COURSE TECHNOLOGY
CENGAGE Learning™

Security+ Guide to Network Security Fundamentals, Fourth Edition

Network Attacks

Denial of service Attacks

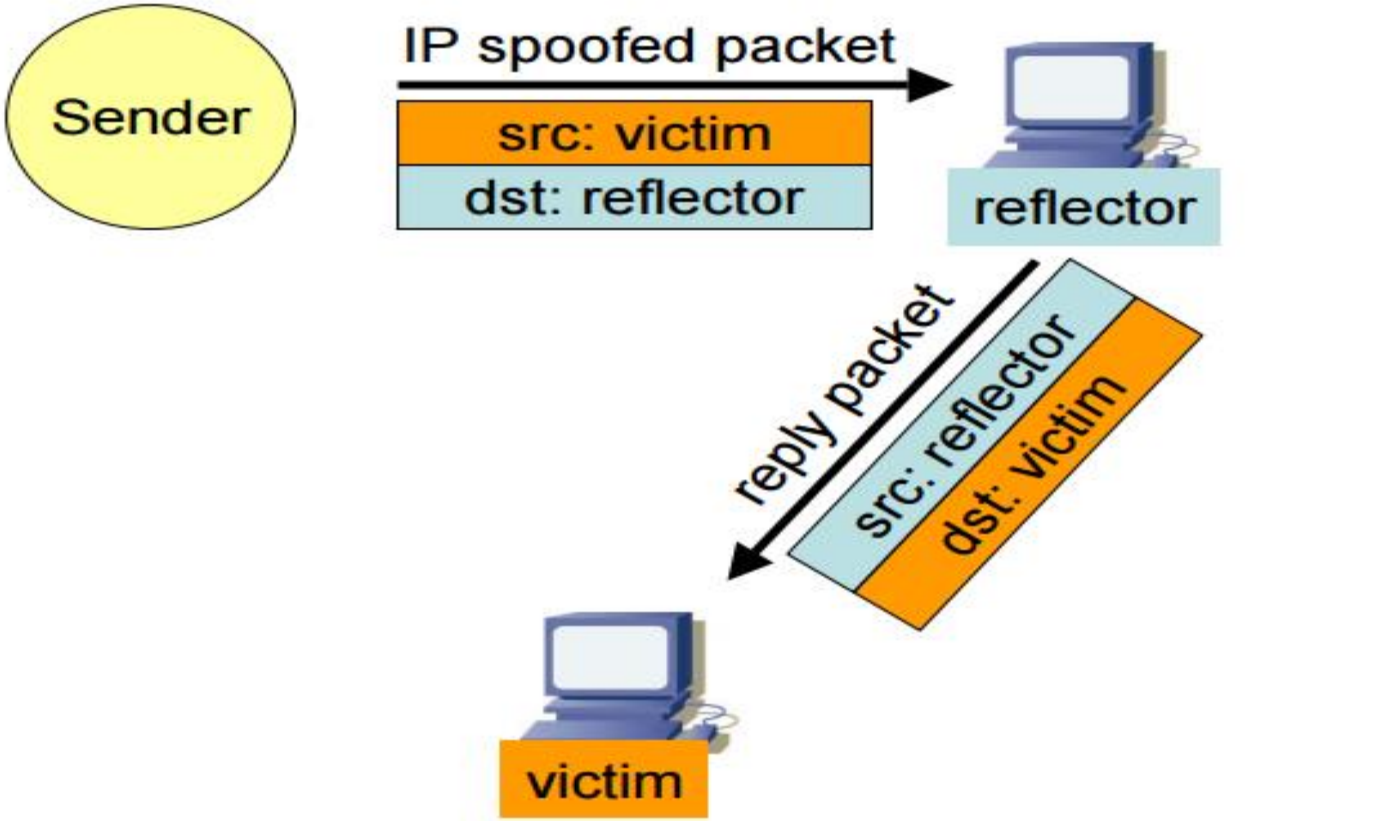
Introduction: What is DoS?

