TASK:

Protect - LDAP Vulnerability

CONDITIONS:

Given a target Domain, a Domain Controller (DC), and an administrative account

STANDARDS:

1.) Team member determines the naming convention that will be used for re-naming of the built-in Administrator account

2.) Team member opens the Active Directory Users and Computers (ADUC) console on the workstation and locates the built-in Administrator account within the Organizational Unit (OU) structure

3.) Team member changes the name of the Administrator account to the agreed upon naming convention

4.) Team member creates a new account named “Administrator” as a regular user account and assigns it no additional rights or privileges

5.) Team members query the DC to obtain login information

6.) Team members output the login information to a comma-separate values (CSV) file and compares against verified logins

7.) Team members set up and run scan for vulnerabilities over network

8.) Team members go through ADUC security settings and compare against standards

9.) If vulnerability has been found and restoration is requested by OU, team members Removes the newly created Administrator account, and renames Administrator account

END STATE:

Vulnerability allowing unverified logins has been resolved

AND/OR

Target domain Administrator account has been renamed and alternate dummy account named “Administrator” with no rights or privileges has been created

NOTES:

Microsoft recommends the steps as provided rather than disabling the account. Disabling the Domain Administrator account can cause issues across a range of services and assets.

Tools:

Active Directory Event Viewer: A useful program to view login events and filter specific activities

Commands:

Open Active Directory Users and Computers(GUI):

```
C:\> dsa.msc
```

Rename local administrator account:

```
C:\> wmic useraccount where name='Administrator' call rename name='NewAdminName'
```

Create account named Administrator, but with no permissions, and only after default Administrator accounts is renamed (Warning if done wrong, could result in lockout):

```
C:\> net user Administrator NewPassword /ADD /PASSWORDCHG:NO
C:\> icacls C:\*.* /remove Administrator /T
```

REFERENCES:

https://christophergeiger3.github.io/UConn-x-National-Guard-Documentation/scenario1/

REVISION HISTORY:

19 APR 2021