Protecting Critical Infrastructure

SCADA Network Security Monitoring

August 1, 2008
(Revision 6)

Table of Contents

Introduction

SCADA Systems

The term “SCADA” is an acronym which stands for “Supervisory Control and Data Acquisition”. It represents a family of protocols which can be used to monitor and manage a variety of machinery and equipment involved with many activities including:

- Power generation and distribution
- Manufacturing processes
- Large-scale Chemical processes
- Transportation of materials

SCADA systems are used for many different types of processes which require monitoring, reporting or control from a computer system. SCADA devices are managed and report information to control centers through a variety of protocols including DNP3, ICCP and MODBUS protocols. SCADA systems are used for control of systems requiring both human and automated interaction.

SCADA Security

Since SCADA networks control very critical processes, any discussion of hackers taking them over or a worm causing an outage quickly escalate into “Hollywood” or “worse-case” scenario. Too often we see examples in the movies (such as Trinity in “Matrix 2” breaking into a power system) or books about how easy it is for these networks to be compromised.

The reality is that the actual SCADA protocols are subject to the same sorts of attack techniques that email, web servers, and file transfer protocols are subject to. These include denial of service, buffer overflows, and so on. Any vendor who sells a SCADA device may have made the same sort of programming errors that Cisco, Microsoft, or any number of other vendors have made.

To make matters worse, the SCADA devices themselves reside on a network which may have other types of traditional vulnerabilities. For example, the servers that run a SCADA protocol may also be running an unauthorized web server or have an un-patched kernel. Any vulnerability in an underlying device on a SCADA network may ultimately result in a potential to control or disable the entire SCADA network.

Assessing the Security of SCADA Networks

From a technology point of view, SCADA networks (that run over routed protocols like IP) are like any other network. They have various nodes and communicate over various protocols. Nodes are added and removed over time as well. However, there are two significant technical differences.

First, SCADA networks tend to make use of older equipment. This is not to say a new SCADA network built today would use Windows NT as compared to Windows 2003, it is that a SCADA network built in 1995 did not see a need to upgrade to Windows 2003. This is also true for the network infrastructure. Second, SCADA networks also run the DNP3, ICCP, and MODBUS protocols. These protocols are just like any other type of protocol such as HTTP, DNS or SMTP in that they have their own “expectations” and “rules” for client and server

communication, timing, data encoding, and data formatting.

Besides the technological differences, there are also much larger political differences. SCADA networks often need to run 24x7 or account for a process that directly generates revenue to the organization. Because of this, any notion of a "security issue" can become politicized. This can directly impact how often security assessments are performed, what is done with the information once it is discovered, and how corrective actions are implemented.

During the past decade, the "network vulnerability scanner" has become a standard tool for quickly and actively discovering all hosts on a network, which services they were running, and which vulnerabilities were present. Unfortunately, the techniques of port scanning, service fingerprinting, and rapidly probing hosts to determine the present vulnerabilities has had negative impact on SCADA networks. Vulnerability scans and network discovery scans have been responsible for locking devices, disrupting processes, and casing erroneous displays in control centers.

Tenable Network Security does offer both active and passive SCADA monitoring solutions. Users of the Nessus vulnerability scanner can obtain a set of vulnerability audits for SCADA devices available through our ProfessionalFeed plugin subscription. These plugins support active network probes as well as traditional host-based software audits. Tenable's Passive Vulnerability Scanner (PVS) also can sniff network traffic and produce vulnerability reports for systems running specific SCADA protocols and services.

Many organizations have adopted network policies and procedures that forbid "traditional vulnerability scans" on production networks because they may cause a repeated outage. These policies and procedures are usually adopted because it is too difficult to actually remediate the root cause of the security issues. In these cases, Tenable would recommend usage of the Passive Vulnerability Scanner. This would allow discovery of not only SCADA specific information, but all network vulnerabilities.

Why the sudden concern about SCADA systems?

First, because SCADA systems are typically used in private and public organizations that provide critical services to the general population such as water, power, telecommunication and other energy, we typically think of these as critical infrastructure. Secondly, various studies and assessments have revealed that there is a lack of security in SCADA systems due to their fragile nature and their susceptibility to disruption with traditional vulnerability assessment techniques. Thirdly, private and public organizations have placed more reliance on the Internet and COTS software which expose SCADA networks to new vulnerabilities. Finally, SCADA networks have always been targets for terrorists, extremists and activists. However, since 9/11 there has been an increased focus and validated threat on these targets. So securing them is in our national best interest.

