Name: Adwait Purao Batch: V
Uid: 2021300101 Div: BE COMPS B

Introduction and Types of Attacks

Introduction

Denial of Service (DoS) attacks aim to disrupt network services by exhausting resources like bandwidth, CPU cycles, or memory.
Distributed Denial of Service (DDoS) attacks are more sophisticated, involving multiple compromised machines (zombies) to overwhelm a target. These attacks have evolved from simple technical pranks to tools for extortion and sabotage, with modern variants exploiting vulnerabilities to execute large-scale disruptions.

Types of DoS/DDoS Attacks

Network-Based Attacks:

TCP SYN Flooding: Exploits half-open TCP connections, overwhelming the target's connection table.
ICMP Smurf Flooding: Sends forged ICMP requests to broadcast addresses, flooding the victim with replies.
UDP Flooding: Overwhelms a target by sending

a high volume of UDP packets, similar to flash crowds but malicious.
Host-Based Attacks:

Exploit vulnerabilities in specific applications or systems, such as causing excessive RSA decryption during SSL handshakes or triggering hash collisions in data structures.
Why DoS/DDoS Attacks Succeed
The Internet's design prioritizes functionality over security, making it vulnerable to resource misuse.
Attackers exploit decentralized management and insufficient inter-network cooperation, hindering effective defenses.

Taxonomy and Defense Mechanisms

Taxonomy of Attacks
Scanning: Techniques used to identify vulnerable systems:

Random Scanning: Probes random IPs for weaknesses.
Hitlist Scanning: Uses precompiled target lists for faster propagation.

Name: Adwait Purao Batch: V
Uid: 2021300101 Div: BE COMPS B

Signpost Scanning: Leverages infected systems' communication patterns.
Permutation Scanning: Utilizes shared pseudo-random IP permutations to avoid redundancy.
Spoofing: Fakes source IP addresses to evade detection:

Random Spoofing: Uses arbitrary IPs.
Subnet Spoofing: Masks addresses within the attacker's subnet.
Fixed Spoofing: Mimics the victim's IP.
Target Types:

Server Applications: Focused on disabling specific applications.
Network Access: Overloads communication channels.
Infrastructure: Targets critical components like DNS servers.
Impact:

Disruptive: Completely halts services.
Degrading: Slows services, impacting user experience.

Name: Adwait Purao Batch: V
Uid: 2021300101 Div: BE COMPS B

Defense Mechanisms
Commercial Tools: Firewalls, Intrusion Detection Systems (IDS), and security-enhanced routers monitor traffic, apply rate-limiting, and filter malicious packets.
Redundancy: Backup servers and distributed access points can mitigate single-point failures.
Ingress Filtering: Blocks spoofed packets by validating source IPs at network edges.

Advanced Defense Strategies and Wireless Networks

Advanced Defense Technologies :
Victim-Side Defenses:

Hop-Count Filtering: Identifies spoofed packets based on inconsistencies in TTL values.
Capability Filtering: Ensures only authorized senders can transmit large volumes of data to a destination.
In-Transit Network Defenses:

Name: Adwait Purao Batch: V
Uid: 2021300101 Div: BE COMPS B

Pushback Mechanism: Rate-limits suspicious traffic at upstream routers to prevent congestion.
IP Traceback: Identifies the attack source by marking packets with path details.
Distributed Puzzles: Requires clients to solve computational challenges before being granted network access.
Overlay Networks:

Secure overlay services like DefCOM or SOS reroute legitimate traffic through trusted nodes, isolating malicious activity.
DoS in Wireless Networks
Wireless networks face unique challenges due to shared communication channels and limited resources.

Physical Layer Attacks: Jamming and signal interference can disrupt communication.
MAC Layer Attacks: Exploiting vulnerabilities in packet transmission protocols to disrupt connections.
Network Layer Attacks: Manipulating routing

protocols in ad hoc or sensor networks to cause disconnections.

Conclusion

DoS and DDoS attacks exploit systemic flaws in the Internet and wireless networks, requiring diverse and layered defense strategies. Future solutions must focus on collaboration, secure protocol design, and proactive monitoring to mitigate evolving threats effectively.

.