- DoS attack is an attempt (malicious or selfish) by an attacker to cause a victim to deny service to its customers
  - DoS is an action that prevents the authorized use of **networks**, **systems**, or **applications** by exhausting resources such as CPU, memory, bandwidtch, and disk space
- Categories of resources that could be attacked
  - **Network bandwidth**
    - Related to the capacity of network links connecting a server to the wider Internet
  - **System resources**
    - Overloading/crashing network handling software (e.g., SYN spoofing, ping-of-death – a “huge” ping packet)
  - **Application resources**
    - Overloading the capabilities of a web server application (e.g., valid querries)

Dos Attacks

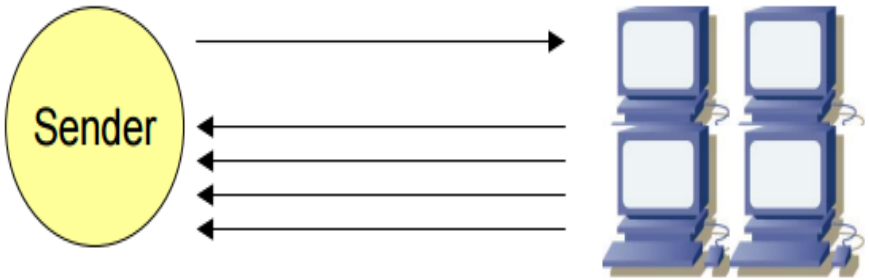
- Dos attacks uses two basic techniques of attack
  - Reflection
  - Amplification

reflection

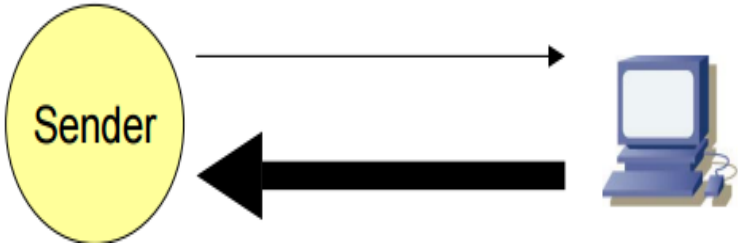

Sender
IP spoofed packet
src: victim
dst: reflector
reflector
reply packet
src: reflector
dst: victim
victim
Desktop
sidris