What You Will Learn

This paper will discuss a variety of SCADA security issues, including an analysis of how active vulnerability scans can disrupt older networks and how Tenable's solutions, including passive network monitoring, can help avoid this. In addition, this paper will discuss how Tenable's solutions can be used to facilitate the Department of Energy recommendations to improve SCADA networks.

Example SCADA Network Attacks

Different Types of Attacks

This section of the paper will discuss various attack scenarios against SCADA networks. They vary in complexity, intent, and require access vectors for execution. The purpose in this section is to give the reader a sense of the many different types of security issues that a vulnerable SCADA network represents.

Effecting Display and Status Screens

A majority of SCADA networks have some sort of "master control panel" or "command center". For reliability, most networks have multiple control centers.

Attackers who gain access to a SCADA network can use a variety of techniques to alter the information consumed by the control center. Insiders to the network may be able to compromise servers on the network and change their data. Outsiders to the network may be able to exploit a vulnerability which gives them similar access to that of an insider.

In either case, information about key processes can be altered at the source of the data to present different information to operators and control systems.

In the case of a worm outbreak, SCADA protocols which send "update" information may be prevented from sending their data. This could cause a display to indicate older data which is no longer accurate. In the case of a hostile intruder who is making unauthorized changes to the infrastructure, they may be able to hide their changes to avoid detection from a control center.

Taking Over the Command Center

If the command center is not protected by security patches, firewalls, intrusion prevention and other mechanisms, it may be possible for an intruder to gain complete control over the SCADA networks.

Modern control centers use a combination of Unix, Windows and Web Based SCADA management tools. Each of these tools may be installed on any number of vulnerable operating systems and applications such as Apache or Microsoft web servers.

An attacker who has control over the SCADA network may not even need to understand the underlying SCADA protocols. Instead they will likely be presented with any user interface that a normal control center operator would use. These displays often include documentation and procedures for emergencies and change control. This information can be used by a remote attacker to understand how to control the SCADA network.

Both the Nessus SCADA checks and the Passive Vulnerability Scanner set of plugins can identify a variety of SCADA management applications and diagnostic software. This can be used to help create "lists" of important devices and then monitor them for attack and access through log analysis.

Disrupting Processes

Any SCADA system which manages a real-time or 24x7 operation can be used to prevent

that operation from occurring. Attackers, intruders and malicious insiders can use network vulnerabilities to send “shut off” and “power off” messages to equipment performing a variety of processes.

If direct manipulation of the SCADA devices is not possible, it may also be possible to prevent communication from a control center to the SCADA devices. This may be all that is required for a hostile agent to prevent “normal” operations of a SCADA network device.

Since SCADA devices are usually physically inconvenient to get access to, an intruder may be able to keep the key systems powered off or out of commission and override any commands sent.

These effects can also be manifested in the case of a worm outbreak. Increased bandwidth usage, support systems being infected with viruses and loading down CPUs can keep a control center from managing their SCADA equipment.

One of the SCADA probes supported through the Nessus ProfessionalFeed is to test if a system that speaks the DNP3 protocol supports an unsolicited response. Typically, DNP3 is used much like SNMP in a polling mode. However, a remote device may be configured to send new information in real-time to the management node via a DNP3 unsolicited response. If this is the case, it may be possible for an adversary remote to the management station or console, to flood it with messages that may consume CPU resources, have false data or prevent legitimate messages from being received.

Damaging Equipment and Property

Lastly, since SCADA devices control many different physical processes, it may be possible to not only disrupt or disable operations, but it may also be possible to create permanent damage.

There are simply too many combinations of physical processes and any safety controls which may be in place to truly assess this vulnerability. Most SCADA plants do not have a “self destruct” sequence we see in the movies. Instead, most high availability or 24x7 physical plants have a variety of physical and electronic safety precautions. For example, anything that moves at all likely has a governor on it which limits a top speed, regardless of what the SCADA control unit says. Similarly, ovens, power generators, power relay stations, and so on all have physical safety limitations built into them for what they can and cannot do.

