



**Process Control Systems
Industry Conference**



**U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability**

Bandolier: Auditing Control System Security with the Nessus Vulnerability Scanner



DOE Roadmap Vision

- ◆ **In 10 years control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.**
- ◆ **Goals:**
 - Measure and assess security posture
 - Develop and integrate protective measures
 - Detect intrusion and implement response strategies
 - Sustain security improvements

DOE Roadmap and Bandolier

◆ Goal

- Measure and Assess Security Posture

◆ Milestones

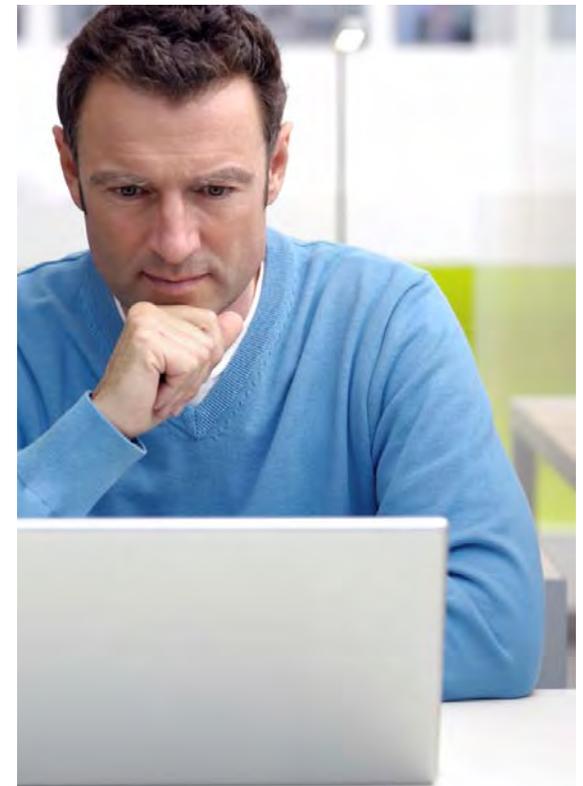
- Helps meet all mid-term milestones for goal:
 - Asset owners performing self-assessments of control systems
 - Metrics available for benchmarking security
 - Asset owners performing compliance audits of control systems

◆ Challenge

- Addresses the Roadmap challenge of “limited ability to measure and assess cyber security posture” and partially addresses the challenge of “no consistent cyber security metrics”.

Identifying the Problem

- ◆ **How do we establish an optimal / best possible secure configuration for our control system servers and workstations?**
- ◆ **How do we verify that this configuration has not changed over time?**
- ◆ **Can we do this using existing security tools at a low or no additional cost?**



The Solution: Bandolier

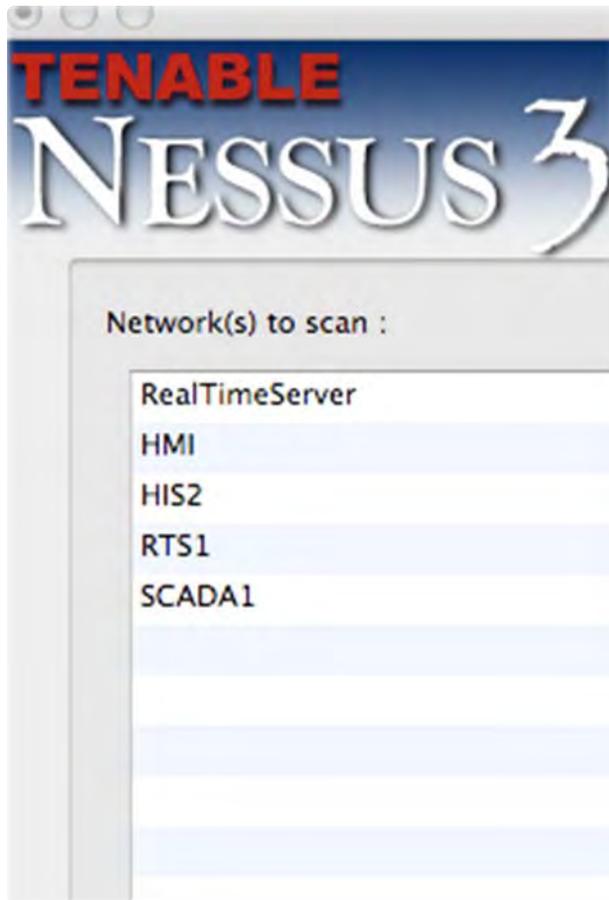
Collaborate with vendor and asset owner partners to identify the optimal security configuration

Assess and extract security configuration data using Digital Bond's expertise (various tools and methods)

Create audit files that can be used in Nessus and other scanners

Deliver through Digital Bond's subscriber content and vendor support channels

Nessus Compliance Checks



- ◆ **Safer than traditional scanning**
 - Secure management connection, not a scan
- ◆ **Evaluates the “known good” rather than the “known bad”**
- ◆ **Customizable for local security policy**
- ◆ **Exporting to OVAL/XCCDF for use in other vulnerability scanners and security tools**

Multiple Levels of Testing

Operating System Settings

- Policies
- Account Management
- Logging
- Ownership and Permissions
- Services
- Processes
- Windows Registry
- Configuration Files