amplification

1. multiple replies



2. bigger reply



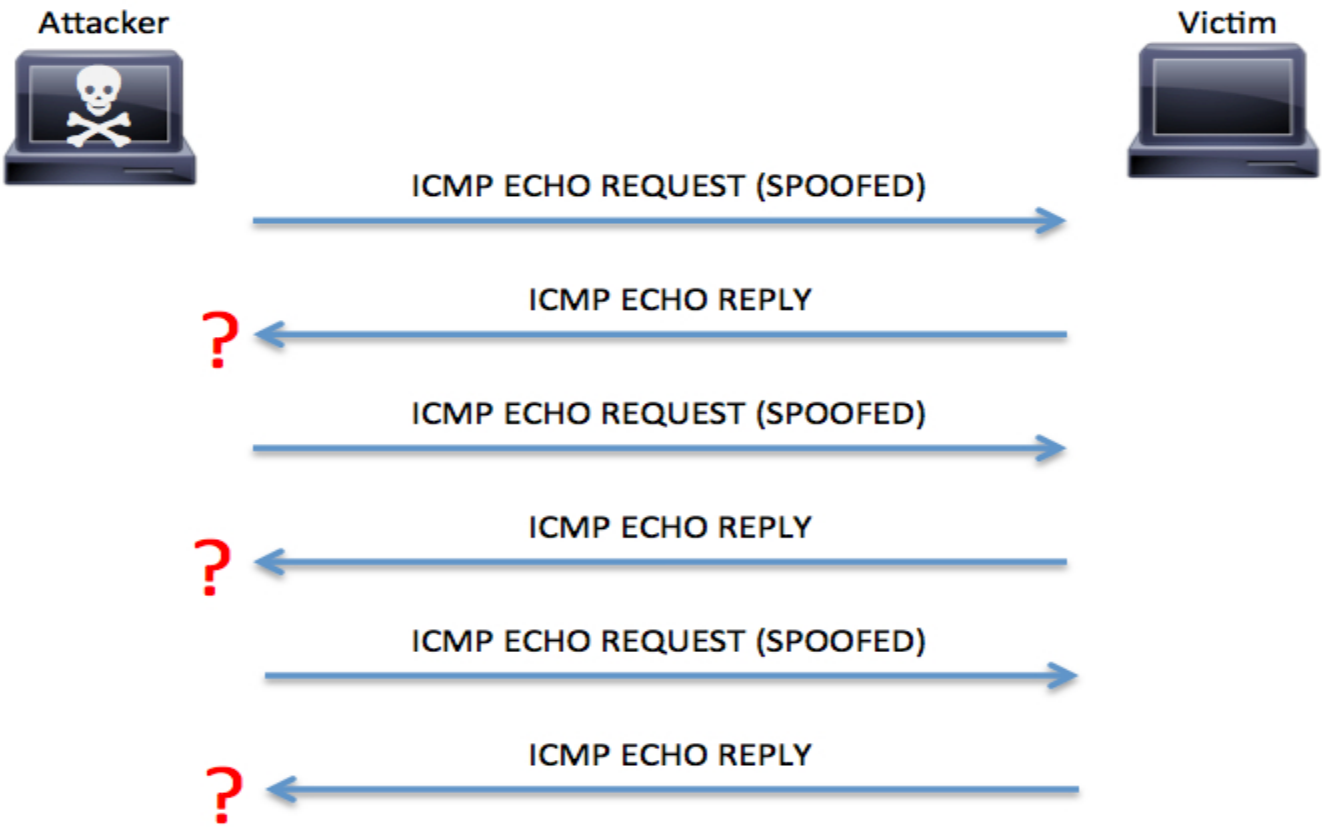
DOS Attacks

- Denial of service (DoS)
  - Ping flood attack
    - Ping utility used to send large number of echo request messages
    - Overwhelms Web server (target server)
    - Ping of Death: famous ping attack using a large packet size and large number of ping requests.
  - Smurf attack
    - Ping request with originating address changed
    - Appears as if target computer is asking for response from all computers on the network

