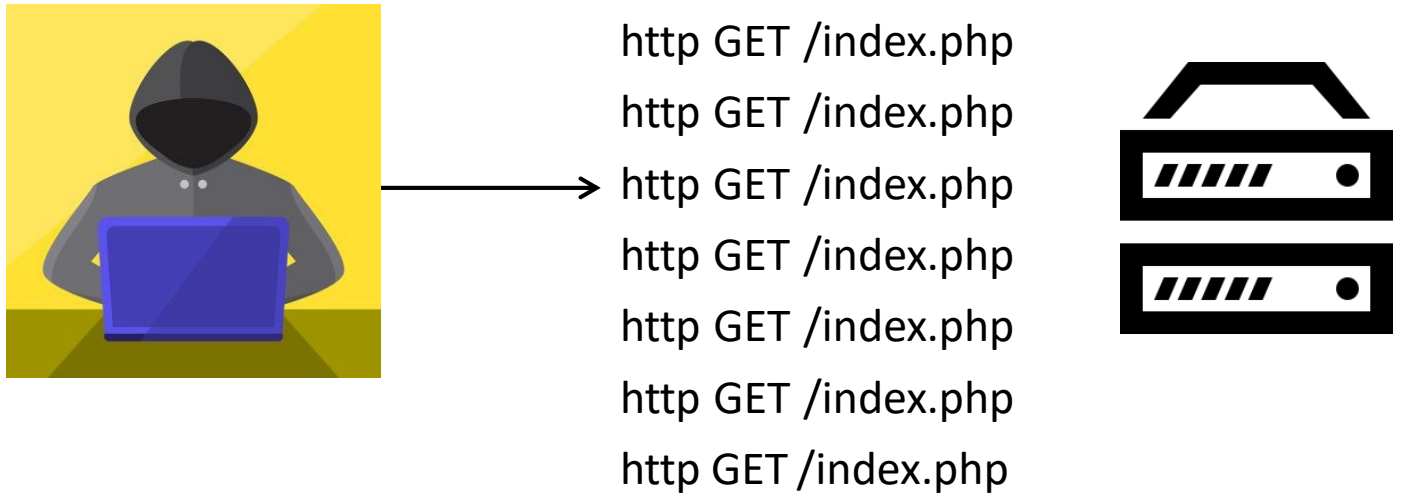
Server Vulnerabilities

Dr Rosanne English

Denial of Service (DoS)

An attack which targets servers to overload them in some way such that legitimate service is stopped, impacting availability of the server



Approaches to DoS

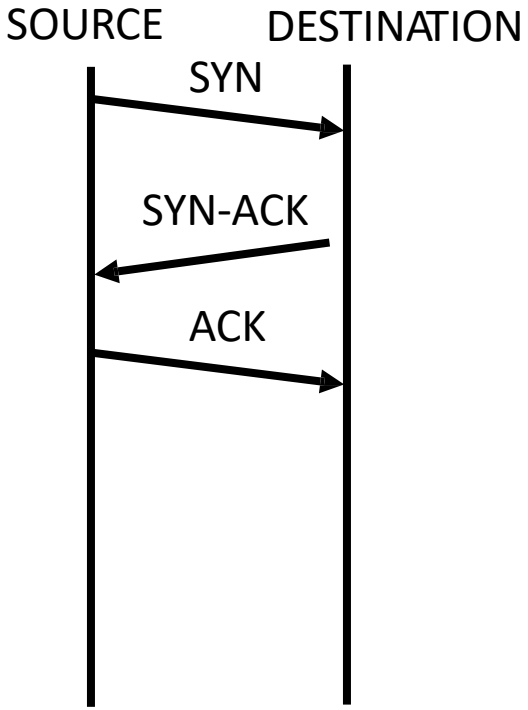
- Service request flood
- Bandwidth flood
- Ping of Death
- SYN Flood

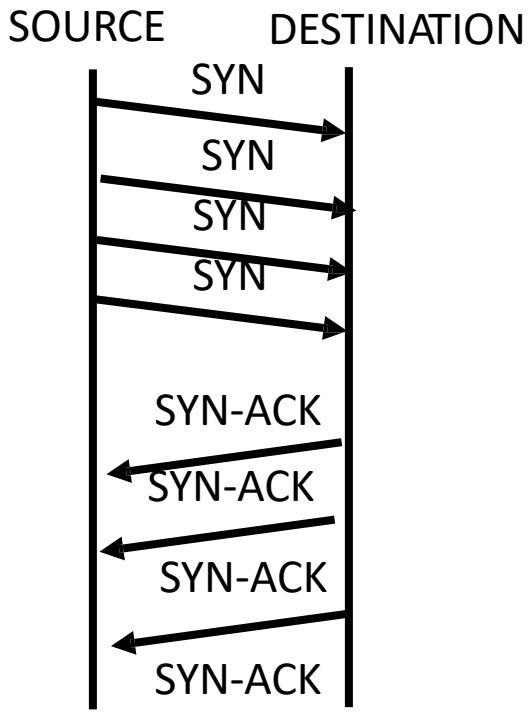
Ping of Death

- Attacker deliberately sends an IP packet larger than the 65,536 bytes allowed by the IP protocol
- Not as common today due to patches by OS vendors

