Windows Hardening/Defense

Presented by Brian Woodward
Review of the Basics

• Log in with least amount of privileges
• Always use Firewall and AV
• Monitor channels for security advisories and alerts
• Know your system(s)
Patch Early, Patch Often

- Unpatched Systems are the lowest of low hanging fruit
- Have a patch policy documented and stick with it
- Review patches as they are released and determine criticality based on the exploit, threat footprint for your system(s), and whether or not there is a POC or fully weaponized exploit in the wild
- When possible, test patches before rolling out in production on servers
- Most clients should have automatic updates enabled for the OS and any application listening on a socket or used with untrusted data (java, adobe, browsers, etc..)
- Servers should be updated during maintenance windows if possible and depending on criticality (of threat and server)
Exploiting known vulns

- With PenTest apps it is very easy to discover if a server is vulnerable (Nessus, metasploイト, etc..)
- SNMP hacking to reveal server uptime (for Windows it is OID 1.3.6.1.2.1.1.3.0)
- For critical always-on systems they may not have been rebooted for months/years
- Easy to back-date in a vulnerability database and see which patches require a reboot and know for certain they aren’t properly applied
- If you have an account on the server you can use “net statistics server” or “net statistics workstation” to determine uptime.
Security Compliance Manager (SCM)

- This is the framework used for Stripping, Hardening, and Compliance purposes
- Use this to make a Gold/Master image for mass distribution or for individual stand-alone machines
- Explicit guides are defined for hardening the registry and other file system settings
- Templates for OS, Roles, Features, and Applications
- With System Center 2012 you can apply industry standard compliance templates for PCI, FISMA, ISO, HIPAA, etc.
## Account Lock

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Microsoft</th>
<th>Customized</th>
<th>Severity</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account lockout threshold</td>
<td>0 invalid logon a</td>
<td>50 invalid logon a</td>
<td>3 invalid logon a</td>
<td>Critical</td>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy</td>
</tr>
<tr>
<td>Reset account lockout counter after</td>
<td>0</td>
<td>15 minute(s)</td>
<td>60 minute(s)</td>
<td>Critical</td>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy</td>
</tr>
<tr>
<td>Account lockout duration</td>
<td>Not defined</td>
<td>15 minute(s)</td>
<td>30 minute(s)</td>
<td>Critical</td>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy</td>
</tr>
</tbody>
</table>

## Password Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Microsoft</th>
<th>Customized</th>
<th>Severity</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum password length</td>
<td>0 characters</td>
<td>12 character(s)</td>
<td>15 character(s)</td>
<td>Critical</td>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy</td>
</tr>
<tr>
<td>Minimum password age</td>
<td>0 days</td>
<td>1 day(s)</td>
<td>7 day(s)</td>
<td>Critical</td>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy</td>
</tr>
<tr>
<td>Password must meet complexity req</td>
<td>Disabled</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Critical</td>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy</td>
</tr>
<tr>
<td>Maximum password age</td>
<td>42 days</td>
<td>90 days</td>
<td>30 days</td>
<td>Critical</td>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy</td>
</tr>
<tr>
<td>Store passwords using reversible encryption</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Critical</td>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy</td>
</tr>
<tr>
<td>Enforce password history</td>
<td>24 passwords req</td>
<td>24 password(s)</td>
<td>99 password(s)</td>
<td>Critical</td>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy</td>
</tr>
</tbody>
</table>

## IE9 Computer Security Compliance 1.0

### Advanced View

#### Authentication Types

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Microsoft</th>
<th>Customized</th>
<th>Severity</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon options</td>
<td>Prompt for user name</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Important</td>
<td>Computer Configuration\Adm</td>
</tr>
<tr>
<td>Logon options</td>
<td>Automatic logon</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Important</td>
<td>Computer Configuration\Adm</td>
</tr>
</tbody>
</table>

#### Certificate Management

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Microsoft</th>
<th>Customized</th>
<th>Severity</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check for server certificate revocation</td>
<td>Disabled</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Important</td>
<td>Computer Configuration\Adm</td>
</tr>
<tr>
<td>Prevent ignoring certificate errors</td>
<td>Disabled</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Important</td>
<td>Computer Configuration\Adm</td>
</tr>
</tbody>
</table>

#### Key Management

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Microsoft</th>
<th>Customized</th>
<th>Severity</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn off Encryption Support</td>
<td>Disabled</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Critical</td>
<td>Computer Configuration\Adm</td>
</tr>
</tbody>
</table>

