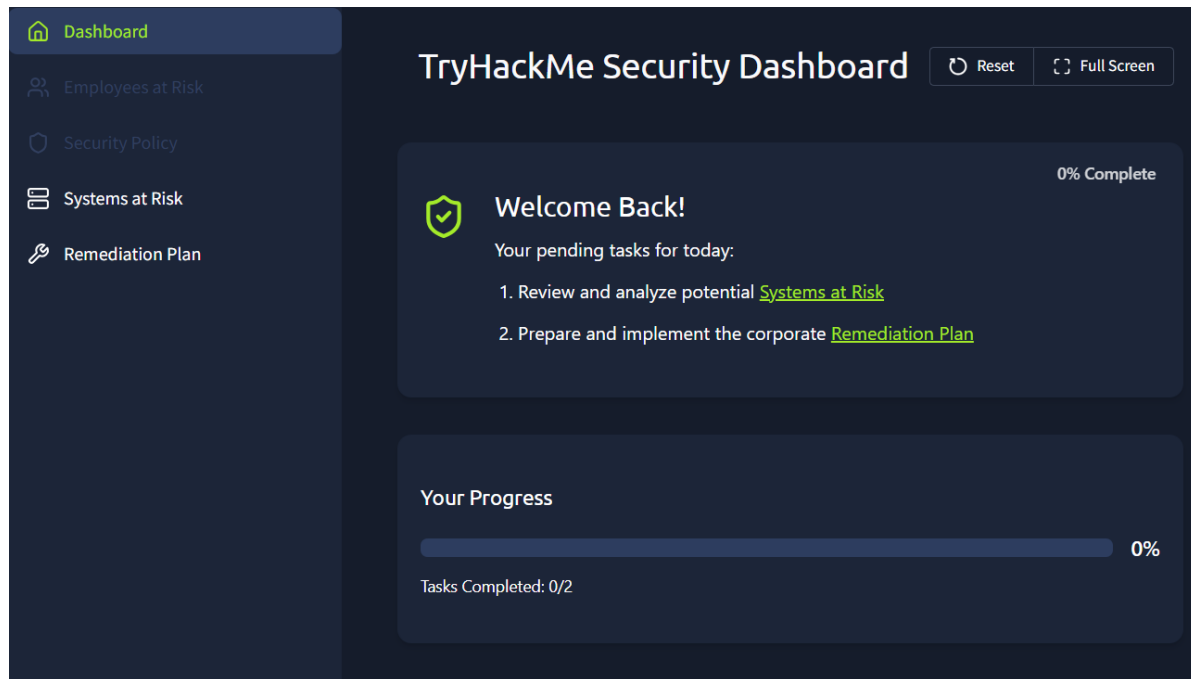


Objective: For this lab, continue your SOC analyst journey at TryHackMe. This time, decide what to do with the **Systems at Risk** and choose the best measures to protect your systems at the **Remediation Plan** tabs.



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

HQ-MAIL-02 at Risk: Action Required

The penetration team reported that our Exchange mail server is affected by CVE-2024-49040. They managed to breach the server thanks to that CVE and said anyone could do it since our server is Internet-exposed.

What action should be taken?

Ask IT to immediately change passwords of all mail users

Ask IT to apply a patch and update Exchange

Restrict access to the HQ-MAIL-02 server to only office IPs

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.

Correct Decision!



You chose to address the root cause - patch the vulnerability. Now hunt for threats that slipped in before you applied the patch!

Next Alert

Corporate Website at Risk: Action Required

The threat actors managed to brute-force an admin panel of our WordPress website and replaced the main page with malware links and gambling ads.

What action should be taken?

Restore the website from backups and close the alert

Update all website components to the latest version

Change the admin's password to a more secure one

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

Correct Decision!



You mitigated the root attack cause - breached credentials. You should now rush to restore the changed pages and look for the left backdoors!

