SYSTEMS REFERENCE CARD

Scenario 3: "Blackout Friday" — FIDS & PA Architecture

Distribute to IT/Cybersecurity Team (Team B) at Exercise Start
FOR TRAINING USE ONLY

EXHIBIT A: NCIA NETWORK ARCHITECTURE

NCIA uses VLAN segmentation with a Palo Alto PA-850 core firewall enforcing inter-VLAN rules. The following VLANs are relevant to this incident:

VLAN	Name	Key Systems	Notes
10	Server	AODB, FIDS Server, Payment Gateway, DC, DNS	The FIDS management console (web interface on port 8080) runs on the FIDS server at 10.1.10.25.
20	Admin	Staff workstations, IT, Finance, HR	Normal admin operations.
30	Security	CCTV, NVR, PACS	Isolated. Not affected.
50	Passenger Ops	FIDS displays, gate mgmt, check-in kiosks, **PA Controller**	The IP-based PA controller (Cisco UCM for PA) lives at 10.1.50.10. PA zones are managed via a web admin interface on port 443.
70	Guest WiFi	Public passenger WiFi, captive portal	Should be FULLY ISOLATED from all internal VLANs. Guest WiFi clients should only reach the internet via the captive portal.

EXHIBIT B: FIDS ARCHITECTURE

NCIA's FIDS is a three-tier system:

- **FIDS Server** (10.1.10.25, VLAN 10): Windows Server running Infax FIDS application. Pulls flight data from AODB. Pushes content to displays. Has a web-based management console on **port 8080** (HTTP, not HTTPS) for content management, display control, and system configuration.
- **FIDS Displays** (VLAN 50): 38 thin-client displays throughout the terminal. They receive content from the server. They don't store data locally.
- **Management Access**: The FIDS management console is intended to be accessible ONLY from VLAN 20 (Admin). Firewall rule should permit VLAN 20 → VLAN 10:8080 and deny all other sources.

Key Question: Who else can reach port 8080 on the FIDS server? If anyone outside VLAN 20 can reach it, the FIDS server is exposed.

EXHIBIT C: PA SYSTEM ARCHITECTURE

NCIA's PA system was upgraded 18 months ago from a legacy analog system to an IP-based system:

- **PA Controller** (10.1.50.10, VLAN 50): Cisco Unified Communications Manager (UCM) configured for PA zone management. Web admin interface on **port 443** (HTTPS). Controls all PA zones: terminal-wide, per-concourse, per-gate, and emergency.
- **PA Endpoints**: IP speakers throughout the terminal. Managed by the UCM controller.
- **AOC Console**: Physical PA microphone and control panel in the Airport Operations Center. Connected to the PA controller via the VLAN 50 network. Operators use the console for routine announcements.

• **Admin Credentials**: The PA controller was installed by Convergent AV Solutions 18 months ago. The web admin interface credentials were set during installation.

Key Question: What are the admin credentials on the PA controller? Were they changed from the vendor default after installation?

EXHIBIT D: FIREWALL RULE EXCERPT — GUEST WIFI ISOLATION

The following firewall rules govern Guest WiFi (VLAN 70) traffic. Examine them carefully — is VLAN 70 truly isolated?

#	Source	Destination	Service	Action	Notes
47	VLAN 70	Internet	HTTP/HTTPS	ALLOW	Guest WiFi internet access via captive portal.
48	VLAN 70	VLAN 10	DNS (53)	ALLOW	Guest WiFi DNS resolution via internal DNS server.
49	**VLAN 70**	**VLAN 50**	**HTTPS (443)**	**ALLOW**	**"Captive portal redirect" — added 6 months ago during WiFi upgrade. Intended to allow portal auth flow. Grants Guest WiFi access to ALL of VLAN 50 on 443.**
50	VLAN 70	Any	Any	DENY	Default deny — should block everything else from Guest WiFi.

Rule 49 is the vulnerability. It was added during a WiFi infrastructure upgrade 6 months ago. The intent was to allow Guest WiFi clients to reach the captive portal authentication server (which happens to be on VLAN 50). But the rule is overly broad: it permits VLAN 70 (Guest WiFi) to reach **anything on VLAN 50 over HTTPS (port 443)**. The PA controller's web admin interface is on VLAN 50, port 443.