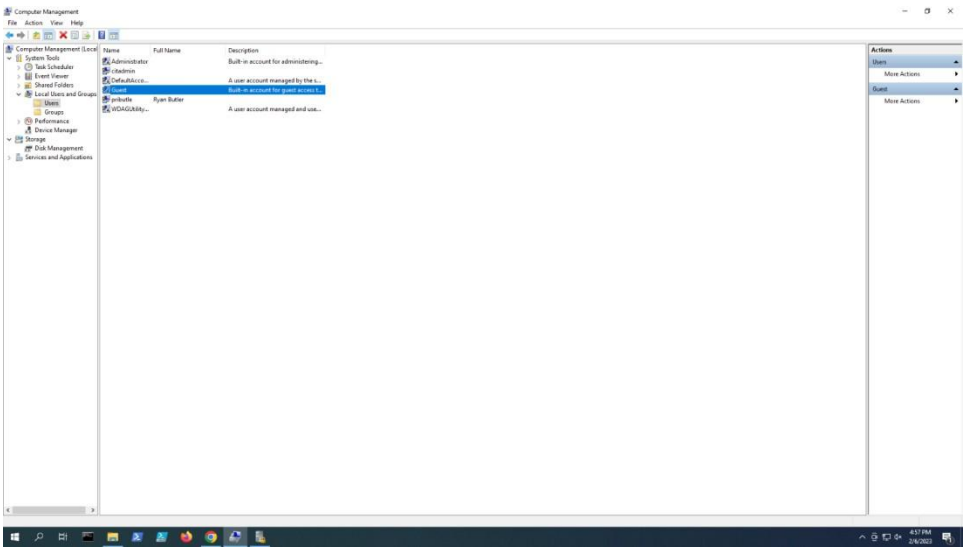
OVERVIEW:

The goal of this lab was to perform a hardening procedure on a system. This was done on the lab machine in the CIT 007b classroom. The hardening process implemented different settings and configurations that could be performed on a windows machine through different tools like computer management, local security policy, and event viewer.

ANALYSIS:

The first step was to log onto a windows machine. This was done in the CIT 007b classroom, using the CITADMIN account.

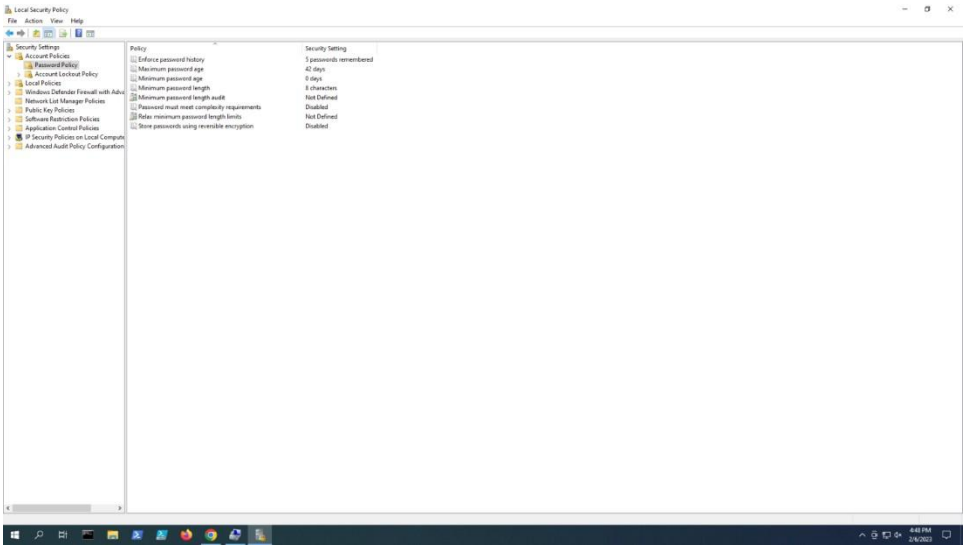
The next step was to make sure the Guest account was disabled. This was done in computer management. Which can be accessed by right-clicking the windows icon in the bottom right. Under users the Guest account can be disabled.



The next step that was taken to harden the system was to change the local security policy. This can be accessed by using the windows key + r and entering secpol.msc.

The first change we are going to make to the local security policy is a change to passwords. They can be changed here Security Settings > Account Policies > Password Policy Then the following changes were made:

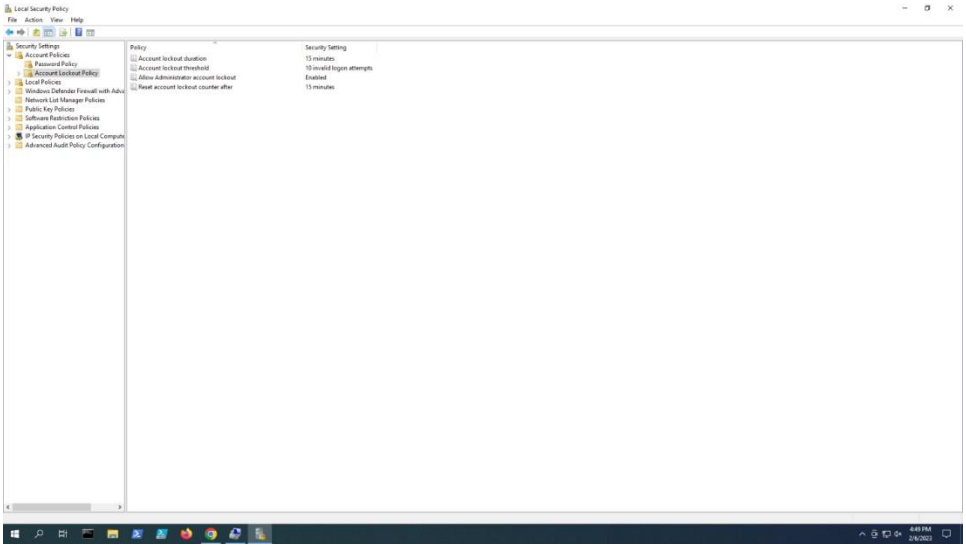
- Minimum Password length: 8
- Enforce Password History: 5



The next change to policy that was made was the account lockout policy. Found at Security Settings > Account Policies > Account Lockout Policy.

Then the following changes were made:

- 15 minutes for Account lockout duration
- 10 invalid logon attempts for the Account Lockout Threshold
- 15 minutes for Reset account lockout counter



The final change to the local security policy was to change our audit policy. Found at *Security* Settings > Local Policies > Audit Policy

The login audits were changes to report failed attempts. They appeared under the event ID 4625. Using the right shift google chrome was attempted to be used by a different user. A random password was then entered to simulate a failed attempt.

Using the event viewer these failed login attempts could then be viewed.