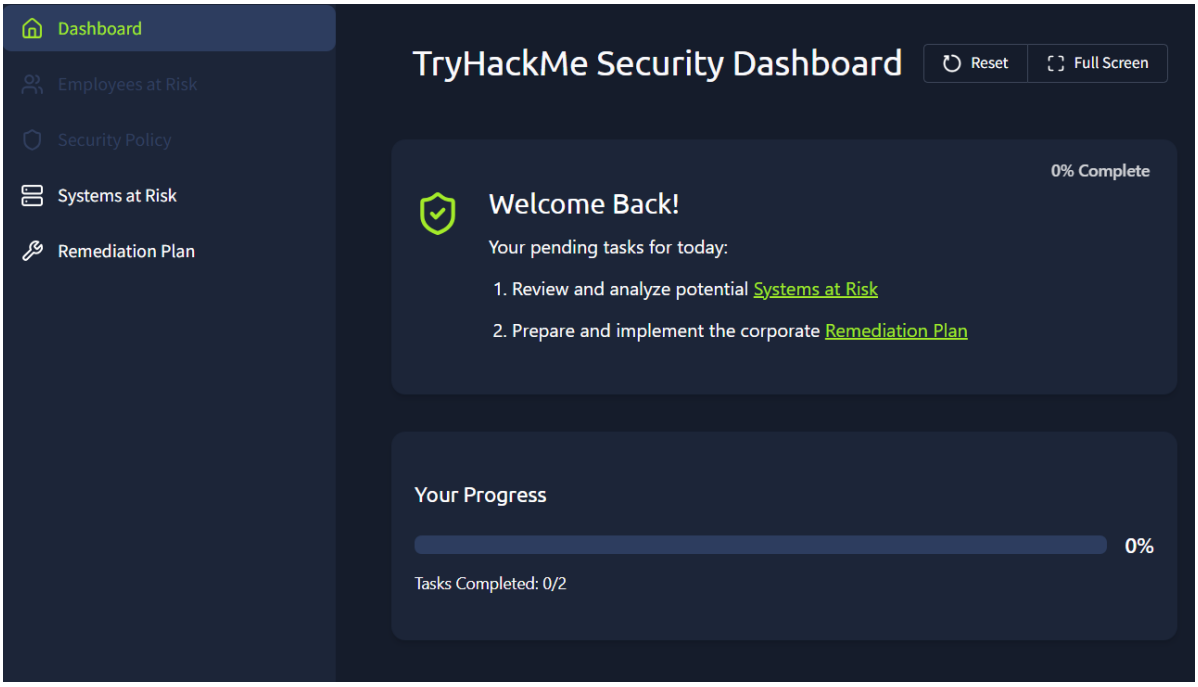
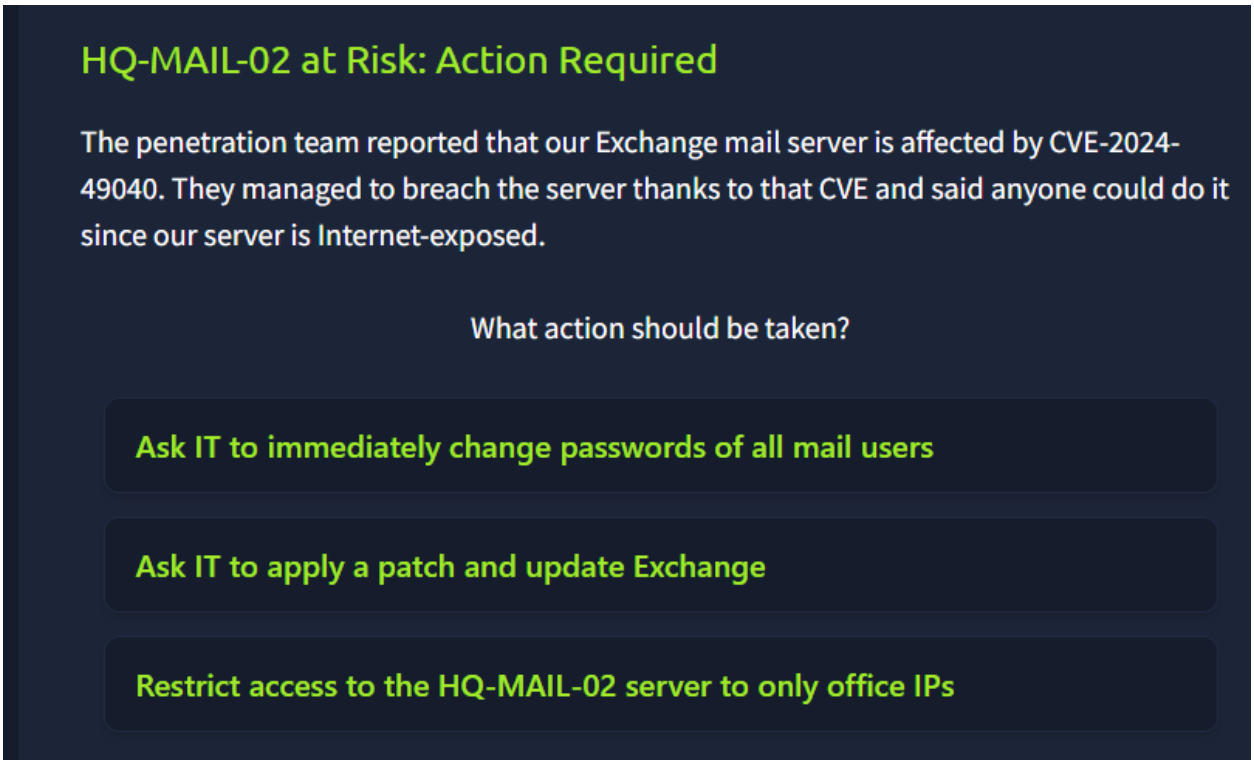
SYSTEMS RISK AND REMEDIATION CHALLENGE 2025/12/18

