Security baselines for Windows 8.1, Windows Server 2012 R2 and Internet Explorer 11 - FINAL

Microsoft is pleased to announce the final release of security baseline settings for Windows 8.1, Windows Server 2012 R2 and Internet Explorer 11. Some of the highlights of the new security baselines (many of which we intend to backport to older versions of Windows and IE):

* Use of new and existing settings to help block some Pass the Hash attack vectors;
* Recommendations to control the storage of plaintext-equivalent passphrases;
* Blocking the use of web browsers on domain controllers;
* Incorporation of the Enhanced Mitigation Experience Toolkit (EMET) into the standard baselines;
* Removal of the recommendation to enable "FIPS mode" (this is discussed in greater detail in this blog post: [Why We’re Not Recommending “FIPS Mode” Anymore](http://blogs.technet.com/b/secguide/archive/2014/04/07/why-we-re-not-recommending-fips-mode-anymore.aspx));
* Removal of almost all service startup settings, and all server role baselines that contain only service startup settings.

Settings are provided as four separate sets of baselines, for the following configurations: Windows 8.1, Windows Server 2012 R2 Domain Controller, Windows Server 2012 R2 Member Server, and Internet Explorer 11. The attachment to this blog post includes scripts to apply those baselines to a computer’s local policy and GPO backups you can import into Active Directory Group Policy.

There are a few changes between these recommendations and the beta version we released in April. We discuss those changes in more detail in two other blog posts: one about most of the changes, and another detailed post about the issues around account lockout recommendations.

While we are preparing the content in the format used for inclusion in the Security Compliance Manager (SCM), we are making the baselines available as a download package attached to this blog post. The download includes a Word document describing various aspects of the changes from baselines for earlier versions of Windows and IE, a spreadsheet listing all the baseline settings and highlighting all the new and updated settings, Group Policy Objects (GPOs), scripts and utilities to import the full complement of settings into local group policy for evaluation and testing, a new custom ADMX to expose some important settings that aren't currently exposed by Windows as Group Policy settings, and WMI filters to ensure that GPOs are applied to appropriate systems.

Download and extract the attached "Win81-WS2012R2-IE11-Baselines-FINAL.zip". It contains the following folders:

* **Documentation**: "Recommended Security Baseline Settings.docx" is a Word doc that categorizes and describes all the new and updated settings (you should probably start here); this folder also contains "SCM Windows 8.1 and 2012 R2 Settings.xlsx", an Excel spreadsheet that describes the full set of recommended settings.
* **Administrative Template**: an ADMX and (US English) ADML file surfacing some "pass the hash"-relevant settings through the Group Policy editor. (Note: the Local\_Script folder contains scripts that install these files to the appropriate location.)
* **GP Reports**: Group Policy reports formatted as HTML files (for those who prefer that format over Excel spreadsheets).
* **GPOs**: Group Policy Object backups for the four separate sets of baselines described earlier. These can be imported into Active Directory Group Policy.
* **Local\_Script**: This directory contains three batch files that apply appropriate settings to the current machine: 81\_Client\_Install.cmd, 2012R2\_DomainController\_Install.cmd, and 2012R2\_MemberServer\_Install.cmd.
* **WMI Filters**: This directory contains .MOF files that you can import into your Group Policy configuration to ensure that GPOs are applied only to the appropriate systems.

We will follow up on this blog when the SCM cab files become available.