With that statement in mind, consider the side effects of an insider who knows where the safety mechanisms are and has malicious intent to affect some sort of damage inside those parameters. Examples include disabling air conditioning in a data center or allowing chemical processes to occur longer (such as baking) which require physical cleaning before the equipment can be recovered.

Limitations of Active Scanners

Quick Review of “Active” Scanners

A network vulnerability scanner generates a wide variety of IP packets to discover other active nodes, what services they are running and what vulnerabilities are present. They are often targeted against a broad range of IP addresses and methodically sweep through the

range until each IP has been “scanned”. Scanners have different techniques for determining if a host is alive and for choosing which methods should be employed to discover running services.

Impact to SCADA Protocols

There is nothing really “insecure” about the core SCADA protocols of DNP3, ICCP and MODBUS. The issue is how various SCADA manufacturers have implemented these protocols.

During a port scan, a vulnerability scanner may attempt to open up a port “listened” to by one of the SCADA protocols. If the implementation of the SCADA protocol is not robust, it may lead to a crash or a denial of service. The specific failure mode results in the combination of implementation flaws and scan method. Some failure modes cause immediate “crashes” and some may take several queries to result in a “crash”. Still other failure modes result in slow performance or cutting off access to other services.

For example, Tenable has observed implementation issues on various embedded devices that have a web server. When the web server was accessed with any type of URL other than what the device was expecting, it did not crash right away, but after several requests of this type, the web server was not accessible. What was occurring was that the web server did not handle errors correctly and left a “socket” (for writing data to disk) opened. After so many requests, the embedded OS did not have any more available sockets and the web server ceased to accept new connections.

Tenable has also observed poorly written network daemons which do not handle “port scanning” very well. A “port scan” is used by a vulnerability scanner to attempt many different network connections to a target device. There is no data transferred by these connections, but at the network layer, a connection is established and then immediately severed. Any sort of embedded device running a service that always expects a certain set of bytes or a hand-shake when it is invoked might not receive that when it is port scanned. What can make matters worse is that some vulnerability scanners will “stuff” some payload data into the connection in an attempt to illicit responses and perhaps fingerprint the protocol. So there is a second case where data is received, but the daemon does not know how to process it or recover from the error.

This is extremely relevant to SCADA protocols. A majority of the SCADA devices operate on “embedded” devices. If any of these devices have implemented their SCADA protocols in such a way that errors are not handled gracefully, they could open themselves up to inadvertent denial of service attacks. During a network vulnerability scan, port scans and network probes of SCADA protocols can cause the devices to lock up or become unavailable.

Impact to Older Operating Systems and Network Infrastructure

Similar to issues with SCADA devices, “older” operating systems such as Windows 95, OS/2, Windows NT, Windows 2000, and older versions of Solaris all have a variety of “denial of service” issues which can occur during network vulnerability scanning. Similar issues are known for older versions of Cisco routers and switches.

Many of these attacks have been well documented and are understood by the operating system vendors and the security community. However, for whatever reason, these systems are often present on older SCADA network implementations.

Although the technology involved is not particular to SCADA, if one of these older operating systems is running a SCADA client or server application, any impact to the underlying system will also impact the SCADA application.

Specific Nessus SCADA Checks

Nessus ProfessionalFeed subscription customers and Security Center users have access to several SCADA specific plugins. These plugins were developed for Tenable Network Security by Digital Bond to specifically test and identify a wide variety of common SCADA devices. The list of new plugins and a short description of what they do includes:

