MASTER INJECT DECK

Scenario 5: "Carbon Copy"

North Coast International Airport (NCIA)
Print and cut. Deliver at times indicated in the MSEL.
CONTROLLER DOCUMENT — NOT FOR PLAYER DISTRIBUTION (until delivered)

CONTROLLER DOCUMENT

INJECT I-01 Phase 1 — 0:10

MENDEZ LOCATED — CLONE CONFIRMED

FROM: Security Officer

TO: All Teams

DELIVERY: In-Person Report

CONTENT (Read aloud or hand to players):

"I found Carlos Mendez. He's in the Concourse A kitchen — SkyWay Catering prep area. He's been there since just after 7 o'clock, his coworkers confirm it. I showed him the alert. He has his badge right here on his lanyard. He says he didn't go anywhere near Door S-4 at 7:38 — he was elbow-deep in breakfast trays. His badge looks normal. Standard NCIA badge — photo, hologram, barcode, everything. He has no idea how his credential showed up at two doors at once. Oh, and one thing — I asked him about Wednesday. He says he had a normal shift. Nothing unusual. He used the Vendor Break Room on his morning break like he always does."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

Clone confirmed: Mendez was in the kitchen while "his badge" was at S-4. This eliminates the system glitch theory. The mention of "Wednesday" and the "Vendor Break Room" is a breadcrumb. If IT has been studying the PACS log, they should be starting to look at the Wednesday entries. The V-1 double-tap at 125 kHz is the capture event. Don't point it out — let them find it. If the team asks to take Mendez's badge for analysis: good instinct. A technical examination could confirm whether the card's 125 kHz credential was recently interrogated.

INJECT I-02 Phase 1 — 0:18

FREQUENCY ANALYSIS — THE CLONE'S SIGNATURE

FROM: IT Team Analysis (or Facilitator if IT hasn't identified this)

TO: All Teams

DELIVERY: Technical Briefing — IT presents to the room

CONTENT (Read aloud or hand to players):

"We've been going through the PACS log line by line. Here's what we found. Every access event we can confirm as the real Carlos Mendez — his 06:55 entry at S-4, his kitchen access, all his normal movements — reads at 13.56 MHz. That's the modern iCLASS frequency. Encrypted. Secure. But the duplicate events — the ones that triggered the alert — all read at 125 kHz. That's the legacy ProxCard frequency. Unencrypted. No authentication. Here's what that means: whoever cloned Mendez's badge didn't crack the encrypted 13.56 MHz credential. They captured the legacy 125 kHz credential number that his card also broadcasts for backwards compatibility with our older readers. A $25 device called a Proxmark3 can do this from a few inches away — you just stand near someone in a crowd, hold the device near their badge, and it captures the credential in about two seconds. Then you write it to a blank card. Total cost: under $30. The clone can only work on doors that still have 125 kHz readers. We have 12 of them."

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

This is the technical breakthrough. The frequency difference is the key evidence. If the IT team identified this themselves from the log before this inject — excellent. Award them recognition. If they didn't catch it, deliver this as a facilitator-led finding and use it as a teaching moment about reading PACS logs. The "12 legacy readers" number should make the team realize: every one of those 12 readers is vulnerable to the same attack. This isn't just about Mendez's badge — it's about every badge in the building.

INJECT I-03 Phase 1 — 0:26

THE WEDNESDAY CLUE (NUDGE — USE IF NEEDED)

FROM: Facilitator

TO: IT Team

DELIVERY: Quiet prompt to the IT table — not announced to the full room

CONTENT (Read aloud or hand to players):

The facilitator approaches the IT table quietly: "You've been focused on Thursday — the day of the alert. But the PACS log covers 72 hours. Go back to Wednesday. Look at Mendez's access pattern. Is there anything that stands out?" (The answer: Wednesday at 10:22:38 and 10:23:05 — two reads at Door V-1, both at 125 kHz, 27 seconds apart. Mendez's badge was read at the legacy frequency twice at the same door in under 30 seconds. That's not someone badging in and badging out — it's a Proxmark3 in close proximity triggering a phantom read on the 125 kHz antenna.)

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

ONLY use this inject if IT has not independently spotted the Wednesday V-1 anomaly by 0:26. If they've already found it, skip this inject. The double-tap is the "aha" moment. When IT spots it, they should realize: the badge was captured Wednesday morning in the Vendor Break Room. That's a public-adjacent space where Mendez takes his break. Someone sat near him, held a hidden reader close to his badge, and captured the credential. The second read (27 seconds later) is the Proxmark3 interrogating the card a second time to verify the capture. Security should ask: "Is there CCTV in the Vendor Break Room?" (Answer: yes, but V-1 is a public-adjacent area — anyone could have been sitting near Mendez without raising suspicion.)

