Network Security | Ivan Notes 2022

- **Networking**
  - WAN
    - X.25
      - OG protocol
    - Frame relay
      - replaced x.25
    - ATM
      - replaced Frame relay
    - MPLS
      - replaced ATM, current
  - Wireless
    - WiFi
      - Protocols
        - 802.11a, b, g, n, ac, ax
      - Enceryption
        - WEP
          - OG
        - TKIP
          - temporary until WPA2
        - WPA / WPA2
    - WiMAX
      - 802.16
      - for metropolitan areas
    - GSM / CDMA
      - voice and data services, being replaced by 4G, 5G
    - Microwave

- IP Addressess
  - IPv4, IPv6
  - IPv4 classes
    - A, B, C
  - IPv4 Private
    - RFC1918
- Converged Protocols
  - VoIP
  - iSCSI & FCoE
- Network Authentication
  - PAP
    - OG
  - CHAP
  - EAP
    - widely used
  - PEAP
    - wrapper for EAP
- Network Attacks
  - phases
    - recon
      - passive
    - enum
      - active
    - vuln analysis
    - exploitation
  - Eavesdropping
  - SYN flood
  - IP spoofing
  - DoS/ DDoS
  - MiTM

- ARP poison
- Virtualization
  - VLAN
    - logically segment networks
  - SDN
    - create virtualized software defined network on top of physical network - mainly used in cloud
- Common Commands
  - ipconfig / ifconfig
  - ping
  - traceroute
  - whois
  - dig

Network Defense

- Defense in Depth
- Segmentation / partitioning
  - network perimeter
  - DMZ
  - bastion host
  - proxy
  - NAT / PAT
- firewalls
  - packet filtering
  - stateful packet filtering
  - circuit proxy
  - application
- inspection
  - IDS
  - IPS
  - IDS / IPS location

- host based
- network based
  - in-line
  - mirror, span, promiscuous
- IDS / IPS detection methods
  - pattern
    - signature analysis
  - anomaly
    - stateful matching
    - statistical
    - protocol
    - traffic
  - white & black lists
  - sandbox
- honeypots & honeynets
- ingress vs egress
- endpoint security

Remote Access

- Tunneling
  - GRE
  - PPTP
  - L2TP
  - Encryption
    - VPN (tunneling + encryption)
      - IPSec
        - authentication header
        - encapsulating security payload
        - tansport mode
        - tunnel mode
        - IKE

- security association
- SSL/TLS
  - mutual authentication
- SOCKS
- SSH

- Remote Authentication
  - RADIUS
  - TACACS+
  - Diameter
- Remote Access/Mgmt
  - SNMP
  - Telnet