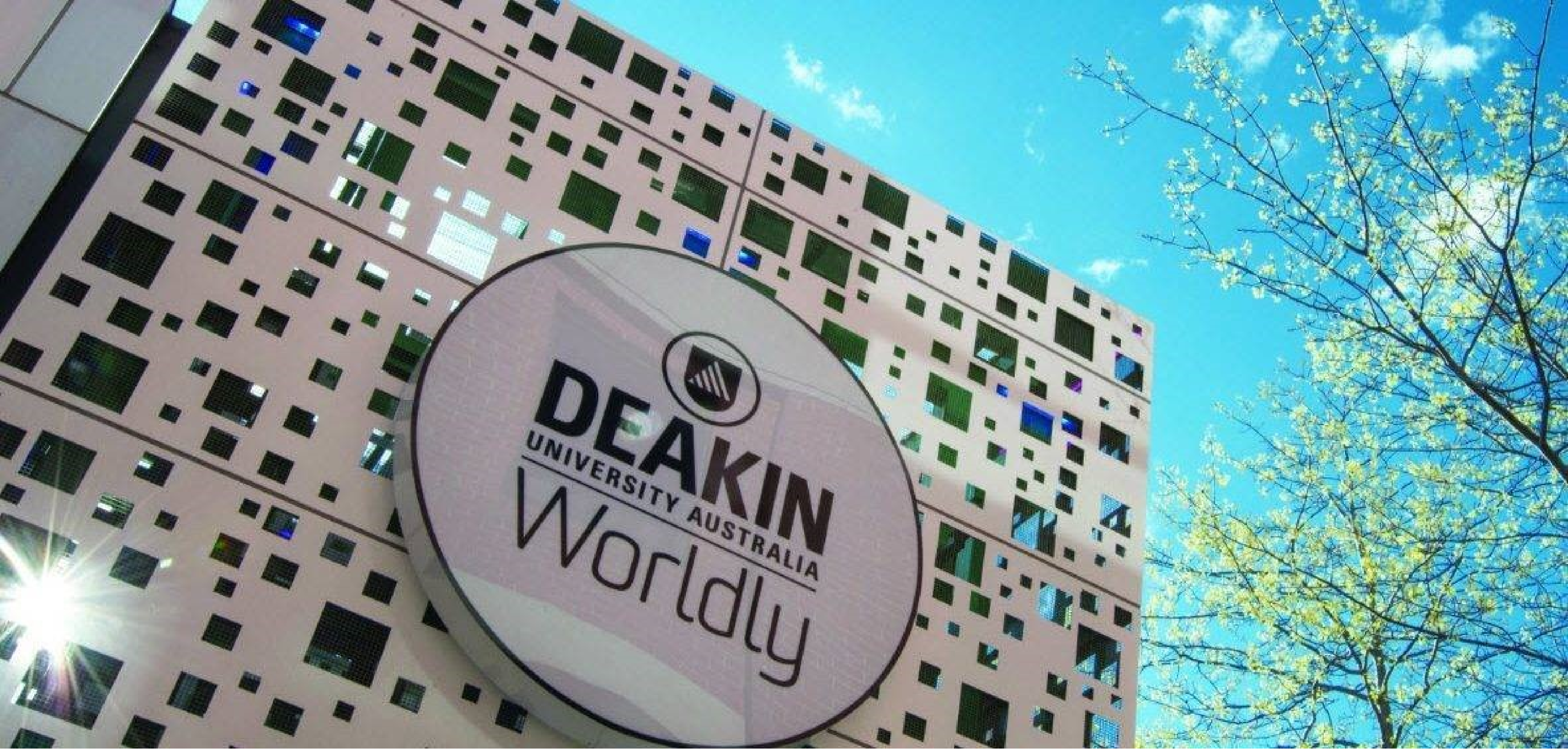


SIT382 SYSTEM SECURITY

Week 03

Denial of Service Attacks

Previous lecture - Malware

- Malware classification
- Malware terminology
- Propagation
    - Viruses
    - Worms
    - Spams and Trojans
- Payload
    - System corruption
    - Zombie, bots
    - Keyloggers, phishing, spyware
    - Backdoors, rootkits
- Countermeasures

Outline

- Concept of denial of service attacks
- Flooding attacks
- Distributed denial of service attacks
- Application-based bandwidth attacks
- Reflector and amplifier attacks
- Defences
- Common responses

Learning objectives

- Explain basic concept of denial of service attack
- Understand nature of flooding attack
- Describe distributed denial of service attack
- Explain application-based bandwidth attack
- Explain reflector and amplifier attack
- Summarise defences and common responses

Nature of denial-of-service attacks

- “Denial of service (DoS) is an action that prevents or impairs the authorised use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space” - NIST SP 800-61
- Resources to be attacked
    - Network bandwidth
        - Overload capacity of the network links connecting a server to the wider Internet
    - System resources
        - Packets to consume limited resources: temporary buffers, tables of open connections, etc.
        - Poison packets whose structure triggers a bug
            - Example: ping of death (sends malformed/oversized packets using ping command with spoofed source IP)
    - Application resources
        - Overload the capability of a server and limit its ability to respond to requests

