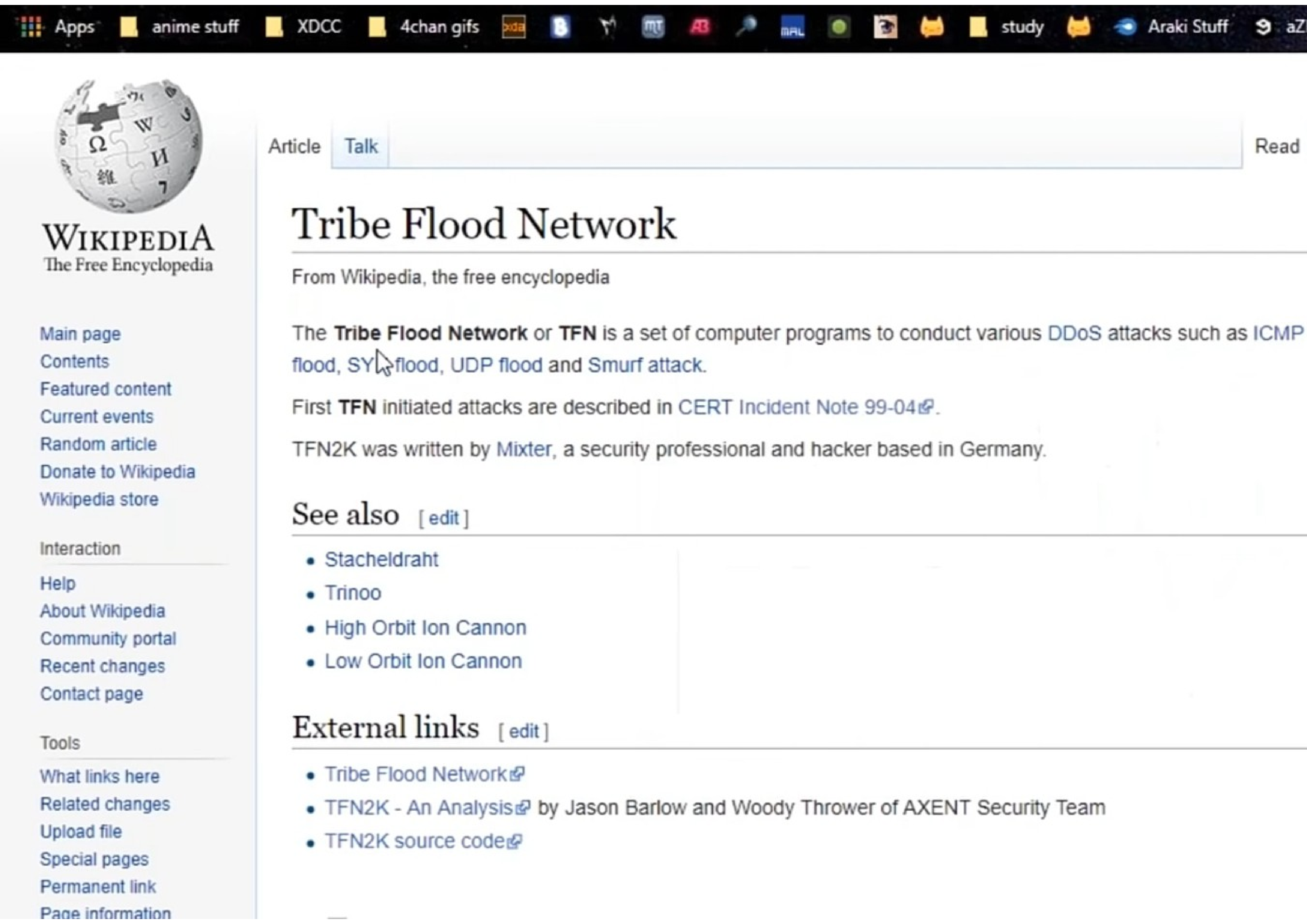
ICMP echo request

1. First, the client sends a SYN packet to the server in order to initiate the connection.

2. The server then responds to that initial packet with a SYN/ACK packet, in order to acknowledge the communication.

3. Finally, the client returns an ACK packet to acknowledge the receipt of the packet from the server. After completing this sequence of packet sending and receiving, the TCP connection is open and able to send and receive data.





Tribe Flood Network

From Wikipedia, the free encyclopedia

The **Tribe Flood Network** or **TFN** is a set of computer programs to conduct various DDoS attacks such as ICMP flood, SYN flood, UDP flood and Smurf attack.

First **TFN** initiated attacks are described in CERT Incident Note 99-04.

TFN2K was written by Mixter, a security professional and hacker based in Germany.

See also [edit]

- Stacheldraht
- Trinoo
- High Orbit Ion Cannon
- Low Orbit Ion Cannon

External links [edit]

- Tribe Flood Network
- TFN2K - An Analysis by Jason Barlow and Woody Thrower of AXENT Security Team
- TFN2K source code