INJECT I-04 Phase 2 — 0:35

THE CLONE'S PATH — HEADED FOR INFRASTRUCTURE

FROM: IT Team Analysis

TO: All Teams

DELIVERY: IT presents movement timeline to the room (use whiteboard)

CONTENT (Read aloud or hand to players):

"We've mapped the clone's complete movement through the building this morning: 07:38:12 — S-4 (125 kHz) — Clone enters sterile side through Concourse A boundary. 07:44:09 — M-3 (125 kHz) — Clone enters Maintenance Corridor B. This is back-of-house. 07:51:33 — E-2 (125 kHz) — Clone enters Electrical Room B. Stays inside. 08:03:17 — M-3 (125 kHz) — Clone exits through maintenance corridor. That's 12 minutes in E-2. 08:07:44 — S-6 (125 kHz) — Clone exits to non-sterile side via Concourse B boundary. Notice the pattern: they didn't go near the gates. They didn't go near the ramp. They didn't go anywhere near passengers or aircraft. They went straight to Electrical Room B — which houses the network switch closet for Concourse B — spent 12 minutes inside, and left through a different exit than they entered. This wasn't random. They knew exactly where they were going."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

The path tells the story: this was a targeted operation. Entry on one side, target in the middle, exit on the other side. Classic infiltration pattern. At this point, Ops should order an immediate physical inspection of Electrical Room B. IT should go with them. If nobody suggests it, push: "The clone was inside your network closet for 12 minutes. Has anyone gone to look at what's in there?"

INJECT I-05 Phase 2 — 0:43

CCTV — A FACE AND A BACKPACK

FROM: Security / CCTV Review Team

TO: All Teams

DELIVERY: In-Person Report

CONTENT (Read aloud or hand to players):

"We pulled CCTV from the cameras covering Door S-4 and Door S-6. Door S-4 at 07:38 — we see a male subject, approximately 5 foot 10, wearing a grey maintenance-style jumpsuit, black baseball cap, and a lanyard with a badge. The badge appears to be a plain white card — there's no photo, no hologram, no NCIA markings. He holds it to the reader and walks through. Door S-6 at 08:07 — same subject exits. He's now carrying a black backpack on one shoulder. We reviewed the S-4 entry footage again — he had the backpack going in too, but it was compact and flat. Coming out, it looks like it still has something in it but it's lighter. We do NOT recognize this individual. He's not in our employee or vendor photo database. The grey jumpsuit could pass for a maintenance worker at a glance, but it has no company logo or name patch. There is no camera in the maintenance corridor or inside Electrical Room B."

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

Key details for the team to catch: (1) The white badge = blank T5577 card. No NCIA badge looks like that. (2) The backpack was fuller going in — he brought equipment. (3) No camera in the corridor or E-2 = gap. (4) The grey jumpsuit with no logo = deliberately generic disguise. Security should capture the best still frame for law enforcement. They should also check: is there CCTV of the Vendor Break Room on Wednesday around 10:22? (Yes — but the capture device is concealed, so you'd only see someone sitting near Mendez.)

INJECT I-06 Phase 2 — 0:52

THE DISCOVERY — ROGUE WIRELESS ACCESS POINT

FROM: IT Inspection Team

TO: All Teams

DELIVERY: IT reports back from Electrical Room B (excited and alarmed)

CONTENT (Read aloud or hand to players):

"We found something. In Electrical Room B, behind the UPS battery backup unit — someone mounted a device. It's a modified TP-Link wireless router, about the size of a paperback book. It's connected via Ethernet cable to Port 23 on our Cisco Catalyst 2960 switch, and it's drawing power from a USB cable plugged into the UPS. The device has two external antennas. It's broadcasting a hidden SSID — we can only see it with a wireless survey tool. The signal is strong enough to reach the Concourse B parking structure. This is a rogue wireless bridge. Someone can sit in a car in the parking lot, connect to this device, and they're on our internal network. No VPN. No firewall. No authentication. They're just... in. The device MAC address is 50:C7:BF:8A:2E:1D — that's a TP-Link manufacturer prefix. It's been powered on for approximately 30 minutes — since Sorin installed it."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

THIS IS THE ANSWER. The badge clone was the delivery mechanism for a rogue network device. Physical access = cyber access. This is the physical-cyber convergence lesson. IT should immediately want to know: what can this device reach? Is anyone connected to it right now? Has any traffic passed through it? The next inject (I-07) answers the first question. The second and third are for the team to figure out (check wireless client associations, check switch port traffic counters). CRITICAL: Tell IT to document and photograph the device BEFORE touching it. It's evidence. If they yank it immediately, they lose forensic data.

