Network devices, Firewall, IDS, IPS , NCSS 2020 (Module - 4 : DISSA Course) **Part 4**

Arijit Chakraborty

Feb 27 , 2022

Types of Network Topologies

- *#1)* ***BUS Topology:***
- Every network device connected to single cable & transmits data **only in 1 direction.**
- **Advantages:**
- Cost-effective
- Can be used in small networks.
- Very less cable is required when compared to other topologies.
- **Disadvantages:**
- If cable gets faulty then the whole network will fail.
- Slow in operation.
- Cable has limited length.

- ***RING Topology:***
- Each computer connected to another computer in the form of a ring with last computer connected to first one.
- Each device - 2 neighbors. data flow is unidirectional & bidirectional
- **Advantages:**
- Easy to install and expand.
- Can be easily used for transmitting huge traffic data
- **Disadvantages:**
- Failure of one node will affect the whole network.
- Troubleshooting is difficult in a ring topology.

- ***STAR Topology:***
- All nodes are connected to a single network device through a cable.
- **Advantages:**
- If one node fails, then it **will not affect the whole network** and the network will run smoothly.
- Troubleshooting of fault is easy.
- Simple to operate.
- **Disadvantages:**
- High cost.
- If central node gets faulty = whole network will get interrupted

- ***MESH Topology:***
- Every node **connected to another one with a point to point topology** & **every node connected to each other.**
- **Advantages**:
- It is robust.
- Fault can easily be detected.
- Very secure
- **Disadvantages**:
- Very costly for Installation & configuration

TCP IP

- IP = how **to address & route each packet to make sure it reaches right destination**.
- Each gateway computer on network checks this IP address to determine where to forward the message.
- **Uses of TCP/IP**
- used to provide remote login over network, for:

✓ interactive file transfer,

✓ to deliver email,

✓ to deliver webpages over the network

Common TCP/IP protocols

- **HTTP (Hypertext Transfer Protocol)**, = communication between web server and web browser;
- **HTTPS (HTTP Secure)**, = secure communication between a web server and a web browser;
- **FTP (File Transfer Protocol)**, = transmission of files between computers.

Types of Transmission Media

- ***1. Coaxial Cable:***

= 2 conductors which are parallel to each other. Copper used as a central conductor & surrounded by PVC installation with outer metallic wrapping.

- **Cable TV network** providers also widely use **Coaxial cable in entire TV network.**
- ***2.Twisted Pair Cable***
- **Most popular** wired transmission medium. Cheap & easier to install than coaxial cables.
- 2 conductors (copper), each having their **own plastic insulation & twisted with each other**. One is grounded & other **used to carry signals** from sender to receiver.
- used in LAN & telephone landline connections **-** has high-bandwidth capacity

3. *Fiber Optic Cable:*

- made up of a **core surrounded by a transparent cladding material**
- It uses **properties of light for signals** to travel between them.
- used in WAN
- Optic fiber = flexible & transparent fiber - consists of **silica glass** or plastic.
- Optic fibers transmit signals in form of light between 2 ends of fiber = **they permit transmission over longer distances & higher bandwidth** than coaxial & twisted pair cables or electrical cables.

Network layout & domains

- **A. Trusted Zone –**
- secure zone with restricted access.
- **Consists of –**
- storage,
- database &
- management servers = not directly accessible to outside zone.
- Trusted zone **separated using strong access** control & firewall, - additional level of security to infrastructure.

- B. De-militarized Zone – (DMZ)
- "neutral zone" between internal network & outside extranet network.
- Small network = lies between trusted internal network (LAN) & un-trusted external network (Internet).
- DMZ is isolated using security gateway (i.e., firewall) to filter traffic between DMZ & private network.
- DMZ itself has security gateway in front to filter incoming traffic
- DMZ contains devices accessible to Internet traffic, such as Web, FTP, SMTP & DNS servers
- Goal of DMZ = allow access to resources from untrusted networks while keeping private network secured
- DMZ server = resides in DMZ & used to externalize resources to public network

IDS and IPS

- Intrusion detection is the process of monitoring the events occurring in network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies.
- Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents.
- These security measures are available as intrusion detection systems (IDS) and intrusion prevention systems (IPS), which become part of network to detect and stop potential incidents.

CYBER FORENSIC

- **Digital Forensic**
- *"Process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law)."*
- **Digital Evidence** =
- any information, data of probative value stored in binary form, transmitted , received by an electronic devices.

Bharat Pe case -The Issues..

- ✓ Payments allegedly made to “dubious” recruitment firms,
- ✓ Expenses running into crores of rupees spent on “non-existing” vendors
- ✓ “questionable invoices” created to substantiate such spends —
- ✓ Alvarez & Marshal findings into fintech firm BharatPe’s corporate governance practices.
- A&M’s probe claims it found that over Rs 50 crore was paid to 30 vendors who appeared to be “non-existent”
- Co-founder Ashneer Grover’s wife and the firm’s controller till recently, Madhuri Grover, is linked to both fraudulent schemes
- One is the irregularities in recruitment and second revolves around paying non-existent vendors
- Forensic report , dated 24 January 2022 was submitted to BharatPe board.
- BoD had arrived at a decision to terminate the services of Grover based on the preliminary report, even as it has commissioned a comprehensive report.

National Cyber Security Strategy 2020- Data Security Council of India

- **India is second-fastest digital adapter among 17 of most-digital economies globally, rapid digitisation require forward-looking measures to boost cybersecurity.**
- **National Cyber Security Strategy 2020 is being formulated by the Office of National Cyber Security Coordinator at the National Security Council Secretariat.**
- **Cyber Security is *protecting cyber space including critical information infrastructure from attack, damage, misuse and economic espionage.***
- **The National Security Council (NSC) of India is a 3-tiered organization that oversees political, economic, energy & security issues of strategic concern.**