Part 2: Digging Deeper – Identities, System Access, and Day-to-Day Security Tasks

Let's dive deeper and combine PowerShell with other technologies. The technology section of this part mostly explores the ways that attackers can enumerate, bypass, hijack, and compromise key components such as the operating system itself, Active Directory, and Azure AD/Entra ID. On July 11, 2023 Microsoft renamed Azure AD to Entra ID. As this was just shortly announced before this book was released, we will refer to Entra ID just as Azure Active Directory, Azure AD, or AAD in this part. This part is not only of interest to red teamers but also to blue teamers who want to learn how adversaries are trying to abuse well-established solutions in order to protect themselves from such attacks. Additionally, you will get a lot of useful extra information about concepts, protocols, and mitigation, and many more interesting insights.

We'll first explore PowerShell's capabilities to access the system: we will not only look into working with the registry and WMI but we will also find out how you can leverage .NET, as well as native Windows APIs, and how you can compile and run custom DLLs and unmanaged code from PowerShell. Ever wondered how it is possible to run PowerShell without calling powershell.exe? Don't worry – after working through this part, you will know.

In the Active Directory chapter, we will dive into enumeration – with or without the Active Directory PowerShell module – as well as into ac-

cess rights, authentication protocols, credential theft, and mitigation tactics. We will also look into the recommended Microsoft security baselines and the Security Compliance Toolkit.

When talking about Active Directory, Azure AD is not far away; therefore, we will also investigate this technology from a PowerShell security perspective. Azure AD security is not a broadly well-known topic, and in this chapter, you will learn how to differentiate between Active Directory and Azure AD and about fundamental Azure AD concepts. You will learn which accounts and roles make useful targets for attackers and how Azure AD can be enumerated. Last but not least, we will explore several credential theft techniques and also look into mitigating them.

In ***Chapter 8*** and ***Chapter 9***, this book also provides you with red and blue team cookbooks. Both parts first explore the common PowerShell tools for both intents and then provide many useful PowerShell code snippets that you can use for your own purposes – no matter whether you are a blue or red teamer.

This part has the following chapters:

- ***Chapter 5***, *PowerShell Is Powerful – System and API Access*
- ***Chapter 6***, *Active Directory – Attacks and Mitigation*
- ***Chapter 7***, *Hacking the Cloud – Exploiting Azure Active Directory/Entra ID*
- ***Chapter 8***, *Red Team Tasks and Cookbook*
- ***Chapter 9***, *Blue Team Tasks and Cookbook*