INJECT I-07 Phase 2 — 1:00

THE TRUNK PORT — TOTAL NETWORK EXPOSURE

FROM: IT Team — Switch Analysis

TO: All Teams

DELIVERY: IT presents technical findings to the room

CONTENT (Read aloud or hand to players):

"We examined the switch configuration. Port 23 — the port the rogue AP is connected to — was originally configured as an access port on VLAN 60, which is the Baggage/OT VLAN. But it's been reconfigured. It's now a trunk port. For the non-IT folks: an access port only carries traffic for one VLAN — one network segment. A trunk port carries traffic for ALL VLANs. That means whoever connects to this rogue AP doesn't just see Concourse B operational traffic — they see everything: VLAN 10 — Server: Payment gateway, AODB, FIDS, Domain Controller. VLAN 20 — Admin: Executive workstations, HR, Finance. VLAN 30 — Security: Cameras, NVR, PACS controller. VLAN 40 — Retail: POS terminals, vendor systems. VLAN 60 — Baggage/OT: Baggage handling, gate management. VLAN 99 — Management: Switch admin interfaces, firewall management. Our entire network perimeter — firewalls, IDS, everything we invested in to keep people out — is completely irrelevant. This device is INSIDE the perimeter. It's like we built a fortress and someone put a door in the back wall. One more thing: the switch management credentials. To reconfigure that port from access to trunk, someone had to log into the switch CLI. That means they knew the password. I checked — we use the same management credentials on every IDF closet switch in the building. If they knew one password, they knew all of them."

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

This is the technical climax. The trunk port means total exposure. The shared switch credentials mean every closet is equally vulnerable. Key questions the team should be asking: — Has any traffic actually passed through the rogue AP yet? (Check port counters.) — Are there any wireless clients currently associated with the hidden SSID? (Check with a wireless survey tool.) — Did the switch generate any syslog messages when the port config changed? (Probably not — because they don't have syslog-to-SIEM configured for switch events.) — Can we see the switch config change in a running-config diff? (Yes — the config was modified at 07:53, which is within the 12-minute E-2 window.)

INJECT I-08 Phase 3 — 1:10

IDENTITY — CYBERCRIME AS A SERVICE

FROM: TSA / FBI Response

TO: Security / All Teams

DELIVERY: Phone Call — Facilitator role-plays FBI agent

CONTENT (Read aloud or hand to players):

"This is Special Agent Reeves with the FBI Cyber Division. We ran your CCTV capture through our facial recognition system. Potential match: Viktor Sorin, age 34, Ukrainian national. He entered the U.S. on a B-1 business visa three weeks ago. Sorin is flagged in the Interpol cybercrime database. He's not a hacker himself — he's an access broker. He works for a cybercrime-as-a-service operation based in Odesa. His specialty is physical infiltration. He gains access to facilities, installs hardware, and sells the resulting network access to clients — whoever's willing to pay. He's done this at two European airports, a port authority in Rotterdam, and a power utility in Poland. Same MO every time: clone a badge, plant a device, get out. Here's what concerns us: Sorin doesn't care what his clients do with the access. It could be data theft. It could be espionage. It could be pre-positioning for something worse. The access is for sale. And right now, your airport is the product. That rogue AP — if it's still live, we'd very much like to watch who connects to it."

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

Sorin's profile establishes this as a professional, repeatable attack against infrastructure targets. The FBI's interest in keeping the AP live ("we'd very much like to watch who connects") sets up the A/B/C decision in I-09. The phrase "your airport is the product" should land hard. The team isn't just dealing with a badge clone — they're dealing with a marketplace where access to their network is being sold to an unknown buyer.

INJECT I-09 Phase 3 — 1:18

DECISION POINT — WHAT TO DO WITH THE ROGUE AP

FROM: Facilitator

TO: All Teams

DELIVERY: Facilitator presents options to the room

CONTENT (Read aloud or hand to players):

The facilitator frames three options:

OPTION A — "PULL THE PLUG"
Disconnect the rogue AP immediately. Disable Port 23. The network is secured within minutes. But whoever hired Sorin will know the device was found — the access they purchased goes dark. They'll try another method. You've won this round, but the adversary adapts.