#### Least Functionality

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Microsoft</th>
<th>Customized</th>
<th>Severity</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Pop-up Blocker</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Important</td>
<td>Computer Configuration\Adm</td>
</tr>
<tr>
<td>Turn on ActiveX Filtering</td>
<td>Disabled</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Critical</td>
<td>Computer Configuration\Adm</td>
</tr>
<tr>
<td>Use Pop-up Blocker</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Important</td>
<td>Computer Configuration\Adm</td>
</tr>
<tr>
<td>Access data sources across domains</td>
<td>Disabled</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Important</td>
<td>Computer Configuration\Adm</td>
</tr>
<tr>
<td>Disable &quot;Configuring History&quot;</td>
<td>Disabled</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Important</td>
<td>Computer Configuration\Adm</td>
</tr>
<tr>
<td>Scripting of Java applets</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Important</td>
<td>Computer Configuration\Adm</td>
</tr>
<tr>
<td>Logon options</td>
<td>Prompt for user name</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Important</td>
<td>Computer Configuration\Adm</td>
</tr>
<tr>
<td>Use SmartScreen Filter</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Critical</td>
<td>Computer Configuration\Adm</td>
</tr>
</tbody>
</table>
DISA Security Technical Implementation Guides (STIGs) and SCAP

- The STIGs and NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems
- STIGs are lists of all controls and what their values must be in order to be compliant
- In process of migrating to using NIST’s SCAP (Security Content Automation Protocol) to automate compliance monitoring
- Most newer auditing tools have SCAP integration already in place
- DISA FSO Gold Disk was used for older systems (W2k8R1 and Vista are last supported) for automated auditing
You can compare settings of the .INF via the Security Configuration and Analysis Snap-In as above or by using DISA’s provided .XML STIG Viewer on the next slide
Rule Title: System halts once an event log has reached its maximum size.

STIG ID: 3.015 Rule ID: SV-25033r1_rule Vuln ID: V-1091

Severity: CAT III Class: Unclass

Discussion:
A system that is configured to halt if an event log becomes full can create a denial of service situation.

Documentable: No

Responsibility:
System Administrator

Check Content:
Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view.

Navigate to Local Policies -> Security Options.

If the value for “Audit: Shut down system immediately if unable to log security audits” is not set to “Disabled”, then this is a finding.

The policy referenced configures the following registry value:

Registry Hive: HKEY_LOCAL_MACHINE
Registry Path: \System\CurrentControlSet\Control\Lsa

Value Name: CrashOnAuditFail
Value Type: REG_DWORD
Value: 0
NIST Special Publications

- [http://csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html)
- Various SPs that cover a wide range of topics
- SP 800-53 Rev3: Recommended Security Controls for Federal Information Systems and Organizations
- SP 800-61 Rev2: Computer Security Incident Handling Guide
- Many more both published and those still in draft
TIME STAMPS

Control: The information system uses internal system clocks to generate time stamps for audit records.

Supplemental Guidance: Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Related control: AU-3.

Control Enhancements:

(1) The information system synchronizes internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source].

References: None.

Priority and Baseline Allocation:

<table>
<thead>
<tr>
<th>P</th>
<th>LOW AU-8</th>
<th>MOD AU-8 (1)</th>
<th>HIGH AU-8 (1)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>FAMILY:</th>
<th>AUDIT AND ACCOUNTABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU-8</td>
<td>TIME STAMPS</td>
</tr>
<tr>
<td>AU-8.1</td>
<td><strong>ASSESSMENT OBJECTIVE:</strong></td>
</tr>
<tr>
<td></td>
<td><em>Determine if the information system uses internal system clocks to generate time stamps for audit records.</em></td>
</tr>
<tr>
<td></td>
<td><strong>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</strong></td>
</tr>
<tr>
<td></td>
<td><em>Examine:</em> [SELECT FROM: Audit and accountability policy; procedures addressing time stamp generation; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records].</td>
</tr>
<tr>
<td></td>
<td><em>Test:</em> [SELECT FROM: Automated mechanisms implementing time stamp generation].</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AU-8(1)</th>
<th>TIME STAMPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU-8(1).1</td>
<td><strong>ASSESSMENT OBJECTIVE:</strong></td>
</tr>
<tr>
<td></td>
<td><em>Determine if:</em></td>
</tr>
<tr>
<td></td>
<td><em>(i) the organization defines the frequency of internal clock synchronization for the information system;</em></td>
</tr>
<tr>
<td></td>
<td><em>(ii) the organization defines the authoritative time source for internal clock synchronization; and</em></td>
</tr>
<tr>
<td></td>
<td><em>(iii) the organization synchronizes internal information system clocks with the organization-defined authoritative time source in accordance with the organization-defined frequency.</em></td>
</tr>
<tr>
<td></td>
<td><strong>POTENTIAL ASSESSMENT METHODS AND OBJECTS:</strong></td>
</tr>
<tr>
<td></td>
<td><em>Examine:</em> [SELECT FROM: Audit and accountability policy; procedures addressing time stamp generation; security plan; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records].</td>
</tr>
<tr>
<td></td>
<td><em>Test:</em> [SELECT FROM: Automated mechanisms implementing internal information system clock synchronization].</td>
</tr>
</tbody>
</table>
Application Management

