|  |  |
| --- | --- |
| Inject Report # | Team 11 |

Member Assigned:

|  |  |
| --- | --- |
| Request: | Configure a windows password policy with these specific attributes:  *1. All four types of characters (1 upper case character, 1 lower case character, 1 special character, 1 number) 2. 15 Character Minimum 3. Lockout the user after 5 failed password attempts in 15 minutes 4. Set the lockout period to last 15 minutes 5. Maximum of 90 days before a user’s password must be changed 6. Remember the last 3 passwords 7. No password hints. 8. Minimum password age of 1 day for non-service accounts 9. Disable storing passwords with reversible encryption 10. Enable password complexity requirements 11. Set Kerberos time tolerance to 5 minutes* |
| Steps Taken: | This is done through Windows Active Directory. The group policy management console is opened, then the user navigates to the domain section, and then to group policy objects where the default domain policy is located. The policy is edited in the domain policy editor where the required attributes are added. |
| Screenshots (if applicable): | EXAMPLE – DO NOT USE/SUBMIT IN FINAL INJECT |
| Report Details (e.g., address questions that were asked in inject) | GPO Report Here  Code : Get-GPOReport -Name "TestGPO1" -ReportType HTML -Path "C:\GPOReports\GPOReport1.html"  DO NOT SUBMIT THIS CODE IN FINAL INJECT |
| Any remaining vulnerabilities/issues | Devices not secured:  Policies that could not be implemented (if any): |
| Additional Info: |  |