Example network for bandwidth-based DoS attack

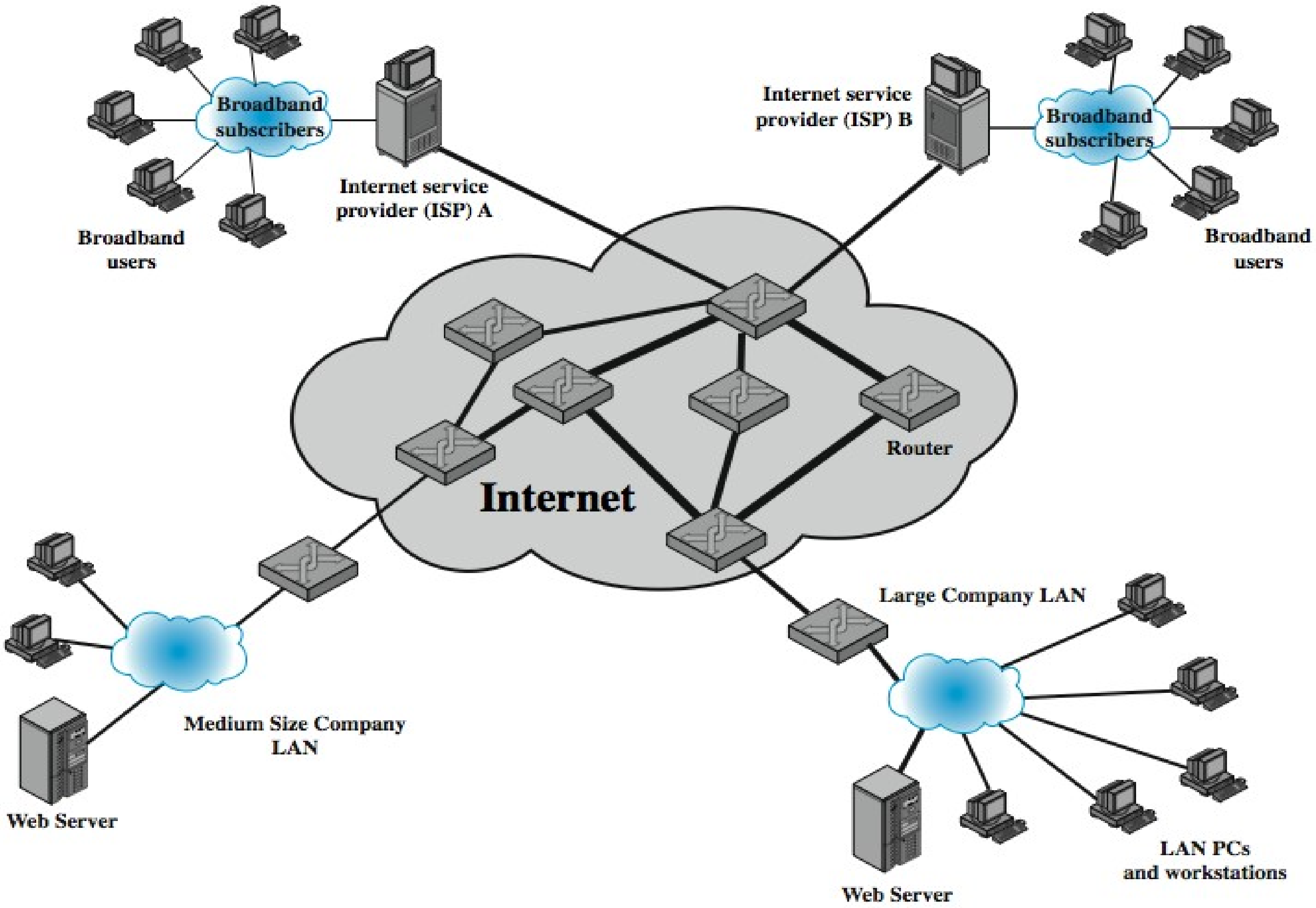


Figure 7.1 (Stallings et al., 2017)

Classic DoS attacks - flooding attack

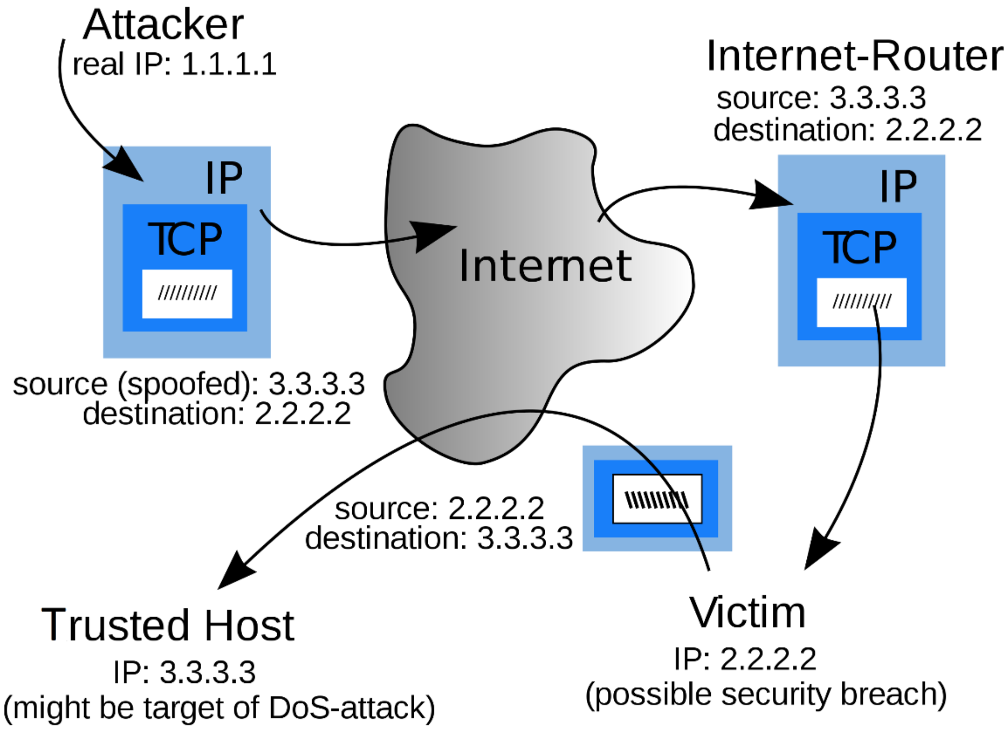
- Aim
  - Overwhelm the capacity of the network connection to the target organisation
- Example
  - Use a flooding ping command that targets a web server in the organisation
- Source of the attack
  - Source address specified in ICMP echo request
  - Mostly spoofed source address
    - Hide identity
    - Not affect network performance (host must respond to all echo requests with an echo reply)

Source address spoofing

- Use forged source addresses
  - Usually via the raw socket interface on operating systems
- DoS attack
  - Generate large volumes of packets to the target system
  - Usually use randomly selected source addresses for each packet
- Benefit
  - Harder to identify attacking systems
  - Flow of packets through the routers along the path from the source to the target system must be identified
- Reason of easy forgery
  - Development of TCP/IP occurred in cooperative and trusted environment

Source address spoofing (cont.)

