NETWORK EVIDENCE PACKET

Scenario 6: "Friendly Fire" — IT/Cybersecurity Reference

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

EXHIBIT A: FIREWALL RULE LOG — PALO ALTO PA-850

The following shows the last 5 firewall rule changes, extracted from the Palo Alto management console. Focus on the most recent entry.

Change #	Timestamp	Admin	Action	Rule Description
CM-2026-0083	Mon 14:22	j.kelley	ADD rule	Allow VLAN 50 → VLAN 10 : TCP 443 (FIDS HTTPS)
CM-2026-0084	Mon 16:05	j.kelley	MODIFY rule	Update VLAN 20 → VLAN 10 : Add TCP 8443 (Admin console)
CM-2026-0085	Tue 09:10	j.kelley	ADD rule	Allow VLAN 60 → VLAN 10 : TCP 5432 (BHS database)
CM-2026-0086	Tue 11:30	m.chen	MODIFY rule	Update IDS signature set v4.7.2
CM-2026-0087	**Wed 09:45**	**j.kelley**	**ADD rule**	**"Block inbound from 185.220.0.0/16 per TI-2026-0312"**

Analyst Note

Change CM-2026-0087 was executed by user **j.kelley** (Jordan Kelley, IT Manager) at 09:45 AM — two minutes before the outage. The stated purpose was to block inbound traffic from IP range 185.220.0.0/16, which appeared on a CISA threat intelligence advisory (TI-2026-0312) as a known source of scanning activity.

The intended rule should **only affect inbound traffic from the internet**. It should NOT affect traffic between internal VLANs. Unless it was written incorrectly.

EXHIBIT B: THE ACTUAL FIREWALL RULE (CM-2026-0087)

Here is the rule as it appears in the Palo Alto running configuration:

```
Rule Name: TI-2026-0312-Block
Rule Type: Security
Source Zone: any
Source Address: any
Destination Zone: any
Destination Address: 10.1.40.0/24
Application: any
Service: any
Action: DENY
Log: yes
Position: 3 (above default inter-VLAN allow rules)
```

What's Wrong With This Rule?

This exhibit is the core puzzle piece. The intended rule was supposed to block external inbound traffic from 185.220.0.0/16. But look at what was actually written:

- **Source Zone: any** — Should have been "Untrust" (the external/internet zone). "Any" means ALL zones — including internal VLANs.
- **Source Address: any** — Should have been 185.220.0.0/16. "Any" means ALL source addresses.
- **Destination Address: 10.1.40.0/24** — This is the Retail VLAN (VLAN 40) subnet. The original intent was probably to protect the retail subnet from the external threat. But combined with Source = any, this blocks ALL traffic TO the Retail VLAN — including internal traffic from VLAN 10 (Server).
- **Position: 3** — This rule was inserted ABOVE the default inter-VLAN allow rules. Firewalls process rules top-down. This deny rule is evaluated before the allow rules — so it wins.

Translation: This rule says "deny all traffic from anywhere going to the Retail VLAN." That's why the payment gateway (VLAN 10) can't talk to the POS terminals (VLAN 40) — the firewall is blocking it. And it's also why the Concourse B FIDS and kiosks are degraded — collateral damage from the same over-broad rule affecting traffic paths that transit VLAN 40 subnets.

EXHIBIT C: SIEM ALERT LOG (LAST 24 HOURS)

The following SIEM alerts are relevant to the investigation. Note which are real threats and which are noise.

Time	Alert	Source	Severity	Analysis
Tue 14:17	Unusual API queries against RetailLink cloud portal	RetailLink vendor alert	MEDIUM	RetailLink's own monitoring flagged unusual query volume from IP 45.33.49.22. This is RetailLink's problem — it's their cloud portal, not NCIA's network. RED HERRING for the exercise.
Wed 02:00	Failed SSH attempt to 10.1.99.1	Firewall auth log	HIGH	3 failed SSH login attempts from 185.220.101.34 targeting the firewall management interface. This is the real external scanning that prompted the threat intel advisory TI-2026-0312. These attempts FAILED. No access was gained. This is what motivated Kelley to write the blocking rule — but the rule itself is the problem.
Wed 09:45	Firewall config change — new deny rule added	Firewall syslog	INFO	This is CM-2026-0087. The rule that caused the outage. Logged as a routine config change. No alert triggered because config changes by authorized admins are classified as INFO, not WARNING.
Wed 09:47	Bulk connection failures: VLAN 40 → VLAN 10	Network monitor	CRITICAL	47 POS terminals simultaneously lost connectivity to the payment gateway. This alert fired 2 minutes after the firewall rule change. Correlation = causation.
Wed 09:48	FIDS display heartbeat lost (4 units)	FIDS monitor	HIGH	Concourse B food court FIDS displays lost connection. Collateral damage from the same rule — the FIDS server's return traffic crosses VLAN 40 address space.

EXHIBIT D: CHANGE MANAGEMENT LOG

The IT change management system entry for CM-2026-0087:

Field	Value
Change ID	CM-2026-0087
Submitted By	Jordan Kelley (IT Manager)
Date Submitted	Wed 09:30 AM
Date Executed	Wed 09:45 AM
Approval	Self-approved. (NCIA policy allows IT Manager to self-approve "emergency" threat mitigation changes.)
Description	Block inbound traffic from IP range 185.220.0.0/16. Source: CISA Advisory TI-2026-0312 (scanning activity from known malicious infrastructure). Protect Retail VLAN from external threat.
Risk Assessment	Low — Blocking a single external IP range. No impact to internal operations expected.
Rollback Plan	Delete rule TI-2026-0312-Block if issues observed.
Post-Change Verification	NOT COMPLETED. (Kelley was called to a meeting at 09:46 and did not verify inter-VLAN connectivity after applying the rule.)