NTP Amplification Attack

Weapon of mass destruction

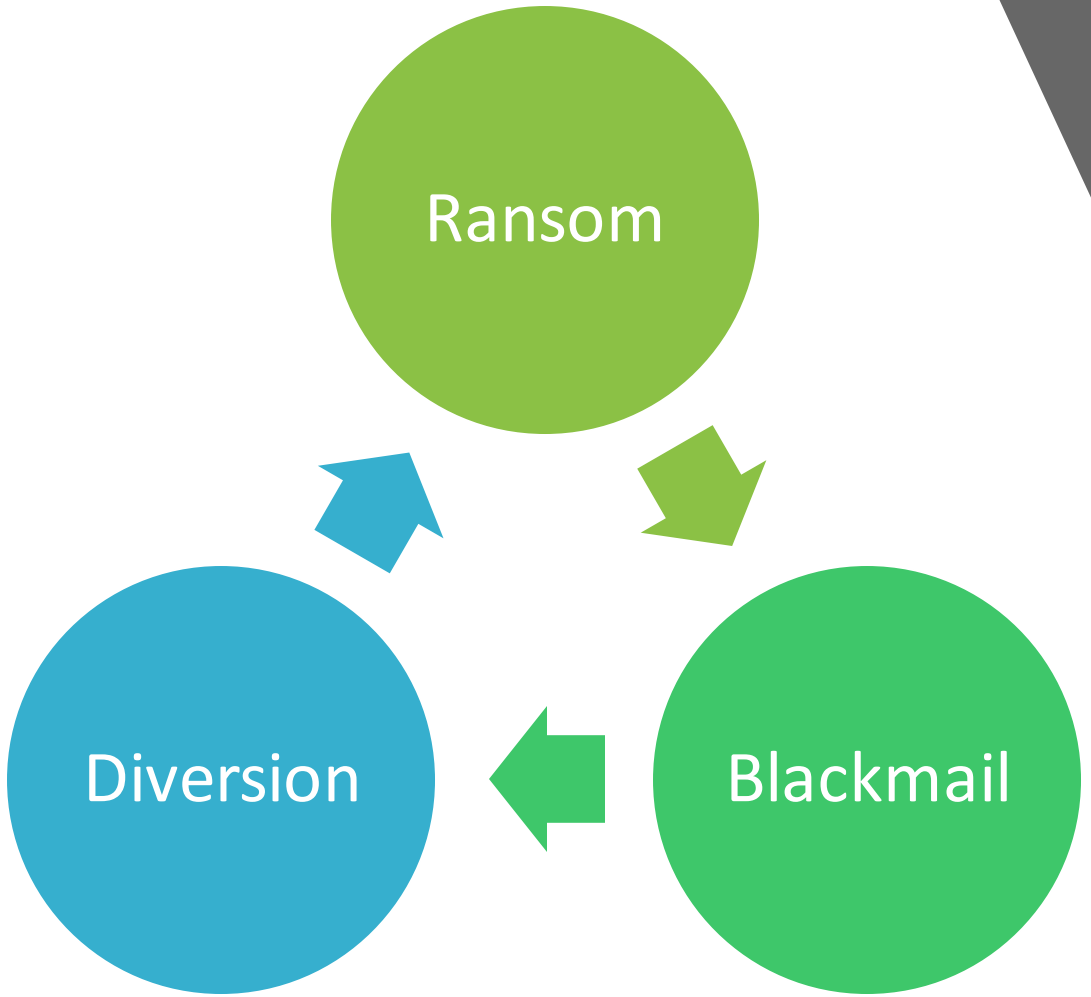
Agenda

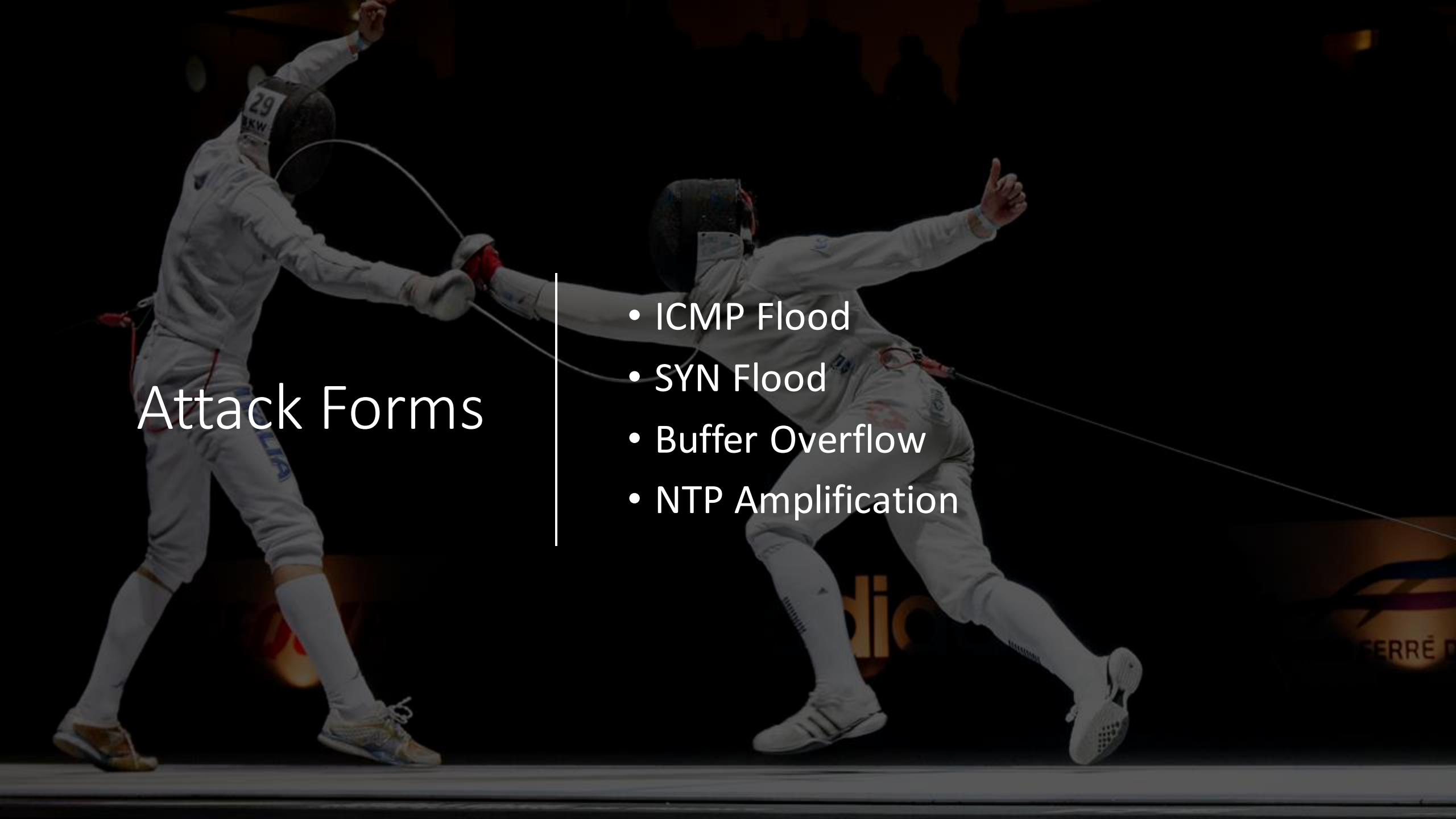
- DoS, oldest trick in the book.
- Attack Forms
- NTP Protocol
- NTP Architecture
- IP Spoofing
- Amplified DDoS
- Questions

DoS, oldest trick in the book.

An attack meant to shut down a system or render it inaccessible

Why?