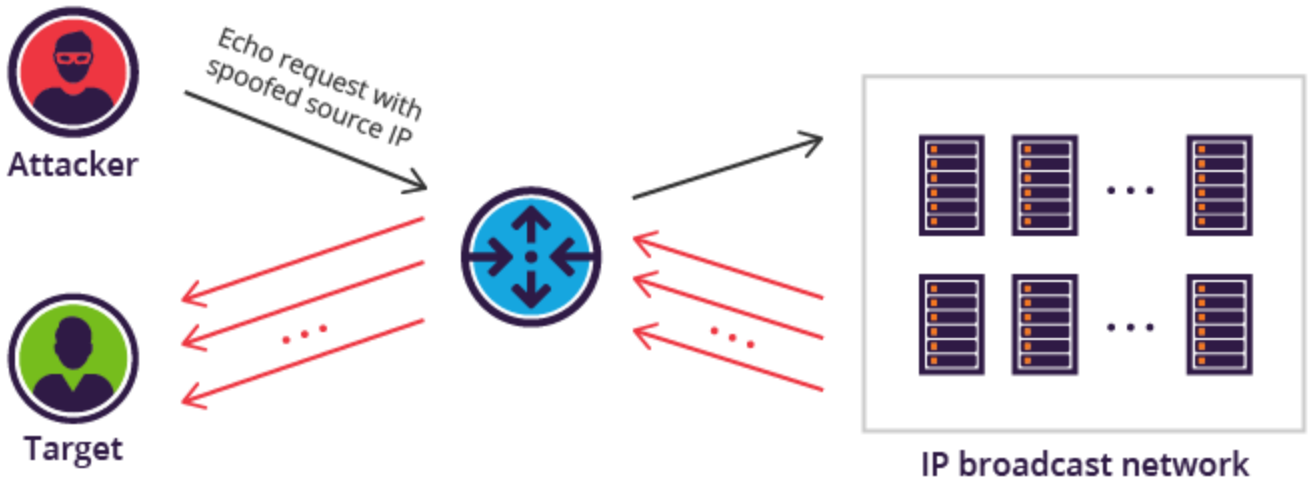
Dos Attacks

- Denial of service (DoS) (cont'd.)
  - SYN flood attack
    - Takes advantage of procedures for establishing a connection
- Distributed denial of service (DDoS)
  - Attacker uses many zombie computers in a botnet to flood a device with requests
  - Virtually impossible to identify and block source of attack

