

Team: Team 6

Inject Number: 18

Inject Duration: 45 Minutes

Inject Start Date/Time: Sat, 05 Mar 2016 19:04:33 +0000

From: Infrastructure Mgr

To: Server Team

Subject: GPO and AD Security Policies

I just got a memo from our independent auditors that they'll need to see copies of our IT policies during their next audit - the problem is we don't have any. I need you to ensure that the domain GPO takes into account AD security best practices. As with all reports, it is expected that any and all copied text be properly cited.

At a minimum we'll need the GPO that meets the NIST SP800-53 standard to apply to AD - Microsoft Best Practices for Securing Active Directory. Example criteria is:

- Enable domain level password complexity requirements
- Enforce password history (24)
- Define a minimum password age (1)
- Define a maximum password age (at least 42)
- Define a minimum password length (8)
- Rename the Administrator and Guest accounts
- Disable the "Do Not Require CTRL+ALT+DEL" logon setting
- Create a legal disclaimer logon banner presented at login
- Disable Administrative Shares
(HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters)

- 1) Submit documentation showing that GPO's have been configured. You can accomplish this by submitting the HTML report exported from the group policy manager.
- 2) Please write and upload a policy document to support the configuration.

NOTE: Teams who fail to cite the source of copied text will not receive more than 50% of the maximum score of the inject.

Thank you.

Infrastructure Mgr