ICMP Attack
sending a bunch of ICMP data
Smurf attack
type 8 (req) is sent, wait for type 0 (rep)
SRC IP spoofing
defense → no dir-bcast, IP filters
Fraggle attack
the same as smurf, but UDP is used
ICMP port scan
using the unreachable to check the IP presence
OS Fingerprint
checking the reply to see OS-specific data (TTL)
Ping of death
using improper values - size bigger than 65.535B

Man In The Middle (MITM)
attacker relays the communication of the victim
between the SRC and DST, hidden intercept
defense → SSL/TLS, certificates, VPNs ...

Replay attack
sensitive information are delayed/repeated
similar to MITM
defense → using timestamps and accurate time

Spoofing
easy concept - setting the invalid SRC IP
part of DoS/DDOS/TCP Syn
defense → RFC 1918/2827

Backdoor
process to bypass the authentication
worms/apps can create the backdoor to let the attacker access the victim's device
defense → IDS, relies on discovering them

DoS/DDoS
Distributed Denial of Service
goal is to make the service unavailable
due to overloading the circuit
due to overloading the CPU/Memory
DoS - from one device, DDoS - from many
botnet - Robot Network, the group of attackers

Virus/Worms
malware - malicious software
replication of itself by executing app
infecting other files/systems
resident - sits in the RAM, non-resident - in HDD
boot-sector viruses
Worms are apps, self-replicating
causing the damage of the net -e.g. eating BW
deleting files, sending emails ...
defense → Antivirus, Firewalls, up-to-date DB

Day Zero attack
the vulnerability is exploited right before the SW is released
zero-day virus → not known virus
using sandbox for new apps/SW

Host Header Attack
getting/sending email from/to another domain
cache poisoning
HTTP header injection - X-site scripting
trusted patterns, dangerous patterns
link-poisoning, social engineering

Wireless Attacks
Rogue AP
listening to the communication
breaking the WEP - intercepting
MAC spoofing
Evil Twin - rogue AP pretends being legitimate
Wireless IPS

SW/OS Exploit
exploit - uses a vulnerab to take an advantage
hacking - breaking the security, using exploits
white hat- testing, ethical hacker, non-profit
black hat - personal/business gain
gray hat - between black/white

Attacks tools
vulnerability scanner
brute-force attack
password cracking - dictionary attack
packet analyzer - analyzing the flows
phishing (spoofing) - hiding the real ID
rootkit
social engineering
worms/viruses/trojans

Intrusion Detection/Prevention
IDS → identifying the attack, no mitigation
IPS → identifying and mitigating the attack
NIPS - Network IPS, whole subnet, many hosts
network sensor
HIPS - Host IPS, one end-host (logs, processes ..)
end-host agent
signature - attack definition
pattern-based
traffic-based
baseline breaking traffic
signature engine - parser and inspector
examines indiv signatures
True Positive - alarmed attack traffic
True Negative - allowed non-attack traffic
False positive - alarmed non-attack traffic
False Negative - allowed attack traffic

Packet Filter
engine that analyzes the input/output traffic
possibility of filtering (blocking)
IP-based - SRC,DST, subnet, protocol ...
L4-based - TCP/UDP, SRC/DST

Content Filter
mostly HTTP header
Java, ActiveX applet examin
URL filtering
Packet Inspection
SPI - Stateful inspection
maintains legitimate traffic records
creates the legit record for outgoing traffic
Firewall feature
legit traffic leaves the point of inspection
→ record is created in the state table
return traffic is then checked in the Stable

Network Admission Control (NAC)
examines the end hosts before it enters net
guest network (quarantine)
Posture assessment - auth process
user assessment
device assessment
802.1x, MS AD, Cisco NAC appliance
BYOD concept, agent-less assessment
SW-based agent
Cisco NAC Agent - Win-based agent
can check SW version, updates, antivir ...
Cisco ISE

QoS Marking Attacks
possible higher costs due to using better QoS
change the QoS marking
Config Attack
change of the CE config
long-term attack
Data Fwd Attack
generating traffic with high QoS
injecting the traffic just to fill the class