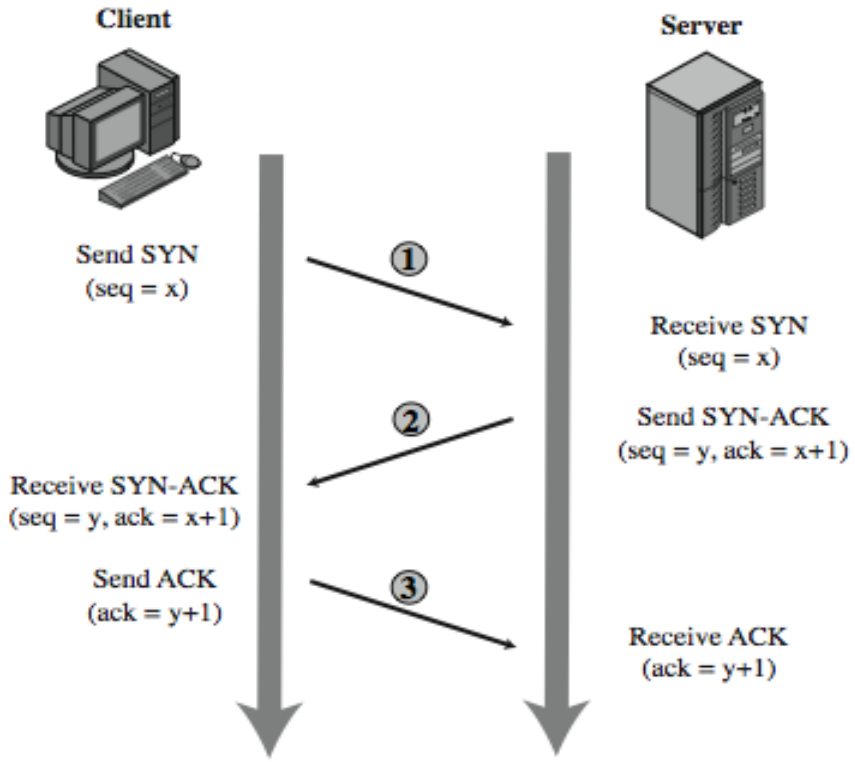
Ping Flood - Network Attacks



SMURF Ping Flood



SYN FLOOD
