protocols & devices

application - layer 7

ftp, tftp, bootp, snmp, rlogin, smtp, mime, finger, telnet, ncp, ssh, afp, smb, http, api

\* Gateways and Proxy Servers doing conversions

presentation - layer 6

ASCII, TIFF, GIF, JPEG, MPEG, MIDI - Universal format

session - layer 5

netbios, nfs, sql, rpc

transport - layer 4

tcp, udp, ssl, tls (port #s create sockets)

network - layer 3 (routers)

ipv4, ipv6, icmp, rip, igmp, ospf, bgp

data link - layer 2

slip, ppp, arp, rarp, l2f, l2tp, pptp

ethernet, token ring, x.25, frame relay, atm

\* Bridges, switches - two sublayers llc & nac

physical - layer 1

high-speed serial interface (hssi), x.21, eia/tia-232, eia/tia-449, sonet

\* amplifiers, repeaters, hubs, media - Patch Panels

most weak on layer 1-2

3-5 good

6, 7 harder to secure

tools

port scanners

packet sniffers

network scanners

ids - (packet sniffer with rules applied to it)

ips

Port Scanners

Used to identify what ports are listening on os to accept service connections

identify potential weaknesses in networks, identifies what's open & available

Scanning tools Perform portscans first to start vulnerability ID process

Tools:

Nmap

Strobe

Packet & Network sniffers

operate at layers 2-3 of OSI model

examine traffic in real-time

capture & log packets across a network

follow pcap format

Tools:

TCPDump - best

Tehthereal

Tcpslice

tcpreplay

ngrep

wireshark - best

netdude

network scanners

argus, wireshark, nessus, retina, appscan, sara, saint (SCAP based outputs)

firewall

access control component which allows/denies traffic between two networks

filters based on ip addr & domain, packet header or content, services, ports, protocols

- domain & access to outside

- admin domains of dissimilar policy

- networks where boundary must be controlled

Combination of software & hardware

different levels

Commonly placed at network perimeter (restricts access from one network to another)

Host-based firewalls shield systems from others on LAN using separate software or OS firewall

Access control mechanism & filters traffic

Filters mac addresses

ACL - Access Control Lists

Filter or forward based on source & destination IP addr & port #s in packet headers

Static Packet Filter Firewall

Simple & fast method to stop unwanted or incoming traffic

examines header for ip addr, ports, protocol type to compare its ACL

minimum security for low-risk environments

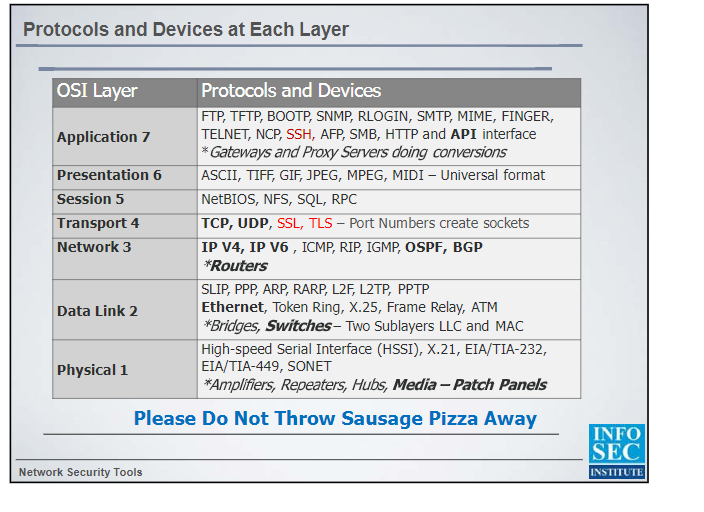
screening routers with rules for accepting or rejecting data based on ACL

Cannot keep session state information

All outgoing traffic is allowed

Dynamic Stateful Firewall

Keeps track of state or dialog process of a communication stream between internal & external hosts



When examining network device or appliances:

Retrieve the logs

Secure workstation, server or device

Use alternate method of access (direct console, remote terminal, Web interface). If possible, image copy or store

Research the device