Task 7 – Identify and Remove Suspicious Browser Extensions

Objective

To identify potentially harmful browser extensions, analyze their permissions, remove or disable suspicious ones, and ensure a safer browsing environment.

Tools Used

- Web Browser: **Google Chrome**
- OS: **Windows**

Background

Browser extensions can access sensitive data such as browsing history, website content, and account information. Reviewing extensions regularly helps reduce risks like data theft, adware infections, and browser hijacking.

Step-by-Step Investigation

1. Opened Browser Extension Manager

Navigated to:

chrome://extensions/

All currently installed extensions were listed.

2. Extension Inventory & Security Review

	Extension Name	Purpose	Permissions Observed	Source	Status	Security Notes
1	Adobe Acrobat PDF Tools	PDF viewing, edit & sign	Can read website data	Chrome Web Store	Disabled	Safe, but unnecessary for daily browsing
2	Chrome Remote Desktop	Remote access to PC	Manage downloads & communicate w/native apps	Chrome Web Store	Disabled	Safe, but not needed currently

No unknown or malicious extensions found.

Security Assessment

Although both extensions were legitimate and from official sources, they hold **high-level permissions**:

- Read/change data on all websites
- Interact with system-level applications

Since they are **not used frequently**, disabling them helps:

✓ Reduce privilege exposure
✓ Improve security posture
✓ Optimize browser performance

Remediation Actions Done

Action	**Result**
Disabled 2 unused extensions	Reduced attack surface
Restarted browser	Performance stable
Verified no pop-ups or redirects	No malicious behavior found

Conclusion

Your browser is clean — **no suspicious extensions present**.
You successfully followed a professional SOC-style process:

- Asset inventory ✓
- Vulnerability review ✓
- Least-privilege enforcement ✓
- Documentation ✓

You demonstrated practical **endpoint security** and **secure hygiene** skills. Great job!

Learnings

- Install extensions only from **trusted sources**.
- Check permissions before installing.
- Disable/remove unused extensions to reduce risk.
- Periodically audit browser extensions (Monthly recommended).
- Malicious extensions can:
    - Steal login data
    - Inject ads
    - Track browsing activities
    - Redirect to phishing websites

Deliverables Summary

- **Suspicious Extensions Found:** None
- **Extensions Disabled:** Adobe Acrobat PDF Tools, Chrome Remote Desktop
- **Browser Status:** Stable & secure
- ## Overall Summary
  In this task, I audited my Google Chrome browser to identify any suspicious or potentially harmful extensions. I reviewed each extension's permissions, source, and usage to assess their security impact. Both installed extensions were legitimate, but since they were not frequently used, I disabled them to reduce the browser's attack surface. After restarting the browser, performance remained stable with no unusual behaviour. This activity helped improve endpoint security, ensure a safer browsing experience, and enhance my practical skills in identifying and mitigating browser-related threats.