Objective: For this lab, continue your SOC analyst journey at TryHackMe. This time, decide what to do with the **Systems at Risk** and choose the best measures to protect your systems at the **Remediation Plan** tabs.



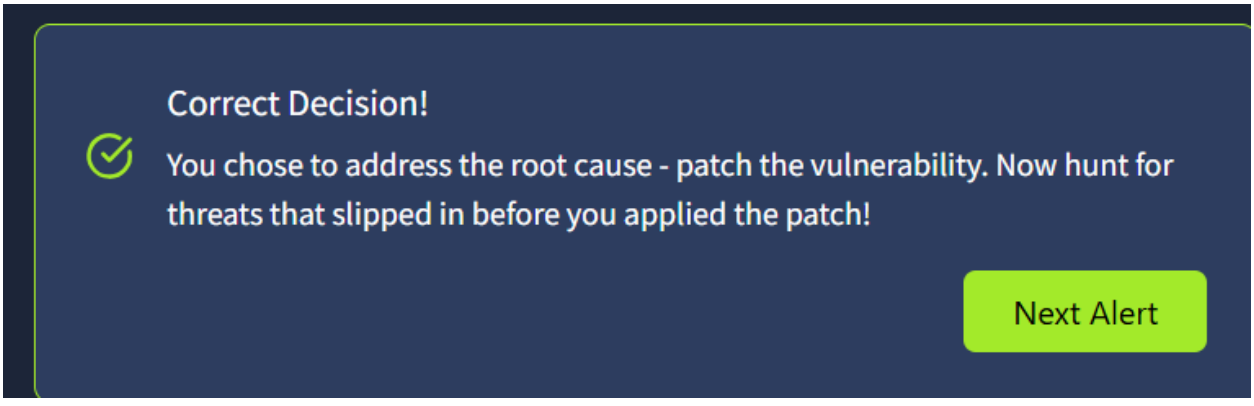
STEP 1: What flag did you receive after completing the "Systems at Risk" challenge?



