- Filename: eccouncil-ceh31250-v11-3-1-1-network-scanning-types.md
- Show Name: CEHv11 (312-50)
- Topic Name: Recon Techniques - Scanning
- Episode Name: TCP Communication

==

TCP Communication

Objectives

- Recognize the 6 TCP communication flags and point out their purpose
- Explain the process of TCP/IP communications

- What is the first thing we need to know about TCP Communications?
    - Connection oriented
    - Utilizes 6 'Control Flags'
        - 1 bit each
        - 4 flags for connection management
            - Synchronize (SYN)
            - Acknowledge (ACK)
            - Finish (FIN)
            - Reset (RST)
        - 2 flags for system instruction
            - Push (PSH)
            - Urgent (URG)
- What details do we need to know about the connection management flags?
    - SYN
        - Initiation to establish connection between hosts
        - Sequence number synchronization
    - ACK
        - Signals that host is ready to or has received data
    - FIN
        - Signals that transmission is over and connection is terminated
    - RST
        - Signals an error
            - Aborts connection
- What details do we need to know about the system instruction flags?
    - PSH
        - Controls the sending and receiving of data in buffers
            - Increases the efficiency of that process
    - URG
        - Prioritize this data

- What is the TCP 3-way handshake?
    - Proper establishment of a TCP connection
        - SYN --> SYN/ACK --> ACK --> CONNCETION ESTABLISHED!
- Is there any way to see the 3-way handshake process?
    - Wireshark