Part 3: Securing PowerShell – Effective Mitigations In Detail

In this part, we will mostly concentrate on mitigations that can help you to secure your environment efficiently. However, again, although we will focus on a lot of blue team stuff, this section also helps red teamers understand how mitigation technologies work, what risks they contain, and how adversaries are attempting to develop bypasses.

First, we'll explore J**ust Enough Administration** (**JEA**), a feature that helps with delegating administrative tasks to non-administrative users. Although this feature is not very well known widely, it can be a game-changer. In this part, we will dive deep into JEA and its configuration options, and we will learn how to simplify the initial deployment.

Next, we will look into code signing and Application Control. You will learn how to plan for deploying Application Control, and throughout our journey, we will work with Microsoft's Application Control solutions AppLocker and **Windows Defender Application Control** (**WDAC**). You will familiarize yourself with how those solutions are configured and audited. You will also gain insights into how PowerShell will change when Application Control is configured.

Dive into the **Antimalware Scan Interface** (**AMSI**) – learn how it works and why it is really helpful in the fight against malware. We will also look into ways that adversaries bypass this useful feature, by either surrogating it or obfuscating their malicious code.

Many other features can help you mitigate risk in your environment; therefore, at the end of this part, we will glance at many different features that can help you improve your posture. We will look into secure scripting, the desired state configuration, hardening strategies for systems and environments, and attack detection with **endpoint detection and response (EDR)** software. We are not diving deep in this last section and you are more than welcome to explore some of the features mentioned further to learn more about them and possibly use them in your environment.

This part has the following chapters:

- ***Chapter 10***, *Language Modes and Just Enough Administration (JEA)*
- ***Chapter 11***, *AppLocker, Application Control, and Code Signing*
- ***Chapter 12***, *Exploring the Antimalware Scan Interface (AMSI)*
- ***Chapter 13***, *What Else? – Further Mitigations and Resources*