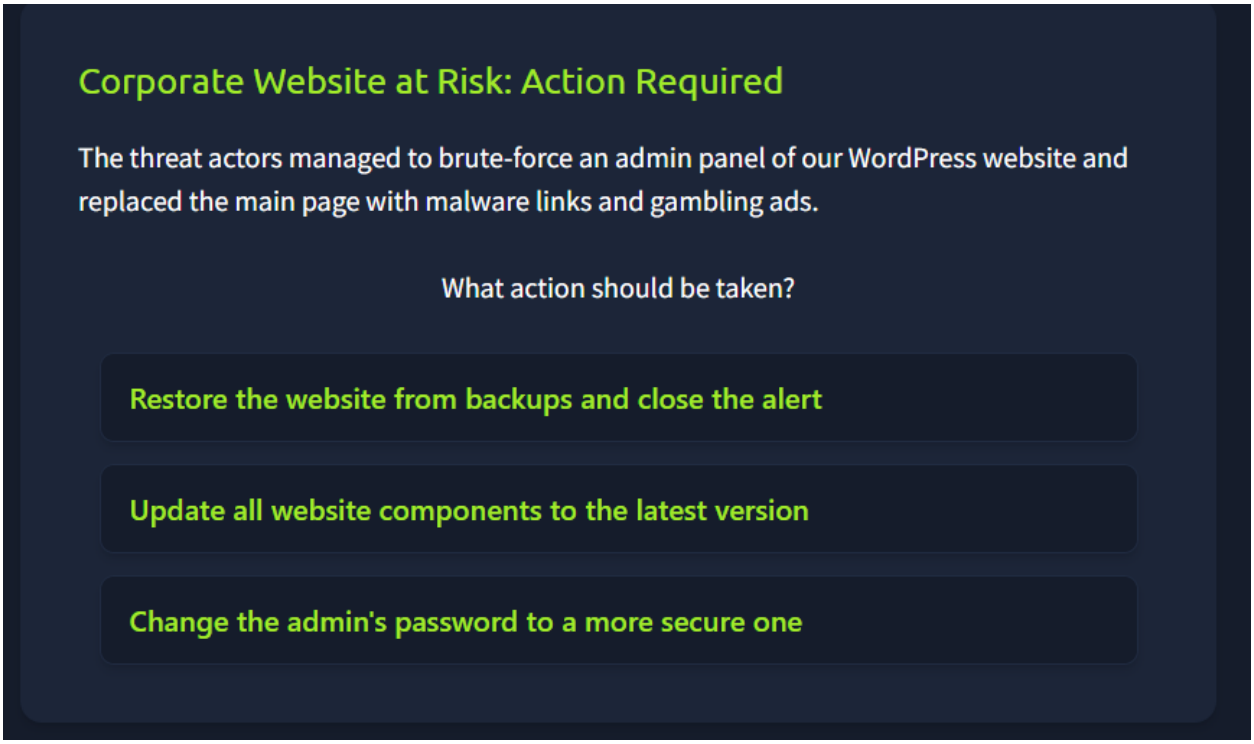
I looked up the vulnerability CVE-2024-49040

Description - Microsoft Exchange Server Spoofing Vulnerability.

