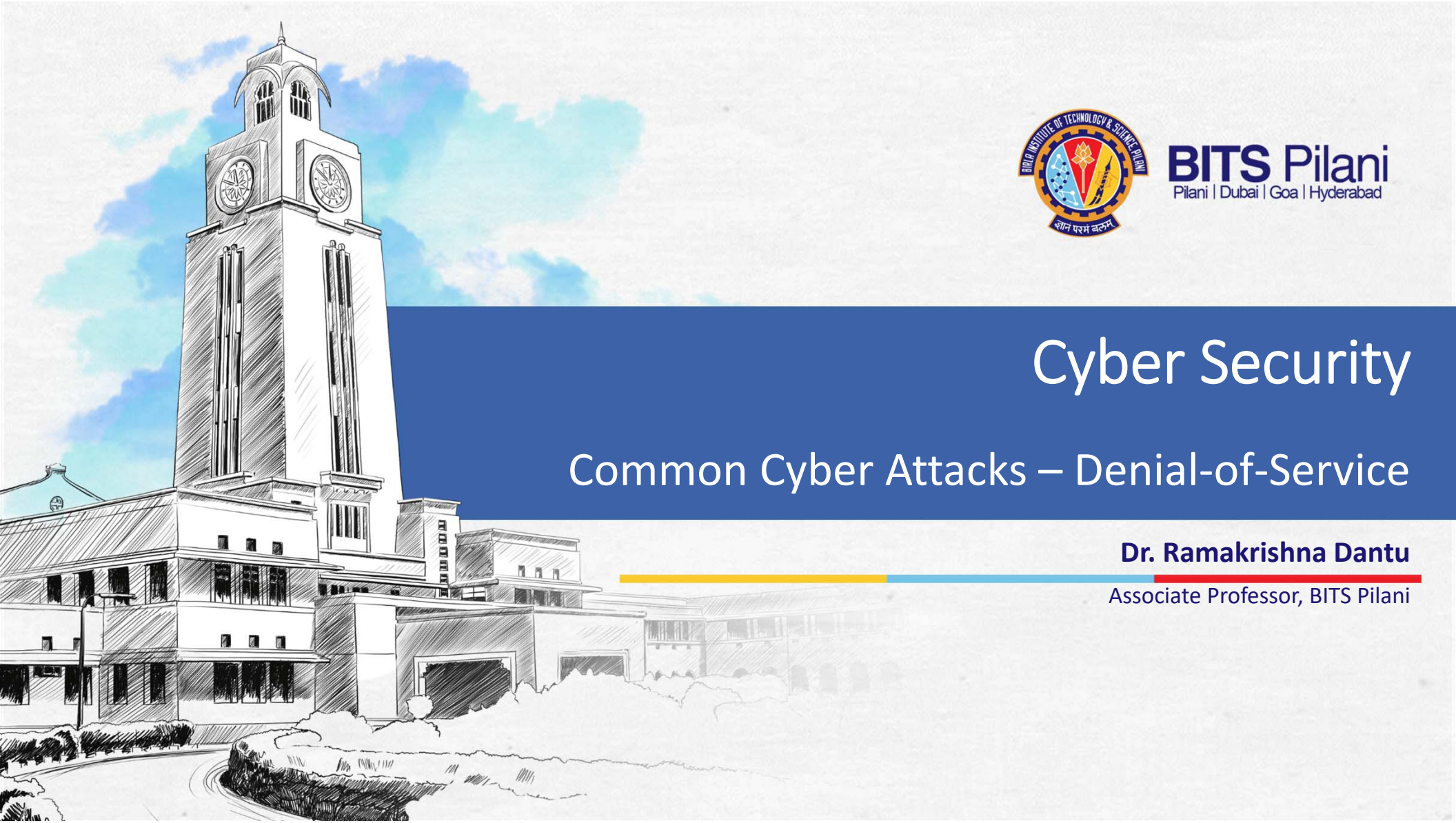


BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Common Cyber Attacks – Denial-of-Service