- **Areva/Alstom Energy Management System** - Identifies if the remote host is running an Areva/Alstom EMS Server.
- **DNP3 Binary Inputs Access** - Read binary inputs using DNP3 from RTU/IED.
- **DNP3 Link Layer Addressing** - Determines link layer address of DNP3 station by iterating through likely values.
- **DNP3 Unsolicited Messaging** - Determines whether the DNP3 outstation supports unsolicited responses.
- **ICCP/COTP Protocol** - COTP (ISO 7073) is running on the host and may be part of an ICCP server, MMS application or substation automation device that uses IEC61850/UCA.
- **ICCP/COTP TSAP Addressing** - Determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values.
- **LiveData ICCP Server** - Identifies hosts running a LiveData ICCP server.
- **Matrikon OPC Explorer** - Identifies hosts running Matrikon's OPC Explorer tool. These hosts may also have additional diagnostic tools and trust relationships.
- **Matrikon OPC Server for ControlLogix** - Identifies hosts running a Matrikon OPC Server for Allen-Bradley ControlLogix PLC.
- **Matrikon OPC Server for Modbus** - Identifies hosts running a Matrikon OPC Server for Modbus devices and used to access data from PLCs, RTUs and IEDs. OPC servers are commonly used in SCADA and DCS systems to exchange data between different vendor systems and disparate applications.
- **Modbus/TCP Coil Access** - Modbus uses a function code of 1 to read "coils" in a Modbus slave. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a "write coil" message.
- **Modbus/TCP Discrete Input Access** - The Modbus protocol function code of 2 reads discrete inputs from Modbus slaves. The ability to read discrete inputs may help an attacker profile a system.
- **Modicon Modbus/TCP Programming Function Code Access** - Finds hosts with the proprietary Modbus/TCP function code 126 active. An attacker that is able to gain network access to devices like this may be able to reprogram PLC logic or otherwise impact the integrity of physical processes.
- **Modicon PLC CPU Type** - Uses an SNMP Get Request to obtain the Model Information of a Modicon PLC.
- **Modicon PLC Default FTP Password** - Checks for the default FTP username and passwords on a Modicon PLC.
- **Modicon PLC Embedded HTTP Server** - Finds Modicon PLCs running an embedded HTTP server used for configuration or monitoring.
- **Modicon PLC HTTP Server Default Username/Password** - Tests HTTP servers on Modicon PLCs for the default user name and password.

- **Modicon PLC IO Scan Status** - Uses an SNMP Get Request to obtain the scan status of a Modicon PLC.
- **Modicon PLC Modbus Slave Mode** - Uses an SNMP Get Request to obtain the Modbus mode. The Modbus mode is direct, gateway, unit or some combination of these three types. The Modbus mode could help an attacker determine the type of attack necessary against the PLC.
- **Modicon PLC Telnet Server** - Tests Modicon PLC Telnet servers for the default user name and password.
- **Modicon PLC Web Password Status** - Uses an SNMP Get Request to obtain the Web Password Status of a Modicon PLC.
- **National Instruments Lookout** - Identifies hosts running the National Instruments Lookout Application.
- **OPC DA Server** - Identifies hosts running the OPC Data Access Server.
- **OPC Detection** - Finds hosts with OPC application components installed.
- **OPC HDA Server** - Identifies hosts running an OPC Historical Data Access Server.
- **Siemens S7-SCL** - Identifies hosts that contain Siemens S7-SCL Development Tool(s).
- **Siemens SIMATIC PDM** - Identifies hosts running the Siemens SIMATIC PCS 7 PDM Application.
- **Siemens-Telegyr ICCP Gateway** - Identifies hosts running a Siemens Telegyr ICCP Gateway server.
- **Sisco OSI / ICCP Stack** - Identifies hosts running a Sisco OSI/ICCP stack, and most likely acting as an ICCP server.
- **Sisco OSI Stack Malformed Packet Vulnerability** - Identifies hosts running a version of the Sisco OSI stack that can be crashed by a malformed packet.
- **Tamarack IEC 61850 Server** - Identifies hosts that may be running an IEC 61850 server developed by Tamarack Consulting, Inc.
- **Telvent OASyS System** - Identifies hosts running a Telvent OASyS Server.

Performing Active SCADA Scans With Nessus

Tenable has the following recommendations for performing active vulnerability assessments with the Nessus scanner:

- If you have a SCADA test lab, start scanning those devices to identify any potential impact.
- When scanning operational SCADA devices, ensure that a second device is available for “fail over” and also ensure that the device operators are informed of the scheduled scanning.
- If you have access to data from a Passive Vulnerability Scanner, consider tailoring your scan to more robust device such as operating systems which were produced in the last five years.
- For configuring Nessus scans to be “safe”, make sure scan polices have “safe checks” enabled and “thorough tests” disabled. Tenable has previously blogged about “safe checks” usage for Nessus. The blog address is http://blog.tenablesecurity.com.