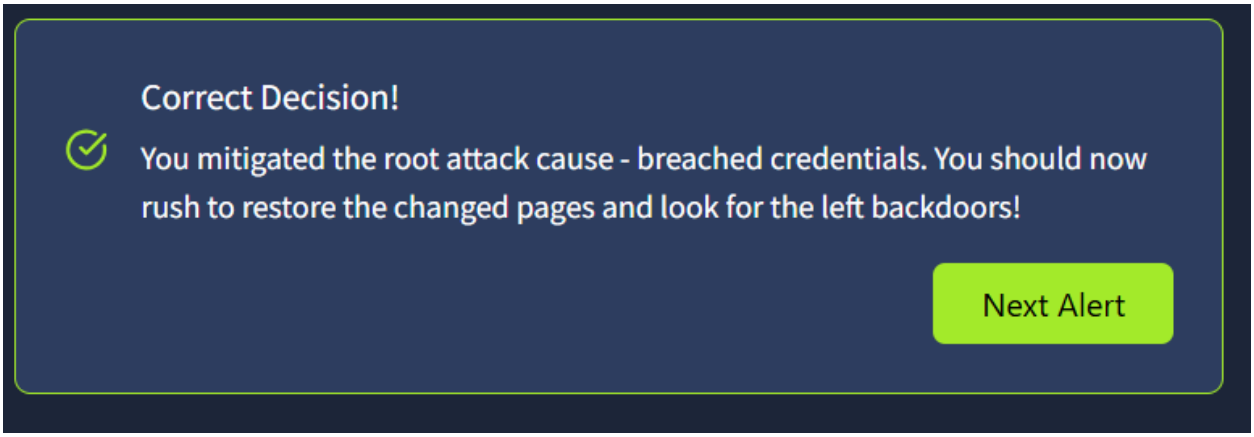
Since this was an attack done by our pentest team, the best option would be to go with Asking IT to apply a patch and update Exchange.



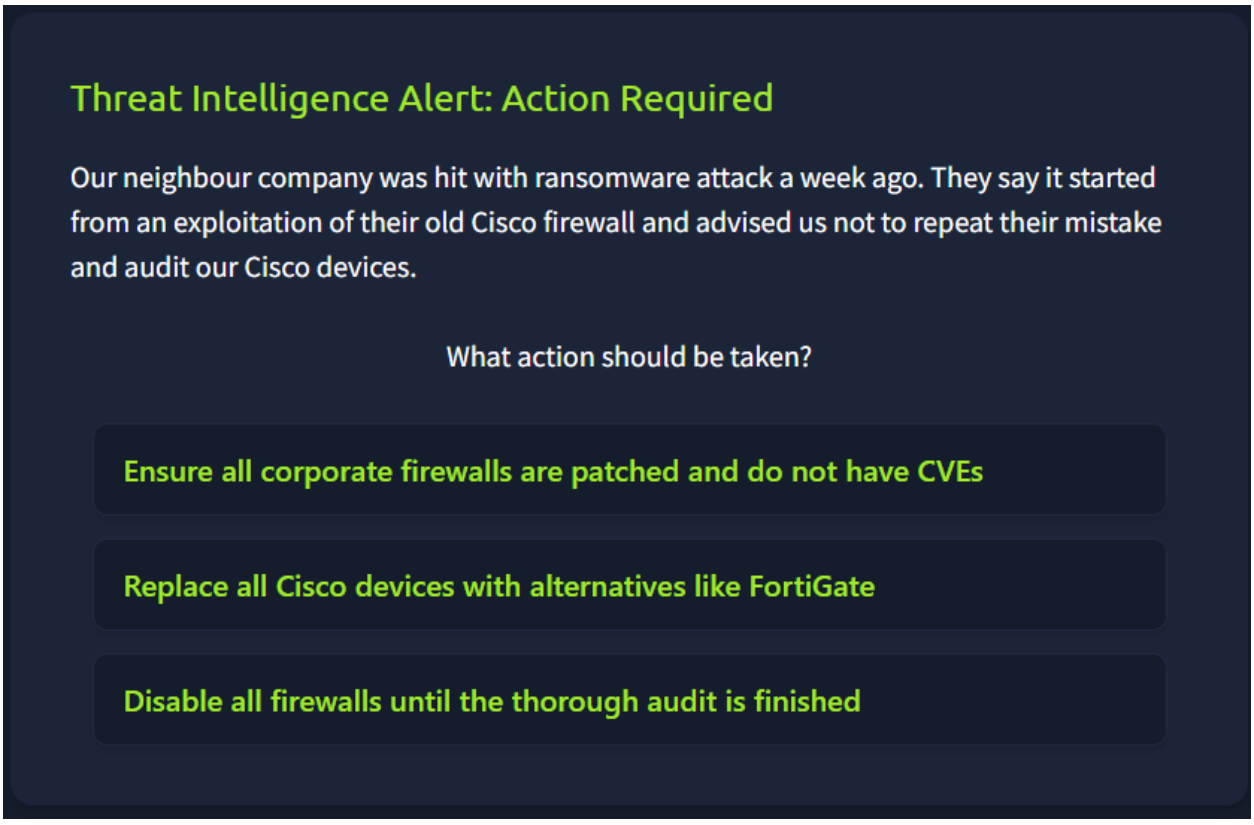
.