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Common Cyber Attacks

Agenda

- Common Cyber Attacks – Practical Strategies for Identification, Containment and Mitigation:
  - Malware Attacks
    - E.g., Ransomware Attacks
  - Denial of Service Attacks
  - Session Hijacking and Man-in-the-Middle Attacks
  - Phishing and Spear Phishing Attacks
  - SQL Injection Attacks
  - Zero Day Exploits
  - DNS Tunneling Attacks

Common Cyber Attacks

innovate achieve lead

Types of Attacks

- Software Attacks
  - Malware
    - Adware
    - Virus
      - Boot virus
      - Macro virus
      - Memory-resident virus
      - Non-memory-resident virus
    - Polymorphic Threats
    - Spyware
    - Trojan horses
    - Worms
    - Virus and Worm Hoaxes
    - Zero-day attack
  - Back Doors
    - Maintenance hook
    - Trap door
  - Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
  - Email Attacks
    - Mail Bomb
    - Spam
  - Communications Interception Attacks
    - Packet Sniffer
    - Spoofing
    - Pharming
    - Man-in-the-Middle
    - Domain Name System (DNS) cache poisoning or DNS spoofing
    - Session hijacking or TCP hijacking.

Source: Principles of Information Security by Whitman and Mattord

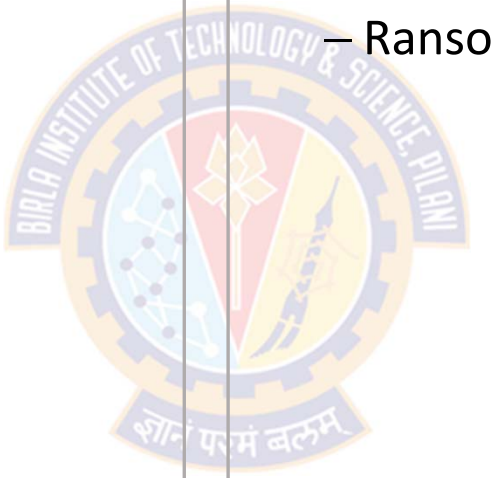
Common Cyber Attacks

innovate achieve lead

Types of Attacks

- Espionage or Trespass
  - Password Attacks
    - Brute Force
    - Dictionary Attacks
    - Rainbow Tables
    - Social Engineering
- Human Error or Failure
  - Social Engineering
    - Advance-fee fraud (AFF)
    - Phishing
    - Pretexting
    - Spear phishing

- Information Extortion
  - Ransomware



Source: Principles of Information Security by Whitman and Mattord

Denial-of-Service Attacks

Denial-of-Service Attacks

Overview

- DoS attack is an attempt to compromise the availability of a service
  - It does so by hindering or blocking completely the provision of some service
- The attack tries to exhaust some critical resource(s) associated with the service
  - E.g., flooding a Web server with a large number of spurious requests makes the server unable to respond to valid requests from the users in a timely manner
- Reasons for attacks include:
  - financial extortion, hacktivism, state-sponsored attacks
    - Hacktivism is the use of computer-based techniques such as hacking as a form of civil disobedience to promote a political agenda or social change
  - Some attacks on bank systems were a diversion from the real attack on their payment switches or ATM networks
  - In Dec 2010, a handful of websites that cut ties with WikiLeaks were temporarily taken down
    - This includes Visa and MasterCard websites

