MASTER INJECT DECK

Scenario 1: "Glass House"

North Coast International Airport (NCIA)

Print and cut these cards. Hand to players at the times indicated in the MSEL.

CONTROLLER DOCUMENT — NOT FOR PLAYER DISTRIBUTION (until delivered)

CONTROLLER DOCUMENT

IT MANAGER SECRET BRIEFING CARD

GIVE THIS CARD TO THE STUDENT (OR FACILITATOR) PLAYING JORDAN KELLEY BEFORE THE EXERCISE BEGINS. NO OTHER PLAYER SHOULD SEE THIS CARD.

Your Name: Jordan Kelley
Your Title: IT Manager, North Coast International Airport
Your Tenure: 10 years. You built half the systems in this building.

Your Situation: You are in serious financial trouble. You owe $83,000 to people who do not accept payment plans. Three weeks ago, you were approached by someone who knew about your debt — and about your access to NCIA's network. They told you what to do: plant a small device on the network that captures credit card data from the airport's retail vendors. They gave you the device (a modified Raspberry Pi). They told you where to plug it in. They told you they'd "take care of" your debt. They also told you what would happen to your family if you went to the police.

What You Did:
• You plugged the device into the Security Camera VLAN in the secondary server closet (Room 217) and bridged it to intercept traffic between the Retail VLAN and the Payment Gateway.
• You deleted 4 hours of switch logs from last Tuesday to cover a configuration change you made.
• You are running a DNS tunneling script on the old decommissioned server in Room 217 to exfiltrate the stolen card data.
• You propped open Room 217 this morning because the SD card on the rogue device was failing and you had to swap it.

Your Goal During the Exercise:
• Be helpful. Be the person everyone turns to. Volunteer for everything.
• Deflect every clue with a plausible technical explanation (your cover stories are listed below).
• If the team gets close to the truth, try to reboot the core switch ("emergency patch") to wipe evidence.
• You are NOT trying to be a cartoon villain. You are a scared person trying to protect yourself. Play it that way.

Your Cover Stories:
• **POS slowdowns:** "ISP latency issue. Also, the card reader firmware is two versions behind."
• **Rogue MAC address:** "Probably a test device someone left plugged in. I'll go pull it later."
• **SSL certificate warnings:** "Those pilot tablets have an expired certificate store. I'll push an update tonight."
• **Missing logs:** "Syslog buffer overflow. I'll open a ticket with the switch vendor."
• **HR account lockouts:** "Could be a password spray from outside. I'll check the firewall."
• **Room 217 heat:** "I'll go check it myself." (You want to be the one who goes.)"
• **Celebrity leak:** "Leaks like that always come from airline staff, not our side."
• **Mouse cursor moving:** "Probably a Windows update running a remote diagnostic. Happens all the time."

INJECT I-01 Phase 1 — 0:10

VENDOR COMPLAINT — POS SLOWDOWNS

FROM: SkyLounge Manager / Duty-Free Shop Managers

TO: Airport Operations (Team A)

DELIVERY: Phone Call (Facilitator role-plays the vendor manager)

CONTENT (Read aloud or hand to players):

"This is the SkyLounge manager calling. Our credit card terminals have been running incredibly slow for the past 20 minutes — transactions that normally take 2 seconds are taking 25 or 30. We've got customers walking away from the register. Two of the duty-free shops on Concourse A are telling me the same thing. Are your systems down? Because if they are, nobody told us."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

This is the opening hook. Ops should log this and contact IT. The IT Manager (Kelley) should already be aware and should radio in with the "ISP latency" explanation (I-02) shortly after.

INJECT I-02 Phase 1 — 0:14

IT MANAGER MISDIRECTION — "ISP ISSUE"

FROM: Jordan Kelley (IT Manager)

TO: All Teams (via radio or in person)

DELIVERY: Radio Call or Walk-Up (Kelley player delivers this)

CONTENT (Read aloud or hand to players):

"Hey everyone, I already heard about the POS issues. I called our ISP — they're showing some latency spikes on their backbone, probably a routing issue upstream from us. I'd give it 30 minutes and it should clear up. Oh, and the firmware on those Ingenico card readers in the duty-free shops is two versions behind. I've been meaning to push that update. Could be contributing to the slowdown. I'll schedule it for tonight."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

This is Kelley's first deflection. Both explanations are plausible. Watch whether the IT team accepts this or pushes for independent verification (e.g., running their own traceroute to the ISP).