TCP Connection Handshake



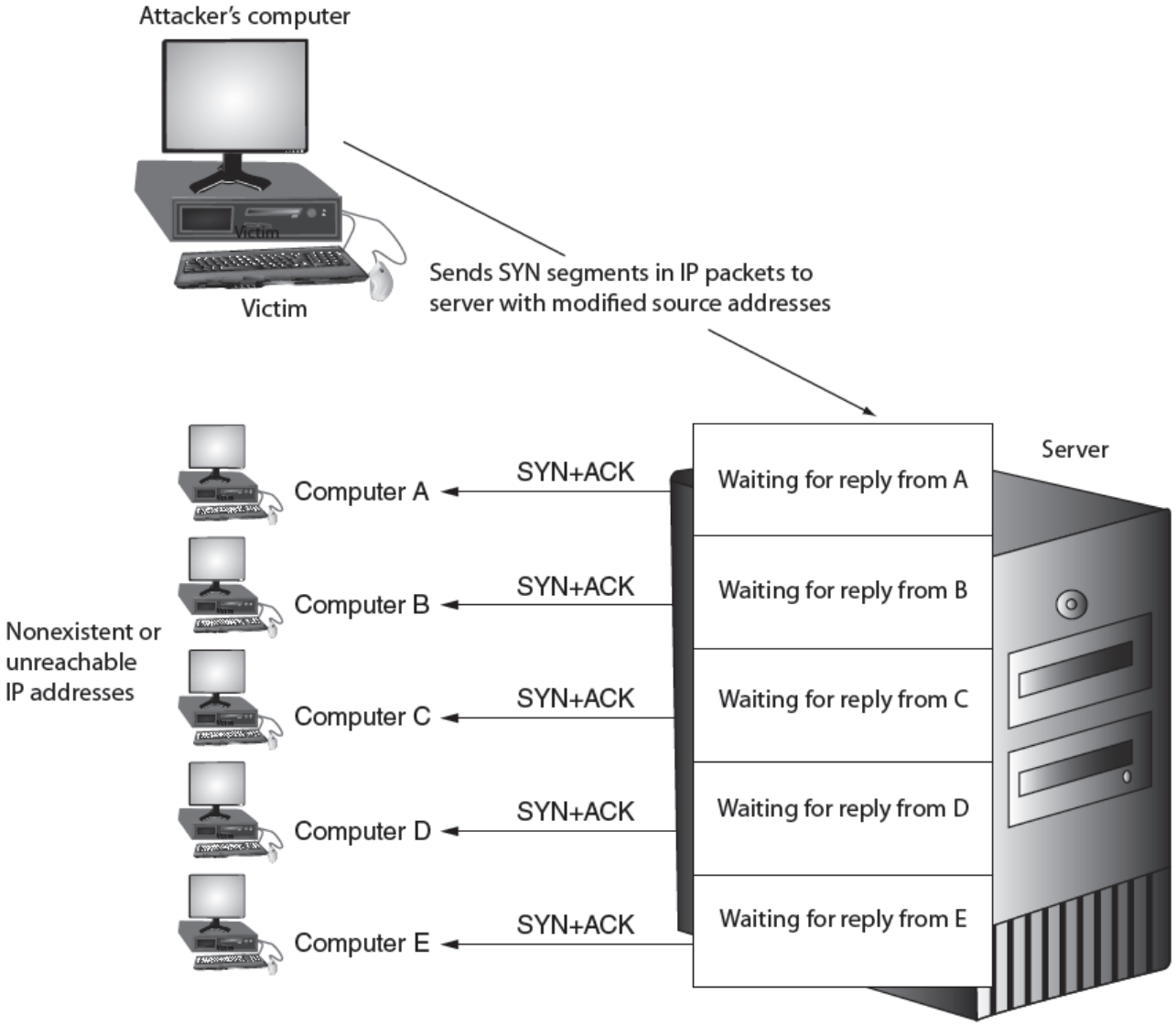
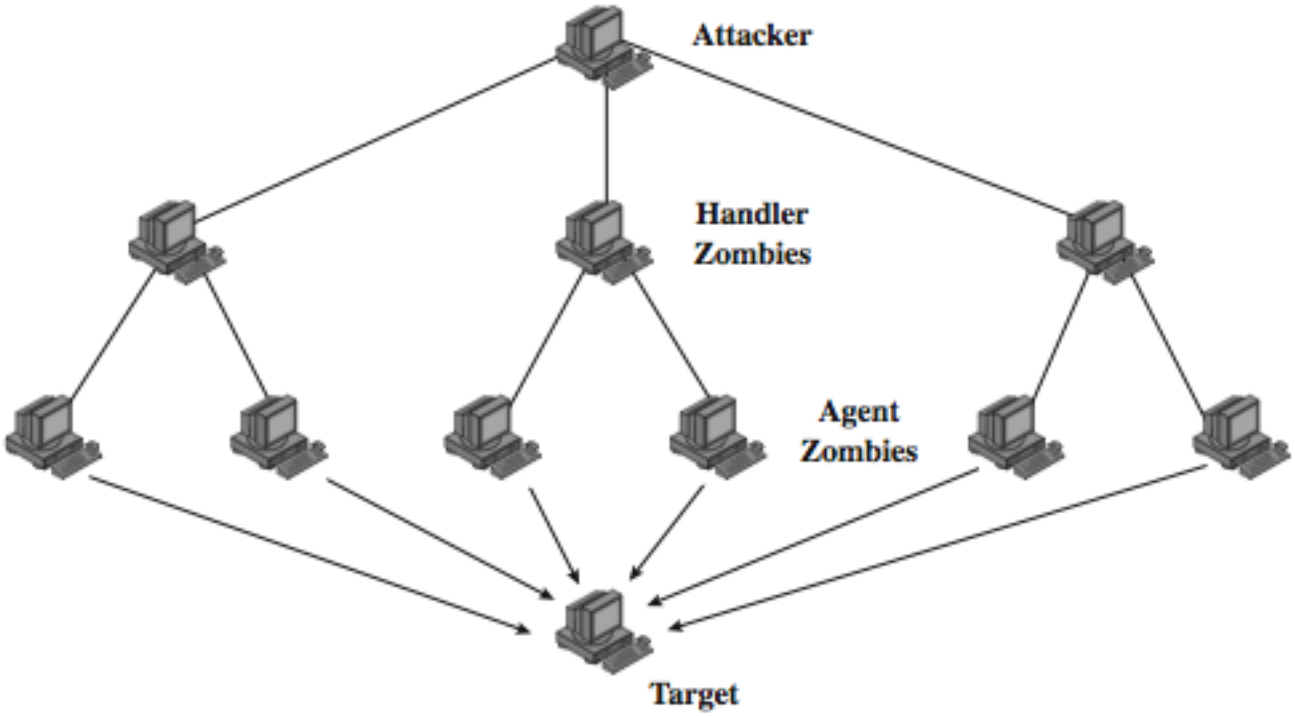


