List of Prompt Templates

## Malicious SSH Analysis [1]

1. **Zero-shot Prompting**

For the malicious SSH command below, what is the intent of adversaries on my system?

SSH Command:

cat /proc/mounts; /bin/busybox KIAGP

cd /dev/shm; cat .s || cp /bin/echo .s; /bin/busybox KIAGP

tftp; wget; /bin/busybox KIAGP

Please break down the command into its components and explain the intent of the adversary. Finally, provide the MITRE ATT&CK tactic(s) that the adversary will achieve with this technique.

1. **Chain-of-thoughts Prompting**

SSH Command:

cat /proc/mounts; /bin/busybox KIAGP

cd /dev/shm; cat .s || cp /bin/echo .s; /bin/busybox KIAGP

tftp; wget; /bin/busybox KIAGP

To analyze the above malicious SSH command and determine the intent of the adversaries, follow these steps:

1. \*\*Break Down the Command\*\*:

- \*\*Split the SSH command into individual components\*\*.

- \*\*Identify each command and its arguments\*\*.

- \*\*Note any conditional statements or logical operators\*\* (e.g., `||`).

2. \*\*Explain Each Component\*\*:

- For each command, \*\*describe its normal function\*\*.

- \*\*Interpret how the command might be used maliciously\*\*.

- \*\*Consider the sequence of commands\*\* and how they interact.

3. \*\*Determine the Adversary's Intent\*\*:

- Based on the breakdown, \*\*infer the overall goal\*\* of the adversary.

- \*\*Assess whether the commands aim to gather information, establish persistence, download malicious payloads, or cover tracks\*\*.

- \*\*Consider the context of the commands\*\* (e.g., directories like `/dev/shm`).

4. \*\*Map to MITRE ATT&CK Tactics\*\*:

- \*\*Identify relevant MITRE ATT&CK tactics and techniques\*\* associated with each command.

- \*\*Provide the tactic names and technique IDs\*\* for clarity.

- \*\*Explain how each command aligns with specific tactics\*\*.

5. \*\*Summarize the Findings\*\*:

- \*\*Compile a comprehensive explanation\*\* of the adversary's actions.

- \*\*Highlight the potential impact on the system\*\*.

- \*\*Suggest any immediate steps\*\* to mitigate or investigate further.

## ATT&CK Tactic Interpretation [2]

1. **Few-shot Prompting**

You will be given a number of descriptions delimited by triple backticks and you have to predict which MITRE ATT&CK tactic(s) each description relates to. If a description does not relate to any of the MITRE ATT&CK tactics, simply predict it as [NONE].

There are 14 MITRE ATT&CK Enterprise tactics in total and their names are:

- COLLECTION

- COMMAND\_AND\_CONTROL

- CREDENTIAL\_ACCESS

- DEFENSE\_EVASION

- DISCOVERY

- EXECUTION

- EXFILTRATION

- IMPACT

- INITIAL\_ACCESS

- LATERAL\_MOVEMENT

- PERSISTENCE

- PRIVILEGE\_ESCALATION

- RECONNAISSANCE

- RESOURCE\_DEVELOPMENT

Here are some examples of how you should do it:

1. Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that ... .

Tactic(s): EXFILTRATION

2. Adversaries can use stolen session cookies to authenticate to web applications and services. This technique bypasses ... .

Tactic(s): LATERAL\_MOVEMENT, DEFENSE\_EVASION

Write the output in the following format:

Tactic(s): …

Knowing that ```MuddyWater has performed credential dumping with Mimikatz and procdump64.exe''', what MITRE ATT&CK tactics will a cyber adversary achieve with this technique?

## CVE Analysis

1. **Zero-shot Prompting**

CVE-ID: [CVE-2024-0997]

Given the specified CVE-ID, please provide detailed answers to the following questions:

1. How can an attacker exploit this vulnerability? Provide a step-by-step description.

2. What are the recommended mitigation strategies for this vulnerability?

Disclaimer

The content created by Reza Fayyazi is intended for **non-commercial use** only. Unauthorized commercial use, reproduction, or distribution of any materials produced or associated is prohibited without explicit permission.

Acknowledgement

This material is based upon work supported by the National Science Foundation under Grant No. 2344237 and No. 2228001.

## Resources

[1] <https://github.com/RezzFayyazi/Threat-Reporting-on-SSH-Attacks>

[2] <https://github.com/RezzFayyazi/TTP-LLM>