‹ Dashboard

Windows Security: Getting Started

Why Windows Security?

Windows is the most popular enterprise operating system in the world. This makes it an important asset to secure from attackers. Windows security is a vast subject and this introductory set of labs aims to get you started!

Why labs? Cybersecurity is a very practical subject and hands-on labs are the only way to have actionable insights that you can use in the real world.

Prerequisites?

- Windows basics: networking, using the terminal and administrative tools
- Linux basics: basic administrative commands using a terminal

What will you learn in the Windows Security section?

The following topics will be covered in the subsections below:

Basic Exploitation

This section covers the exploitation of the Windows services or applications with the help of intel gathered in the recon phase. You will learn to use tools such as Metasploit, Mimikatz, Impacket, etc. in this phase.

Post Exploitation

On a compromised target system, you will learn to use different tools and techniques to access the organization's (target system) valuable information. This could be in the form of a file, a database, an excel sheet, etc. This section focuses more on the use of the tools and scripts that will help you get to the target system's valuable information.

Service Exploitation

Windows systems have multiple services that are exposed - RDP, SMB, WinRM, etc. In this section, we will look at learning about these services and how to audit them.