Security Countermeasures

– Lecture (2) – Types of attacks - I

– Information Security Department

- 2nd Class- Second Course
- 5 February /2024

By

Assist. Lecturer : **Nuha Kareem Hameed**

Email : NuhaKareem@uobabylon.edu.iq

Learning Objectives

- Describe the most common network attacks, including session hacking, denial of service, and buffer overflow.
- Explain how these attacks are executed.
- Identify basic defenses against those attacks.
- Configure a system to prevent denial of service attacks.

DoS

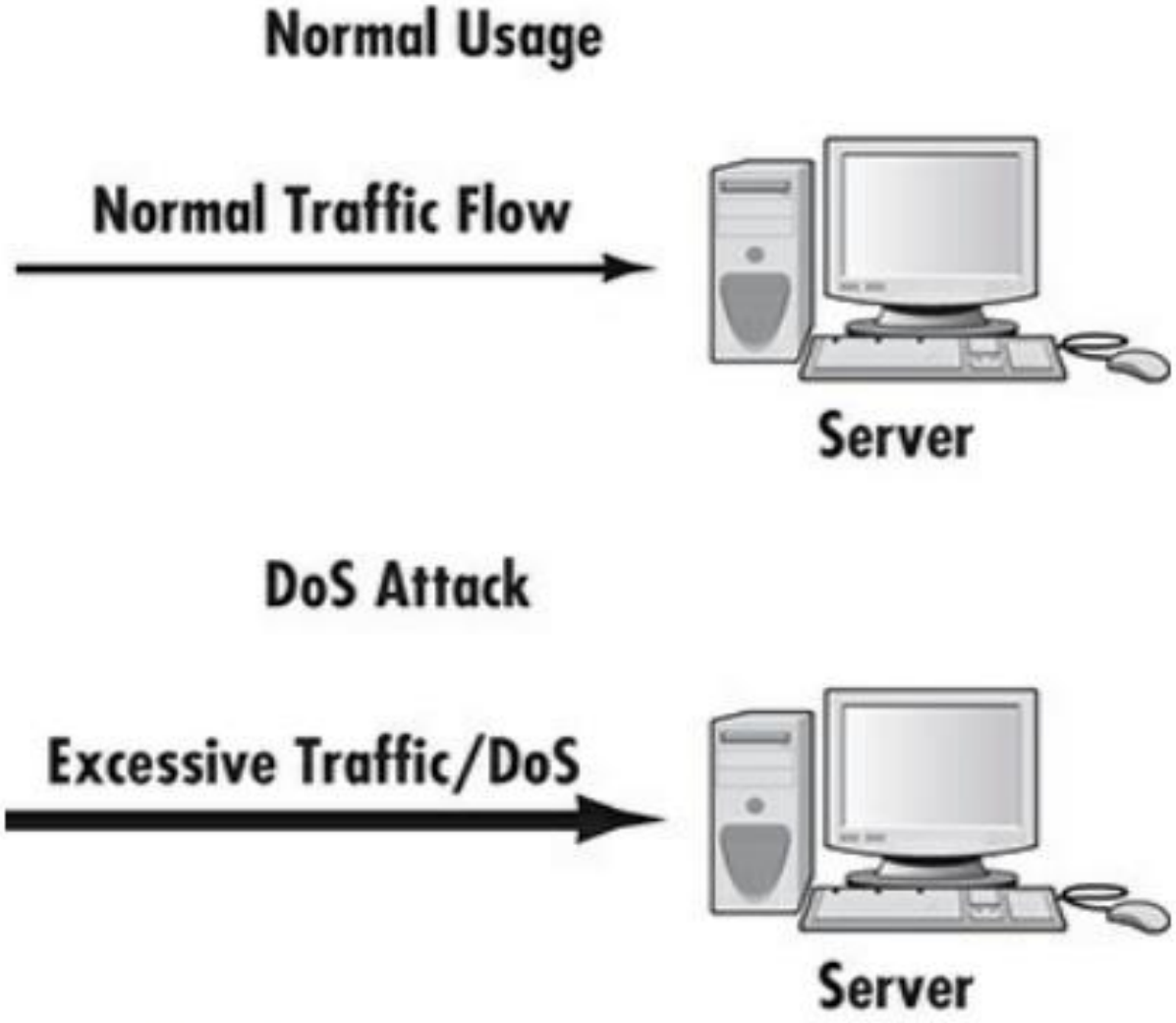
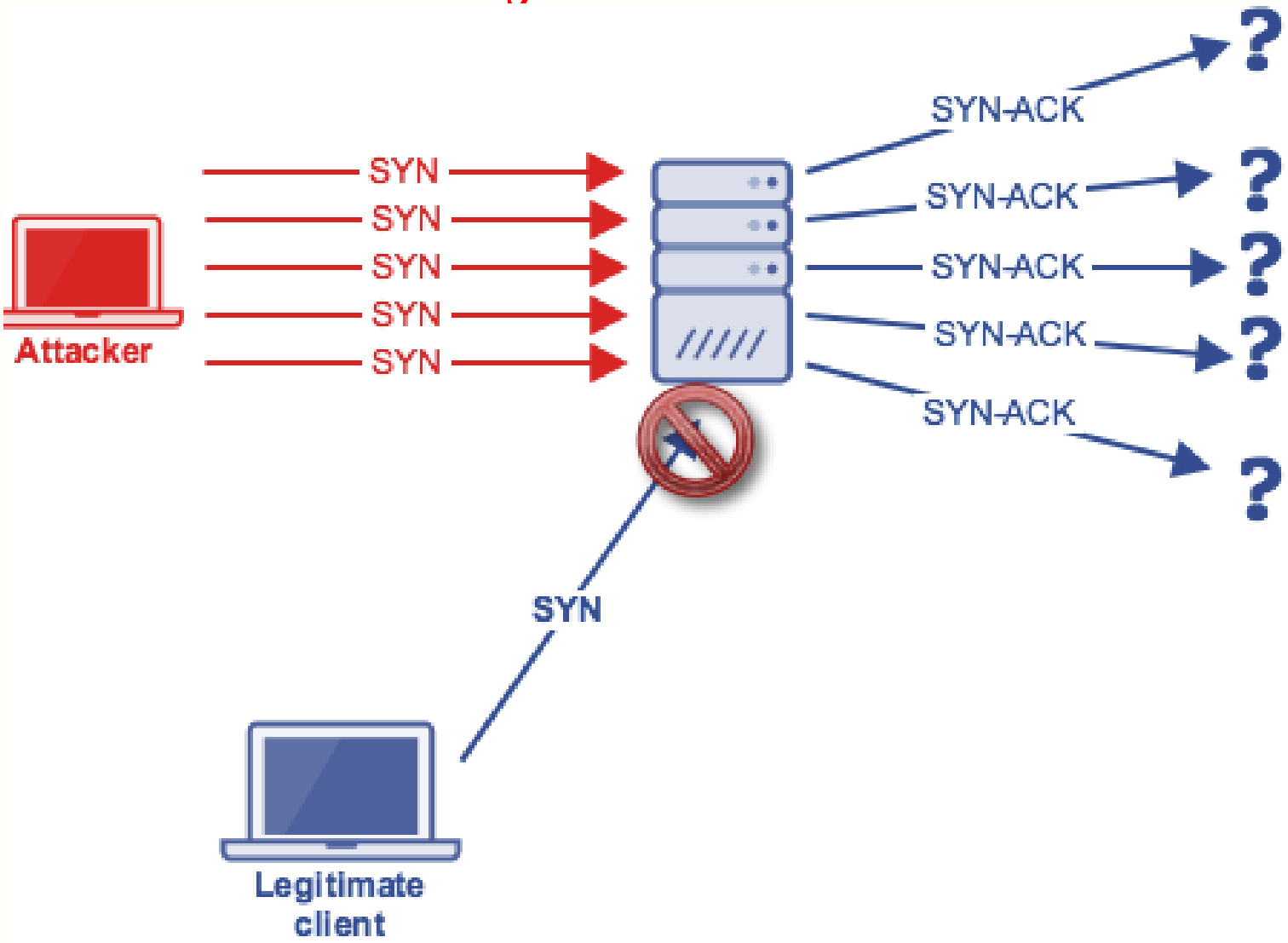


