Contents

1 Introduction

The goal of these documents is to provide a baseline foundation for the Windows team members. Please update and improve the documentation wherever you see fit.

I think there are 5 categories to cover:

1. Deployment to Proxmox

2. Setup of Active Directory

3. Setup of the CA

4. Setup of the DFS / highly available files

5. Hardening

6. Planning (for the competition, timelines)

7. Offense (to practice)

8. Powershell commands (to reference in one spot)

Each category has an associated folder

This is my knowledge of Windows. I have tried to include everything I think could be useful to you. I encourage you to do the same, add more sections and flesh out the sections with your own experience.

I made a dedicated powershell pdf so we can easily reference them. Note that powershell commands are not case sensitive.

There could be unpatched CVEs during the competition. A list of them can be found here. For example, CVE-2020-0796 was severe and would surely have been used by the red team.

You will be using Remmina a lot, make sure to click "share folder" to send files over RDP. The folder is visible under "This PC". Windows defender can remove files from the share folder.