CLASSIFIED: Investigation Evidence

Cyber Academy Middle School — Account Lockout Incident

⚠ Your Mission

Several student accounts have been locked out due to failed login attempts. The IT department has gathered evidence. Your detective team must investigate.

Questions to answer:

- Is this a security incident or coincidence?
- What happened and why?
- What should the school do next?

Document A: Login Attempt Logs

Source: School authentication server

```
USERNAME        DATE        TIME       ATTEMPTS   STATUS

jsmith2025     11/18/25    3:45 AM      12       LOCKED
mgarcia2025    11/18/25    3:47 AM      15       LOCKED
kchen2025      11/19/25    3:44 AM       8       LOCKED
rjones2025     11/19/25    3:46 AM      10       LOCKED
tpatel2025     11/20/25    2:15 PM       3       SUCCESS
akim2025       11/20/25    8:30 AM       1       SUCCESS
bwilson2025    11/21/25    3:45 AM       9       LOCKED
```

Document B: Password Security Analysis

Source: IT Department security audit

```
USERNAME        COMPLEXITY   LAST CHANGED   PATTERN DETECTED

jsmith2025       WEAK         8/15/25       Birthday-based (Jake0823)
mgarcia2025      WEAK         8/15/25       Pet name + year (Buddy2025)
kchen2025        WEAK         8/15/25       School name + numbers (CyberAcad123)
rjones2025       MEDIUM       10/01/25      Random with substitutions (R@nd0m99)
bwilson2025      WEAK         8/15/25       Favorite team (Lakers24)
tpatel2025       STRONG       11/01/25      Passphrase (correct-horse-battery)
akim2025         STRONG       11/15/25      Random generated
```

Document C: Social Media Activity (Public Posts)

Source: Publicly visible student social media

@JakeSmith_2025 — August 23: “Best birthday ever!   Thanks everyone!”

@Maria_Garcia — September 5: “My dog Buddy is the cutest! ” [photo of golden retriever]

@KatieChen — October 10: “Cyber Academy spirit week! Go Eagles! #CyberAcad123”

@RJ_Jones — November 1: “Changed my password to something actually random this time lol”

@BrandonW — October 28: “Lakers game tonight! Lebron is the GOAT #Lakers24ever”

@tanyapatel — November 10: “Finally using a password manager like my mom keeps telling me”

Document D: Network Analysis

Source: School firewall and network monitoring

```
FAILED LOGIN ATTEMPTS - SOURCE ANALYSIS


IP Address:        203.45.67.89
Geolocation:       Outside school district (unknown location)
User Agent:        Mozilla/5.0 (compatible; AutoBrute/2.1)
Connection Type:   VPN/Proxy detected

TIME PATTERN ANALYSIS:
  11/18 attempts: 3:45 AM - 3:47 AM (2 minute window)
  11/19 attempts: 3:44 AM - 3:46 AM (2 minute window)
  11/21 attempts: 3:45 AM (single timestamp)

EXCEPTION:
  tpatel2025 login (SUCCESS): 2:15 PM, School IP, Normal browser
  akim2025 login (SUCCESS): 8:30 AM, School IP, Normal browser
```

Document E: IT Help Desk Tickets

Source: School IT support system

Date	Student	Issue	Resolution
11/18	Jake S.	“Can’t log in, says account locked”	Password reset issued
11/18	Maria G.	“Account locked out this morning”	Password reset issued
11/19	Katie C.	“Locked out again! Didn’t do anything”	Password reset, advised stronger password
11/19	Ryan J.	“Account locked, I just changed my password last month!”	Password reset issued
11/21	Brandon W.	“Same thing happened to me now”	*Pending investigation*

Document F: Student Interview Notes

Source: Brief conversations with affected students

Jake S.: "I didn't try to log in at 3 AM! I was sleeping!"

Maria G.: "This is so annoying. I have a really easy password so I don't forget it."

Katie C.: "I use the same password for everything, is that bad?"

Ryan J.: "I actually tried to make mine harder to guess. Why did this still happen to me?"

Brandon W.: "I post about the Lakers all the time. You think someone guessed my password from that?"

Investigation Tips

- Look for patterns across documents
- Consider what's similar AND what's different
- Think about what someone would need to know to do this
- Ask: What does the evidence show? What's still uncertain?

Security Detective Teams — NICE K12 2025