Week 4 Ass 2 Task 1 Peer Programming

Task Overview

You will work in a group to implement and test a defensive cybersecurity technology.
If you miss your Week 4 tutorial, you will need to submit a recorded video showing your group working on the peer programming task.

Code Reuse

You are encouraged to search for and reuse good quality code in this unit. You are encouraged to use tools such as ChatGPT in this unit. All sources of code should be referenced. For websites and web services, the inclusion of a commented URL in the reused code is a sufficient reference. Deprecated code, for example, PowerShell scripts that use ping, should not be reused.

Sharing of artefacts, for example, code or virtual machines, between groups is not permitted. You can share artefacts with other members of your group.

Repository

Create a private Git repository, for example, on GitHub. Invite your tutor, the unit coordinator and your group members to the private repository.

Due

The Peer Programming task is due in Week 4.

Return

The Peer Programming task will be marked with the Defend task (due in Week 6). Feedback will be provided within 2 weeks of the due date.

Submission Overview

Submit artefacts to both your private code (Git) repository and to the unit website. Submit a link to your private repository to the unit website. All group members must submit. If you miss your Week 4 tutorial, you will need to submit a recorded video showing your group working on the peer programming task.

Criteria Overview

You will be marked on aspects such as the quality of your scripts including your testing scripts including functionality, modularity, style, code reuse, documentation, lack of deprecated features, level of automation and use of code repository tools.

You will also be marked on your teamwork including your individual contributions; your communication quality and quantity; your interpersonal style; and the performance of your team including its decision making and self-management. Example behaviours that we will be looking for include:

- How well do team members learn from and respond to each other?
- Does one person dominate the group and the contributions?
- Are decisions made by one person sufficiently challenged by other members?

- Does the team manage dysfunctional behaviours such as free riders?
- Time management - we want you to have fun in your group but … does the team manage excessive distractions?

Scenario

You work at the Monto Caravan and Cabin Park. Your boss has asked you to improve the cybersecurity of her workstation. You will develop a portfolio of evidence of the implementation and testing of a safeguard. Your evidence will include PowerShell scripts and a PowerPoint slideshow containing, for example, screenshots of your testing.

Topic 2 Implement safeguard CIS 2.5 Allowlist Authorised Software

Your boss uses the Win11 virtual machine. Download the Win11 virtual machine from the unit website and import it into Virtualbox. Setup a shared folder on Win11 for your scripts.

To implement an allowlist of authorised software you will configure Windows Defender Application Control (WDAC) in Win11. The following instructions are a guide. You can make improvements as you see fit.

1. Create a PowerShell script called defend.ps1.
2. Pre-test: write a function testWDAC() that:
    a. Attempts to run an "unauthorised" app such as keyfinder.exe and checks whether the app has been run successfully, for example, using Get-Process.
3. Document your code.
    a. Clean up your code using PSScriptAnalzyer
    `PS> Invoke-ScriptAnalyzer defend.ps1`
    b. Run the code and collect testing screenshots for your portfolio.
    c. Commit your code to your Git repository.
4. Write a function setupWDAC() that compiles a block WDAC policy to a .cip file using `ConvertFrom-CIPolicy`
5. Add code to your script that checks the first argument of the command line:
    a. If the first argument is testWDAC, call the testWDAC () function. For example, the following command line would call testWDAC():
    defend.ps1 testWDAC
    b. Improve your code to call the other functions in your script based on the command line argument.
6. Write a function enableWDAC() that uses `citool.exe` to apply the WDAC block policy (.cip)
7. Post-test: rerun testWDAC() to check if the "unauthorised" app is now blocked.
8. Write a function resetWDAC() that removes the WDAC block policy using `citool.exe`

Collect Evidence

Prepare a PowerPoint presentation that collects evidence of the implementation of your safeguard. Include evidence such as screenshots of:

1. Testing: including pre-tests and post-tests for each safeguard
2. Style: include output of PSScriptAnalzyer for each script.

Task Submission

Include a link to your private repository in your PowerPoint slideshow. Commit your PowerPoint slideshow to your private Git repository. Submit your PowerPoint slideshow to the unit website. All

group members must submit. If you miss your Week 4 tutorial, you will need to submit a recorded video showing your group working on the peer programming task.

Task Criteria

Each of the following marking criteria have equal weighting.

Criteria	Indicative of 100%	75%	50%	25%	0%
Automation and Testing	Excellent level of automated installation and configuration ← Pre- and Post-tests demonstrate effect of safeguards ←			→ Insufficient evidence of automation → Insufficient testing or poorly chosen test cases	→ No automation or no testing
Code functionality, style, documentation & repository management	Consistent, reasonable layout← Excellent functions documentation ← Git commits showing regular script & function development by all group members ←		→Lack of modularity, e.g. poor or no functions →Uses deprecated functionality	→ Insufficient Git commits → Not all group members committing to Git → Scripts not available via Git repository	
Peer Programming Teamwork	Excellent individual contributions, communication & team management← Challenges groupthink ←		→Free riders are not confronted →Decisions not sufficiently challenged →One person dominates		→No evidence of teamwork