- Only install applications from well known (trusted) sites
- Pirated Software and/or Keygens are very risky (very little in life is free)
- May contain rootkits/keyloggers/spyware/malware, never install on production machines
- If installing risky software, do so in a VM and use FileMon/RegMon (newer version called ProcMon) to see exactly what happens
- Minimize applications that are installed on production machines & make sure those that are installed are frequently updated
- Disable any services/features/roles that aren’t needed, every installed application or service may add an additional attack vector
Physical Access

• Very easy to compromise most machines once you have physical access

• Always ensure production equipment has physical controls in place to limit access (this includes kiosk machines)

• Be wary of any unknown dongles plugged into any device

• Always lock screen when not in use, preferably have it do so automatically via Group Policy or Local Security Policy

• Make sure Autorun is disabled for all computers so that if somebody plugs in a found USB Key or DVD that contains malware it doesn’t automatically infect machines

• Anything that leaves a secure location should have full disk encryption (your car is not a secure location)
Audit, Audit, Audit

• Not only should you enable Auditing, but actually review the audit logs frequently and set up alerts to warn you about risky behavior if able to.

• You should review audit logs, but also audit your configuration periodically to make sure nothing has been changed.

• Microsoft Baseline Security Administrator (MBSA) can help identify where you are lacking in Microsoft patches and basic configurations rather easily.
- Broken up into multiple sections
- Each link goes to more detail showing exactly what was queried and why it passed/failed
- Also provides link showing what is needed to resolve the vulnerability
More Audits

• Perform periodic penetration tests between remediation efforts to ensure vulnerabilities are being fully eliminated
• At times you may have to perform multiple updates to resolve one issue or additional reboots
• Nessus Home Feed is a great tool for auditing and is free to scan up to 16 IPs using either credentialed or non-credentialed scans
• Periodically validate what ports you are listening on (Fport or TCPView are great) and make sure that matches with what you expect
• Periodically validate your firewall rules to ensure new rules were not created inappropriately
• Can look at running processes using Process Explorer to identify any anomalies
Nessus

192.168.150.100

Scan Information
Start time: Wed Mar 21 14:40:38 2012
End time: Wed Mar 21 15:01:02 2012

Host Information
Netbios Name: WINDOWS2000
IP: 192.168.150.100
MAC Address: 00:0c:2f:17:55:ea
OS: Microsoft Windows 2000 Service Pack 4

Results Summary
<table>
<thead>
<tr>
<th>Level</th>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Info</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>14</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>3</td>
<td>24</td>
</tr>
</tbody>
</table>

Results Details
0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS

Synopsis
It may be possible to send spoofed RST packets to the remote system.

Description
The remote host might be vulnerable to a sequence number approximation bug, which may allow an attacker to send spoofed RST packets to the remote host and close established connections. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc...).

Solution
See http://www.securityfocus.com/bid/10183/solution/

Risk Factor
Medium

CVSS Base Score
5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score
4.1 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References
BID 10183
CVE CVE-2004-0230
XREF OSVDB:4030
XREF IAV:A-2004-0007
Windows Event Log Auditing

• Check logs for suspicious events such as:
  ➢ Event log service was stopped
  ➢ Windows File Protection is not active on this system
  ➢ The protected System file [file name] was not restored to its original, valid version because the Windows File Protection..
  ➢ The MS Telnet Service has started successfully

• Also look for a large number of failed logon attempts or locked out accounts using event viewer (eventvwr.msc) or from the command prompt using eventquery.vbs | more

• If you want to focus on a particular log you can use eventquery.vbs /L security for the security log
How to Commission a Windows Machine

- It is almost impossible to bring up a Windows machine fully patched, which means it could be vulnerable and compromised before it is even able to download and install appropriate updates.
- When possible use Slipstreaming to integrate service packs, security updates, and critical updates to new builds.
- Do not plug the device into the network unless the firewall is enabled and AV is installed.
- Only punch holes to allow outbound communication to Windows Update until you are fully patched.
- Newer versions of Windows will do this for you automatically to limit your vulnerability footprint on first boot.
Recognize Suspicious Behavior

- Identify if your machine is running particularly sluggish or if a single unusual process is eating up all of the CPU.
- Be cognizant if there are system crashes happening frequently and identify which application is causing them.
- View Task Manager to see if there are any unusual or suspicious processes, especially those running under the SYSTEM or Administrator context.
- Review startup registry keys to make sure that only what you expect is starting up on boot in the HKCU or HKLM\Software\Microsoft\Windows\CurrentVersion hive in the Run, Runonce, and RunonceEx keys.
- Actively review user accounts and make sure no unexpected accounts are present.
Vulnerability Research Sites

- NIST’s National Vulnerability database http://Nvd.nist.gov
- Exploit Database http://www.exploit-db.com
- Security Tracker also has some decent resources http://securitytracker.com

Security Advisory and Alert Sites


• [http://SecLists.org](http://SecLists.org) (Bugtraq, Full Disclosure, and others are worth monitoring)

• NIST [http://csrc.nist.gov](http://csrc.nist.gov)

• FBI’s Infragard [https://www.infragard.org](https://www.infragard.org)