Denial-of-Service Attacks

The Nature of DoS Attacks

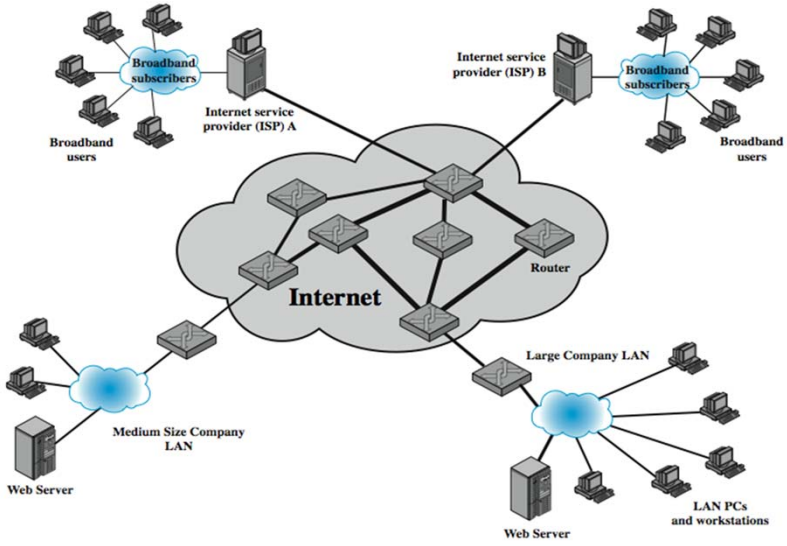
- NIST SP 800-61 defines DoS attack as:
  - "*an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as CPU, memory, bandwidth, and disk space*"
- This definition tells us that several categories of resources can be attacked:
  - A) Network bandwidth
  - B) System resources
  - C) Application resources

Denial-of-Service Attacks

innovate achieve lead

The Nature of DoS Attacks

- A) Attacking Network Bandwidth
  - It relates to the capacity of network links connecting a server to the Internet
    - Typically this is the connection to the Internet Service Provider (ISP)
  - Usually these connections will have a lower capacity than the links between ISP routers
  - For a list of DDoS attacks, refer to:
    - Arora, K. "Impact Analysis of Recent DDoS Attacks." *International Journal on Computer Science and Engineering*, Vol. 3, No. 2, February 2011



Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Denial-of-Service Attacks

The Nature of DoS Attacks

- B) Attacking System Resources
  - A DoS attack targeting system resources typically aims to overload or crash its network handling software
  - Rather than consuming bandwidth with large volumes of traffic, specific types of packets are sent that consume the limited resources available on the system
  - These include:
    - temporary buffers used to hold arriving packets,
    - tables of open connections, and
    - memory data structures
  - The SYN spoofing attack is of this type
    - It targets the table of TCP connections on the server

Denial-of-Service Attacks

The Nature of DoS Attacks

- B) Attacking System Resources – using poison packets
  - This form of attack uses packets that trigger a bug in the system's network handling software
    - Which causes it to crash
  - The system can no longer communicate over the network until this software is reloaded by rebooting the target system
  - This is known as a poison packet
  - The classic *ping of death* and *teardrop attacks*, directed at older Windows 9x systems, were of this form
    - These two attacks targeted bugs in Windows network code
      - ping of death targeted code that handled ICMP echo request packets
      - teardrop targeted code that handled ICMP packet fragmentation
  - Note:
    - ICMP (Internet Control Message Protocol)

Denial-of-Service Attacks

The Nature of DoS Attacks

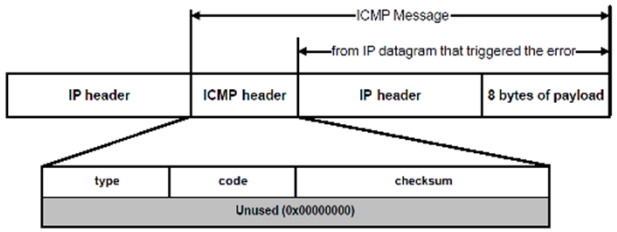
- C) Attacking Application Resources – Cyberslam
  - Attack on applications, such as a Web server, typically involves a number of valid requests, each of which consumes significant resources
  - This then limits the ability of the server to respond to requests from other users
  - For example, a Web server might include the ability to make database queries
  - If a large, costly query can be constructed, then an attacker could generate a large number of these that severely load the server
  - This limits its ability to respond to valid requests from other users
  - This type of attack is known as a *cyberslam*

