Network Security

- OSI (Open Systems Interconnection) Model
  - Application; layer 7 (and basically layers 5 & 6) (includes API, HTTP, etc).
  - Transport; layer 4 (TCP/UDP).
  - Network; layer 3 (Routing).
  - Datalink; layer 2 (Error checking and frame synchronisation).
  - Physical; layer 1 (Bits over fibre).
- Firewall
  - Rules to prevent incoming and outgoing connections.
- NAT (Network Address Translation)
  - Useful to understand IPv4 vs IPv6.
- DNS (Domain Name System)
  - (53)
  - Requests to DNS are usually UDP, unless the server gives a redirect notice asking for a TCP connection. Look up in cache happens first. DNS exfiltration. Using raw IP addresses means no DNS logs, but there are HTTP logs. DNS sinkholes.
  - In a reverse DNS lookup, PTR might contain- 2.152.80.208.in-addr.arpa, which will map to 208.80.152.2. DNS lookups start at the end of the string and work backwards, which is why the IP address is backwards in PTR.
  - DNS configs
    - Start of Authority (SOA).
    - IP addresses (A and AAAA).
    - SMTP mail exchangers (MX).
    - Name servers (NS).
    - Pointers for reverse DNS lookups (PTR).
    - Domain name aliases (CNAME).
- DNS Exfiltration
  - Sending data as subdomains.
  - 26856485f6476a567567c6576e678.badguy.com
  - Doesn't show up in http logs.
- ARP (Address Resolution Protocol)
  - Pair MAC address with IP Address for IP connections.
- DHCP (Dynamic Host Configuration Protocol)
  - UDP (67 - Server, 68 - Client)
  - Dynamic address allocation (allocated by router).
  - `DHCPDISCOVER` -> `DHCPOFFER` -> `DHCPREQUEST` -> `DHCPACK`
- Multiplexing
  - Timeshare, statistical share, just useful to know it exists.
- Traceroute
  - Usually uses UDP, but might also use ICMP Echo Request or TCP SYN. TTL, or hop-limit.
  - Initial hop-limit is 128 for windows and 64 for *nix. Destination returns ICMP Echo Reply.
- Nmap (Network Mapper)
  - Network scanning tool.
- Person-in-the-Middle (PitM)
  - Understand PKI (public key infrastructure in relation to this).

- VPN (Virtual Private Network)
  - Hide traffic from ISP but expose traffic to VPN provider.
- Tor (The Onion Router)
  - Traffic is obvious on a network.
  - Investigating Individuals on Tor Networks
- Proxy
  - 7 Proxies won't help you
- BGP (Border Gateway Protocol)
  - Border Gateway Protocol.
  - Holds the internet together.
- Network Traffic Analysis Tools
  - Wireshark
  - Tcpdump
  - Burp suite
- HTTP(S)
  - (80, 443)
- SSL/TLS
  - (443)
  - Super important to learn this, includes learning about handshakes, encryption, signing, certificate authorities, trust systems. A good primer on all these concepts and algorithms is made available by the Dutch cybersecurity center.
  - POODLE, BEAST, CRIME, BREACH, HEARTBLEED.
- TCP/UDP
  - Web traffic, chat, voip, traceroute.
  - TCP will throttle back if packets are lost but UDP doesn't.
  - Streaming can slow network TCP connections sharing the same network.
- ICMP
  - Ping and traceroute.
- Email Protocols
  - SMTP (25, 587, 465)
  - IMAP (143, 993)
  - POP3 (110, 995)
- SSH
  - (22)
  - Handshake uses asymmetric encryption to exchange symmetric key.
- Telnet
  - (23, 992)
  - Allows remote communication with hosts.
- IRC
  - Understand use by hackers (botnets).
- FTP/SFTP
  - (21, 22)
- RPC
  - Predefined set of tasks that remote clients can execute.
  - Used inside orgs.
- Service Ports

    - 0 - 1023: Reserved for common services - sudo required.
    - 1024 - 49151: Registered ports used for IANA-registered services.
    - 49152 - 65535: Dynamic ports that can be used for anything.
- HTTP Header
    - | Verb | Path | HTTP version |
    - Domain
    - Accept
    - Accept-language
    - Accept-charset
    - Accept-encoding(compression type)
    - Connection- close or keep-alive
    - Referrer
    - Return address
    - Expected Size?
- HTTP Response Headers
    - HTTP version
    - Status Codes:
        - 1xx: Informational Response
        - 2xx: Successful
        - 3xx: Redirection
        - 4xx: Client Error
        - 5xx: Server Error
    - Type of data in response
    - Type of encoding
    - Language
    - Charset
- UDP Header
    - Source port
    - Destination port
    - Length
    - Checksum
- Broadcast Domain vs Collision Domain
- Root Store
- CAM Table Overflow