CONTROLLER HANDBOOK

Scenario 5: "Carbon Copy"

Badge Cloning, PACS Forensics & Physical-Cyber Convergence
North Coast International Airport (NCIA)
FACILITATOR / INSTRUCTOR USE ONLY

FACILITATOR DOCUMENT — DO NOT DISTRIBUTE TO PLAYERS

1. EXERCISE OVERVIEW

Duration: 2 Hours

Scope: Puzzle-driven TTX. A cloned airport badge is used to plant a rogue wireless access point in a network infrastructure room. Students must perform PACS forensics, CCTV correlation, RFID technology analysis, physical infrastructure inspection, and rogue device identification. This is the most technically demanding scenario in the series — the IT team leads, and the puzzle has a specific answer they must assemble from evidence.

Exercise Objectives

- **PACS Forensics:** Can IT read PACS logs, identify frequency anomalies, and correlate events across readers?
- **RFID Security:** Do students understand the difference between 125 kHz and 13.56 MHz credentials, and why legacy support creates a cloning vulnerability?
- **Physical-Cyber Convergence:** Do students recognize that a physical intrusion (badge clone) can be the delivery mechanism for a cyber attack (rogue AP)?
- **Infrastructure Protection:** Do students understand the need to protect network infrastructure rooms with the same rigor as other sensitive areas?
- **Network Security Fundamentals:** Can IT identify a trunk port misconfiguration, understand its implications, and develop a containment strategy?

2. THE PUZZLE — SOLUTION MAP

Here is the chain of evidence the students should assemble, in order:

#	Clue	What It Tells Them	Where They Find It
1	Duplicate credential alert	Same badge, two doors, 89 seconds apart. Impossible.	Opening scenario. Given.
2	Mendez confirmed in kitchen	Clone confirmed — Mendez wasn't at S-4 at 07:38.	Inject I-01.
3	Frequency analysis: clone reads at 125 kHz, real reads at 13.56 MHz	Clone is a 125 kHz prox card — unencrypted copy of legacy credential.	PACS log analysis (Exhibit A). IT should catch this.

4	Wednesday V-1 double-tap at 125 kHz	Badge was captured Wednesday in the Vendor Break Room. Phantom read = Proxmark3 in proximity.	PACS log (Exhibit A). May need nudge (I-03).
5	Clone's path: S-4 → M-3 → E-2 (12 min) → M-3 → S-6	Targeted Electrical Room B. Not random. Knew the route.	PACS log (Exhibit C). IT presents timeline.
6	CCTV: Unknown male, grey jumpsuit, white badge, heavier backpack on exit	Clone holder is not an employee. Came prepared. Brought equipment.	Inject I-05.
7	Rogue wireless AP found in E-2 behind UPS	THE ANSWER: Clone was used to plant a rogue network device for persistent remote access.	Inject I-06. Physical inspection.
8	Port 23 reconfigured from access to trunk	Attacker has access to ALL VLANs from the parking lot.	Inject I-07. Technical deep dive.
9	Viktor Sorin — cybercrime-as-a-service	Professional operation. Access was planted to be sold.	Inject I-08.

3. FACILITATOR PERFORMANCE NOTES

Let IT Lead

This is IT's scenario. They have the Forensic Evidence Packet. They should be driving the investigation. If IT is passive, prompt them: "Your team has the PACS logs. What do they tell you?" If IT is dominating and other teams are idle, redirect: "Ops — what's your decision on the morning departure push? Are you locking down?" "Security — the clone holder may still be in the building. What's your plan?"

The Wednesday V-1 Double-Tap

This is the "aha" moment of the exercise. Two reads at the same 125 kHz reader, 27 seconds apart, on Wednesday. It's subtle — most teams won't catch it on their first pass through the log. That's fine. Use inject I-03 to nudge them toward looking at Wednesday if they haven't found it by 0:26. When they do find it, let them work through the implications: "Why would a badge read twice at the same door? Who was near Mendez at 10:22 on Wednesday?"

The 12-Minute Gap

The clone was inside Electrical Room B for 12 minutes. That's the window. Once the team identifies E-2 as the target, they should want to physically inspect it. The discovery of the rogue AP (I-06) is the payoff — the answer to the puzzle. Build to it. Don't rush past the inspection. Let IT describe what they find. Make it feel like a discovery.