Figure 3-9 SYN flood attack

DDoS Control Hierarchy



Poisoning

- ARP poisoning
  - Attacker modifies MAC address in ARP cache to point to different computer

Device	IP and MAC address	ARP cache before attack	ARP cache after attack
Attacker	192.146.118.2 & 00-AA-BB-CC-DD-02	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04
Victim 1	192.146.118.3& 00-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-02
Victim 2	192.146.118.4 & 00-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-02

Table 3-3 ARP poisoning attack

Poisoning (cont'd.)

Attack	Description
Steal data	An attacker could substitute their own MAC address and steal data intended for another device
Prevent Internet access	An attacker could substitute an invalid MAC address for the network gateway so that no users could access external networks
Man-in-the-middle	A man-in-the-middle device could be set to receive all communications by substituting that MAC address
DoS attack	The valid IP address of the DoS target could be substituted with an invalid MAC address, causing all traffic destined for the target to fail

Table 3-4 Attacks from ARP poisoning

Poisoning (cont'd.)

- DNS poisoning
  - Domain Name System is current basis for name resolution to IP address
  - DNS poisoning substitutes DNS addresses to redirect computer to another device
- Two locations for DNS poisoning
  - Local host table
  - External DNS server

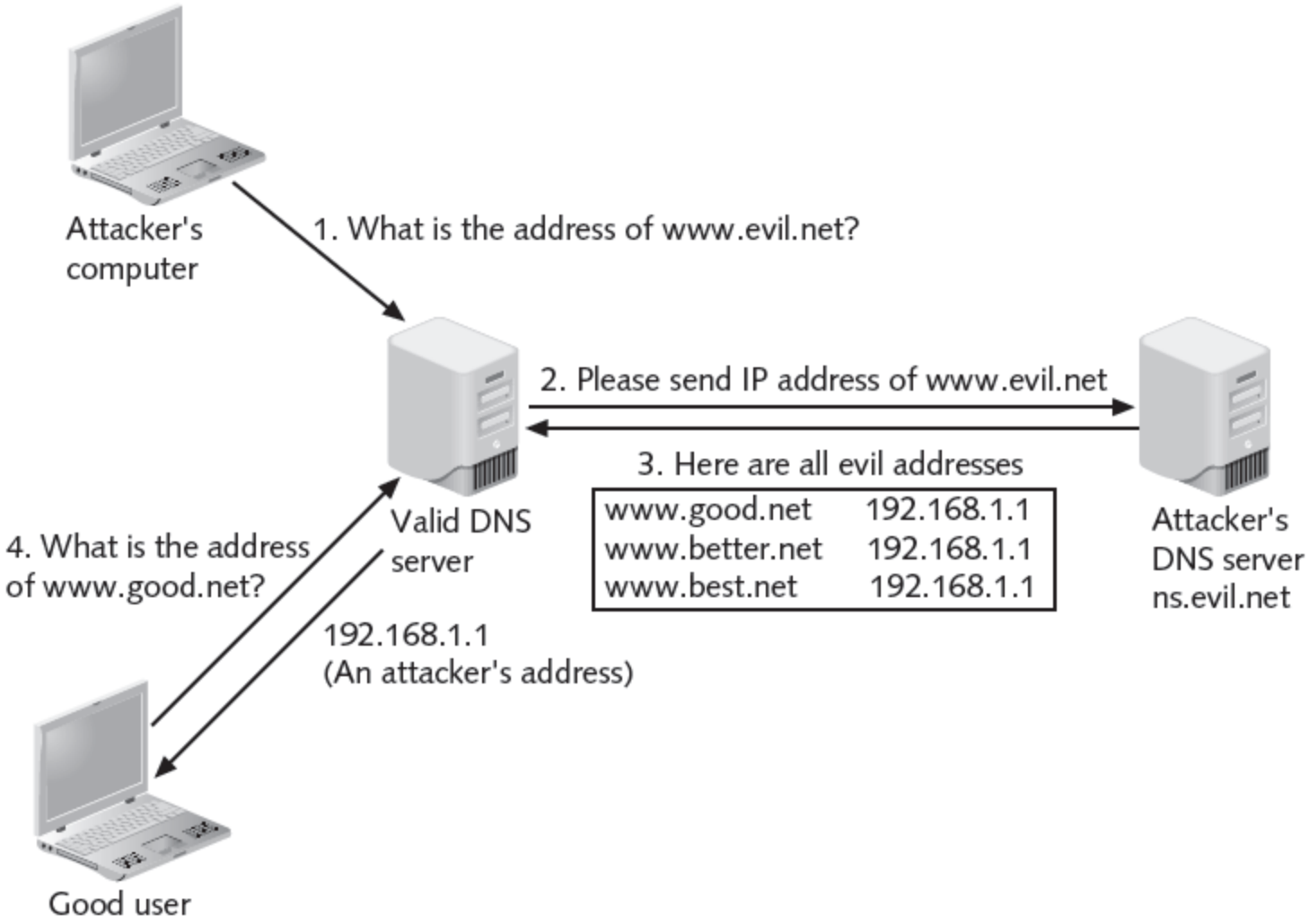