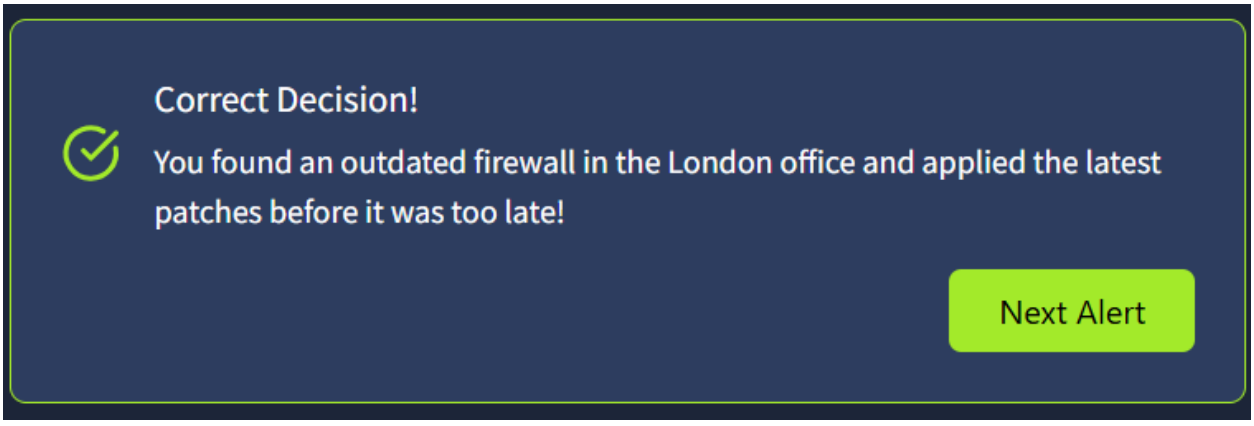
For this scenario, the threat actors had gotten a hold of the admins credentials, so the best option here would be to change the admin's password to a more secure one.



