Learning Objectives: difficulty in packet spoofing, various techniques to exploit systems, DNS attacks, metasploit

Sources of Exploits:

- **Standards**
  - Weak or outdated security standards
  - Inconsistent application across systems
- **Requirements**
  - Missing or unclear security requirements
  - Security not considered during planning
- **Architecture**
  - Poor system structure or network layout
  - Lack of isolation or segmentation
- **Design**
  - Insecure design choices
  - Failure to follow security best practices
- **Implementation**
  - Coding errors and bugs
  - Use of unsafe functions or libraries
- **Configuration**
  - Default or weak settings left unchanged
  - Improperly secured services or ports
- **Operations**
  - Lack of monitoring and maintenance
  - Delayed updates and patching
- **People**
  - Human error and social engineering
  - Lack of training or awareness
- **Mindset**
  - Treating security as optional or an afterthought
  - Focus only on functionality, not protection

Configuration Security
The number one source of access for a hacker
No easy way to view configurations for completeness and very few tools for computing correctness - misconfigurations are easy and common

Networks and network elements are named as an abstraction layer so that network designers/operators can more easily understand the network architecture and functionality. Hackers on gleaning the abstraction layer use it to further develop the network and its exposure.
Discovery techniques can be automated - originally they were done by hand
Good configuration is the first line of defense

General Attack Techniques:
IP Address spoofing: Attacker reconfigures IP address in Windows or UNIX, or enters a spoofed address in an application.
IP spoofing with TCP: attackers can make a TCP connection to a server with a spoofed IP address, but it is not easy. SYN-ACK and any subsequent packets will be sent to spoofed IP address. If the attacker can guess the initial sequence #, can attempt to send commands (send ACK with spoofed IP and correct seq # one second after SYN). TCP uses random initial sequence numbers.
Ways to stop:
Egress Filtering: Stopping and monitoring the flow of information outbound from on network to another - rarely done (stopping packets from leaving networks)
Ingress Filtering: used to ensure incoming packets are actually from the networks from which they claim to originate (stopping packets from coming into network)

Session Hijacking: take control of one side of a TCP connection, marriage of sniffing and spoofing. Attacker is on segment where traffic passes from A to B: attacker sniffs packets, sees TCP packets between A and B and their sequence numbers. Attacker jumps in, sending TCP packets to B; source IP = A's IP.
Principal defense: encryption w/auth protocol

Denial of Service:
Goal: Overwhelm a system, network, or service to make it unavailable to legitimate users.
Types: Includes basic DoS (single source), DDoS (distributed from many sources), and application-layer attacks.
Common Methods: Flooding with traffic (e.g., ICMP, SYN floods), exploiting vulnerabilities, or consuming resources.
Impacts: Service outages, financial loss, damaged reputation, and potential security breaches.
Mitigations: Rate limiting, firewalls, intrusion detection systems, and using cloud-based DDoS protection services.

Land DoS: sends spoofed packet with source and dest address/port the same
Ping of death: sends oversized ping packet
Jolt2: sends a stream of fragments, none of which
have offset of 0. Rebuilding consumes all processor
capacity

IP Fragmentation and Reassembly:
4000 byte datagram, 1500 byte MTU
1480 bytes in data field, offset = 1480/8

SYN Flood: Send Many SYN packets, filling connection queue with half-open connections, can spoof source IP address.
Defense:
Syn Cookies: When SYN segment arrives, host B calculates function
(hash) based on:
•Apache example: Source and destination IP addresses and port
numbers, and a secret number
Host B uses resulting “cookie” for its initial seq # (ISN)
in SYNACK