SYN Flood

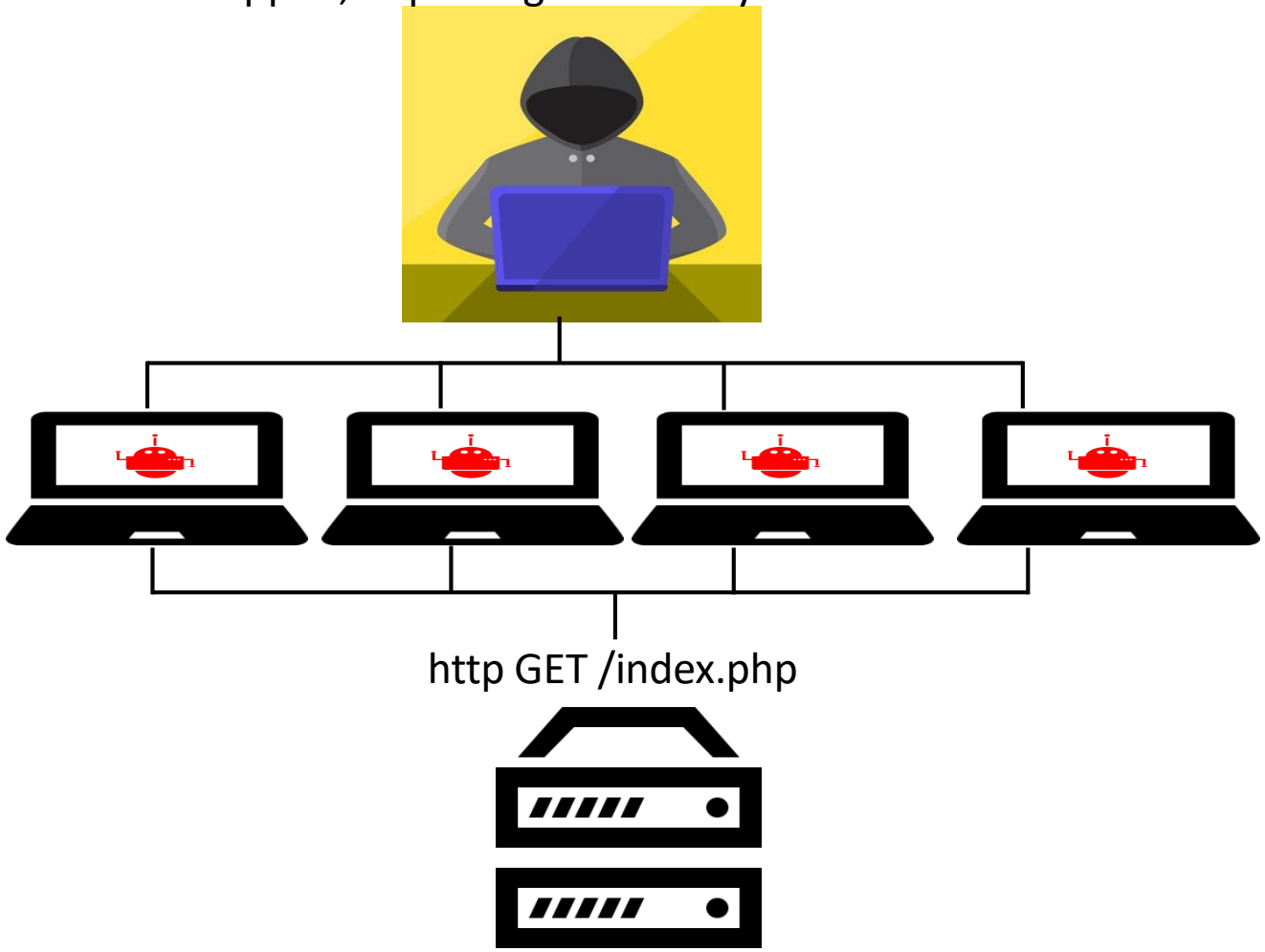
- TCP/IP 3 Way handshake
  - SYN (synchronise) packet send to destination
  - SYN-ACK – synchronise acknowledge sent back to source
  - ACK – source sends ack(knowledge) packet
- SYN flood does not send ACK back, thus the connections remain open which can result in the service overloading





Distributed Denial of Service (DDoS)

An attack which targets servers using multiple bot infected computers (botnet) to overload them in some way such that legitimate service is stopped, impacting availability of the server



Bots, zombies and botnets!

- Bot – a type of malicious software (malware) which allows the attacker complete control of the computer
- Zombie – an internet connected computer infected with a bot
- Botnet - a collection of zombies all used to do things like DDoS