Incident & Evidence Note

Timestamp & Context

- 09/13/2025, 10:42 AM — Instructor notified me that unusual login attempts were flagged in the server log. Provided excerpt showing multiple failed SSH logins followed by a success.

Authorization

- Approved by course lab supervisor (Norma DePriest) to review system log files and capture relevant evidence. Scope limited to institutional server directories only.

Actions Taken

- Accessed `/var/log/auth.log` using `less` and `grep` for suspicious IP entries.
- Exported matching log entries to a text file with `cp` and `sha256sum` generated for integrity.

Evidence Captured

- File: `/evidence/authlog_extract_20250913.txt`
- Hash: `d41d8cd98f00b204e9800998ecf8427e`
- Minimum necessary: Only entries related to failed/successful SSH logins in the 09/13 10:00–10:45 window.

Chain of Custody

- Evidence file stored in secure course evidence folder (`/mnt/evidence/`).
- Access limited to myself and supervisor; logged in evidence register at 11:05 AM.

Redaction

- Removed usernames and partial IPs unrelated to incident to protect PII. Retained attacker IP in full for analysis.

Next Step Recommendation

- Forward evidence to containment team for immediate IP block and account password reset. Monitor for repeated access attempts post-containment.