

1 Security in the Wild: Incident Analysis

Overview In this assignment, you will investigate a recent real-world security incident and analyze it using concepts from class.

Your goal is **not** to explain every technical detail. Your goal is to use security concepts to reason about what happened, who was involved, what went wrong, and why the incident mattered.

Submission Format Submit your work as a separate written analysis of approximately **2–3 pages**. The page count excludes your attack tree and your references. Upload this write-up separately as a PDF to Gradescope. You may use any format you like, but your submission must be readable and well-organized.

Choosing an Incident Choose a real-world cybersecurity incident that occurred between **2021 and the present**.

Your incident must:

- involve a specific security event affecting a real organization, system, application, or group of users;
- provide enough public information to identify important assets, an adversary (or adversary type), and at least one plausible attack path; and
- be supported by credible sources.

Possible incident types include ransomware attacks, data breaches, account compromises, supply-chain attacks, exploitation of software vulnerabilities, social engineering incidents, or attacks on infrastructure.

Do not choose a purely theoretical vulnerability with no associated security incident.

Source Requirements Use at least **two credible sources**. At least one source should be a technical or primary source when one is available.

Possible source types include:

- CISA or other government advisories;
- vendor or organization incident reports;
- security research reports;
- MITRE ATT&CK;
- CVE/NVD entries;
- reputable news organizations.

In your writing, clearly distinguish between:

- facts established by sources;
- conclusions you infer from those facts; and
- assumptions made because public information is incomplete.

2 Required Content

1) **Incident Snapshot** Provide a concise summary of your selected incident in **3–5 sentences**. Include:

- the organization or system affected;
- approximately when the incident occurred;
- what the attacker did; and
- the major consequence of the incident.

2) **Assets and Security Policies** Identify **two important assets** involved in the incident.

For each asset, include:

- the asset itself;
- a specific security policy or expectation that should have protected it; and
- the primary security property most closely related to that policy: **Confidentiality, Integrity, Availability, Authentication, or Accountability**.

3) **Adversary Model** Describe the adversary based on available evidence. Address:

- who the adversary was (or the most likely adversary type);
- the likely motivation or goal;
- capabilities, resources, or access the adversary appeared to have; and
- at least one explicit assumption you are making because information is incomplete.

4) **From Threat to Harm** Describe one important path through the incident using the structure:

Threat → Vulnerability or Weakness → Attack → Harm

Explain this path at a level supported by your sources. Full technical reconstruction is not required.

5) **Attack Tree** Choose one important attacker goal from your incident and construct a small attack tree showing plausible ways to achieve that goal.

Your attack tree must:

- include a clearly labeled **root goal**;
- contain approximately **6–10 nodes**;
- include at least two possible paths to the root goal;
- expand at least one path beyond the first level;
- identify AND and OR relationships where appropriate; and
- clearly identify leaf nodes.

The tree does **not** need to exactly reproduce the historical attack; it should represent plausible attacker paths.

6) MITRE ATT&CK Mapping Identify one MITRE ATT&CK technique or sub-technique relevant to your incident. Include:

- technique name and ID;
- tactic; and
- a brief 1–2 sentence justification of why it applies.

If you cannot identify an appropriate ATT&CK mapping, explain why instead of forcing an incorrect match.

Optional: If the incident involves a specific CVE or CWE, you may identify it and briefly explain how it relates to the incident. A CVE/CWE is **not required**.

7) Risk Analysis Evaluate the risk as if you were assessing it **before the incident** occurred. Include:

- likelihood rating (**Low, Medium, or High**) with reasoning;
- impact rating (**Low, Medium, or High**) with reasoning;
- overall prioritization based on likelihood and impact, including key assumptions; and
- a brief note on what should have been evaluated differently in light of what actually happened.

8) Reflection Include one short reflection on something that surprised you, interested you, or changed how you think about cybersecurity.

9) References List all sources used. For each source, provide enough information for someone else to find it.