CompTIA Security + 2.0 Technologies and Tools

Filename: comptia-secplussy0501-2-1-hardware_and_software_organizational_security
Title: Hardware and Software Orgranizational Security
Subtitle: CompTIA Security+ (SY0-501)

2.1 Hardware and Software Orgranizational Security

- 2.1 Install and configure network components, both hardware- and software-based, to support organizational security
    - Firewall
        - ACL
        - Application-based vs. network-based
        - Stateful vs. stateless
        - Implicit deny
    - VPN concentrator
        - Remote access vs. site-to-site
        - IPSec
            - Tunnel mode
            - Transport mode
            - AH
            - ESP
        - Split tunnel vs. full tunnel
            - Split tunnel
                - Any traffic that is not specifically bound for the corporate network is routed to the Internet via the local LAN
                - Can accelarate the VPN communication by only sending traffic bound for the corporate network through the VPN tunnel
            - Full tunnel
                - All traffic goes through the corporate network including traffic that is destined for the Internet
                - Transmitting all traffic through the corporate network can be bandwidth consuming and slow
        - TLS
        - Always-on VPN
    - NIPS/NIDS
        - Signature-based
        - Heuristic/behavioral
        - Anomaly
        - Inline vs. passive
        - In-band vs. out-of-band
        - Rules
        - Analytics
            - False positive
            - False negative
    - Router
        - ACLs
        - Antispoofing Switch
        - Port security
        - Layer 2 vs. Layer 3
        - Loop prevention
        - Flood guard
    - Proxy
        - Forward and reverse proxy
        - Transparent
        - Application/multipurpose
    - Load balancer
        - Scheduling
            - How the host is chosen
            - Affinity(server-affinity, session-affinity)
            - Round-robin
        - Active-passive
        - Active-active
        - Virtual IPs
    - Access Point
        - SSID
        - MAC filtering
        - Signal strength
        - Band selection/width
        - Antenna types and placement
        - Fat vs. thin
            - LWAPP
            - CAPWAP(Control and Provisioning of Wireless)
        - Controller-based vs. standalone
    - SIEM

        - Aggregation
            - SIEM systems collect a lot of data from multiple event sources, with aggregation the goal is to consolidate different event source data into a single repository make log management more feasible
        - Correlation
            - Applying intelligence to the logs to make it possible to discover event
            - Apply if/then rules to different security events
        - Automated alerting and triggers
        - Time synchronization
            - Time-sensitive event monitoring is important
        - Event deduplication
            - Is also a form of event source aggregation in which exact events are merged into a single event
        - Logs/WORM
    - DLP
        - USB Blocking
            - Hardware and content monitoring of confidential data
            - Implement business policies to ensure employees handle confidential data in a secure manner.
        - Cloud-based
            - Using data/security policies to protect against the use of unsanctioned could services
            - Increasingly challenging to monitor and control with the addition of unmanaged devices like cellphones and tablets
        - Email (*Mention* email gateways perform this too)
            - Email is an critical threat vector for outbound data loss
            - Threat vectors are routes that a malicious attack may use to break defenses
            - To protect against BEC-based attacks (business email compromise)
            - Can be an avenue for phishing and whaling attacks
            - Technologies can implement fine-grained policies that can:
                - Automatic identification and classification
                - Filter data streams for privacy
                - Content and context aware
    - NAC
        - Dissolvable vs. permanent
            - Permanent or persistant
                - Agents stays on the host the agent runs on
                - Allows for continuous compliance monitoring
            - Dissolvable or Non-persistant agents
                - Agent is placed on a website portal, authenticates the user and verifies compliance
        - Host health checks
        - Agent vs. agentless
            - Agentless
                - The NAC functionality is built into the technology requiring neither a dissolvable or permanent agent to run on the client.
                - ADDS is an example of agentless NAC.
                - 802.1X can implement agentless NAC
    - Mail gateway
        - Spam filter
        - DLP
        - Encryption
    - Bridge
        - Wired or Wireless
        - Connects two network segments together
        - Operates at Layer 2 of the OSI Model
        - Today switches are multiport bridges
    - SSL/TLS accelerators
    - SSL decryptors
        - Can be used to ensure that an insider is not sending confidential company IP outbound of the network
        - Can use certificate-copying mechanisms(kind of like a corporate-operated MiTM attack)
    - Media gateway
        - Converting media streams into different formats to make the communication stream interoperable across different network standards
        - Think about placing media on circuit switching networks that originated on a packet switching networks
    - Hardware security module
        - Hardware-based device responsible for guarding cryptographic keys
        - Can be plug-in cards or an external device