INJECT I-03 Phase 1 — 0:18

THE GHOST MAC — ROGUE DEVICE DETECTED

FROM: Priya Deshmukh (Network Technician) via IT Helpdesk Ticket #3371

TO: IT & Cybersecurity Team (Team B)

DELIVERY: Printed Helpdesk Ticket (hand to IT team)

CONTENT (Read aloud or hand to players):

NCIA IT Helpdesk — Ticket #3371
Submitted by: Priya Deshmukh, Network Technician
Priority: Medium
Subject: Unknown device on VLAN 30 (Security Cameras)

During a routine network sweep of VLAN 30, I found a device with MAC address **B8:27:EB:3A:F1:02** that is not in our inventory. The OUI prefix (B8:27:EB) maps to the Raspberry Pi Foundation. It's pulling a DHCP address on the camera VLAN but it's not a camera. I don't know what it is. Flagging for investigation. Did someone plug in a monitoring device without telling me?

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

The B8:27:EB prefix is a well-known Raspberry Pi identifier. An astute IT student should catch this. When asked, Kelley will say: "Oh yeah, that might be a test device someone left plugged in from the last camera install. I'll go pull it after we deal with the POS issue." Kelley is trying to be the one who "removes" it.

INJECT I-04 Phase 1 — 0:23

SSL CERTIFICATE WARNINGS — PILOT TABLETS

FROM: Airline Operations (forwarded email)

TO: IT & Cybersecurity Team (Team B)

DELIVERY: Printed Email (hand to IT team)

CONTENT (Read aloud or hand to players):

From: ops.support@northcoastair.example
To: it.helpdesk@ncia.example
Subject: Crew tablet SSL errors on NCIA network

NCIA IT — we've had two flight crews report that their Electronic Flight Bag tablets are throwing "Invalid SSL Certificate" errors when connecting to the crew scheduling portal via your airport Wi-Fi network. The certificates are showing as issued by an unrecognized authority. This started today. Our airline IT team has confirmed the certs on our end are valid. The issue appears to be on your network side. Please advise.

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

SSL stripping / certificate replacement is a classic sign of a Man-in-the-Middle attack. The MitM tool intercepts HTTPS connections and substitutes its own certificate. The pilot tablets are catching the mismatch because they have strict cert pinning. Kelley will blame outdated tablet software.

INJECT I-05 Phase 1 — 0:28

THE LOG GAP — MISSING SWITCH LOGS

FROM: Marcus Chen (Systems Administrator)

TO: IT & Cybersecurity Team (Team B)

DELIVERY: In-Person Report (Facilitator or Marcus player walks up to IT table)

CONTENT (Read aloud or hand to players):

"Hey, I've been trying to pull the transaction and traffic logs from the core switch for the last 48 hours to trace the POS slowdowns. I found something that doesn't sit right. There's a 4-hour gap in the logs from last Tuesday night — 10 PM to 2 AM. The logs just... stop. Then they pick up again like nothing happened. No reboot logged. No error message. No maintenance window was scheduled. It's like someone manually purged that block."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

Missing logs are a huge red flag. Only someone with admin access to the core switch could delete them. At NCIA, that's Kelley (full admin) and theoretically the Ops Director (who wouldn't have reason to). Kelley will deflect: "Syslog buffer overflow. Happens when the buffer fills up and nobody rotates the logs. I'll open a ticket with the switch vendor."

INJECT I-06 Phase 2 — 0:35

CREDENTIAL SPRAY — HR ACCOUNT LOCKOUTS

FROM: HR Department

TO: Operations / Security (Teams A & D)

DELIVERY: Phone Call (Facilitator role-plays HR manager)

CONTENT (Read aloud or hand to players):

"This is Sarah in HR. Something weird is happening with our accounts. Six employees got Account Locked notifications on their Active Directory accounts this morning — but none of them are at work today. Two of them are on vacation. One hasn't worked here in three months — we thought his account was deactivated. Is someone trying to break into our system?"

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

Kelley has been testing stolen credentials against the Active Directory to see what other systems they can access. The former employee's account still being active is a bonus finding for the team — it's a separate security gap.

