Briefing Doc: Network Protection Systems

Main Themes

- **Network Protection System (NPS):** Any device or system designed to protect a network. This encompasses a variety of technologies, including routers, firewalls, Intrusion Detection and Prevention Systems (IDS/IPS), web filtering, and honeypots.
- **Unified Threat Management (UTM):** A single device combining multiple network protection functions, offering a streamlined approach to security.
- **Layered Security:** Effective network defense requires a layered approach. This involves implementing multiple NPS technologies to create a robust defense-in-depth strategy.
- **Configuration and Management:** Securely configuring NPS devices is crucial. Tools like benchmarks and risk analysis software are essential for maintaining optimal security posture.

Important Ideas and Facts

1. Routers

- **Functionality:** Routers operate at the Network layer of the OSI model, directing network traffic between different segments. They employ routing protocols like link-state, distance-vector, and path-vector to determine optimal paths.
- **Security Role:** Routers can act as a basic network protection system using Access Control Lists (ACLs) to filter traffic based on source and destination IP addresses, protocol type, and port numbers.
- **Cisco Routers:** Cisco routers are widely used. Understanding their components (RAM, NVRAM, Flash memory, ROM, interfaces) and configuration modes (user, privileged, global configuration, interface configuration) is fundamental for network security.

2. Firewalls

- **Purpose:** Control access to all traffic entering and leaving an internal network.
- **Types:** Available as both hardware and software solutions, each with advantages and disadvantages. Hardware firewalls are typically faster and handle larger throughput, while software firewalls offer flexibility.
- **Technologies:** Employ various technologies like Network Address Translation (NAT), access lists, packet filtering, stateful packet inspection, and application layer inspection.
- **Implementation:** Implementing a Demilitarized Zone (DMZ) between the internet and the internal network provides an added layer of security.
- **Cisco ASA Firewall:** A popular firewall that has replaced the PIX firewall, offering advanced features like intrusion detection and prevention and sophisticated application layer inspection.

3. Intrusion Detection and Prevention Systems (IDS/IPS)

- **Purpose:** Monitor network devices, identify attacks in progress, and potentially take action to prevent intrusions.
- **Types:** Exist in network-based and host-based forms, each monitoring activity on network segments or specific hosts.
- **Functionality:** Can be passive (logging and alerting) or active (taking actions like blocking traffic). Anomaly-based systems identify suspicious activity by deviating from established baselines.

4. Web Filtering

- **Importance:** Crucial for blocking access to malicious websites and preventing drive-by downloads. Some web filters can block malicious code before it reaches user workstations.

5. Security Operations Center (SOC)

- **Role:** A dedicated team responsible for security-response functions, using Security Information and Event Management (SIEM) tools to identify attacks and indicators of compromise.

6. Honeypots

- **Purpose:** Lure and trap hackers, distract them from attacking legitimate resources, and gather data on their tactics.
- **Types:** Can be physical or virtual devices configured with vulnerabilities to attract attackers.

Quotes

- "Network Protection System – Any device or system designed to protect a network"
- "Unified Threat Management (UTM) device – Term used to describe a single device that combines many network protection functions"
- "Placing a firewall between a company's internal network and the Internet is dangerous – Leaves company open to attack if a hacker compromises the firewall"
- "Honeypot – Computer placed on the network perimeter… configured to have vulnerabilities"

Conclusion

Implementing a layered security approach using various Network Protection Systems is essential for securing modern networks. Understanding the different NPS technologies, their configurations, and management best practices is crucial for defending against evolving cyber threats.