CS50 Cybersecurity Final Project

1. Required Information

Title: Snowflake Breach – Credential-Based Cloud Compromise
Name: Fernando Corrêa da Silva Júnior
Location: Blumenau – SC, Brazil
edX Username: Fcorrea007
GitHub Username: Fcorrea002
Recording Date: *Insert before publishing*
Incident Date: May 2024
CVE: Not applicable (credential misuse; no software vulnerability)

Why I chose this topic (for verbal introduction):

Because the Snowflake breach illustrates core CS50 Cybersecurity concepts: identity security, authentication failures, cloud security responsibilities, and how credential-based attacks can impact global organizations.

2. What Is Snowflake?

- Cloud-based data warehouse platform
- Used by major enterprises, financial institutions, SaaS companies
- Central hub for storing large volumes of sensitive operational and customer data
- Breach affected multiple organizations across different industries
- Demonstrates how cloud identity weaknesses can scale damage across tenants

3. Summary of the Incident

- Attackers used stolen credentials acquired from infostealer malware
- Multi-Factor Authentication (MFA) was not enabled on affected accounts
- Snowflake environments were accessed through valid username/password
- Attackers performed systematic data extraction across multiple customers
- Breach exposed sensitive datasets such as financial records and user information

4. Attack Timeline

1. Early 2024: Infostealer malware infects user machines
2. Credentials and session tokens harvested

3. Attackers begin testing access on Snowflake customer accounts
4. Unauthorized access successful due to lack of MFA
5. Large-scale automated SQL queries used to exfiltrate data
6. Snowflake and Mandiant publish security advisories (May 2024)
7. Organizations begin emergency rotation of credentials

5. Authentication Failures

- Password-only authentication allowed
- No IP, device, or location verification
- Long-lived sessions; limited session rotation
- Users not enforced under centralized identity governance
- Lack of mandatory MFA created a single point of failure

6. Technical Breakdown

- Attack was not a vulnerability; it was a credential compromise
- Stolen cookies and tokens reused to maintain sessions
- Password reuse increased attacker success rate
- SQL queries executed programmatically for rapid extraction
- API keys and service accounts also targeted
- Shows how weak IAM can bypass strong infrastructure security

7. Impact

- Dozens of global organizations affected
- Customer personal and financial data leaked
- Potential regulatory penalties (GDPR, LGPD, PCI, etc.)
- Incident forced Snowflake to update its security recommendations
- Triggered internal investigations and third-party audits
- Demonstrated cloud supply-chain dependency risks

8. Recommendations

Identity & Access Management (IAM)

- Enforce mandatory MFA for all accounts
- Require SSO with identity federation (Azure AD, Okta, etc.)
- Remove password-only authentication

Monitoring & Detection

- Continuous monitoring for suspicious login behavior
- Alerting for abnormal SQL query patterns
- Session token rotation policies

Architecture

- Apply Zero Trust principles
- Enforce least privilege on both users and service accounts
- Network-level conditional access

9. Conclusion

- Snowflake breach was entirely preventable
- Root cause: IAM failures, not software flaws
- Reinforces CS50 Cybersecurity lessons:
    - Importance of MFA
    - Credential hygiene
    - Cloud shared responsibility model
    - Monitoring and detection
- Demonstrates how identity attacks can bypass even strong cloud platforms

10.Sources

- The Hacker News – “Snowflake Warns of Customer Data Theft” (2024)
- SecurityWeek – “Snowflake Investigates Unauthorized Access”
- Snowflake Official Security Advisory – May 2024
- Mandiant Threat Intelligence Report on Snowflake Incident
- Recorded Future & Hudson Rock malware credential data