Technical Deployment Guide: StingBox

System Overview

StingBox functions as a proactive security control by deploying decoy systems within a network. The system operates on a no-trust basis: legitimate users have no reason to access these decoys. Therefore, any network interaction (scan, ping, or login attempt) is treated as a high-fidelity Indicator of Compromise (IOC), signaling reconnaissance or lateral movement.

Deployment Strategies by Segment

1. Critical Server Subnets (Core Infrastructure)

Objective: Detect lateral movement targeting high-value data and infrastructure.

- **Placement:** Deploy StingBox appliances on the same subnets as Domain Controllers, File Servers, and Database Clusters.
- **Naming Strategy:** Hostnames should simulate legacy, unpatched, or forgotten assets to encourage interaction from attackers seeking vulnerabilities.
- **Recommended Hostnames:**
  - `Finance-Backup-2019`
  - `SQL-DEV-OLD`
  - `DC-OLD-AUTH02`

2. User Workstations and VLANs

Objective: Detect ransomware propagation or lateral movement from compromised endpoints ("Patient Zero").

- **Placement:** Deploy within the DHCP ranges used by legitimate employee laptops and BYOD devices.
- **Naming Strategy:** Hostnames must appear as standard peer devices to blend in with normal network traffic.
- **Recommended Hostnames:**
  - `DESKTOP-JMSMITH`
  - `HP-LAPTOP-04`
  - `WORKSTATION-HR-02`

3. VPN and Remote Access Segments

Objective: Identify unauthorized access using compromised credentials before the attacker moves to internal systems.

- Placement: Assign an IP within the VPN user pool, remote access ranges, or Jump Box segments.
- Naming Strategy: Simulate administrative consoles or intermediate access points.

- Recommended Hostnames:
    - `ADMIN-CONSOLE-REMOTE`
    - `VPN-JUMPBOX-TEMP`

4. Guest Wi-Fi and IoT Segments

Objective: Detect attempts to hop from low-security segments (printers, cameras, guest networks) to high-security networks.

- Placement: Deploy on Guest VLANs and IoT-specific subnets.
- Naming Strategy: Mimic vulnerable peripherals or smart devices.
- Recommended Hostnames:
    - `CONF-ROOM-PRINTER`
    - `LOBBY-CAMERA`
    - `SMART-TV-BOARDROOM`

5. Cloud Infrastructure

Objective: Detect automated scanning for open ports, misconfigurations, or exposed internal assets.

- Placement: Deploy as a virtual appliance within cloud environments (AWS, Azure, etc.).
- Naming Strategy: Suggest misconfigurations or lack of security controls.
- Recommended Hostnames:
    - `TEST-SERVER`
    - `DEV-DB-NO-PASS`

Hostname Configuration Suggestions

The effectiveness of deception technology relies on the credibility of the decoy's hostname. The name must align with internal naming conventions while suggesting exploitability.

Configuration Rules:

1. **Do Not Use:** Generic security terms that identify the device as a trap (e.g., Honeypot, Stingbox, Trap, Security).
2. **Do Use:** Terms that imply high value or low security.
    - *Categories:* HR, Payroll, Finance
    - *Status:* OLD, TEMP, TEST, BACKUP, DEV

Example: An attacker scanning a subnet is statistically more likely to target FILE-SERVER-BACKUP than a generic alphanumeric hostname.

For further information regarding this Document or StingBox products, please contact us at:

- Email: support@stingbox.com
- Phone: (561) 203-8594
- Website: www.stingbox.com
- Mailing Address: StingBox LLC 7190
  SE Federal Hwy Ste 3 Stuart, FL 34997-8693, USA