- Example scenario



Example scenario (“IP address spoofing” n.d.)

Backscatter traffic

- Security researchers (Honeypot Project) advertise blocks of unused IP addresses and monitor packets arriving at those addresses
- Example: if ICMP response packets generated, most likely from a ping flood using randomly spoofed source addresses

Classic DoS attack - SYN spoofing

- Attack the ability of a server to respond to TCP connection requests
  - Overflow tables that manage TCP connections
- Thus legitimate users are denied access to the server
- DoS attack on system resources, specifically the network handling code in the operating system

TCP three-way handshake

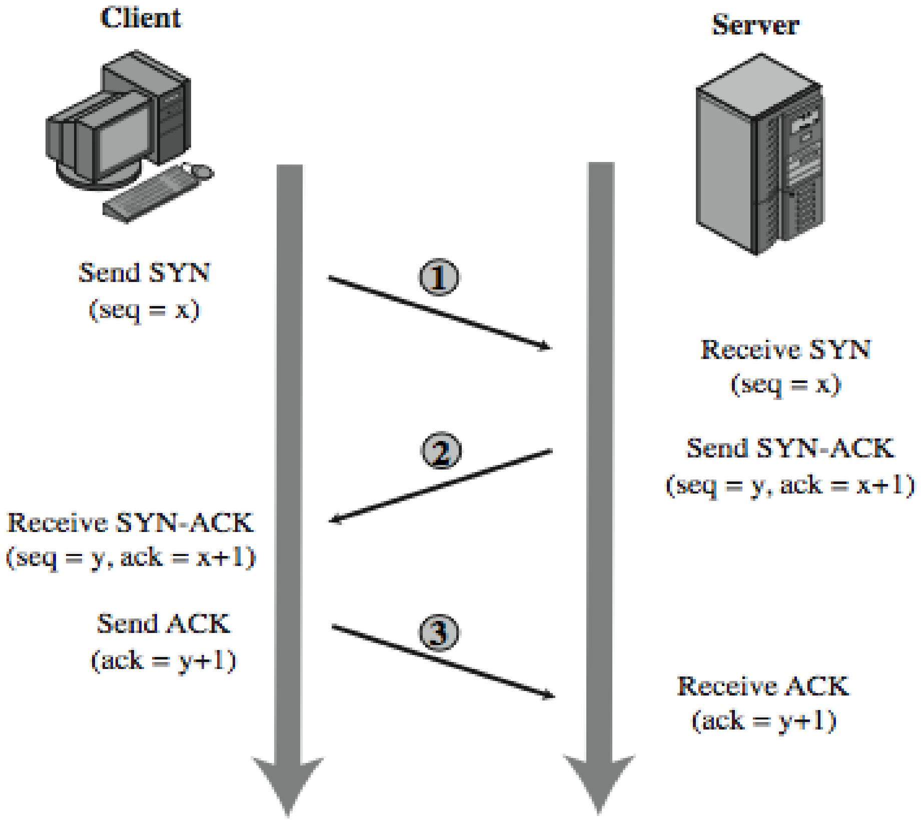


Figure 7.2 (Stallings et al., 2017)

