Active Directory Strategy

Regis University Computer Club

2014

TOP SECRET

This Book was written by M. Poirier on
10 - Jan. 14

This is an addendum to the Strategy Document and should be treated as the same.

This packet was received with a binder. Put whatever information you think is necessary in the back. If you think it is of the highest secret, please omit facts as you may find fit to leave out.

This book was given to

Of Regis University, and is for there eyes only.

____ - ____. ________
day mon. year

Table of Contents

Overview

1. Configure Users/Groups
    a. Create unique Admin user and disable default Admin user
        i. Maybe make an admin for each task to avoid an all powerful user
    b. Create unique Admin group and disable default Admin group
        i. Maybe make a group for each task to avoid an all powerful group
        ii. Be wary of Enterprise Admins, Domain Admins, and Administrators
    c. Reset all passwords.
        i. Send memo to mgmt saying all users need to use the given password and create a new password with the given complexity.
    d. Disable all old accts.
    e. Disable Remote Desktop for all users but my unique admin acct.
        i. Only allow RD from my IP address.
    f. Disable all remote/hidden shares.
2. Set password complexity GPO
3. Configure firewall
    a. Disable Ping (ICMP)
    b. Disable Remote Desktop from all but my IP
    c. Disable psexec.exe
        i. Ports 445 and 139
    d. Disable all IPv6
4. Update Windows
5. Finish Configuring the GPO

Configure Users/Groups

Create Unique Admin User(s) and Disable Default Admin Users

Create Unique Admin Group(s) and Disable Default Admin Groups

Reset All Passwords

Disable All Old Accounts

Disable Remote Desktop for All Users Except My Account

Set Password Complexity GPO

Configure Firewall

Disable Ping (ICMP)

Disable Remote Desktop From All But My IP

Disable PSEXEC.EXE

Disable All IPv6

Update Windows

Finish Configuring the GPO

Appendix A - Useful Websites

Title	URL
A list of common exploits	http://www.commonexploits.com/
AD Security Breach Mitigation Guide	http://blogs.technet.com/b/security/archive/2013/06/03/microsoft-releases-new-mitigation-guidance-for-active-directory.aspx
Some windows exploits	http://www.securitytube.net/video/5035
Microsoft Security Bulletin	http://technet.microsoft.com/en-US/security/dn481339