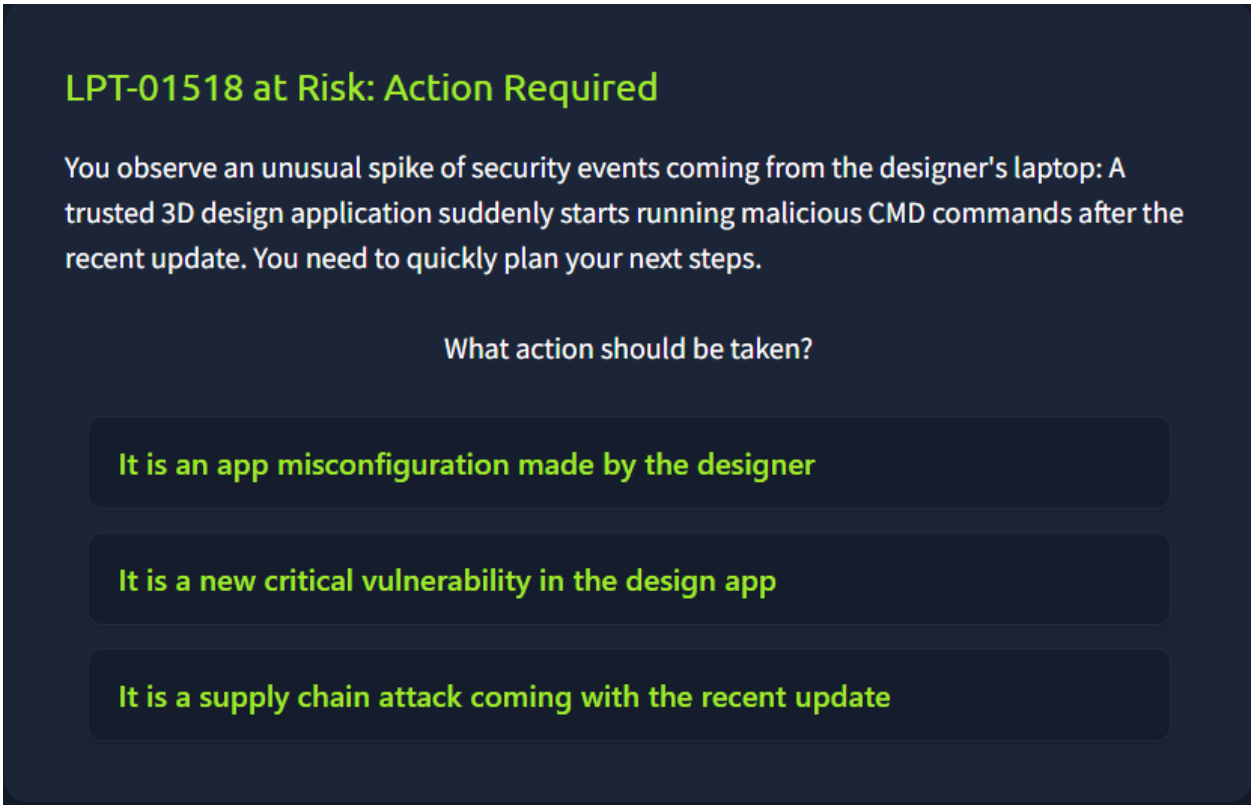
.



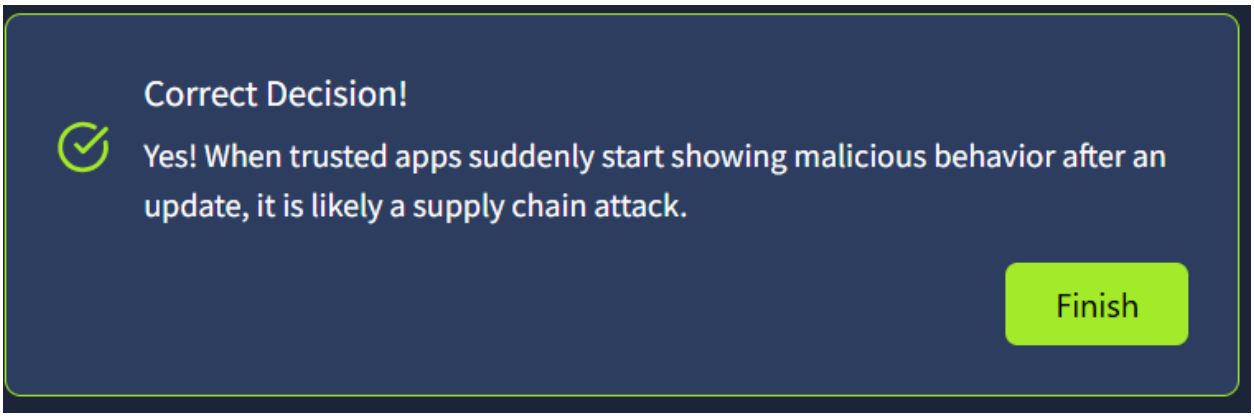
In this scenario, the best option would be to Ensure all corporate firewalls are patched and do not have CVEs.