SYN/ACK packets
y = server seq#
x = client seq#

SYN spoofing attack

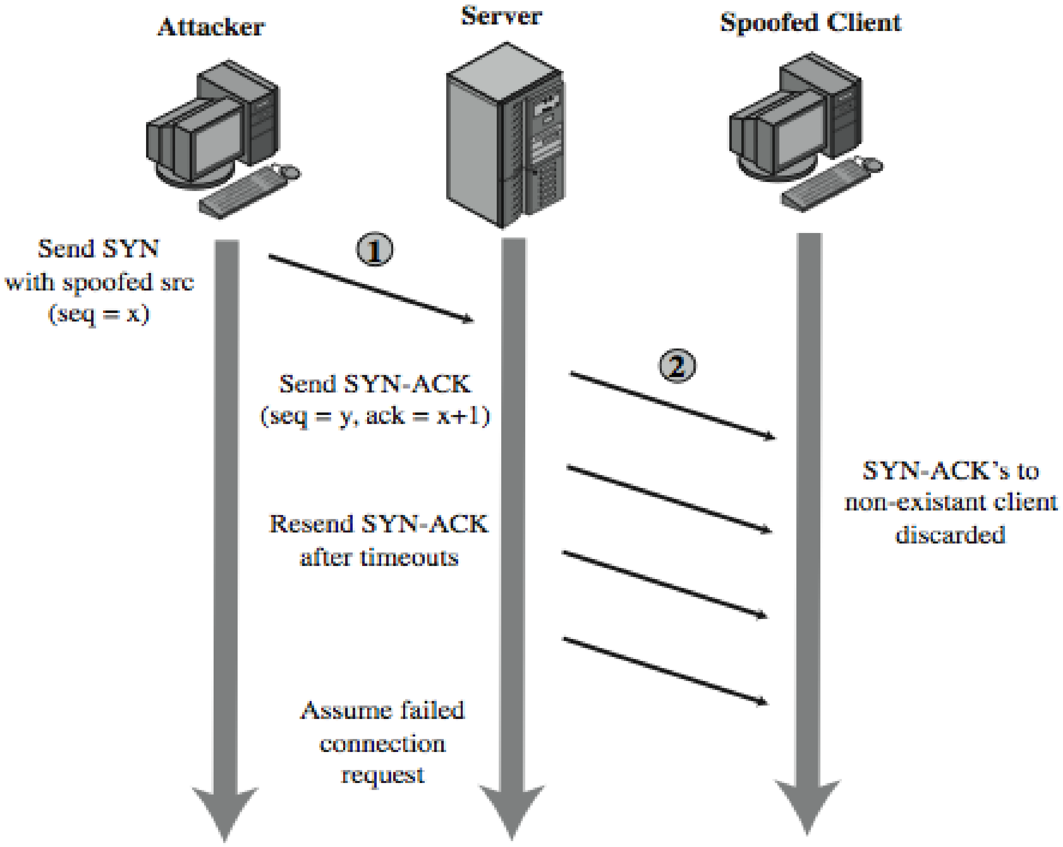

Attacker
Server
Spoofed Client
Send SYN with spoofed src (seq = x)
1
Send SYN-ACK (seq = y, ack = x+1)
2
SYN-ACK's to non-existant client discarded
Resend SYN-ACK after timeouts
Assume failed connection request

Figure 7.3 (Stallings et al., 2017)

SYN spoofing attack (cont.)

- Source of attack
  - Addresses that will not respond to the SYN-ACK with a RST
    - Random source addresses (addresses that may not exist)
    - An overloaded host (that may not send a RST)
- Difference between flooding attack
  - Much lower traffic volume
  - attacker can be on a much lower capacity link
- Countermeasures
  - Use modified TCP connection handling code
    - Cryptographically encode critical information in a cookie that is sent as the server’s initial sequence number
    - Selective drop or random drop an entry of incomplete connection
    - Modify parameters: size of TCP connection table; timeout to remove entries from the table

Common flooding attacks

- Classified based on network protocol used to implement the attack
- Objective: to overload the network capacity on some link to a host
- Single attacking system
  - ICMP flooding
  - UDP flooding
  - TCP SYN flooding
- Multiple attacking system
  - Distributed DoS (DDoS) attacks
  - Reflector attacks
  - Amplifier attacks

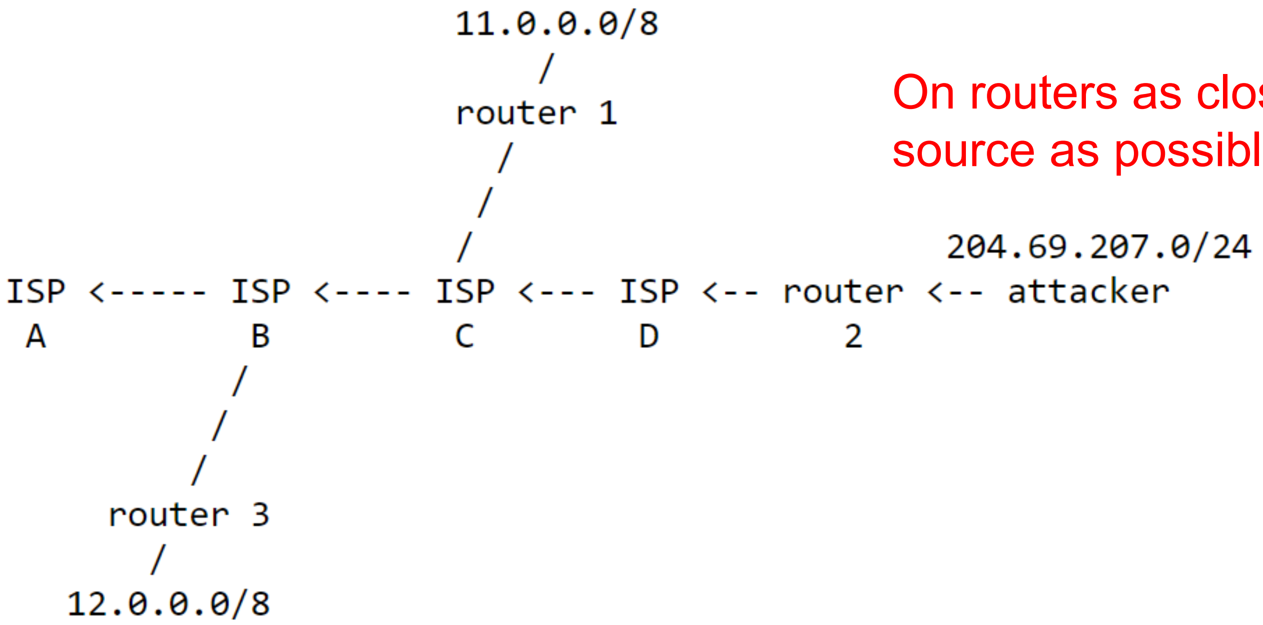
Common flooding attacks (cont.)

- ICMP flood
  - Use ICMP echo request packets
  - Traditionally allowed for network diagnosis, most recently may be filtered by firewalls
  - Countermeasure: impose limits on packet rate
- UDP flood
  - UDP packets directed to some ports (e.g. diagnostic echo service enabled by some server systems)
  - Use spoofed source address if the attack is generated using a single source system
- TCP SYN flood
  - Send TCP SYN (connection request) packets
  - Difference with SYN spoofing attack: aim for volume of packets

Countermeasure against spoofed source address

- Ingress filtering (“RFC 2827” 2000)

On routers as close to source as possible



```
                      11.0.0.0/8
                          /
                      router 1
                        /
                       /
                      /                       204.69.207.0/24
ISP <----- ISP <---- ISP <--- ISP <-- router <-- attacker
 A          B         C        D         2
           /
          /
         /
     router 3
       /
   12.0.0.0/8
```

Restricted forged traffic (“RFC 2827” 2000)

Distributed DoS attacks

- Use multiple systems
  - Often compromised PCs/workstations
  - Forming a botnet