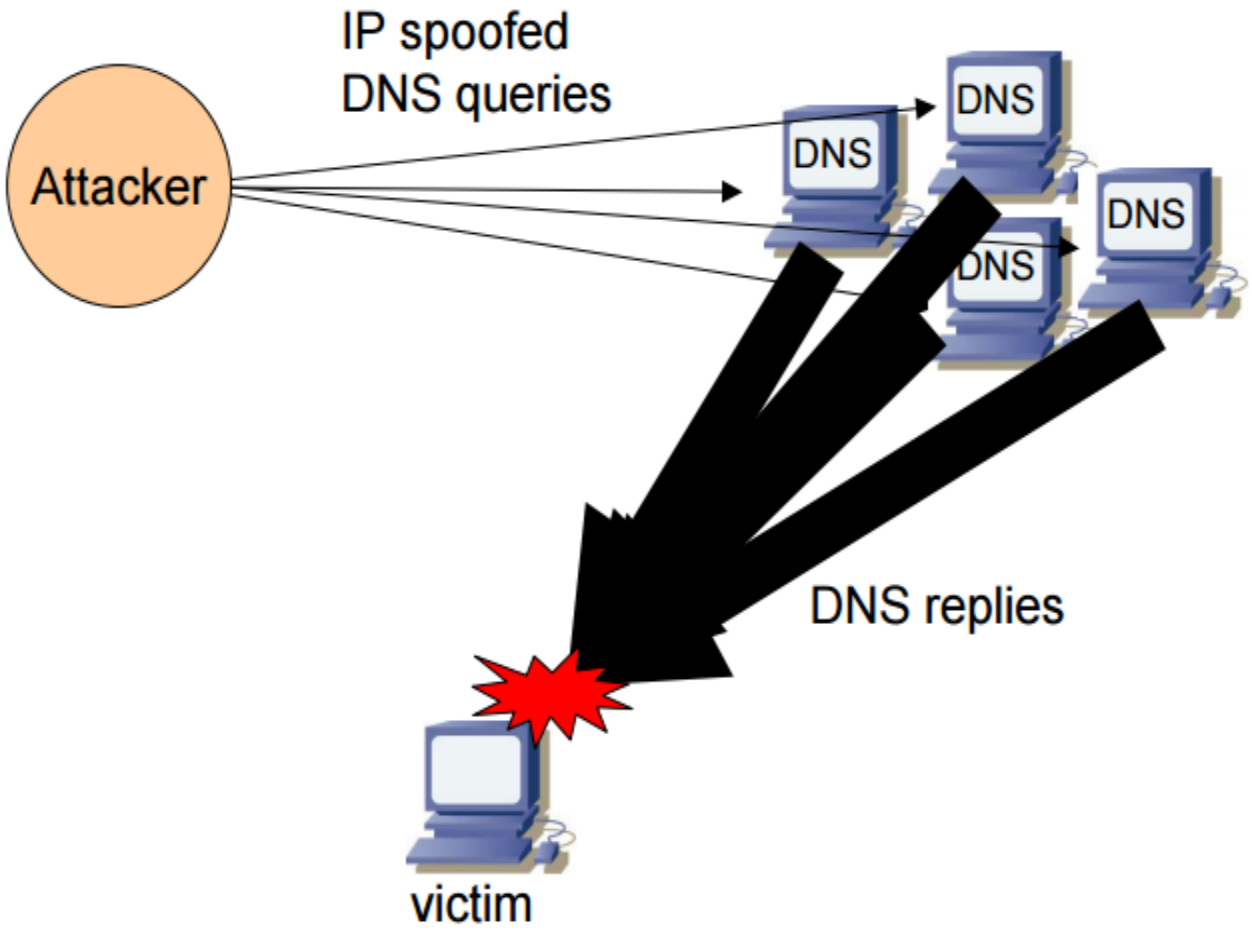


Figure 3-12 DNS poisoning

DNS amplification attack



Attack Prevention

- block spoofed source addresses
  - on routers as close to source as possible
  - still far too rarely implemented
- rate controls in upstream distribution nets
  - on specific packets types
  - e.g. some ICMP, some UDP, TCP/SYN
- use modified TCP connection handling
  - use SYN cookies when table full
  - or selective or random drop when table full

Attack Prevention

- block IP directed broadcasts
- block suspicious services & combinations
- manage application attacks with “puzzles” to distinguish legitimate human requests
- good general system security practices
- use mirrored and replicated servers when high-performance and reliability required

Responding to Attacks

- need good incident response plan
  - with contacts for ISP
  - needed to impose traffic filtering upstream
  - details of response process
- have standard filters
- ideally have network monitors and IDS
  - to detect and notify abnormal traffic patterns

Responding to Attacks

- identify type of attack
  - capture and analyze packets
  - design filters to block attack traffic upstream
  - or identify and correct system/application bug
- have ISP trace packet flow back to source
  - may be difficult and time consuming
  - necessary if legal action desired
- implement contingency plan
- update incident response plan