NETWORK SECURITY (SANS 401.1)

NETWORK ARCHITECTURES

- CONCEPTUAL DESIGN
  - High level design includes the core components of a network architecture
  - Understand overall purpose of the network
- LOGICAL DESIGN
  - Represents each logical function in the system
  - Includes all the major components in the network + their relationship % data flow +services, application names and relevant developmental info but not include server names or addresses
- PHYSICAL DESIGN
  - Last design created before final implementation
  - Knowledge of all details such as OSs, patches and version
- COMMUNICATION FLOW
  - Shows how data can flow in and out of the network
  - Begins with logical architectures " should be diagrammed"
  - Forms foundation for threat mapping
- Valuable data
  - Where it's stored

Threat enumeration

- The process of tracking & understanding critical threats to ur system
- Threat agents
  - Cyber criminals and organized crime
    - heavily sponsored. want to profit from cyber crimes
  - Cyber espionage
    - - very well-funded - hide the intrusion and any compromise
  - Hacktivist
    - Advertise the compromise rather than hide it

Attacks against routers

- Denail of serves
  - Flooding the router with requests(sending large amount of ICMP packets , making router unable to provide services
- Destributed denial of service
  - Uses conscripts army of computers 'ZOMBIE' that are affected by malware designed to send packets to a router all at the same time .
- Packet sniffing
  - Capturing data using malicious program that monitors the network traffic
    - 'Unauthorized access doesn't require direct access the physical network'
- Packet misrouting
  - Router is injected with malicious code that causes him to mistreat packets
    - 'Very difficult attack to find and fix '
- SYN flood 'form of DoS'
  - TCP synchronization packet is used for milicious reasons .Attacker 'll send large number of TCP/SYN packets to targeted server , resulting in unabling server to establish a connection
- TCP reset attack
  - attacker terminates a TCP connection with spoofed packet using a RST bit
    - attacker 'll sniff TCP connection to get SRC IP, SRC PORT, DEST IP. DEST PORT number and ongoing sequence number
- Routing table poisoning
  - Routing table is how routers moves the packets in the network
    - is done by creating unwanted edits to the routing INFOs which broadcasted by routers. Causing severe damage in the network
- Malicious Insider/DISGRUNTLES EMPLOYEE
  - Employee with knowledge can access routers without authorization

NETWORK SECURITY (SANS 401.1)

Attacks against switches

- CDP manipulation
  - CDP packets are enabled by defaults on CISCO switches & transmitted in cleat text.
    With knowing network devices,Attackers can exploit known vulnerabilities
- Mac flooding
  - flooding the content addressable memory table with MAC addresses , overwhelmes switch storage capacity .Forcing switch to act as a hub
- DHCP spoofing
  'Another form of "MAN-IN-THE-MIDDLE'
  - attacker listens for DHCP requests then answer them with his IP address as default gateway
- STP attacks
  - spanning tree protocol allows switch to function by altering the ports so that it can block or forward various condition
    - directly target the spanning tree protocol.
      One type involves sending of RAW configuration bridge protocol data unit (BPDU) packets
- VLAN hopping attack
  - attacker can create&send positioned frames from one VLAN, using spoofed 802.1Q tags in a way the packet ends up on a completely different VLAN without passing through the router
- TELNET attack
  ' misnamed!! '
  - distributed SYN attack

Network topologies

- Physical topology
  - how the network is actually connected
    - how the data actually flow
    -wired or wireless
    -STAR topology is most commom
- Logical topology
  - -How u communicate across wires

Network design

- network segmentation
  - the act of splitting a network from the rest of the network by device (hub, bridge, switch or router) .Each subnet is a network segment
    - firewalls and VLANs provide a way to partition the network into smaller zone
  - implement controls at multiple layers
    the more layers of segments u can add the harder it 'll be for attacker to get in
  - least privilege rule : access should only be provided to the user that is needed and nothing else
  - Protected Enclave :segment of the internal network defined by a common set of security policies
  - Software Defined Network is broad term covering several kind of network technologies with intent of making network as felxible and agile as VM
- Objective
  - - Provide appropriate access from the internal network to the internet
    -Protect the internal network from external attacks
    -Provide defense-in-depth through a tiered architecture
    -Control the flow of INFOs between systems
- Sections
  - public :internet
    Semi-public : DMZ, web, mail, DNS
    -Middleware: separate DMZ from private network
    -Private : INTERNAL SYSTEMS
    - **Firewalls location :**
      between the internet and other networks
      Between the semi-public and private network
      Between sections of varying trust levels
- Goals
  - -any system visible from the internet must reside on the DMZ and can't contain sensitive INFOs
    -Any system with sensitive INFOs must reside on the private network & not be visible from the internet
    -The only way a DMZ system can communicate with a private network system is throught a prozy on middleware tier
    - to know where to place firewall consider the basic paths
      -From private to systems to the internet .
      -From private systems to semi-public servers.
      -From semi-public servers to the internet .
      -From the internet to semi-public servers

Network protocols

- is an agreement or rules of engagement for how computer networks 'll communicate
  - protocol stacks are set of network protocol layers that work together to implement communicatoin
- purpose:
  -standardize the format of a communication .
  -specify the order or timing of communication .
  to allow all parties to determine the meaning of a communication.
- OSI protocol stack
  - LAYER 7 :APPLICATION
  - LAYER 6 :PRESENTATION
  - LAYER 5 : SESSION
  - LAYER 4 :TRANSPORT
  - LAYER 3 :NETWORK
  - LAYER 2 :DATA LINK
  - LAYER 1 :PHYSICAL