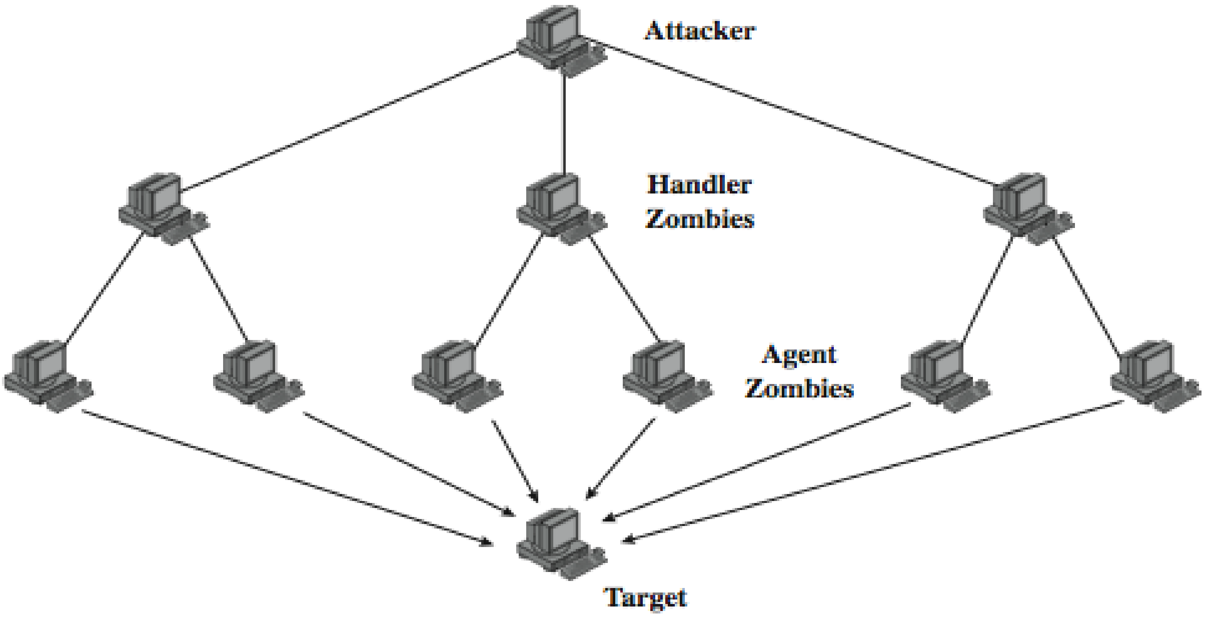
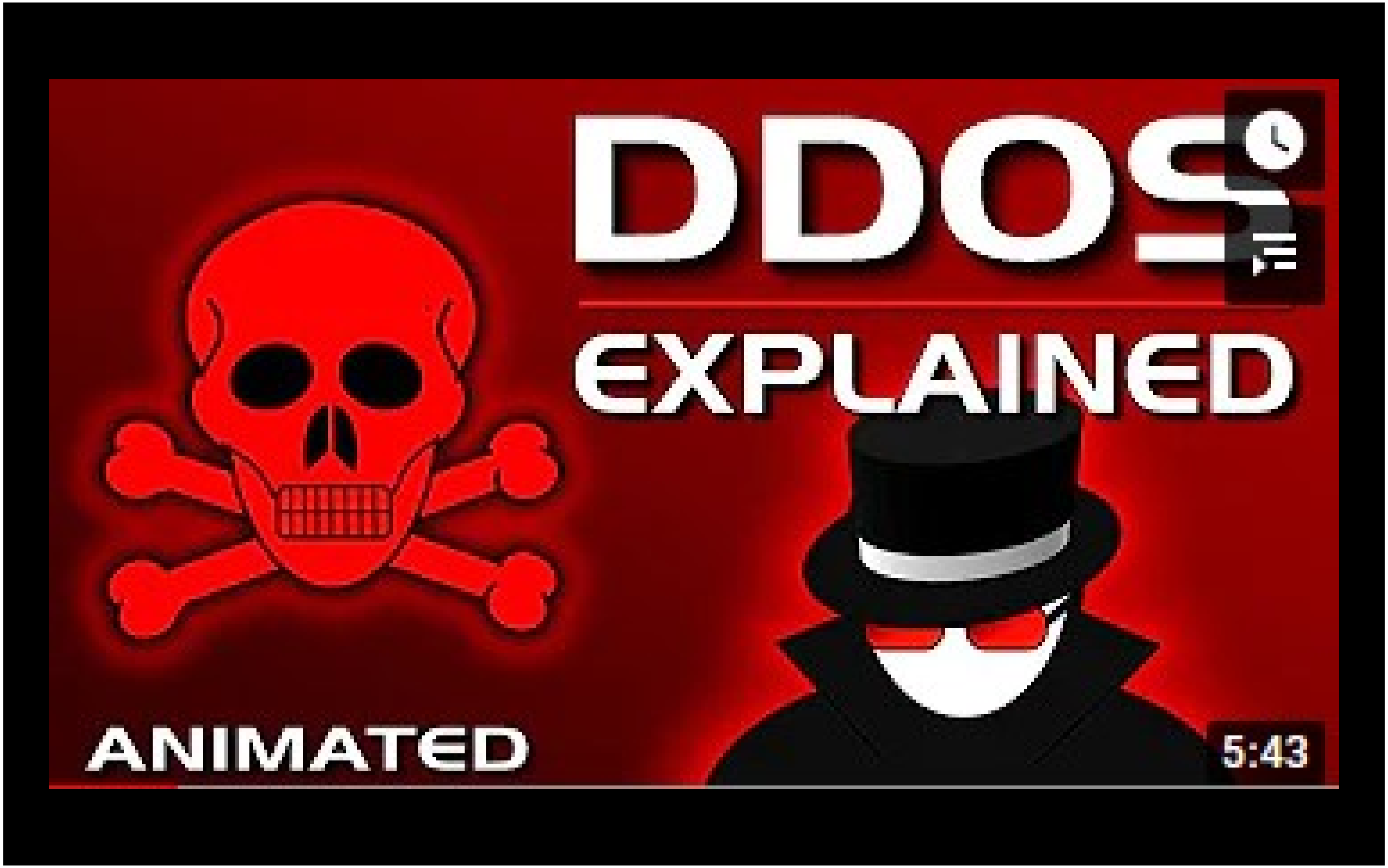