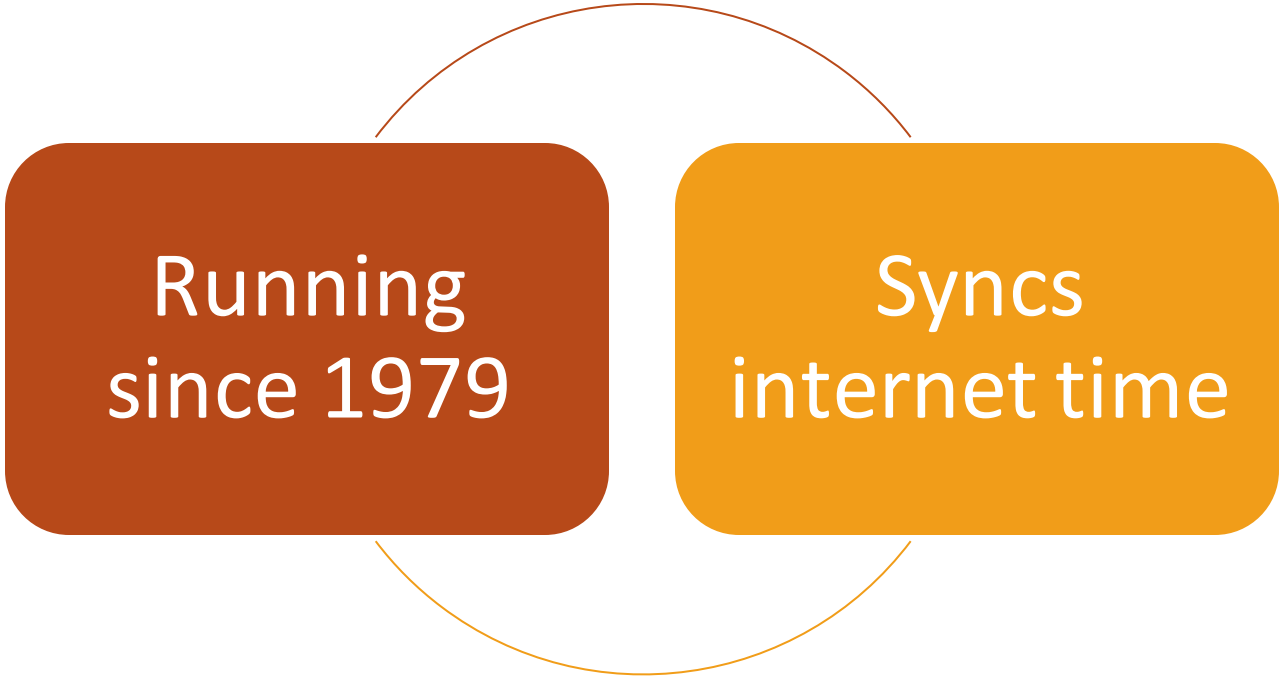

Ransom
Blackmail
Diversion

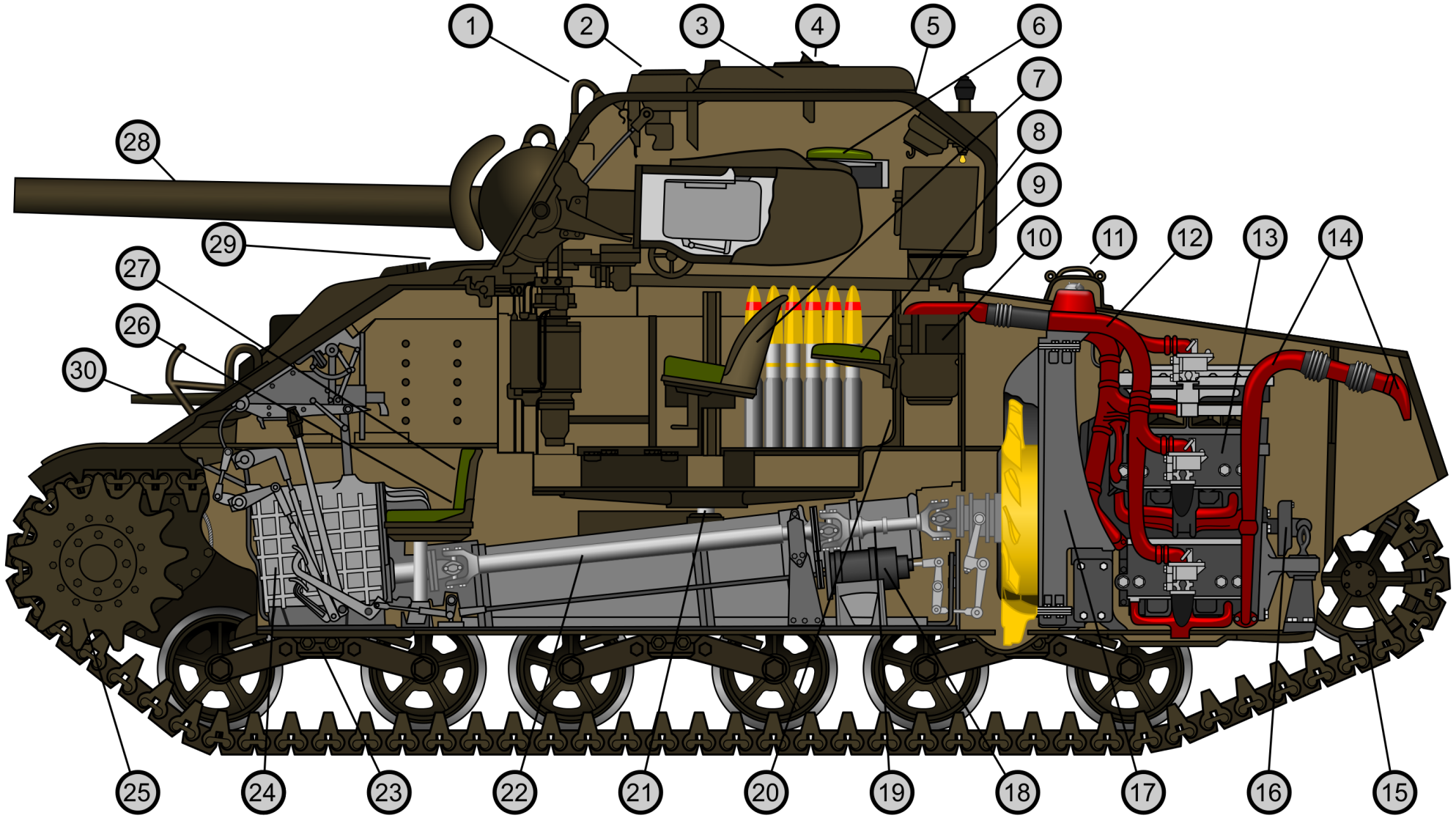


Attack Forms

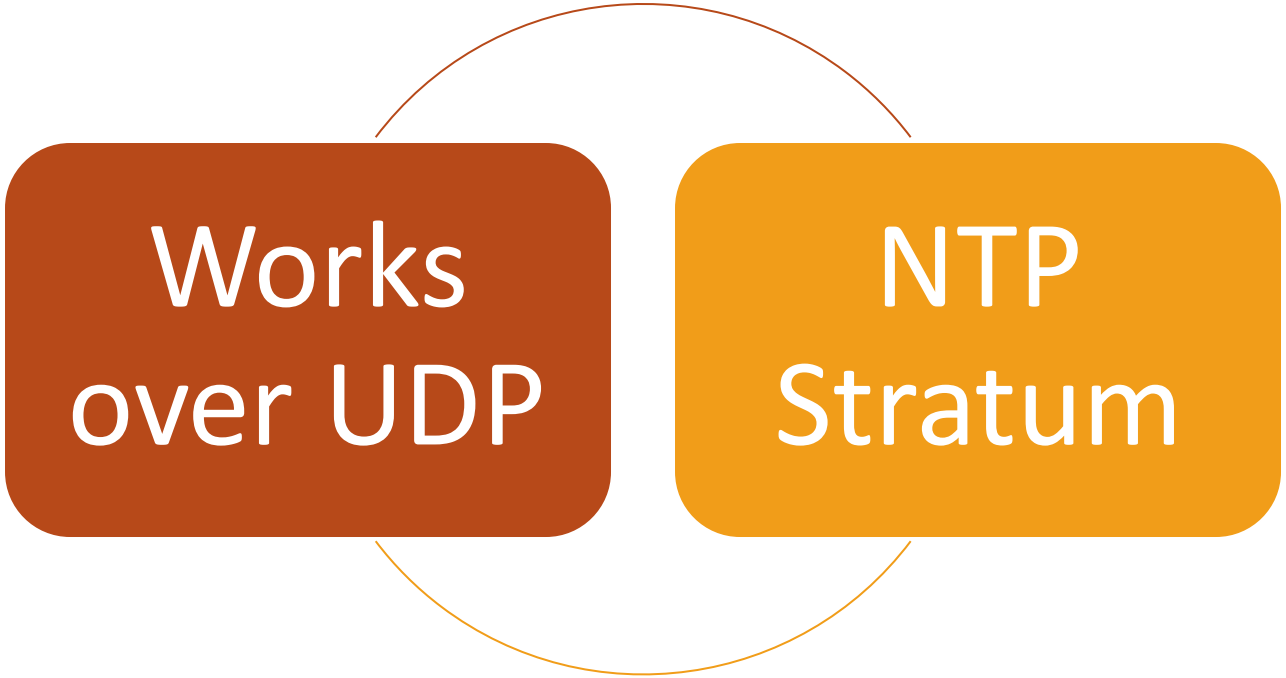
- ICMP Flood
- SYN Flood
- Buffer Overflow
- NTP Amplification

NTP Protocol




1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

NTP Architecture



NTP "*is*" Time Infrastructure

Amplified DDoS

NTP Attack

- CVE-2013-5211
- Past 600 IP
- 206 Times Response

Can I do anything about it?

not much .-.

Questions ^.^

Thank You

May the force be with you!