Political Sensitivity

If an organization responsible for operating SCADA devices feels threatened that vulnerability scanning may impact their operation or indeed show that the operation is running vulnerable applications, they may implement political and technical mechanisms to prevent the scanning.

They may simply ask the security organization or the security organization's management to not scan them. In these cases, there is usually some other form of "assessment" done such as physical inspections, reference server configuration reviews, or even "test lab" auditing. Tenable has observed organizations where these techniques are effective, but have also observed organizations where these techniques were really delay or avoidance tactics.

In cases where there has been a prior incident that "scanning" or a worm outbreak did impact SCADA operations, some organizations have chosen to implement routing and firewall policies to segment the networks. These are effective as long as the perimeter does not change, and Tenable has worked with many different companies running SCADA networks that did not realize other network connections existed outside the firewall.

Tenable Solutions for SCADA Security Monitoring

About Tenable Network Security

Tenable develops an enterprise security software solution suite that provides vulnerability management, intrusion detection, and security event management across entire organizations for effective network security management. Tenable is uniquely positioned to detect vulnerabilities with active and passive scanning and analysis, and host-based patch monitoring for enterprise networks. Key product lines include: Tenable Security Center, for enterprise security management; Nessus Vulnerability Scanner, the leading global technology utilized for vulnerability scanning; Passive Vulnerability Scanner, for passive vulnerability monitoring; and Log Correlation Engine, for secure log aggregation and analysis. More information can be found on these products by visiting our websites at http://www.tenablesecurity.com and http://www.nessus.org.

The next sections will discuss how Tenable's products can be implemented to audit, verify and protect SCADA networks and the benefits that each Tenable module provides.

Tenable's Security Center

The Security Center is fully integrated with Tenable's line of products and is used to manage the information collected by the Log Correlation Engine, Passive Vulnerability Scanner and Nessus vulnerability scanner. The Security Center is a web-based, role-based security management console. It can control and manage active scans and credentialed patch audits with Nessus, and combine this with continuous security updates from the Passive Vulnerability Scanner. This can make auditing SCADA networks much easier. New devices can be quickly identified and devices operating with unauthorized protocols or attempting unauthorized communications can be managed.

The Security Center has the unique ability to automatically "discover" various parts of an enterprise and identify them as an "asset" group. An example of an asset group would be a list of any devices which speak the SCADA DNP3 protocol. This group could be then used as an access control mechanism. Only certain users of the Security Center would have access to this asset list, and only they would be able to analyze, report, or manage the vulnerabilities.

In addition, Tenable customers utilizing the Security Center can build many different types of asset group hierarchies. Security Center groups can overlap. For example, if all SCADA network addresses can be mapped to a physical plant or building, then groups can be created and named after these physical locations. Similarly, if network addresses can be

mapped to a specific SCADA function, then groups can be created as needed for those. Having multiple asset groups allows a manager to view large amounts of security data and quickly identify trends.

Tenable's Passive Vulnerability Scanner

Tenable Network Security offers a network monitoring product that reports a wide variety of security data including active hosts, protocols in use and any vulnerabilities associated with them. The product, known as the Passive Vulnerability Scanner (PVS), is deployed like a sniffer or network intrusion detection system. It monitors network traffic 24x7 and reports on any observed vulnerabilities.

The PVS is ideally suited for monitoring SCADA networks. It passively determines any device which speaks client or server SCADA protocols including DNP3 and MODBUS. While performing this discovery, the PVS can also look for thousands of vulnerabilities in non-SCADA applications such as Apache, Bind and Exchange.

As the PVS discovers what hosts are "alive" and which applications and vulnerabilities they are using, it also catalogs how each host communicates. For any given host, the PVS will log what ports the device "browses" on. This is an excellent way to discern firewall rules or access control policies. For example, the PVS can be used to identify each host on a SCADA network which also uses port 80 for web browsing.

For more intensive analysis, the PVS can also log which unique hosts are communicated with. So for the port 80 example, the PVS can also be configured to not only detect that port 80 is browsed by a node, but also log which other nodes that node connects to on port 80. The same process can be used to identify which nodes communicate on SCADA protocols as well as which other nodes they communicate with.

Since the PVS is a "sniffer", there is NO network impact. As long as the PVS can observe network traffic, it will create a very accurate report of all known SCADA devices and vulnerabilities associated with the monitored network.