Figure 7.4 DDoS attack architecture (Stallings et al., 2017)

DDoS animated demo



Courtesy of YouTube & PowerCert video
https://www.youtube.com/watch?v=ilhGh9CEIwM

Reflector and amplifier attacks

- Process
  - Attacker sends packets to a known service on the intermediary with a spoofed source address of the target
  - Intermediary responds to the target
- Difference with DDoS attacks
  - Intermediaries are systems functioning normally
- Two types
  - Simple reflection attacks
  - Amplifier attacks

Reflection attacks

- Use a service that created a larger response packet than the original request
  - Common UDP services
  - TCP SYN packets
    - Attacker sends SYN packets to chosen intermediaries with spoofed source address of target
    - Intermediaries sends SYN-ACK packets to target
  - DNS
- Choose servers as intermediaries
  - Generate high volume of traffic
  - Obscure attack traffic in the normal high volume traffic
- Countermeasure
  - Ingress filtering (“RFC 2827” 2000)

Reflection attacks (cont.)

- DNS reflection attack
  - Create a self-contained loop between intermediary and target
  - Fairly easy to filter and block due to the rare combinations of service ports

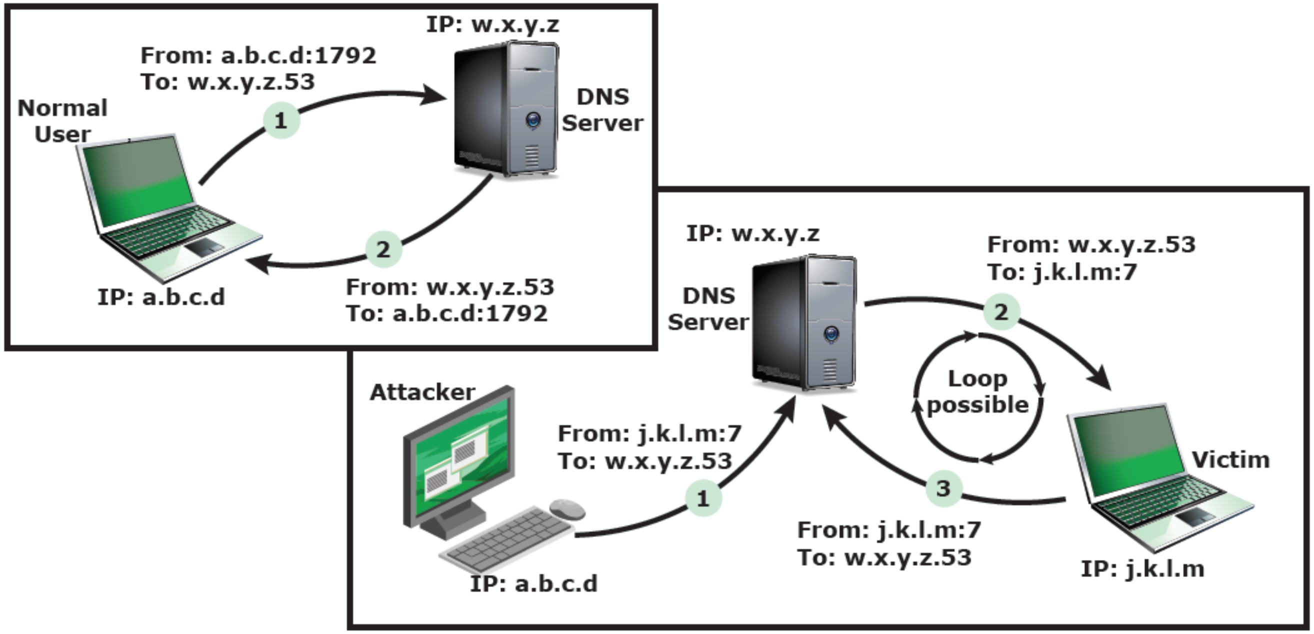


Figure 7.6 (Stallings et al., 2017)

Amplification attacks

- Send a packet with a spoofed source address of the target system to the broadcast address of the network
- Services to be used
  - ICMP echo request packets (e.g. smurf attack)
  - UDP echo service
- Countermeasure
  - Disallow directed broadcasts into the network from outside

