Networks and Network-based Attacks

Internet – MAC,IP,Ports, TCP UDP  
Network Vulnerabilities  
Spoofing Attacks – Session Hijacking and Man in the middle  
Denial of Service

Application Layer – FTP,HTTP,SMTP  
4 Layer – Segments,TCP,UDP  
Internet Layer – Packets (IP addresses)  
Transport – Transport within network, encapsulation, MAC  
Physical Layer -Light, pulses of electricity

TCP/IP  
-IP  
-Port  
MAC(Media Access Control)  
-Unique 48 bit host  
-Always in Hexadecimal  
-Mapped to corresponding IP address by ARP (address resolution protocol)

MAC addresses are “flat”  
-hard-wired into devices

IP addresses are hierarchical  
-Indicates network, host within network,

UDP User datagram protocol  
Best effort service  
No flow control  
No acknowledgement/retransmission  
Unreliable but fast

TCP transmission control protocol  
Acknowledgement (ACK) packets  
If no ACK received, retransmission occurs  
Flow Control  
Reliable but slower than UDP  
Session are negotiated between end-points (starts with a handshake)   
(SYN->SYN-ACK->ACK->connection opens->FIN->ACK-FIN->ACK)  
Flags:   
URG – urgent pointer field  
ACK – acknowledgement field  
PSH – push function  
RST – reset connection  
SYN – synchronize sequence numbers  
FIN – no more data from sender

Browser SYN=1,ACK=0,Source=52138,Dest=80 -> Webserver  
Random Port <-SYN=1,ACK=1,Source=80,Dest=52138 Port 80  
 SYN=0,ACK=1,Source=52138,Dest=80 ->

Network Vulnerabilities

Interception – Packet interception – (Confidentiality)  
Modification Spoofing – Packet interception & modification – (Integrity)  
Masquerade Spoofing – Spoofing original packets – (Integrity and Authentication)  
Interruption – Denial of Service – (Availability)

Anonymity – Identity hidden, attacker can be geographically distant  
Many points of attack (target and origin) – any device to any device  
Sharing – more users having access to more systems increases security risks (clouds)  
System Complexity – difficult to look behind scenes  
Unknown Path – data can take many routes, difficult to predict routes  
Protocol flaws -attacks not anticipated by designers

Protocol Flaws -  
New protocols are publicly posted for review (RFCs)

Preparing an Attack  
Investigates and plans before attacking  
Goal: find out as much as possible  
Social Engineering/Reconnaissance  
Port Scanning: find out what services are provided  
Operating System and Application Fingerprinting  
Bulletin Boards and Chats  
Availability of Documentation

Done by ethical hackers as well as attackers  
Probe for network security weak points  
Most popular: port scanning  
Highlight security problems of machine/network  
Attackers have access to these tools as well  
Many tools, some run on dedicated machines, others run over web

Port Scanning:  
Reconnaissance technique  
Can find out what is running on system by scanning ports  
H scans port 25   
H sends a SYN to B port 25  
RST received  
=B port 25 is closed  
Firewall between H and B  
Firewall configured to block anything from H

Spoofing attacks  
Session Hijacking  
-Intercept and carry on TCP session  
-E.g. Telnet  
Man-in-the-middle  
-Interception and manipulation of source address to reroute response to the attacker

Denial of Service Attack  
Attack on availability   
Does not (usually) do permanent damage -normality is restored when attack stops  
Connection Flooding  
-Attacker sends packets faster than targe system can process them  
-Leads to congestion  
Ping of Death   
-malformed ping packet can be used to make target system crash  
Smurf  
-attacker sends IMCP message all hosts on a subnet using a broadcast address, with victims spooed IP address as source  
Syn Flood (SYN cookies)  
-Attacker sends many syn packets to victim to create half open connections, depleting resources  
Distributed DoS attack makes use of malware agents across a botnet.

Ping of Death  
-Ping usually 84bytes long  
-Can be up to 65535 bytes long  
-Attacker sends a ping packet >65535 bytes  
-Overflows memory buffer available  
-Overwrites important data and causes system crash

DDoS  
-Attacker deploys agent software units to remote machines  
-Usually done by Trojans  
-Attacker sends a trigger signal to botnet  
-Botnet sends attack packets to target system(s)  
DDoS traffic not noticed by owners of individual infected systems  
Aggregate DDoS traffic is noticeable