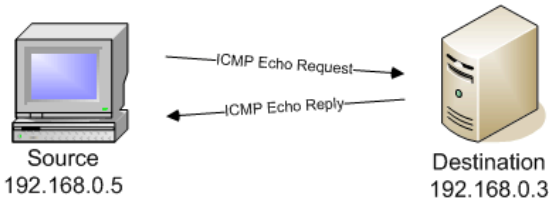
Denial-of-Service Attacks

innovate achieve lead

Classic DoS Attacks

- Internet Control Message Protocol (ICMP)
  - ICMP is a network layer protocol used to diagnose network communication issues
  - The ICMP protocol is commonly used on network devices, such as routers
  - It helps in determining whether or not data is reaching its intended destination in a timely manner
  - ICMP is crucial for error reporting and testing, but it can also be used in distributed denial-of-service (DDoS) attacks





The host must respond to all echo requests with an echo reply containing the exact data received in the request message

Source: https://www.cloudflare.com/learning/ddos/glossary/internet-control-message-protocol-icmp/

Denial-of-Service Attacks

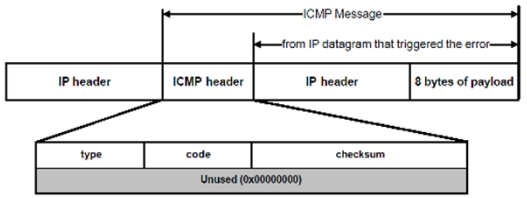
Classic DoS Attack

- Ping Flood Attack
  - The aim is to overwhelm the capacity of the network connection to the target organization
  - The attacker uses a single server with a higher-capacity network connection to generate a higher volume of traffic than the lower-capacity target connection can handle
  - For example:
    - The attacker might use the large company's Web server to target the medium-sized company with a lower-capacity network connection
  - The attack directs a flood of ping commands at the target company's Web server
  - The target router discards some packets, but the remaining ones consume most of the network capacity to the medium-sized company
  - Other valid traffic will have little chance of surviving discard as the router responds to the resulting congestion on this link

Denial-of-Service Attacks

Classic DoS Attack

- Ping Flood Attack Contd…
  - This attack includes source IP address in the ICMP echo request packets
  - From the attacker's perspective, this has two disadvantages
    - One:
      - The source of the attack is explicitly identified
      - Increases the chance of the attacker getting caught and legal action taken in response
    - Two
      - If any ICMP echo request packet received by the target, it would respond to each with an ICMP echo response packet directed back to the sender
        - ✓ This effectively reflects the attack back at the source system
      - Since the source system has a higher network bandwidth, it is more likely to survive this reflected attack
      - However, its network performance will be noticeably affected, again increasing the chances of the attack being detected and action taken in response
  - For both of these reasons the attacker must hide the identity of the source system
  - That is, any such attack packets need to use a falsified, or spoofed, address



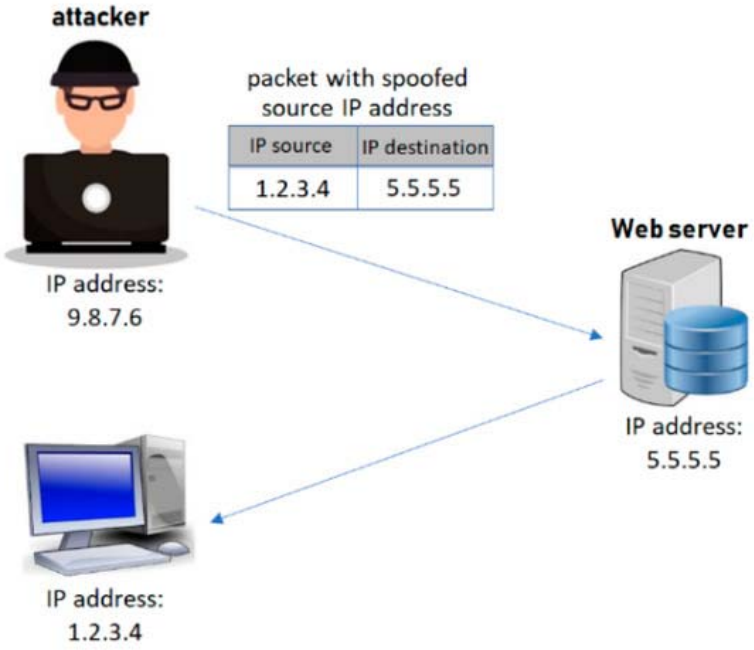
Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Denial-of-Service Attacks