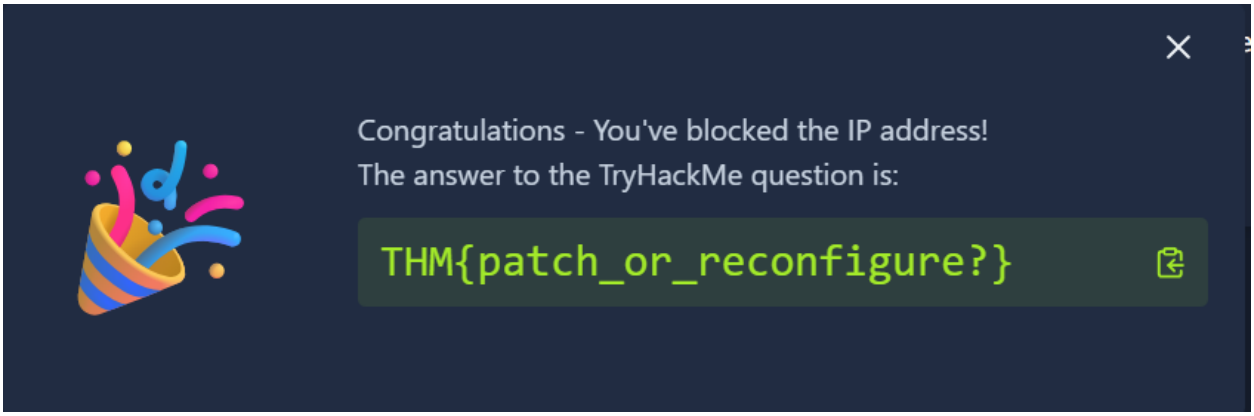


.



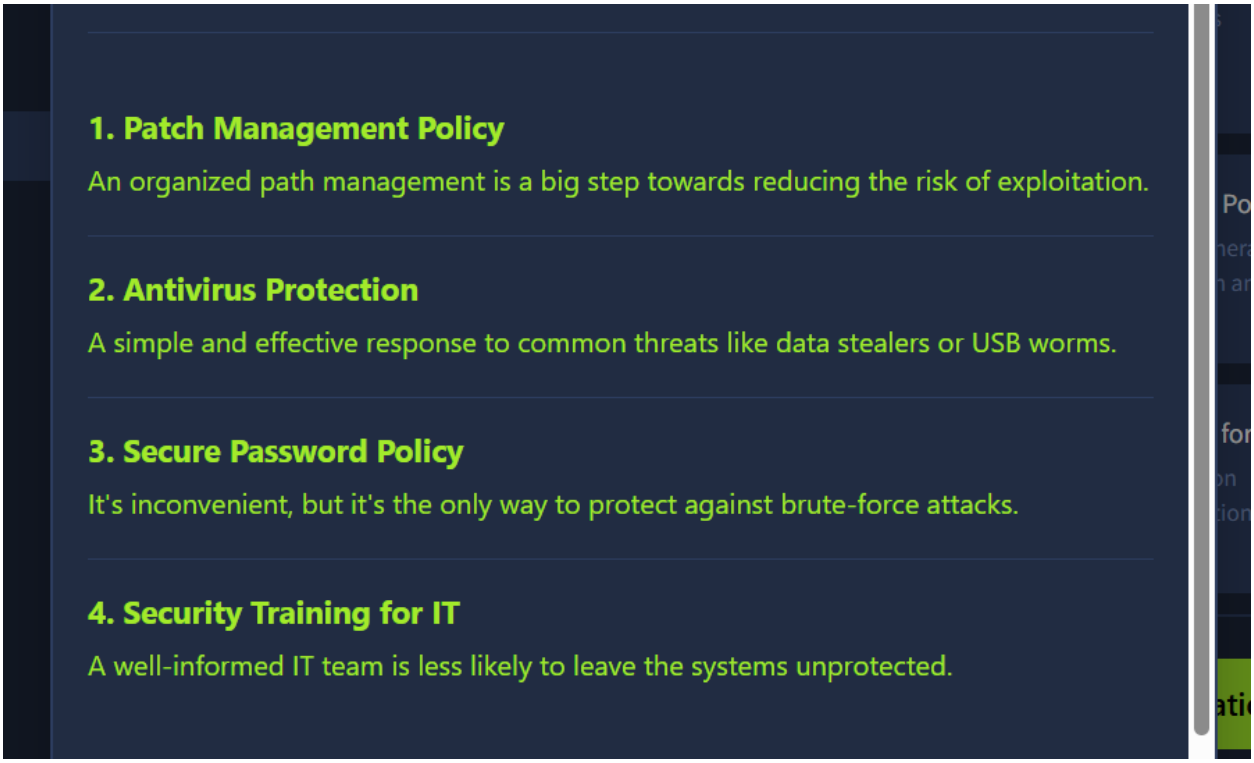
The problem here is the designer's laptop, it holds a plethora of personal apps and this increases the chances of a supply chain attack when updated. This is most likely to be a supply chain attack indeed coming with a recent update.



