|  |  |
| --- | --- |
| TCP/IP – Main protocol for modern network  -Providing IP addressing scheme  -Route Network  -Deliver Packet  -Connection-oriented protocol  -Creating handshake (3-way handshake)   * SYN * FIN * ACK (acknowledge) | UDP – lightweight, not using 3 way handshake |
| OSI MODEL  7. Physical Layer  6. Data link  5. Network Layer  4. Transport Layer  3. Session Layer  2. Presentation Layer  1. Application Layer | |
| IP Address  192.169.1.1/25  Why the range 0-255  NAT – Network Address Translation  Subnetting  IPv4 (32 bits)  IPv6 (128 bits)   * Static - Assigned network IP ADDRESS * DHCP - | **PORT**   * 16 bit binary number port |
| ICMP – Internet control Message Protocol – is the housekeeping protocol of the internet.   * Ping command * Traceroute (traceroute -I erertech.com) |  |
|  |  |
|  |  |
|  |  |
| NMAP | |
| Open port  Closed port  Filtered  Unfiltered | Scanning Multiple Systems (separate by spaces)  >nmap 192.168.1.1 192.168.1.6  >nmap 192.1.681.1,3,6  Range IP Address  >nmap 192.168.1.1-100  Reading in file  >nmap -iL {Name Of the file} |
| Scanning with IPv6 |  |
| How to discovery with nmap (Host Discovery)  >arp -a | Discovery Flag   * -Pn – no host discovery * -PS – TCP SYN Request * -PA TCP ACK request * -PU UDP request * -PE ICMP echo request * -PR ARP request   e.g. nmap -PS23 102.168.1.75/255 |
| DNS Options in NMAP | TCP Scanning with Nmap   * -sS – TCP syn scan * -sT – TCP connect scan * -sN – TCP NULL Scan * -sF – TCP FIN Scan * -sX – TCP Xmas Scan * -sA – TCP ACK Scan * -sW – TCP window Scan * -sM – TCP Maimon Scan |
| UDP Scanning with Nmap – Fast the connection, not guarantee it will reach the port   * Nmap -sU –min-rate 500 {IPADDRESS} | Selecting port to scan   * Nmap -p 80,443 {ipaddress} * Nmap -F {ipaddress} (100 ports) * Nmap -p http, https |
| Scanning Operating System   * Nmap -O {ipaddress} | Scanning Version Detection   * Nmap -sV {IPADDRESS} |
| Scanning shortcut   * Nmap -A -T4 {ipaddress} |  |
|  |  |
| Scanning output   * -oN – save as textfile * -oX – Machine-readable XML file * -oG – greppable file | Scanning output  >sudo nmap -sS -sV -oN sample.txt {ipaddress} |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |