SRC

Types of attacks:

- Disruption Attacks (Denial of service or signal jamming)
  -Multiple small devices generating traffic to a specific target, can be TCP or UDP; At source we can try to detect anomalous behaviour by checking destinations of traffic changes and their periodicity

> ⚠ **How to mitigate at target?**
>
> 1. Using load-balancers to distribute traffic
> 2. For TCP we can use session resets in the firewalls, which is an abrupt closure of a specific session; All information about the connection is erased
> 3. For UDP/DNS, block requests from unknown external DNS servers, although it doesnt work with large botnets (blocks IP spoofing and attack amplification)

Important attack phases:

1. Infiltration

```
1. This happens when an attacker gains access to private
information/protected domains and may include installation of ilicit
software in compromised machines; They may also be remotely controlled
(C&C). They are the hardest to detect since there's a lot of human
endeavours involved, and they are really hard to monitor;
Enterprises/Companies must have specific rules for network applications in
the internal network. Attackers can gain access through phishing, credential
stealing, or social engineering. The network/systems are also vulnerable to
0-day attacks, since there is no knowledge of the threat before it happens.
```

2. Propagation

```
1. The attacker must gain more knowledge to access more relevant protected
domains/private information.
```

3. Exfiltration

```
1. This is when an outcome must be tranfered to the outside network;
Attackers can also tranfer it to a less important point in the internal
network that can be lost, and then transfer it to the outside.
```

> ⓘ **Point 2. and 3.**
>
> These attacking phases are not so hard to detect, since in every case there are communication patterns that are broken, and that can be more easily detected. This can range from specific ports/ip's to traffic ratio and traffic matrixes.

Access control

- AAA architecture

- Authentication identifies the user
- Authorization defines what the user can do
- Accounting monitors the network usage
  Normally all the information is stored in a separate server (Authentication server).
  The standard for NAC is 802.1X and it provides a secure mechanism to devices wishing to connect to a LAN, and its based on EAP.

RADIUS

- In class we implemented a RADIUS authentication server for a secure AAA architecture.
  - In this protocol, the access device serves as a client for RADIUS
    - RADIUS servers are responsible for receiving user requests and authenticating the server.
    - Firstly, the client authenticates via authentication protocol like EAP, PAP, MS-CHAP, and then exchange keys in RADIUS encapsulated UDP packets.

Flow control

1. Firewalls

- Services
  - NAT
  - Authorization (Packet filtering)
  - Redirecting (Proxying)
  - Secure communications
    - Site-to-site VPN

        - IPSec
    - Remote access VPN
  - DDoS and DoS detection and prevention
- Must be placed in multiple network locations (For big networks)

> **Stateful vs Stateless**
>
> Stateless firewalls control traffic by applying rules to single packets, and are based on the definitions of access lists; They are fast and consume low computing resources. They perform well under heavy traffic load and therefore are really good against DoS attacks. On the other hand, stateful firewalls monitor traffic not on specific packets, but on traffic sessions; They control traffic based on the connection state of a flow, and its state is maintained in a state table that must be synchronised with other firewalls in redundancy scenarios.

- There are several scenarios for redundancy and high availability
  - Active-Backup scenarios
    - Firewalls share same IP and the backup only accepts traffic if the main firewall fails and they are a dedicated sync connection
  - Active-Active scenarios
    - Firewalls have different IP's and both receive traffic; They need a dedicated sync connection for state maintenance
      - Work well with load-balancers
  - Load balancing firewall load
    - Load-balancers distribute traffic through several firewalls
      - They same flow needs to go through the same firewall (forward and back)
      - Firewalls do not need to share dedicated sync connections
      - Allows scalable growth
      - Good against DoS attacks
      - Reduce firewall computing powers
- In a corporate network, ideally, there should be a first level of defense against DDoS composed by stateless firewalls (Access layer); A second level defense of stateful firewalls should also be in the network for general protection.
- Firewall rules must be specified based on traffic source, destination and type.

> **Best practices**
>
> 1. Standardize security policies

2. Block all traffic by default
3. Add exceptions in specific sources/destinations/types
4. Maintain documentation
5. Integrate flow control with existing routing, switching and load balancing

Secure communications

- Point-to-point tunnels
  - Compose an overlay network
    - An overlay network with any degree of privacy is denominated VPN
  - Can be routed through static routes, policy based routing (Route maps), or dynamic routing
- Multipoint tunnels
  - Simpler and more efficient in a network with multiple nodes (Multipoint tunnel)
  - One single interface connects several nodes
  - Routing based on next-hop within overlay network

IPSec

```
- AH (Authentication header)
        - Ensures data integrity
        - Does not provide confidentiality
        - Provides origin authentication
        - Uses hash mechanisms
- ESP (Encapsulated security Payload)
        - Provides data confidentiality
        - Does not protect IP header
- Both security protocols use symmetric key algorithms
- IPSec has two modes
        - Tunnel
                - Gateways provide IPSec services to other hosts in peer-to-
peer tunnels
                - End-hosts are not aware of IPSec protection
                - Provide security across untrusted networks
        - Transport
                - Each end host does IPSec encapsulation, host-to-host
                - IPSec must be implemented in the end-hosts
                - Application endpoint bust also be IPSec endpoint
- A security association is also made, and represents a contract between
```

```
hosts or peers; They describe how IPSec services will be used to protect
traffic
        - Composed by used protocol/mode, communication type, session keys
(IKE, ISAKMP, SKEME) and authentication algorithm
                - Session keys imporve IPSec features by adding flexiblity
and providing authentication for IPSec peers and therefore protecting SA
negotiation
        - Important/Relevant variants of site-to-site VPNs and information
                - IPSec tunnels with static configs
                        - Requires knowledge of all peers
                - IPSec tunnels with dynamic configuration
                        - Hub + spokes configuration
                                - All the VPN traffic goes through a hub
                        - Easily scalable (Add new peers/spokes)
        - IPSec ports
                - UDP port 500 for IKE
                - UDP port 4500 for NAT traversal
        - In remote access VPNs (Remote work)
                - Should have a VPN zone
                        - The traffic is routed back to the firewall using a
different network interface and zone (Never directly to core/internal
network)
```

IPSec tunnels

This basic IPSec tunnels can't protect multicast traffic.
For protection of multicast we should implement IPSec + GRE tunneling

IDS and IPS

- IDS

```
- Identifies intrusions outside the organization
- Monitors unauthorized systems
- Detects misuse from illicit user
- Does not prevent or block threats
- Signals alarm
```

- IPS

```
- Blocks traffic
- Kills processess
- Blocks device access
```

> **Network deployment**
>
> It's basically an IDS with firewall integration

- We can deploy IDS/IPS at:
  - Network level
    - To protect organizations in general
  - Host level
    - To protect specific devices

> **Deployment**
>
> We can deploy this systems with an inline embedded firewall architecture

- This systems should have the following actions types :
  1. alert
  2. pass
  3. drop
  4. reject

SIEM & SOC

- Incorporates several security tools into one application
  - Aggregates logs from multiple systems
    - With rsyslog over TCP
  - Posses tools to identify, collect, and analyse data from the logs or from packet capturing
    - With network tap or switch mirror port (ERSPAN)
  - Include automated features and alerts that might indicate the network is compromised
  - Generate precise reports
  - Own software that discover correlations between events that could indicate a security issue

Data sources/gathering

1. SNMP
    1. Used for acquiring status and usage of nodes and services over time
        1. Network elements/interconnections and deployed services
    2. Used for predicting:
        1. Data flow performance
            1. packet loss
            2. delay/jitter
        2. Nodes performance
            1. Memory/CPU usage
            2. Unstable nodes
        3. Network link usage
            1. Bandwidth
            2. packet counts
        4. Data/flow routing
            1. Allows to understand how data flows and how it should react to disruptive events
2. Flow exporting
    1. Used to characterise users/services in terms of amount of traffic and traffic destinations
        1. NetFlow
3. Packet captures
    1. Used to characterise users/services in small time-scales
    2. Require network components for mirroring
        1. Network tap, switch mirroring
4. CLI Access / Log access
    1. Used to acquire knowledge from past and current state
        1. SSH, TELNET, SCP
        2. rsyslog

Example of SIEM events

- Brute force detection
    - Excessive 404 error from a non-authenticated client (DB Log)
    - Excessive login failures (services or DB Logs) at one or more services
    - Non-matching credentials
        - From internal machines (RADIUS / LDAP)

- Impossible travel
  - Consecutive logins from same user from distant geographic regions
- Anomalous data transfer
  - Analysing by individual source/destination and/or by used protocol/port
  - Download/upload amounts
  - Upload/download ratio
  - Never connected devices
- DDoS attack
  - Excessive connection attempts from "never seen" devices/addresses/regions
    - Ideal detection in the early phase of the attack
      - Usually the first level of firewalls should detect this