Locking Down Windows Vista

Jussi Jaakonaho
Director of Special Operations
Sentor MSS AB

Infosecurity 2007

simply secure

1. Enforce Complex Passwords

- Complex passwords are not enabled by default
- Implement complex passwords will require passfilt-style complexity
- Why is this important?
  - Easy to guess passwords are still the easist way to access any machine (particularly admin or service accounts which tend not to change their passwords as frequently)

2. Reduce the number of cached passwords

- Consider the number of cached passwords you want to allow
- Use 1 cached password for travelling systems, use 0 for desktops on the network
- Why is this important?
  - – Cached password hashes can be dumped using pwhist from toolcrypt.org

3. Disable login through terminal services

- Default setting allows administrators to remotely access the desktop of Vista systems
- Consider removing the ability for remote admins to TS to the system
  - Or set the Deny rule for TS access
- Why is this important?
  - If the admin account becomes compromised, the attacker won’t be able to TS to the Vista system

4. Access this computer from the network

- Default setting allows administrators to remotely access Vista systems via NetBIOS
- Consider removing the ability for remote admins to login to the Vista system
- Why is this important?
  - If the admin account becomes compromised, the attacker won't be able to login remotely to the Vista system over NetBIOS

5. Enforce Digital Signing (client)

- Microsoft network client: Digitally sign communications (always)
  - Default is disabled
  - Consider setting to enabled
- Why is this important?
  - Vista systems are susceptible to hijack via smbrelay
  - A Vista user who visits an evil website may have their password challenge response credentials sent to evil servers
    - http://www.xfocus.net/articles/200305/smbrelay.html

6. Remove system from the network browse list

- By default, Vista systems announce themselves to the network browse master
  - ‘net view /domain:domain_name’ will display a list of all advertised systems
- Consider removing the system from the browse list using the Hidden registry key

```
HKLM\system\ccs\control\services\LanmanServer\parameters\hidden
```

- Why is this important?
  - If the attacker doesn’t see the machine, there is a greater chance they will ignore it.
    - And why advertise yourself if you don’t have to?

7. Prevent anonymous enumeration

- Network access: Do not allow anonymous enumeration of SAM accounts and shares
  - This setting is not enabled by default
- Consider enabling this setting
- Why is this important?
  - Anonymous users can enumerate sensitive system information over NetBIOS connections if this setting isn’t enabled

8. Disable Run Lists

- In Group Policy settings, consider implementing the following settings
  - Computer Configuration\Administrative Templates\System\Logon
    - Do not process the legacy **run** list
    - Do not process the **run once** list
- Why is this important?
  - Malware frequents these keys
  - However, disabling these run keys may also disable some legitimate applications from starting

9. Require Authentication for RPC enumeration

- In Group Policy settings, consider implementing the following settings
  - Administrative Templates\System\Remote Procedure Call
    - RPC Endpoint Mapper Client Authentication
- Why is this important?
  - Without this setting, unauthenticated accounts can query the endpoint mapper (tcp135) and can obtain sensitive information
  - This information may be used to launch attacks
  - Tools exist to anonymously query the rpc endpoints

10. Disable Name Release on demand

- By default, a Vista system will release its NetBIOS name when it receives a release request from any machine
- Consider setting the NoNameReleaseOnDemand attribute
  - allowed WINS servers are the only ones who can then request a release

```
HKLM\System\CCS\Services\Netbt\NoNameReleaseOnDemand
```

- Why is this important?
  - Helps prevent attackers from releasing legitmate names and potentially spoofing your system

11. Safe DLL Search Mode

- By default, a Vista system will look in the local path first to load a DLL
- Consider setting the SafeDLLSearchMode registry key

```
HKLM\SYSTEM\CCS\Control\Session Manager\SafeDllSearchMode
```

- Why is this important?
  - An attacker may place a malicious DLL in the same remote folder as a document or file
  - When the document is launched from this folder, it will load the local DLL, rather than the system DLL
  - This reg key will force the system to look in the system path locations before looking in local app locations

12. Enable the Firewall

- Ensure the firewall is enabled and is set to block all unsolicted inbound traffic
  - Especially important for traveling systems like laptops

13. Apply Patches

- Two Critical vulnerabilities have already been patched for Vista
  - Allowing for both remote code execution and local privilege escalation
- Be sure to patch vulnerable applications on Vista
  - Internet Explorer, Office, Firefox, etc
- Use a patch management application or Microsoft Update on a regular basis

Resources

- Review this Microsoft document for more details and ideas on how to secure Windows Vista

  http://www.microsoft.com/technet/windowsvista/security/security_group_policy_settings.mspx

Contact Information

Jussi Jaakonaho
Director of Special Operations
Sentor MSS AB
jussi.jaakonaho@sentor.se