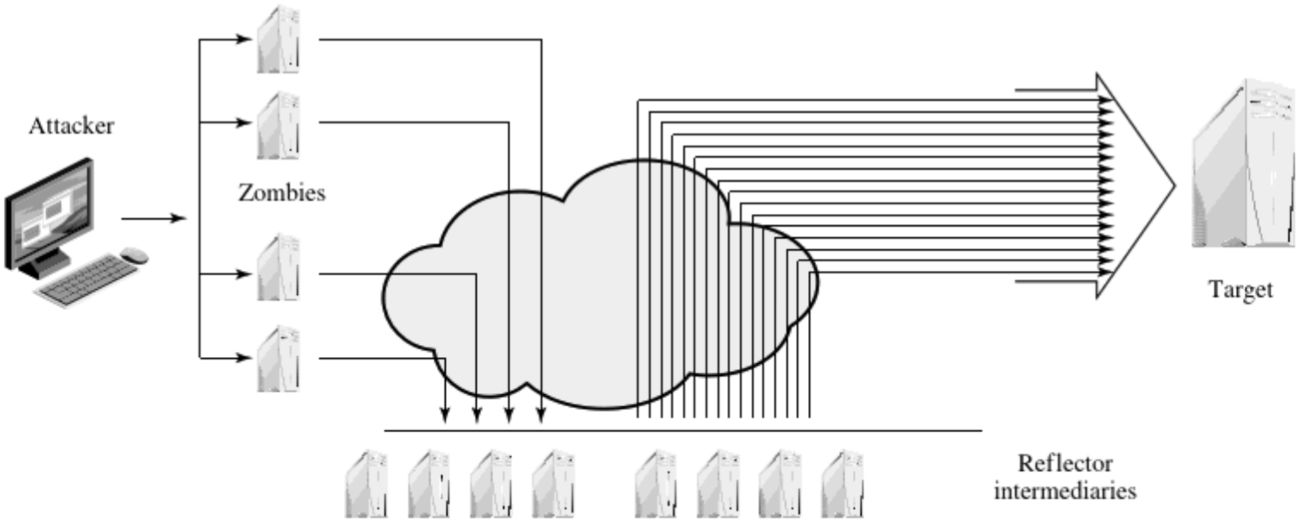


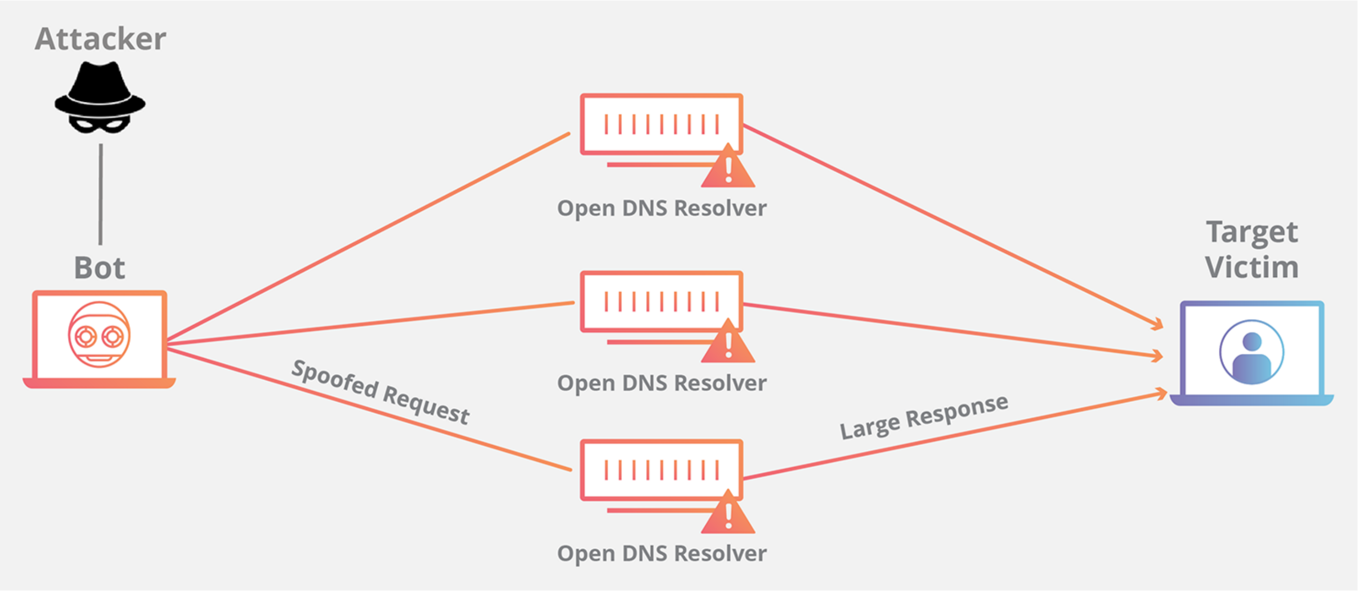
Figure 7.7 (Stallings et al., 2017)

DNS amplification attacks

- Use packets directed at a legitimate DNS server as the intermediary system
  - Attacker creates DNS requests with the spoofed source address of the target system
  - DNS server sends responses to the target
    - Traditionally a 60 byte UDP request packet can result in a 512 byte UDP response (amplification)
    - Most recent protocol could allow larger responses of over 4000 bytes, to support extended DNS features (e.g. IPv6, security)
- Countermeasure
  - Ingress filtering (“RFC 2827” 2000)

DNS amplification DoS attacks

- Exploit recursive DNS name servers
- Countermeasure
  - Ingress filtering (“RFC 2827” 2000)
  - Limit recursive responses to internal clients (“RFC 5358” 2008)



Example scenario (Cloudflare, n.d.)

Application-based bandwidth attacks

- Force the victim system to execute resource-consuming operations (e.g. website searches)
- Two example protocols used in the attacks
  - SIP flood
  - HTTP-based attacks
- Countermeasure
  - Enable a form of graphical puzzle (captcha) to distinguish legitimate human requests

SIP flood

- Session Initiation Protocol (SIP)
  - VoIP call setup protocol
  - Text-based protocol
  - Two types of messages: requests and responses
- SIP INVITE scenario
- Flood attack
  - Send many INVITE requests to a proxy
  - Proxy server resources depleted in handling requests
  - Network bandwidth capacity consumed
  - Call receiver flooded with forged calls