OPTION B — "HONEYPOT"
Leave the rogue AP connected but reroute its traffic to an isolated monitoring environment. Let the client connect. Capture their traffic, IP address, tools, and techniques. Feed them disinformation — dummy AODB data, fake PACS configs. Work with the FBI to trace the client. High intelligence value. But it requires IT sophistication and there's risk if the isolation isn't airtight.

OPTION C — "SILENT KILL"
Reconfigure Port 23 back to an access port on VLAN 999 — an unused, empty VLAN. The rogue AP still appears powered on and connected, but it can't reach anything real. The client doesn't know the device has been neutralized until they try to use it. Less intelligence than Option B, but also less risk. Buys time for law enforcement to work the Sorin angle.

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

Let the room debate. Each option has real trade-offs. Option A: Safe but loses intelligence opportunity. Ops will like this. Option B: Maximum intelligence but requires high technical skill and airtight isolation. FBI will advocate for this. Option C: Elegant compromise. IT may gravitate here. Risk: if the client does a connectivity check and finds the VLAN is dead, they'll know something changed. Push each side: "What if your isolation fails and the client gets real access?" (B) "What if Sorin has a second device you haven't found?" (A) "What if the client checks latency or ARP tables and realizes the VLAN is empty?" (C) Ops makes the final call.

INJECT I-10 Phase 3 — 1:26

SYSTEMIC VULNERABILITY ASSESSMENT

FROM: Facilitator

TO: All Teams

DELIVERY: Facilitated Discussion — use the whiteboard

CONTENT (Read aloud or hand to players):

The facilitator asks the team to identify every systemic failure that enabled this attack:

"This entire operation cost about $200 in hardware and exploited vulnerabilities that have been in your system for years. Let's map them: 1. How many 125 kHz legacy readers do you have? (12.) Cost to replace: approximately $500 per reader, $6,000 total. Cost of this incident: ? 2. Why do your modern iCLASS badges still broadcast a 125 kHz credential? Can you disable the legacy chip? (Yes — if all readers are upgraded.) 3. Port 23 was an open, unused port. Why wasn't it administratively disabled? Do you have a policy for disabling unused switch ports? 4. The switch credentials are the same on every closet. Why? What would per-device credentials with RADIUS authentication look like? 5. Is there 802.1X on any of your switch ports? (No.) What would 802.1X have done here? (Blocked the rogue AP from connecting.) 6. Did the switch generate an alert when the port config changed from access to trunk? (No.) Why not? 7. There's no camera in Electrical Room B. Why not? What other infrastructure rooms lack camera coverage? 8. Do you do periodic rogue wireless AP surveys? (Probably not.) What would that process look like?"

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

This is the wrap-up learning discussion. Each question maps to a specific remediation: 1. Replace legacy readers ($6K investment) 2. Disable 125 kHz on dual-frequency badges 3. Administratively disable all unused switch ports 4. Unique per-device credentials + RADIUS/TACACS+ 5. Deploy 802.1X port authentication 6. SNMP traps + syslog alerting for config changes 7. CCTV in all IDF closets and electrical rooms 8. Monthly rogue wireless surveys Write these on the whiteboard as the team identifies them. This becomes their takeaway remediation plan.

INJECT I-11 Phase 3 — 1:32

REMEDIATION PLANNING

FROM: Facilitator

TO: All Teams

DELIVERY: Facilitated Discussion

CONTENT (Read aloud or hand to players):

Each team addresses their area:

IT: Rogue AP disposition. 802.1X deployment timeline. Switch credential rotation. Port security policy. VLAN audit — are there other trunk ports that shouldn't be? Wireless survey schedule. SIEM integration for switch events.

Security: Badge audit — which vendors still have legacy-only credentials? Legacy reader replacement priority. Camera coverage for infrastructure rooms. TSA notification — access control breach. Physical security of IDF closets. Review of badge issuance process — are blank cards secured?

Ops: Airline communication — any service impact from switch reconfiguration? Timeline for legacy reader replacement (vendor coordination required). Temporary compensating controls — post guards at legacy-reader doors?

PIO: If this goes public — "Airport badges can be cloned for $25" — what's the statement? What's the proactive message? "We discovered and neutralized a sophisticated attack through our monitoring systems"?

■ **CONTROLLER NOTE (DO NOT READ TO PLAYERS):**

Push for specifics. "When will the legacy readers be replaced? Next week? Next month? Next fiscal year?" The answer reveals organizational priorities. The strongest takeaway for the exercise: this was a $200 attack that exploited backwards-compatible technology left in place for convenience. The fix is straightforward but requires investment and decision-making.

END OF MASTER INJECT DECK