The A/B/C Decision

The rogue AP disposition (I-09) is the exercise's strategic decision point. Pull the plug is safe. Honeypot is sophisticated but risky. Silent kill is elegant but requires confidence. There's no wrong answer — but each has real trade-offs. Let the room debate. The FBI character should lean toward Option B (intelligence value) while Ops should lean toward Option A (network safety). IT should be the tiebreaker.

4. PACING GUIDE

Phase	Clock	Duration	Notes
0: Briefing	0:00 – 0:10	10 min	Distribute packets. Let IT study the Forensic Evidence Packet — they need a few minutes with the PACS log.
1: Confirm the Clone	0:10 – 0:35	25 min	Mendez located. Frequency analysis. Wednesday V-1 discovery. This phase is detective work. Let IT work through the log. Use the nudge (I-03) if needed.
2: Trace the Path	0:35 – 1:10	35 min	Movement timeline. CCTV ID. Physical inspection of E-2. Rogue AP discovery. Trunk port analysis. This is the technical core. Give IT room to work through it.
3: Who and Why	1:10 – 1:40	30 min	Sorin ID. A/B/C decision on the rogue AP. Systemic vulnerability assessment. Remediation planning. Transition from puzzle-solving to strategic planning.
4: Debrief	1:40 – 2:00	20 min	3-Up / 3-Down. Focus on: legacy technology risk, physical-cyber convergence, the $25 attack that bypassed a multi-million-dollar security system.

5. EVALUATION & GRADING RUBRIC

Metric	Assessment Criteria
Metric 1: PACS Forensics (30 Points)	**Fail:** IT treated this as a system glitch or couldn't read the PACS logs. **Pass:** IT confirmed the clone via the frequency analysis (125 kHz vs. 13.56 MHz). **Excellence:** IT found the Wednesday V-1 double-tap independently, identified it as the capture event, mapped the complete clone movement path, and calculated the 12-minute E-2 window.
Metric 2: Rogue Device Identification (25 Points)	**Fail:** Team didn't inspect Electrical Room B, or inspected but missed the rogue AP. **Pass:** Team found the rogue AP and identified it as a network bridge. **Excellence:** IT identified the trunk port reconfiguration, understood the all-VLAN implication, and recognized that the attacker had prior knowledge of the switch model and VLAN structure.
Metric 3: Containment Decision (20 Points)	**Fail:** Team couldn't agree on a disposition for the rogue AP, or made a decision without understanding the trade-offs. **Pass:** Team chose an option and articulated the reasoning. **Excellence:** Team evaluated all three options, considered FBI/CISA equities, and made a decision that balanced network security with intelligence gathering.
Metric 4: Systemic Remediation (25 Points)	**Fail:** Team treated this as a one-time incident. Didn't address the legacy reader vulnerability. **Pass:** Team identified legacy 125 kHz readers as the root vulnerability. **Excellence:** Team produced a comprehensive remediation plan: disable legacy mode, deploy 802.1X, rotate switch credentials, disable unused ports, add CCTV to infrastructure rooms, implement switch config change alerting.

6. HOT WASH GUIDE

- **The $25 Attack:** "A Proxmark3 costs $25. A T5577 blank card costs $0.50. With these two items, someone bypassed your entire physical access control system. What does that tell you about the ROI of eliminating legacy 125 kHz readers?"
- **Physical-Cyber Convergence:** "The badge clone was a physical attack. The rogue AP was a cyber attack. They were the same operation. Does your security department talk to your IT department? How often? About what?"

• **Infrastructure Protection:** "Electrical Room B has no camera and is protected by a 125 kHz legacy reader. It contains a switch that connects to your entire network. Is that consistent with how you protect your other critical assets?"

• **Network Segmentation:** "Port 23 was reconfigured from access to trunk. That gave the attacker every VLAN. If you had 802.1X and switch port monitoring, would this attack have succeeded?"

• **The Parking Lot Problem:** "Someone could sit in the Concourse B parking lot and access your internal network wirelessly. How do you detect rogue wireless devices? Do you do periodic wireless surveys?"

END OF CONTROLLER HANDBOOK