- Filename: eccouncil-ceh31250-v12-12-1-1-ids-and-ips.md
- Show Name: CEHv12 (312-50)
- Topic Name: Network and Perimeter Hacking: Evading Firewalls, IDS, and Honeypots
- Episode Name: IDS and IPS
  ==========

IDS and IPS

Objectives:

- Define what an IDS/IPS is and explain its function and basic process
- List and define the different types of IDS/IPS

- What is an IDS?
    - Network traffic inspection for known attack signatures/behaviors
        - Protocol Anomaly Detection
    - Placement can be inside, outside, or on both sides of your network
        - Detection generates an alert
- What is an IPS?
    - Like an IDS, but can take action to stop detected attacks
        - "Active" IDS
- Types of Intrusion Detection and Prevention Systems
    - Network Based
    - Host Based
- IDS/IPS Alert Types
    - True Positive => Attack detected & Alert Sent
    - False Positive => False Alarm (no attack but Alert was sent)
    - True Negative => No attack and therefore no Alert
    - False Negative => Attack not detected & no Alert
- IDS/IPS Solutions
    - Snort
        - Snort Rules found in `/etc/snort/rules/`
            - Check out **scan.rules**
                - Explain some of the details of a rule
                    - Mention custom rules
        - DEMO Snort
            - FROM LINUX LITE
            - `sudo snort -A console -q -c /etc/snort/snort.conf -i ens33 -K ascii`
                - **-A** = Alert Type
                - **-q** = Quiet. Don't show banner or status report
                - **-c** = Config file
                - **-i** = Network adapter
                - **-K** = Output type (default is pcap)
            - FROM PARROT
                - `sudo nmap -sX -n -Pn -F 192.168.241.136`
            - LOGS
                - `/var/log/snort/IP/`
                    - cat files in that dir for packet info (sudo needed)

    - Bro/Zeek
    - AlienVault
    - Suricata
    - Mobile
    - Yara
        - https://yara.readthedocs.io/en/stable/
- IDS/IPS Evasions
    - We've talked about some already
        - Packet Fragmentation
            - Session Splicing
        - Decoys
        - Obfuscations
            - Encoding data (unicode/base64/etc)
        - DoS Attacks against the IDS/IPS
            - Some IDS/IPS systems fail OPEN
        - Insertion Attacks
            - IDS will allows garbage(invalid/malformed) packets
        - But endpoint will reject them
        - Evasion Attacks
            - Messes with stream reassembly so that the IDS misses part of the attack
        - TTL Atttacks
            - Attacker must have knowledge of network topology for this to work
            - Attack broken up in to multiple fragments
                - Fragments are set with high and low TTLs
            - Low TTL fragments get dropped before reaching target
                - 1st frag reaches target
                - 2nd frag is discarded
                - 3rd frag reaches target
                - 2nd frag is resent with high TTL and reaches target
                - Target assembles frags
- Defenses
    - Baselines
    - Updates and patches
    - Block known-bad