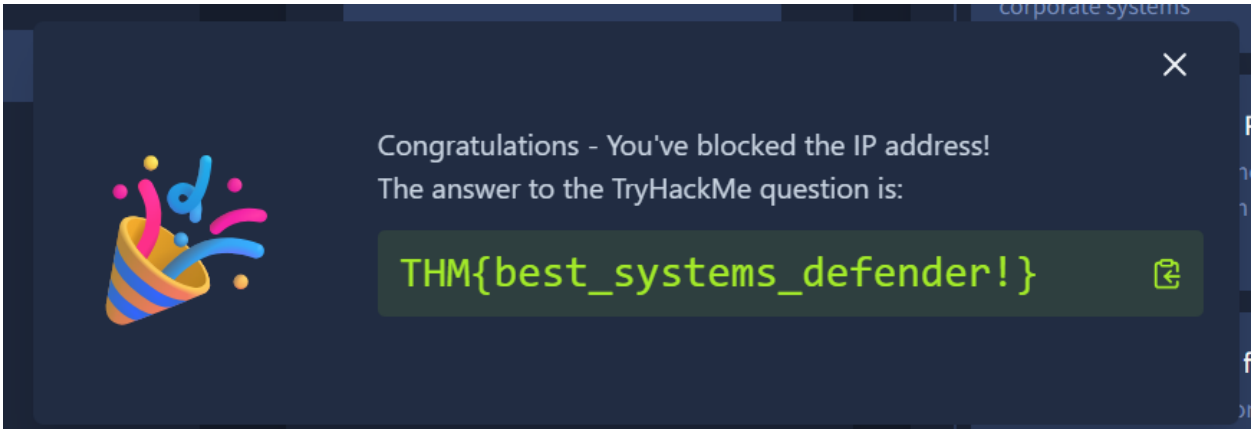


We caught the first flag.

STEP 2: What flag did you receive after completing the "Remediation Plan" challenge?



I provided the following policies.



Then got the flag.

Conclusion Summary

In this Systems Risk and Remediation Challenge, I applied a SOC analyst mindset to identify vulnerable systems and select appropriate remediation actions based on realistic attack scenarios. By assessing risks such as an Exchange Server spoofing vulnerability (CVE-2024-49040), compromised administrator credentials, unpatched firewalls, and a high-risk endpoint exposed to supply chain threats, I demonstrated the ability to prioritise security issues and recommend practical, impact-focused responses. The exercise reinforced the importance of timely patching, credential hygiene, and policy-driven controls as core defensive measures. Successfully completing both the *Systems at Risk* and *Remediation Plan* stages validated my understanding of risk assessment, remediation planning, and decision-making aligned with real-world SOC operations.