Austin Bannister

The main goal of this project before CoViD-19 was to set up two teams, red and blue, to perform a CTF. We had issues with the VM and scheduling, so not everything went to plan. I was part of blue team, and it was my task to harden the VM. I think I did okay, we got a good grade, but I wasn’t able to get the feedback I wanted. I followed a few different checklists online, and I think I implemented everything correctly.

Other names (censored for their own privacy)

Tsai \*\*\*\*\*\*\*\*\*\*\*\*\*

Nick \*\*\*\*\*\*\*\*

Eric \*\*\*\*\*

Corey \*\*\*\*\*\*\*

Cristin \*\*\*\*

Semester Project: Blue Team

Windows Server 2008 R2 Hardening

This document details steps taken to secure a virtual machine running Windows Server 2008 R2. Security considerations were not made for the fact that this is a virtual machine, meaning we treated this guest system as a physical machine, eliminating the host system as a target. I left it to my groupmates to review CVEs and perform further hardening past what I completed, but that did not get done, again due to Covid and scheduling, as one of the blue team members had to go home to Taiwan.

Admin Password: CY450!

Checklist:

|  |  |
| --- | --- |
| Security Measures | Completion State (Complete, In Progress, Improbable) |
| Update guest OS to current vendor version | Complete |
| Create user and admin accounts with strong password policy | Complete |
| Implement principle of least privilege | In Progress |
| Implement strong firewall rules | Complete |
| Disable unnecessary services | Complete |
| Configure Drive Encryption if possible (e.g. bitlocker) | Improbable |
| Disable unnecessary shares | Complete |
| Constrain Firewall Rules | Complete |
| Audit Log Events | Complete |
| Review CVEs for current version, make considerations based on these. | In Progress |
| Place flag for user account password | Complete |
| Place flag for admin account password | Complete |