Supporting Application Settings

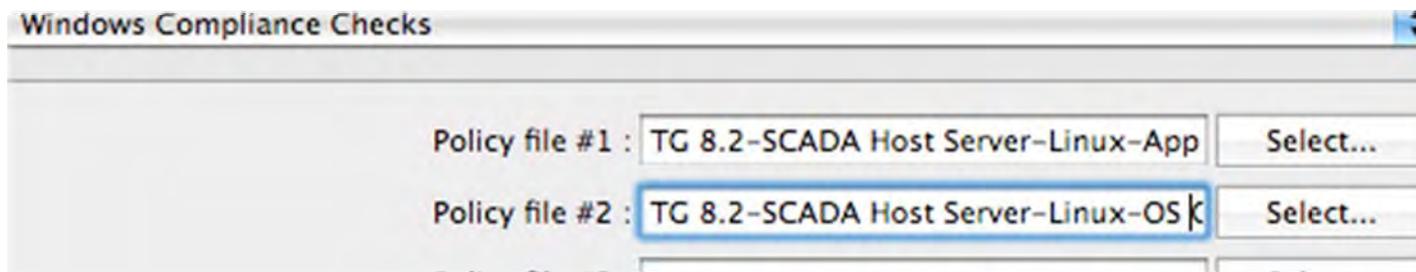
- Web Servers
- Application Servers
- Database Servers
- SSH Servers
- LDAP Servers
- Authentication Libraries

Control System Application Settings

- Authentication and Authorization
- Configuration Files
- Default Accounts
- Logging
- Application File Ownership and Permissions
- Services

Audit File Structure

- ◆ Customizable for site-specific policies
- ◆ Each application component has two files
 - Baseline OS File
 - Application-specific File
- ◆ Can be used individually or in tandem



Example: Baseline Operating System Checks

```
<item>  
name: "Minimum password length"  
value: 8  
</item>
```

```
<custom_item>  
type: FILE_CHECK  
description : "Permission and ownership check /etc/passwd"  
file: "/etc/passwd"  
owner: "root"  
group: "root"  
mode: "644"  
</custom_item>
```

Example: Application Specific Checks

```
<custom_item>  
type: FILE_CONTENT_CHECK  
description: "Determine if permissions are set correctly for the RealTime Server  
(bobjAcknowledge)"  
value_type: POLICY_TEXT  
value_data: "c:\program files\ControlSystemApp\config\Realtime.cfg"  
regex: "bobjAcknowledge.*"  
expect: "bobjAcknowledge, Permission - Control_SCADA"  
</item>
```

```
<custom_item>  
type: FILE_CONTENT_CHECK  
description: "Verify that interactive logins are disabled for the ems user"  
file: "/etc/passwd"  
expect: "ems:x:0:15:SCADA Super User:/lg/.*"  
regex: "ems:x:0:15:SCADA Super User:/lg/./sbin/nologin"  
</custom_item>
```

Bandolier Audit Files: Alpha Release

◆ TelventOASyS DNA 7.5

- Engineering Station (Windows Server 2003)
- Historical Server (Windows Server 2003)
- RealTime Server (Windows Server 2003)
- XOS Workstation (Windows XP)

◆ Siemens Spectrum Power TG 8.2

- SCADA Host Server (Linux)
- SCADA Workstation (Windows XP)
- Web Host (Windows Server 2003)

Bandolier Audit Files: Coming Soon

◆ Audit Files for These Control System Applications

- ABB Ranger
- AREVA e-terra
- Emerson Ovation
- Invensys Wonderware
- Matrikon OPC Server
- OPC Foundation UA Server
- OSIsoft PI
- SNC-Lavalin ECS GENe

Using the Bandolier Audit Files for Nessus

◆ Prerequisites

- Digital Bond Site Subscription (\$100/year)
- Nessus Professional Feed Subscription (\$1,200/year)
 - Many organizations already have a Nessus subscription

◆ Operational Requirements

- UNIX/Linux Hosts
 - SSH Connection (TCP Port 22)
 - root account or set of credentials that can use “su” or “sudo”
- Windows Hosts
 - SMB Connection (TCP Port 445)
 - Administrator credentials

Interpreting the Audit Results

◆ Nessus Scan Results

- Non-compliant
- Inconclusive
- Compliant

◆ Additional Information

- Severity Rating
- Category (based on ISA99 Foundational Requirements)
- Link to page on Digital Bond site
 - More documentation
 - Validation and remediation information



The screenshot shows the output of a Nessus scan for host 'rts1'. It includes scan time details, a table of vulnerability counts, and host information.

rts1

Scan time :
Start time : Wed Jul 23 16:46:15 2008
End time :

Number of vulnerabilities :

Open ports :	0
Low :	47
Medium :	7
High :	84

Information about the remote host :

Operating system :	
NetBIOS name :	
DNS name :	

Report Example

Unix Compliance Checks

"Ownership and permission check for the /scada directory" : [PASSED]
b22002
<http://www.digitalbond.com/research/bandolier/b22002>

Nessus ID : [21157](#)

Unix Compliance Checks

"Verify that interactive logins are disabled for the ems user" : [PASSED]
b22003
<http://www.digitalbond.com/research/bandolier/b22003>

Nessus ID : [21157](#)

Unix Compliance Checks

"Verify that scada-install account has been removed" : [PASSED]
b22004
<http://www.digitalbond.com/research/bandolier/b22004>

Nessus ID : [21157](#)

Summary

- ◆ Establishes optimal security configurations for control system servers and workstations
- ◆ Allows an asset owner or operator to verify the secure configuration has not changed over time
- ◆ Delivers at least twenty audit files for use in Nessus and other scanners
- ◆ Alpha release audit files available



More Information

- ◆ **SCADApedia Articles**

- www.scadapedia.com

- ◆ **Digital Bond Website and Blog**

- www.digitalbond.com

- ◆ **Contact Us**

- info@digitalbond.com



Questions?

Jason Holcomb
Security Consultant and Researcher
Digital Bond, Inc.
holcomb@digitalbond.com