CIP-007/R1 System Configuration Baseline/Security Control Testing

Kevin B. Perry
kperry.re@spp.org · 501.614.3251
Agenda

• Requirement overview
• What we have seen to date
• What really needs to be done
• How you get there
Requirement Overview

R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
Requirement Overview

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.
Current Practices - Environment

- Most entities have test environment for SCADA/EMS environment
  - Usually no fail over capability
  - May feed real-time data
  - Representative systems

- Some entities use standby systems
- Some entities use their backup site
- What about the network? Support systems? IDS/IPS? Access control, monitoring, and authentication systems?
Current Practices - Testing

• Most entities just look at open ports

• Some entities look at minimum controls specified by CIP-007/R8 (Cyber Vulnerability Assessment)
  – Ports and services
  – Controls for default accounts, passwords, community strings

• Some entities perform comprehensive review

• Rarely achieve best practice (comprehensive review usually comes close)
What Are Security Controls?

• How do you “harden” your Cyber Assets?
  – Remove unnecessary software?
  – Disable unneeded services?
  – Remove, rename, disable system user accounts?
  – Configure strong user account policies?
  – Define user rights?
  – Control use of removable media?
  – Require use of a locking screen saver?
  – Allow Remote Desktop?
What Should You Be Doing?

- Start with the typical... Ports and services
  - Look at both open ports and running services
  - Look at more than “listening” ports
  - Look at both TCP and UDP ports
  - Identify and verify service(s) connected to open port

- Things to consider
  - Ports are sometimes dynamic – it is OK to define an acceptable ports range
  - Not all services raise listening ports
What Should You Be Doing?

• Check local user account controls
  – Ensure no controls were altered by the implemented patch or update
  – Controls may include:
    ▪ Minimum and maximum password age
    ▪ Minimum password length
    ▪ Complexity requirements
    ▪ Password history
    ▪ Dictionary checking
    ▪ Account lock out
What Should You Be Doing?

• Verify no user accounts were created of modified unexpectedly.

• If new accounts were found:
  – Verify need for any new accounts
  – Secure any new accounts per CIP-007-3 / R5
  – Remove or disable newly created accounts if truly not required
  – Update baseline documentation as necessary

• Don’t forget community strings on networking devices

• Check status of SNMP on networking devices
What Should You Be Doing?

• Check anti-virus and other anti-malware software
  – Is anti-virus /other anti-malware software installed?
  – Are signature files up to date?
  – Is anti-virus/other anti-malware running?
  – Are there any alerts arising from the update?

• Verify security logging is enabled

• Logs are being locally recorded and/or forwarded to syslog system
What Should You Be Doing?

• Verify status of system monitoring tools
  – Local tools are still installed and operating properly
  – Remote monitoring systems are still able to access updated Cyber Assets and collect security event information

• Verify local security configuration parameters and policies are unchanged

• Verify installed update doesn’t require any “new” patches
How Do I Do That?

- Configuration baseline
  - Created when system is first installed
  - Kept up to date as system is modified
  - Compare current system against baseline

- Tools and Resources
  - System configuration standards/recommendations
  - Operating system Command Line Interface commands
  - Operating system views
  - Application software views
  - System audit utility
How Do I Do That?

• Baseline Configuration Standards/Recommendations
  – Center for Internet Security baseline documents
    http://www.cisecurity.org
  – NERC Security Guidelines
    http://www.esisac.com
  – Microsoft recommendations
  – Vendor recommendations
How Do I Do That?

• Command Line Interface Operating System Commands (MS Windows)
  – Ipconfig /all
  – Netstat –boan
  – Net user
  – Net accounts

• Netstat –boan (or –anp) also works in many Unix environments

• For AIX, use Netstat –antp and Netstat –anup
How Do I Do That?

- Microsoft Windows Control Panel / Administrative Tools
How Do I Do That?

- Microsoft Windows Control Panel / Administrative Tools / Local Security Policy / Password Policy
How Do I Do That?

- **net accounts**

  Force user logoff how long after time expires?: Never
  Minimum password age (days): 1
  Maximum password age (days): 90
  Minimum password length: 8
  Length of password history maintained: 24
  Lockout threshold: Never
  Lockout duration (minutes): 30
  Lockout observation window (minutes): 30
  Computer role: WORKSTATION
How Do I Do That?

- Microsoft Windows Control Panel / Administrative Tools / Local Security Policy / Audit Policy
How Do I Do That?

- Microsoft Windows Control Panel / Administrative Tools / Local Security Policy / Security Options
### How Do I Do That?

- **Netstat –boan**

  Active Connections

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
<th>PID</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>127.0.0.1:5354</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
<td>1396</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[mDNSResponder.exe]</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>127.0.0.1:5354</td>
<td>127.0.0.1:1028</td>
<td>ESTABLISHED</td>
<td>1396</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[mDNSResponder.exe]</td>
<td></td>
</tr>
<tr>
<td>UDP</td>
<td>0.0.0.0:1027</td>
<td><em>:</em></td>
<td></td>
<td>1396</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[mDNSResponder.exe]</td>
<td></td>
</tr>
</tbody>
</table>
How Do I Do That?

- net user

User accounts for \MYPC

-----------------------------------------------

Administrator            ASPNET                   Guest
HelpAssistant            myaccount               SUPPORT_388945a0
How Do I Do That?

Status - Symantec Endpoint Protection

Status

Your computer is protected.

No problems detected.

The following Symantec Security components are installed on your computer:

- **Virus and Spyware Protection**
  - Protects against viruses, malware, and spyware
  - Definitions: Tuesday, May 01, 2012 r2

- **Proactive Threat Protection**
  - Provides zero-day protection against unknown threats
  - Definitions: Thursday, April 26, 2012 r11

- **Network Threat Protection**
  - Protects against Web and network threats
  - Definitions: Saturday, April 28, 2012 r1
How Do I Do That?
How Do I Do That?

• In Cisco IOS, display the running configuration and look for the SNMP information:

Router#show running-config

Building configuration...

...

...

snmp-server community public RO

snmp-server community private RW

....

....
How Do I Do That?

• NIST Information System Audit Logging Requirements

• SANS Information System Audit Logging Requirements
  – http://www.sans.org/resources/policies/info_sys_audit.doc
How Do I Do That?