FIGURE 2-2 The DoS concept

DoS

- Overloading a target system is easier to do if you have more than one machine attacking it.
- It allows the attacker to launch the attack from other people's machines.
- In DoS attack , the real problem for the attacker is avoiding being caught

Sync flood


SYN
SYN
SYN
SYN
SYN
Attacker
SYN-ACK
SYN-ACK
SYN-ACK
SYN-ACK
SYN-ACK
?
?
?
?
?
SYN
Legitimate client

SYN flood: Defending with Micro Blocks

- Micro blocks seek to avoid SYN floods by changing the way the server allocates memory for any given connection request.
- Instead of allocating a complete connection object, the server is altered so that it only allocates a micro-record.
  - Newer implementations of this technique allocate as little as 16 bytes for the incoming SYN object.
- The specifics on how to set up micro blocks are specific to a given operating system.
- This is a less common technique.
  - Many network administrators are not even aware of this possibility

SYN flood : Defending with Bandwidth Throttling

- A common method to defend against DoS attacks is for the firewall or intrusion detection system to detect excessive traffic from one or more IP addresses and restrict that bandwidth.
  - This is using bandwidth throttling to mitigate the DoS attack

SYN flood : Defending with SYN Cookies

- As the name SYN cookies suggest,
  - this method uses cookies, not unlike the standard cookies used on many websites.
- With this method, the system does not immediately create a buffer space in memory for the hand-shaking process.
  - Rather, it first sends an SYN/ACK (the acknowledgment signal that begins the handshaking process).
  - The SYN/ACK contains a carefully constructed cookie, generated as a hash that contains the IP address, port number, and other information from the client machine requesting the connection.
  - When the client responds with a normal ACK (acknowledgment), the information from that cookie will be included, which the server then verifies.
    - Thus, the system does not fully allocate any memory until the third stage of the handshaking process.
- The SYN cookie requires some tradeoff between performance and **security:** overhead resources required.
- **The optimal solution** would be to have a very high-performance server (or server farm) that can handle the overhead and to implement SYN cookies.

SYN flood : Defending with RST Cookies

- Another cookie method that is easier to implement than SYN cookies is **the RST cookie**.
  - In this method, the server sends a wrong **SYN/ACK** back to the client. The client should then generate an RST (reset) packet telling the server that something is wrong.
  - Because the client sent back a packet notifying the server of the error, the server now knows the client request is legitimate and will now accept incoming connections from that client in the normal fashion.
- **This method has two disadvantages**.
  - First, it might cause problems with some earlier Windows machines and/or machines that are communicating from behind firewalls.
  - Also, some firewalls might block the return SYNACK packet.

Smurf attack

- The Smurf attack is a popular type of DoS attack.
  - It was named after the application first used to execute this attack.
- In the Smurf attack,
  - an **ICMP packet** is sent out to the broadcast address of a network,
  - but its return address has been altered to match one of the computers on that network, most likely a key **server**.
- All the computers on the network will then respond by pinging the target computer.
  - ICMP packets use the Internet Control Message Protocol to send error messages on the Internet.
  - Because the address the packets are sent to is a broadcast address, that address responds by echoing the packet out to all hosts on the network, who then send it to the spoofed source address.
- Continually sending such packets will cause the network itself to perform a DoS attack on one or more of its member servers.
- This attack is both clever and simple.
- This can be accomplished via some software such as a virus or Trojan horse that will begin sending the packets.

