

BANDOLIER

A DIGITAL BOND RESEARCH PROJECT

Thank you in advance for your participation in Digital Bond's Control System Security Research Project funded by the Department of Energy, National Energy Technology Laboratory. The first phase of this project to develop Nessus Compliance Policy Files that will test if your systems are in the proscribed, hardened configuration. This portion of the project is called Bandolier.

In this document we will give an overview of Bandolier and a list of actions we need from you to develop Nessus Compliance Policy Files for your systems.

NESSUS COMPLIANCE POLICY FILES

Tenable Network Security's Nessus Vulnerability Scanner has two plugins that test "compliance" with a vendor or asset owner recommended configuration. One of the plugins is for Windows systems and the other is for *nix systems. These two compliance plugins are available for Tenable Direct Feed customers. A Direct Feed costs \$1200/year and also provides immediate access to new plugins, support and access to the SCADA plugins that Digital Bond developed for Tenable.

With a compliance plugin, Nessus can audit a system against a secure configuration as described in the compliance policy file. **Bandolier will create the Compliance Policy Files so you can use Nessus to audit the security configuration for up to five different types of systems on your control systems.**

The approach is straightforward:

Step 1: Select the systems you want to be part of the project.

There are some factors that make a system more applicable for this project:

- Select a system running a relatively current operating system.
For example, do not select a system running Windows 98 or NT.
- Select a system that can be secured.
A system that cannot be patched or must be configured in a highly vulnerable manner will be of little use. The audit will only verify it is an insecure state.
- Select a system that is widely deployed.
HMI or Operator Consoles are ideal candidates because this will allow a quick and consistent audit of many systems. Similarly, if you are using the same DCS at many power plants the systems in that DCS would be an ideal choice.
- Select a critical system
This may be contrary to the previous criteria, but a critical control server might be a good candidate for a Compliance Policy File even if there is only a primary and backup

system. The Compliance Policy File will identify if anyone has made changes to the secure configuration.

- Similar systems with different configurations can have their own Compliancy Policy
A HMI might run the exact same software as an Engineering Workstation, but the permissions on the system could be quite different.

Step 2: Develop a secure, hardened configuration for each system

The idea here is to great a gold standard configuration for each system that all systems of that type will be measured against. This step is extremely important.

Ideally your SCADA or DCS vendor will assist you with this, but unfortunately many do not. Digital Bond is available to assist you with this step as well. We recommend a conference call between the asset owner, vendor and Digital Bond to determine the best way to get a hardened configuration.

Step 3: Digital Bond will develop the Compliance Policy Files

Once the secure, hardened configuration is available, Digital Bond will create the Compliance Policy Files. This will require a visit to the asset owner or vendor site to gather information on the secure, hardened system. Each system should take between 4 and 8 hours and will not require the asset owner or vendor to be involved, although they are welcome to be with Digital Bond during every step.

Step 4: Test the Compliance Policy Files and train the asset owner

Digital Bond will return to test the Compliance Policy Files. We will run the audit against a system with known changes as well as any other system the asset owner specifies. During this visit we will train the asset owners how to perform the audit and analyze the results.

The Nessus Compliance Plugin will take the values and settings defined in the Compliance Policy File and compare these to the values and settings in the system under audit. This will be a very detailed comparison. Some examples to show the power and breadth of this audit include:

- Verifying file, service and launch access control lists and permissions
- Verifying the USB drives are disabled
- Verifying default accounts have been removed
- Verifying minimum password lengths and other password policy settings
- Verifying critical configuration files have not changed
- Verifying audit settings

You may recognize some of these tests as verifying NERC CiP requirements. There are many, many more audit tests in the Compliance Policy File. The good news is you will not need to specify each test. Simply configure the system in the secure, hardened manner, and Digital Bond will be able to extract all the settings for the Compliance Policy File.

The Nessus audit results are in three categories.

1. High or Holes: The setting in the system being audited conflicts with the setting in the Compliance Policy File. The Nessus report will list the details of the non-compliance.
2. Medium or Warnings: The audit results for a specific setting are inconclusive.
3. Low or Notes: The audit results for a specific setting match the Compliance Policy File.

Ideally a Nessus report will be show only Low or Note findings for all the settings in the Compliance Policy File.

The Nessus Compliance Audit is different than a vulnerability scan. The Compliance Audit will connect to the system using Administrator credentials and gather the required information. The Compliance Audit will not be sending a series of packets from 1,000's of plugins and analyzing the responses like a typical vulnerability scan. Therefore the Compliance Audit results are more accurate and much less likely to cause any impact on your systems.

ASSET OWNER ACTIONS

1. Identify up to five different systems that will be part of Bandolier. Digital Bond will develop up to five Nessus Compliance Policy Files for each asset owner partner in this project.
2. Develop a secure, hardened configuration for each of the five systems. Digital Bond is available to assist with this, and the vendor should be involved if they will cooperate.
3. Schedule a convenient time for Digital Bond to visit and gather data for Compliance Policy Files.

We look forward to working with you do develop this automated security audit capability for your control systems.