NETWORK SECURITY (SANS 401.1)

Network protocol

OSI protocol stack

LAYER 7 : APPLICATION

INTERACTS WITH THE APPLICATION TO DETERMINE WHICH NETWORK SERVICES ARE REQUIRED

LAYER 6 : PRESENTATION

ENSURING THE DATA SENT FROM ONE SIDE OF CONNECTION IS RECEIVED IN A USEFUL FORMAT TO THE OTHER SIDE

LAYER 5 : SESSION

HANDLES THE ESTABLISHMENT AND MAINTENANCE OF CONNECTIONS BETWEEN SYSTEMS . NEGOTIATES THE CONNECTION,SETS IT UP, MAINTAINS IT AND MAKES SURE INFOs IS SYNC ON BOTH SIDES

LAYER 4 : TRANSPORT

INTERACTS WITH UR DATA AND PREPARES IT TI BE RANSMITTED ACROSS NETWORK , ENSURING RELIABLE CONNECTIVITY

LAYER 3: NETWORK

HANDLES THE NETWORK ADDRESS SCHEME AND CONNECTIVITY OF MULTIPLE NETWORK SEGMENTS - DESCRIBING HOW SYSTEMS ON DIFFERENT NETWORK SEGMENTS FIND EACH OTHER

data from one layer of the stack can be understood only by the corresponding layer on the remote computer
as u go down the stack, each layer adds a header ... as u go up the stack, each layer removes a header

LAYER 2: DATA LINK

CONNECTS THE PHYSICAL PART OF THE NETWORK(CABLES) WITH ABSTRACT PART (PACKETS AND DATA STREAM)

LAYER 1: PHYSICAL

HANDLES TRANSMISSION ACROSS THE PHYSICAL MEDIA (ELECTRICAL PULSES ON WIRES, RADIO WAVES, LIGHT PULSES ON FIBER

TCP/IP PROTOCOL

TCP/IP STACK
-APPLICATOIN (comprises application, presentation and session layer)

-TRANSPORT (TCP)
-internet (IP)

-NETWORK(comprises physical and data link layer)

INTERNET PROTOCOL (IP)

Works at internet layer of TCP/IP stack (layer3 of the OSI model)
-Deals with transmission of packets between endpoints
-Defines the addressing scheme for internet

IP versions

IPV4

-IPV4 ACCOMMODATES 4.2 BILLION UNIQUE ADDRESS WITH 32-BIT ADDRESSS
-No authentication
-Encryption provided by applications
-Best effort transport

HEADER KEY FIELDS

IP version,4BITS(6BITS FOR IPV6) : determines the version of the IP protocol **- Protocol,8BITS :** identifies the encapsulated protocol
-Time-to-liVE(TTL),8BITS : number of hops a packet is allowed to take before it reaches its destination
- fragmentation, 16BITS : used to fragment the packet or break it up onto smaller individual packets
-source address and destination address, 32Bits each : source and destination systems

IPV6

-IPV6 is 128 Bits accommodate 340 undecilion addresses
-Provides authentication of endpoints
-Support for encryption in protocol
- quality of service features provided in the protocol

HEADER KEY FIELDS

version ,4bits : indicates the packet is IPV6 and is always a 6
- TRAFFIC CLASS 1byte/8bits: used to specify the priority of the packet in a quantity of bytes
FLOW LABEL 20BITS: used for QOS management to convey special handling function
PAYLOAD LENGTH 2BYTES/8BITS: specifies the length of the packet in a quantity of bytes

-Next header 1byte/8bits : specifies the next encapsulated protocol in the payload of the packet
-Hop limit 1byte/8bits : used to prevent routing loops by determining the hop limit value at each router (similar to TTL field)
- source address 16 bytes/182bits : source address of the IPV6 station transmitting the packet
-DESTINATION ADDRESS 16bytes/128bits: represents the destination of IPV6 packet

FEATURES

-Extended address space
-Auto configuration support
-Support for IPV6 over IPV4(tunneling)
-Support for IPv4 over IPv6(translation)
-Flexible embedded protocol support
-Support for authentication of endpoints
-Support for encryption

IP label options
-rarely used by legitimate traffic-

-Record router
-IP Timestamp
-Strict source routing
-loose source routing
-If option are used, the header 'll be longer than 20 bytes

ICMP PROTOCOL (INTERNET CONTROL MASSAGE PROTOCOL)

- Report errors or troubleshooting
-Provide network information (the host alive or not)
(ICMPv6 is implemented for IPv6 network)

HEADER:
ICMP type ,8bits: an integer which identifies which type of ICMP packet is being sent
-ICMP code :acts as a sort of subtype -GOOGLE it man !-
-ICMP checksum: computed as 16-bit one's complement of the header and data portion
-ICMP payload

COMMON TYPES AND CODES

TYPE 0: ECHO reply
-TYPE3: DETINATION UNREACHABLE :
Code0:Network unreachable
Code1:Host unreachable
Code3:Port unreachable
Code9:Destination network administratively prohibited
TYPE5: Redirect
TYPE8:ECHO request
TYPE11:Time exceeded
Code0:TTL expires in transit
Code1:TTL expires during reassembly