Next Alert

Threat Intelligence Alert: Action Required

Our neighbour company was hit with ransomware attack a week ago. They say it started from an exploitation of their old Cisco firewall and advised us not to repeat their mistake and audit our Cisco devices.

What action should be taken?

Ensure all corporate firewalls are patched and do not have CVEs

Replace all Cisco devices with alternatives like FortiGate

Disable all firewalls until the thorough audit is finished

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

Correct Decision!



You found an outdated firewall in the London office and applied the latest patches before it was too late!

Next Alert

LPT-01518 at Risk: Action Required

You observe an unusual spike of security events coming from the designer's laptop: A trusted 3D design application suddenly starts running malicious CMD commands after the recent update. You need to quickly plan your next steps.

What action should be taken?

It is an app misconfiguration made by the designer

It is a new critical vulnerability in the design app

It is a supply chain attack coming with the recent update

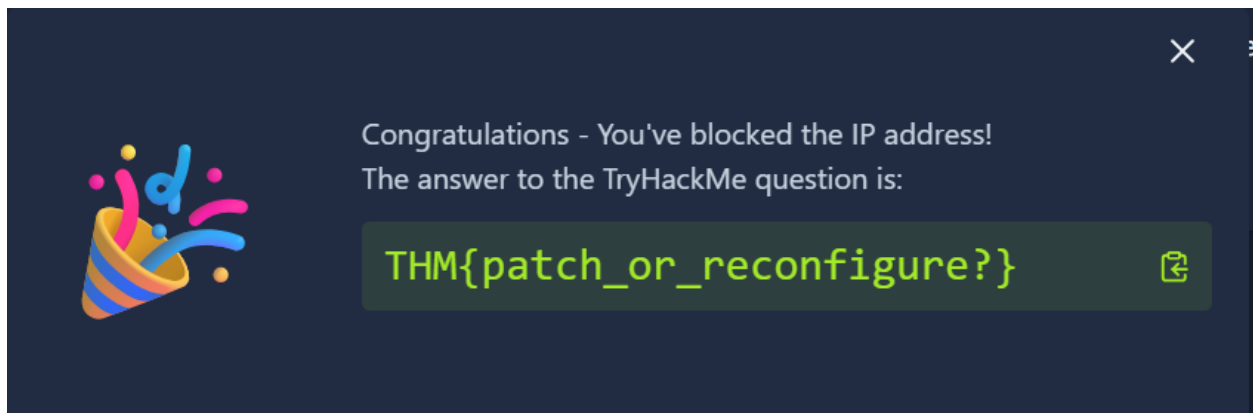
The problem here is the designer's laptop, it holds a plethora of personal apps and this increases the chances of a supply chain attack when updated. This is most likely to be a supply chain attack indeed coming with a recent update.

Correct Decision!