innovate achieve lead

Source Address Spoofing

- DoS Attack Process



Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Denial-of-Service Attacks

innovate achieve lead

SYN Spoofing

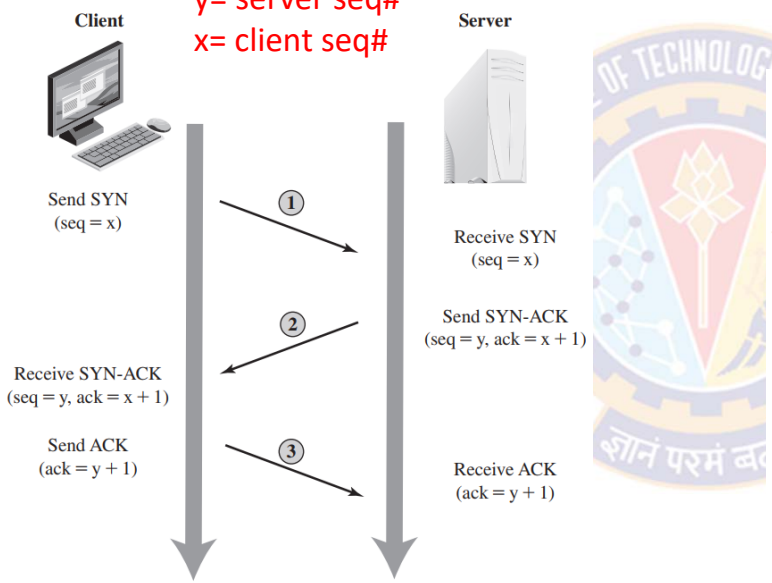
- Common DoS attack
- Attacks the ability of a network server to respond to TCP connection requests by overflowing the tables used to manage connections
- Future connection requests from legitimate users are denied access to the server
- Thus, it is an attack on system resources, specifically the network handling code in the operating system

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Denial-of-Service Attacks

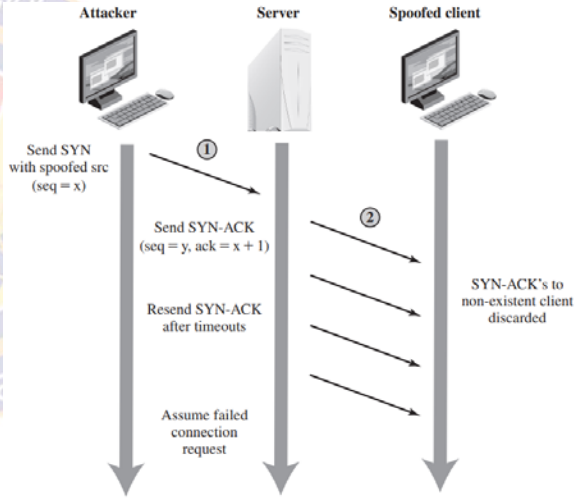
SYN Spoofing

syn/ack pkts
y= server seq#
x= client seq#



Normal TCP Connection Handshake

Assumption: most connections succeed and thus table cleared quickly



SYN Spoofing Attack

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Denial of Service Attacks

innovate achieve lead

Flooding Attacks

- Flooding attacks are classified based on the network protocol being used to implement the attack
- The objective is:
  - to overload the network capacity on some link to a server, or
  - to overload the server's ability to respond to this traffic
- The network link is flooded with malicious packets so that they compete with and overwhelm the valid traffic flowing to the server
- Due to the congestion caused by this traffic in some routers on the path to the targeted server, many packets will be dropped
- Legitimate traffic has a low probability of survival and hence of accessing the server
- Thus, the server's ability to respond to network connection requests degrades or fails completely

Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Denial of Service Attacks

Flooding Attacks

- What type of packet can be used?
  - Any type of network packet can be used in a flooding attack
  - The goal is for the packets to consume all available capacity on some link to the target server
  - The larger the packet, the more effective is the attack
  - Common flooding attacks use any of the ICMP, UDP, or TCP SYN packet types
    - The ping flood using ICMP echo request packets is a classic example of an ICMP flooding attack
    - UDP packets can be directed to some port number, and hence some potential service, on the target system
    - TCP connection request packets using real or spoofed source addresses are sent to the target system

Denial-of-Service Attacks

SYN Spoofing Attack Vs. Basic Flooding Attack

- There is a significant difference in the volume of network traffic between a SYN spoof attack and the basic flooding attack
- The actual volume of SYN traffic can be comparatively low, nowhere near the maximum capacity of the link to the server
- SYN traffic has to be high enough to keep the known TCP connections table filled
- Unlike the flooding attack, this means the attacker does not need access to a high-volume network connection
- The medium-sized organization, or even a broadband home user, could successfully attack the large company server using a SYN spoofing attack

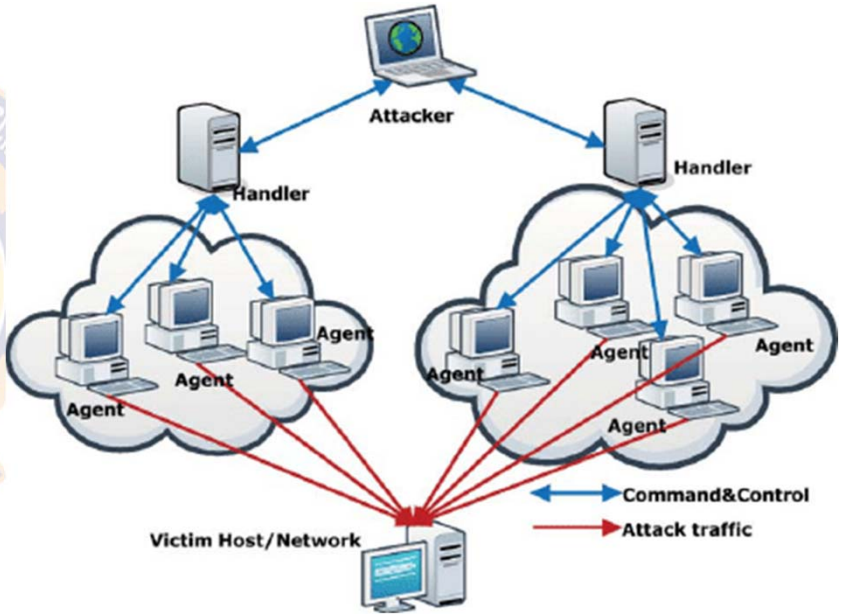
Source: Information Security Principles & Practice by William Stallings & Lawrie Brown

Denial-Of-Service Attacks

innovate achieve lead

DDoS

- DDoS attack involves the use of multiple systems to generate attacks
- These systems are typically compromised user workstations or PCs
- The attacker uses malware to install an attack agent which they can control
  - Such systems are known as zombies
- Large collection of such systems under the control of attacker forms a botnet
- In the Fig., some of the broadband user systems may be compromised and used as zombies to attack the target



Source: Information Security Principles & Practice by William Stallings & Lawrie Brown


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!