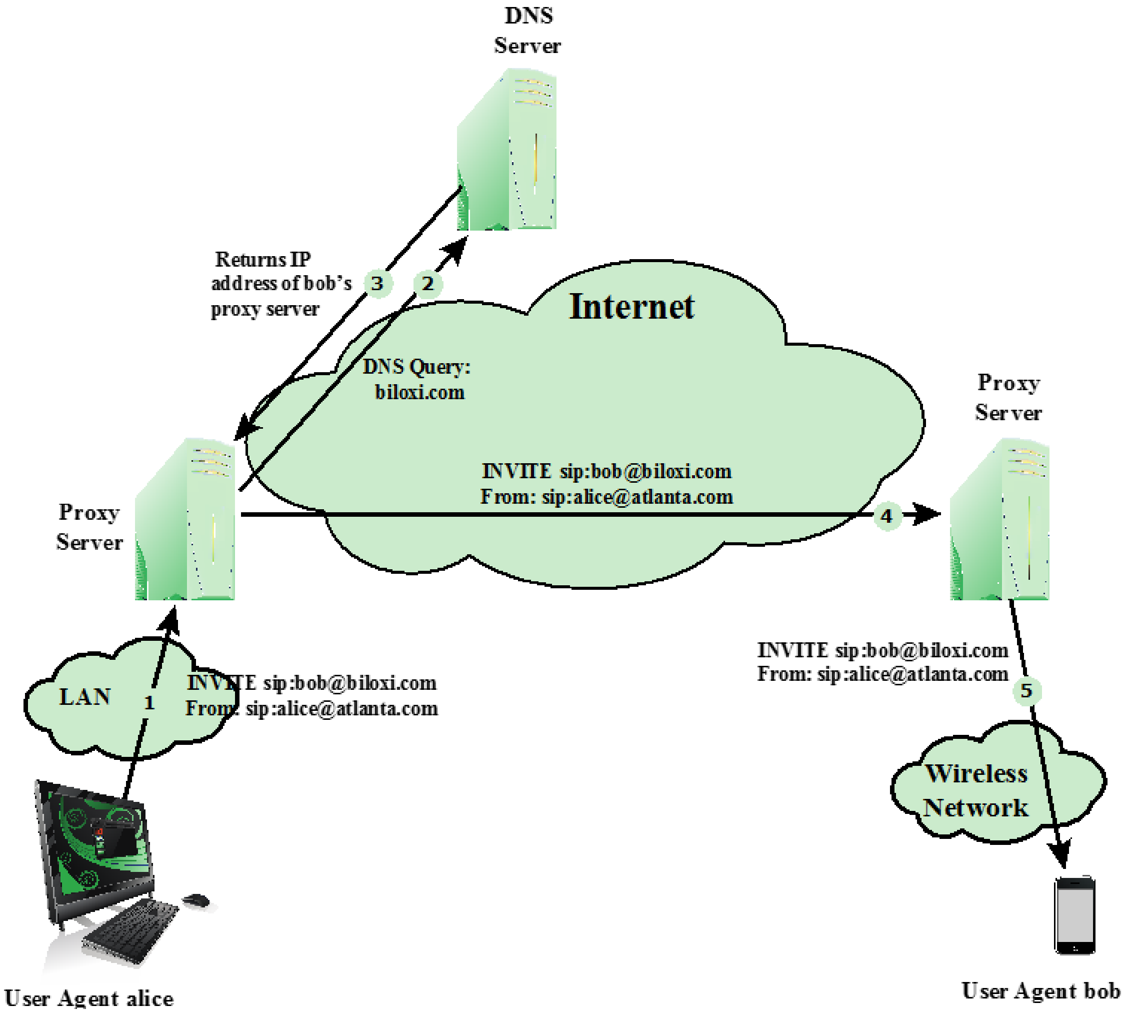

DNS Server
Returns IP address of bob's proxy server
3
2
Internet
DNS Query: biloxi.com
Proxy Server
Proxy Server
INVITE sip:bob@biloxi.com
From: sip:alice@atlanta.com
4
LAN
1
INVITE sip:bob@biloxi.com
From: sip:alice@atlanta.com
INVITE sip:bob@biloxi.com
From: sip:alice@atlanta.com
5
Wireless Network
User Agent alice
User Agent bob

Figure 7.5 (Stallings et al., 2017)

HTTP-based attacks

- HTTP flood
  - DDoS attack with HTTP requests from many bots
- Recursive HTTP flood/Spidering
  - Bots start from a given website page and follow all pages on the provided website in a recursive way
- Slowloris
  - Send multiple incomplete HTTP requests (without a blank line indicating end of header); server opens multiple connections and fills up the maximum concurrent connection pool
  - Not recognised by existing intrusion detection and prevention solutions that rely on signatures
  - Countermeasures
    - Limit rate of incoming connections and timeout
    - Delay binding by load balancing software

Defences against DDoS attacks

- Attack prevention and preemption (before attack)
  - Enforce policies for resource consumption
  - Provide backup resources
- Attack detection and filtering (during the attack)
  - Look for suspicious patterns of behaviour and filter out packets
- Attack source traceback and identification (during and after the attack)
  - Identify source of the attack
- Attack reaction (after the attack)
  - Eliminate effects of the attack

Responding to attacks

- Good incident response plan
  - Details on how to contact technical personnel from an ISP
  - Impose filtering of upstream traffic for DoS attacks
  - Details on how to respond to the attack
- Implement anti-spoofing, directed broadcast, and rate limiting filters
- Network monitors and IDS to detect and notify abnormal traffic patterns

Responding to attacks (cont.)

- Identify type of attack
    - Capture and analyse packets
    - Design filters to block attack traffic or identify and correct system/application bug
- Ask ISP to trace packet flow back to source
    - May be difficult and time consuming
- Implement contingency plan
    - Switch to alternate backup servers
    - Commission new servers at a new site with new addresses
- Update incident response plan

Summary

- Introduced denial of service (DoS) attacks
- Classic flooding and SYN spoofing attacks
- ICMP, UDP, TCP SYN floods
- Distributed denial of service (DDoS) attacks
- Reflection and amplification attacks
- Defenses against DoS attacks
- Responding to DoS attacks

Next lecture – Intrusion detection

- Intrusion detection
  - Basic principles
  - Analysis approaches
  - Host-based, network-based, distributed host-based
  - Cyberdeception
- Firewalls
- Intrusion prevention systems

References

- Stallings, W. and Brown, L. (2017). Computer Security: Principles and Practice. Pearson Education.
- IP address spoofing. Retrieved from https://en.wikipedia.org/wiki/IP_address_spoofing
- RFC 2827 (2000). Retrieved from https://tools.ietf.org/html/rfc2827
- RFC 5358 (2008). Retrieved from https://tools.ietf.org/html/rfc5358
- Cloudflare. DNS Amplification Attack. Retrieved from https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/