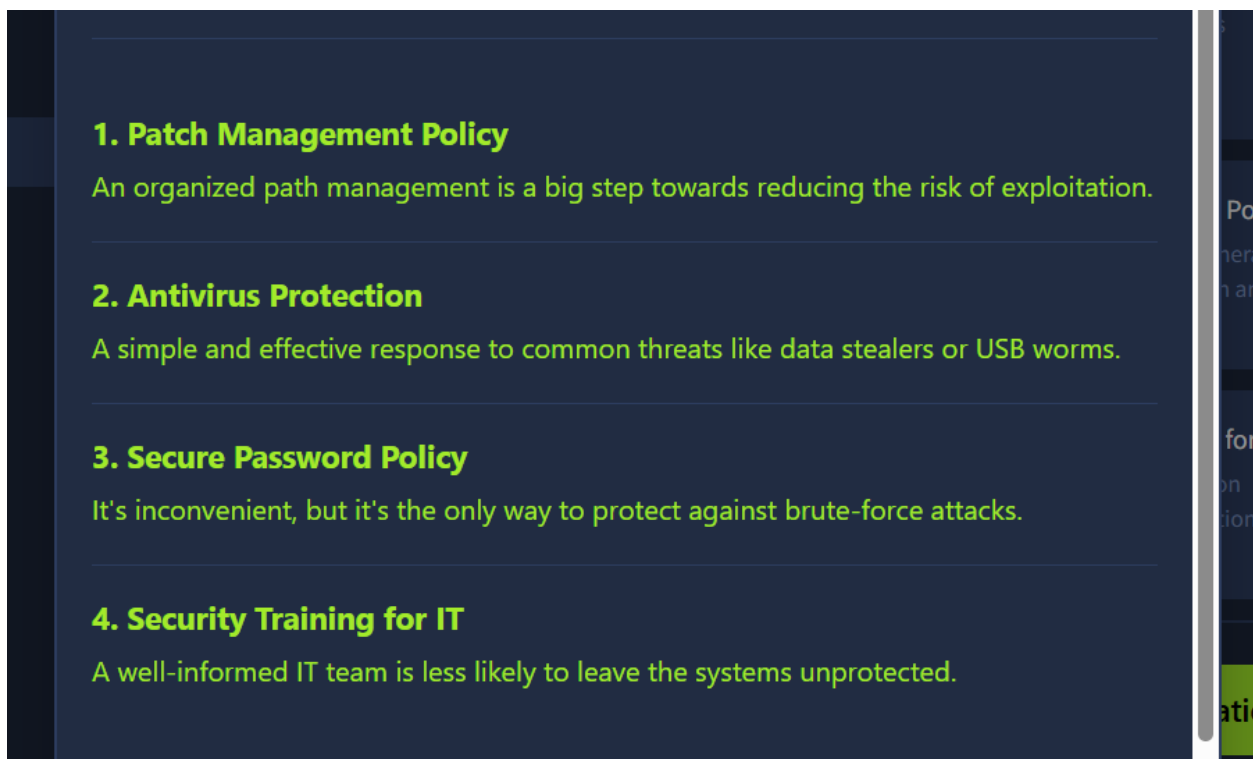
Yes! When trusted apps suddenly start showing malicious behavior after an update, it is likely a supply chain attack.

Finish

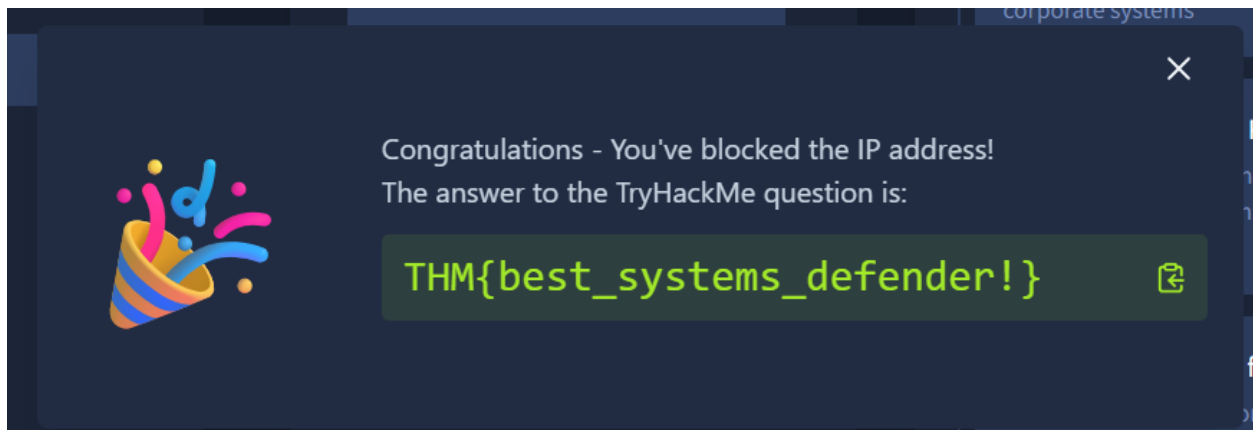


We caught the first flag.

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.