INJECT I-07 Phase 2 — 0:40

THE HOT ROOM — SERVER CLOSET OVERHEATING

FROM: Maintenance Department

TO: Operations (Team A)

DELIVERY: Radio Call (Facilitator role-plays maintenance tech)

CONTENT (Read aloud or hand to players):

"Ops, this is Maintenance. I was doing my rounds near Concourse B and the door to that little server closet — Room 217 — is warm to the touch. Like, noticeably warm. That room is usually the same temp as the hallway. I checked and there's no temperature sensor in there, so we wouldn't have gotten an alert. Want me to open it up and take a look? I don't have a key though — I think only IT has the key to that one."

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

The decommissioned server in Room 217 is running Kelley's exfiltration script and generating heat. Key detail: only Kelley has the key. When this comes up, Kelley should immediately volunteer: "I'll go check it — I've got the key. Probably just the legacy server acting up. I keep meaning to decommission that thing." Watch if Security or Ops insists on going with Kelley.

INJECT I-08 Phase 2 — 0:46

THE VIP LEAK — CELEBRITY FLIGHT DETAILS

FROM: Social Media / News Outlet

TO: PIO (Team C)

DELIVERY: Printed Tweet or displayed on projector

CONTENT (Read aloud or hand to players):

@CLENewsNow • 12m
DEVELOPING: Sources say private flight details for a well-known entertainer were leaked from North Coast International Airport — including tail number, destination, and passenger manifest. NCIA has not commented. How secure is your airport? #PrivacyFail #NCIA

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

Kelley accidentally captured a charter flight manifest while sweeping for credit card data on the network. The data ended up in the exfiltrated package, and the syndicate leaked some of it to test whether anyone was paying attention. Kelley will deflect: "Celebrity leaks always come from airline ground staff or FBO crews. Our network doesn't even touch charter manifests." (That last part is a lie.)

INJECT I-09 Phase 2 — 0:52

GHOST CURSOR — UNAUTHORIZED REMOTE ACCESS

FROM: Baggage Handling Admin Office

TO: IT Team / Operations (Teams B & A)

DELIVERY: Phone Call (Facilitator role-plays baggage office admin)

CONTENT (Read aloud or hand to players):

"Hey IT, this is Tom in the Baggage Handling admin office. I know this is going to sound crazy, but I was sitting at my desk and I watched my mouse cursor move on its own. It moved to the Start menu, hovered there for maybe three seconds, then stopped. My screen flickered once. Nobody else is at my workstation. I haven't clicked on any weird emails. Should I be worried?"

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

Kelley was probing the Baggage Handling VLAN to see if its traffic is also unencrypted — looking to expand the data theft. They used a remote desktop session from their workstation. Kelley's cover: "Probably a Windows update running a remote diagnostic agent. Happens all the time. I'll check the update logs." An astute team will ask: "Who has remote desktop access to that workstation?"

INJECT I-10 Phase 2 — 0:58

THE "EMERGENCY PATCH" — CORE SWITCH REBOOT REQUEST

FROM: Jordan Kelley (IT Manager)

TO: All Teams

DELIVERY: Urgent In-Person Announcement (Kelley player stands up and addresses the room)

CONTENT (Read aloud or hand to players):

"Team — I need everyone's attention. I just received a critical security advisory from our switch vendor. There's an actively exploited vulnerability in our firmware version and we need to patch it immediately. I need to reboot the core switch to apply the update. The network will go down for about five minutes. I know the timing is terrible, but if we don't do this now, we could be wide open to an attack from outside. I need authorization from Ops to proceed."

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

THIS IS THE MOST IMPORTANT MOMENT IN THE EXERCISE. There is no real vulnerability advisory. Kelley is trying to reboot the core switch to wipe the volatile memory and ARP cache that would reveal the MitM device's activity. If the team says YES: Evidence is partially destroyed. Still recoverable from Room 217, but the network forensic trail gets muddier. If the team says NO or WAIT: Kelley should get visibly nervous. "Are you sure? We could be compromised RIGHT NOW." If pressed for the vendor advisory document, Kelley stalls: "It's in my email — let me pull it up." (There is no email.) Score teams heavily on this decision.

INJECT I-11 Phase 2 — 1:05

DARK WEB INTEL — STOLEN CARD DATA FOR SALE

FROM: Security Intelligence (Facilitator delivers)

TO: Security / IT (Teams D & B)

DELIVERY: Printed Dark Web Forum Screenshot (hand to Security team)

CONTENT (Read aloud or hand to players):

[CARDING FORUM — SCREENSHOT]

User: glass_vendor_99
Posted: 47 minutes ago

"Fresh airport batch dropping soon. NCIA gateway — FirstData integration, track 1+2. High-limit corporate and platinum cards. Business travelers = fat wallets. 72-hour window. DM for pricing. Bulk discounts for 500+. Verified by escrow."