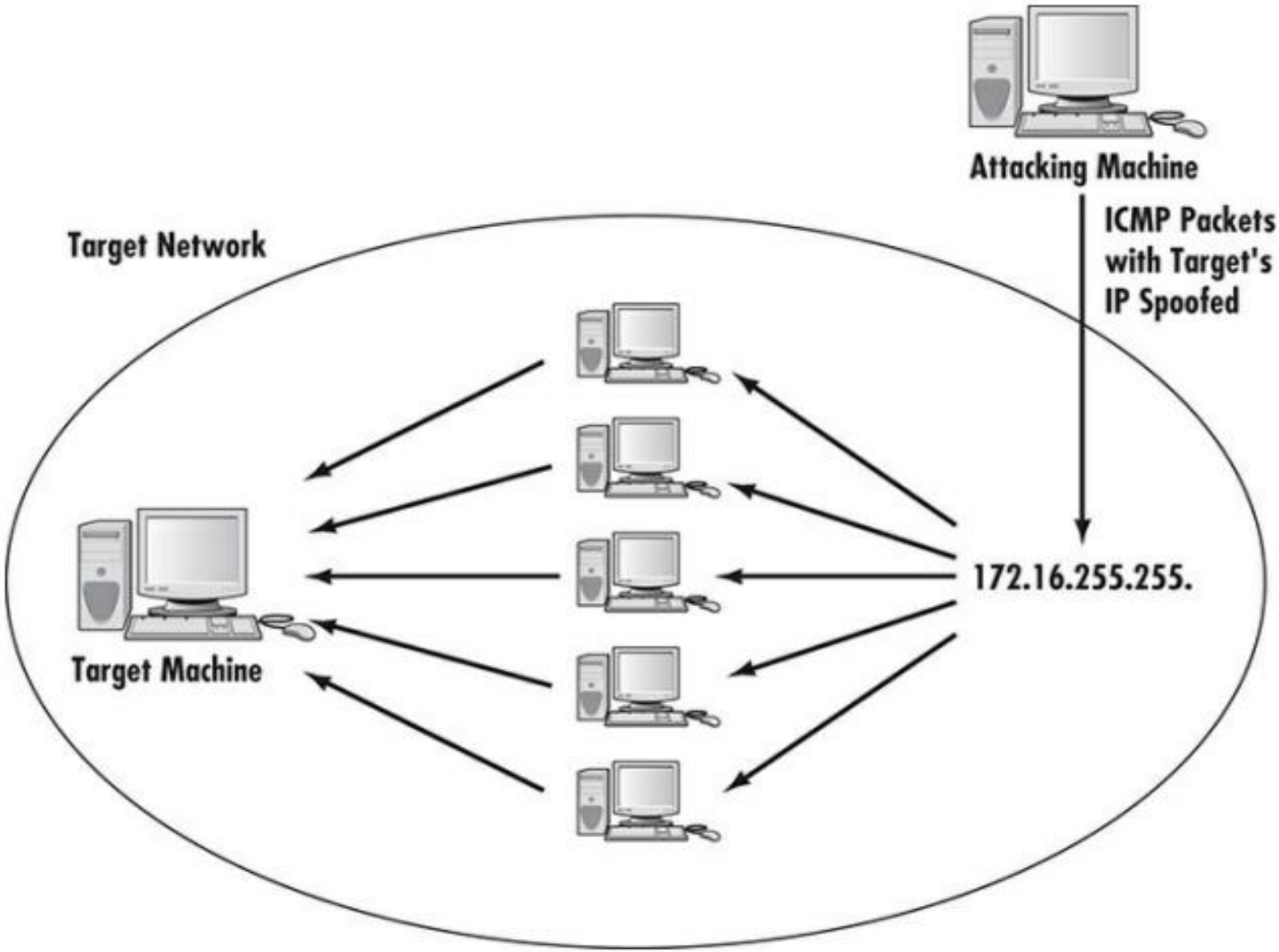


FIGURE 2-4 The Smurf attack

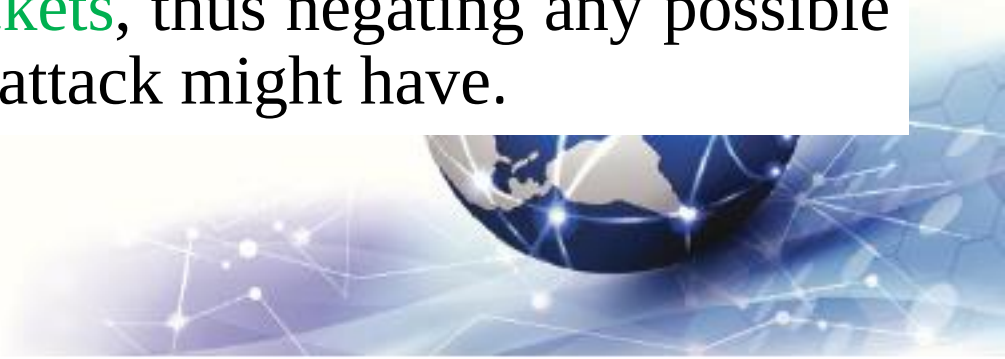
You can protect against the Smurf attack in two ways:

- **The most direct method** is to configure all of your **routers** so that they do not forward any directed broadcast packets.
  - These packets are the cornerstone of the Smurf attack, and if routers do not forward them, then the attack is contained within one **subnetwork**.
- **The second approach** is to guard against Trojan horses.
  - Because the Smurf attack is launched from software delivered via a Trojan horse, preventing that initial delivery will prevent the attack.
  - *Policies* that prohibit employees from downloading applications and guarding a system with adequate virus scanners can go a long way to protecting the system from a Trojan horse, and thus the Smurf attack.

➢ Using a **proxy server** is also imperative. Proxy servers can hide the internal IP addresses of your machine, which makes your system a lot less vulnerable to a Smurf attack.

Ping of Death

- The Ping of Death (PoD), perhaps the simplest and most primitive form of DoS attack, is based on overloading the target system.
- TCP packets are of limited size.
- In some cases simply sending a packet that is too large can shut down a target machine.
- This attack is becoming less common as newer versions of operating systems are better able to handle the overly large packets that Ping of Death depends on.
  - If the operating system is properly designed it will drop any oversized packets, thus negating any possible negative effects a PoD attack might have.



UDP Flood

- UDP is a connectionless protocol, and it does not require any connection setup procedure to transfer data.
- TCP packets connect and wait for the recipient to acknowledge receipt before sending the next packet. Each packet is confirmed.
- UDP packets simply send the packets without confirmation.
  - This allows packets to be sent much faster, making it easier to perform a DoS attack.
- A UDP flood attack occurs when an attacker sends a UDP packet to a random port on the victim system.
  - When the victim system receives a UDP packet, it will determine what application is waiting on the destination port.
  - When it realizes that no application is waiting on the port, it will generate an ICMP packet of destination unreachable to the forged source address. If enough UDP packets are delivered to ports on the victim, the system goes down.

ICMP Flood

- ICMP flood is a term you frequently encounter in security literature.
- In reality it is simply another name for the ping flood used in the experiment.
- ICMP packets are the type of packets used in the ping and tracert (this command is tracert in Windows and traceroute in Linux) utilities

DHCP Starvation

- **DHCP starvation** is another common attack.
  - If enough requests flood onto the network, the attacker can completely exhaust the address space allocated by the DHCP servers for an indefinite period of time.
- There are tools such as Gobbler that will do this for you.
- Preventing incoming DHCP requests from outside the network will prevent this.