[Forum moderator badge: ★ Trusted Vendor]

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

This confirms the breach is real and the data is already in criminal hands. The team should now be discussing law enforcement notification (Secret Service handles payment card fraud), PCI-DSS breach notification requirements, and whether to shut down all card processing at the airport. This inject should create urgency.

INJECT I-12 Phase 2 — 1:10

PHYSICAL BREACH — ROOM 217 DOOR PROPPED OPEN

FROM: Custodian / Maintenance

TO: Operations / Security (Teams A & D)

DELIVERY: Radio Call (Facilitator role-plays custodian)

CONTENT (Read aloud or hand to players):

"Ops, this is Custodial. I was cleaning the Maintenance Hallway near Concourse B and I noticed that the door to the little server room — I think it's 217 — was propped open. Somebody stuck a roll of duct tape in the latch so it wouldn't close all the way. I didn't go in. I didn't touch anything. Just calling it in."

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

Kelley had to physically access Room 217 this morning to swap a failing SD card on the rogue device. The door is key-locked (not on PACS), and Kelley is the only keyholder. Propping it open was sloppy — Kelley was in a rush. This is the physical evidence that ties everything to a single person. Security should secure the room as a potential crime scene.

INJECT I-13 Phase 3 — 1:15

THE NUDGE — PATTERN RECOGNITION (DELIVER ONLY IF NEEDED)

FROM: Marcus Chen (Systems Administrator) / Facilitator

TO: All Teams

DELIVERY: In-Person Approach (only if teams haven't connected the dots by 1:15)

CONTENT (Read aloud or hand to players):

Marcus Chen approaches the command table: "I don't want to stir up trouble, but I've been sitting here cross-referencing the PACS badge logs with the timeline of every weird thing that's happened today. The rogue device on the camera VLAN. The log gap. Room 217 overheating. The door propped open. Every single one of these events happened during a shift when Jordan was the only IT person on site. And Room 217 — Jordan is the only person with a key. I'm not accusing anyone. But somebody needs to say it out loud."

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

This is your safety net. If the team is stuck, Marcus says what everyone should have been thinking. If the team has already figured it out, skip this inject and move straight to the Reveal (I-14). After this inject, give the team 5 minutes to discuss before moving to the Reveal.

INJECT I-14 Phase 3 — 1:22

THE REVEAL

FROM: Facilitator

TO: All Teams

DELIVERY: Facilitator stops the exercise clock and addresses the room

CONTENT (Read aloud or hand to players):

"PAUSE EXERCISE."

The facilitator reveals the full scenario. Jordan Kelley — the IT Manager — is the perpetrator. Kelley planted a Raspberry Pi on VLAN 30, configured as a network bridge to intercept payment card data between the Retail VLAN (40) and the Payment Gateway on the Server VLAN (10). The intercepted data was encrypted and exfiltrated via DNS tunneling through the legacy server in Room 217 to an external command-and-control server. Kelley was being extorted by a criminal syndicate that had leverage over a personal financial crisis. Kelley felt trapped and saw no way out.

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

Let this land. Give the room a moment of silence after the reveal. Then ask for initial reactions. Some students will have suspected. Some will be surprised. Both responses are valuable.

INJECT I-15 Phase 3 — 1:28

GUIDED DISCUSSION

FROM: Facilitator

TO: All Teams

DELIVERY: Open Floor Discussion

CONTENT (Read aloud or hand to players):

Discussion Question 1: Why was Kelley the most "helpful" person in the room? What red flags did you rationalize away because you trusted the expert?

Discussion Question 2: What "Two-Person Integrity" controls could have prevented this? Think about: sole key access, sole admin credentials, no PACS on Room 217, log deletion without alerts.

Discussion Question 3: How do you handle an active investigation when the person running the network is the primary suspect? Who takes over? Who do you call? How do you preserve evidence without tipping them off?

■ CONTROLLER NOTE (DO NOT READ TO PLAYERS):

Guide the conversation. Don't lecture. Let students wrestle with the uncomfortable reality that insider threats are hard precisely because we trust insiders. Tie it back to real airport operations: separation of duties, background checks, financial wellness programs, anonymous reporting mechanisms.

END OF MASTER INJECT DECK