Tenable's Log Correlation Engine

Tenable also offers the Log Correlation Engine (LCE) which can be used to aggregate, normalize and correlate logs from various devices. Any application which generates logs can be consumed by the LCE. These consumed logs can be used for correlation rules as well as analyzed for deviations from previous behavior.

The LCE accepts logs from many applications and operating systems associated with SCADA networks. It also accepts SCADA client and server events from the Passive Vulnerability Scanner. Tenable has written a correlation rule set for the LCE which can specifically alert when a new SCADA client or server is active.

The LCE can also accept input from netflow and direct network traffic monitoring. These logs can be used keep a forensic record of every transaction on a SCADA network. If an outage or incident occurs, the LCE can be used to analyze any traffic or activity which occurred prior to the event.

Lastly, the LCE can analyze both network logs as well as firewall and application logs to summarize remote access sources. This can help identify connections which are originating

"outside" of the SCADA network. These connections may not be secured and could require additional monitoring or access control.

Tenable's Nessus Vulnerability Scanner

Tenable produces the Nessus vulnerability scanner. It can be used to identify many different types of applications and vulnerabilities. When managed by the Security Center, it can effectively be used to monitor the security of SCADA networks.

In high-availability environments, Tenable recommends a combination of active, passive and host-based monitoring. The Nessus scanner performs both network scanning as well as host-based patch and configuration audits.

Tenable's Support for Various Intrusion Detection Systems

Both the Security Center and the Log Correlation Engine accept logs from leading network IDS solutions. Combining NIDS events with logs allows for deeper correlation to reduce false positives as well as to more accurately detect a compromise or denial of service incident.

This also reduces the workload of any staff dedicated to network security monitoring. By using only one console, security staff only needs to become familiar with one set of tools for reporting, analyzing logs and correlating events.

21 Steps to Improving Cyber Security of SCADA Networks

Introduction

The U.S. Department of Energy released a white paper named "21 Steps to Improve Cyber Security of SCADA Networks". The paper describes recommendations for how the security of SCADA networks can be improved. This section will highlight how Tenable's solutions can be applied to facilitate a majority of these recommendations. For each of the items, how Tenable's solutions can help is specifically discussed.

1. Identify all connections to SCADA networks

The Passive Vulnerability Scanner can be used to identify all active SCADA devices through passive network analysis. The Nessus vulnerability scanner can also performs scans of SCADA devices with specific SCADA plugins.

This information can be used to create an asset group within the Security Center. This asset group can then be used to analyze network traffic, access logs, firewall logs and other types of data collected by the Log Correlation Engine. This analysis will identify any network activity and report on all connections to the SCADA devices.

Since larger networks often have a certain degree of complexity in them, the Security Center allows for many different types of asset groups to be defined or discovered. For example, the Passive Vulnerability Scanner might identify a SCADA client, but it might also identify it as a running a Windows operating system. These two pieces of information can be used to help build a specific list of Windows servers running SCADA client applications.

2. Disconnect unnecessary connections to the SCADA network

If an access control policy is put into place which forbids connections from certain networks to other SCADA networks, Tenable can help monitor to enforce this policy.

Usually, any form of network access control is enforced with a firewall or a router. The Log Correlation Engine (LCE) can be used to process the logs from these network devices. It can also be configured with the network addresses which are to be denied access and alert accordingly.

Similarly, many of the logs processed by the LCE can also be modified to alert when an access control violation has occurred. For example, simple log events such as a valid web password can be correlated with the source IP address to find evidence or alert when unauthorized networks connect to the SCADA network.

3. Evaluate and strengthen the security of any remaining connections to the SCADA network

For connections which are authorized, modern solutions to strengthen these points usually involve combinations of firewalls, web proxies, intrusion prevention and virtual private networks. The Log Correlation Engine can help aggregate the various logs generated by these different devices and provide a common report about which assets are accessing the SCADA network.

4. Harden SCADA networks by removing or disabling unnecessary services

The Security Center can be used to manage multiple Passive Vulnerability Scanners and Nessus vulnerability scanners. The data collected by each of these technologies can be used to build different types of asset lists. These lists can then be analyzed for common services and devices running additional services can be highlighted for analysis. Also, devices not part of any particular business asset may also not be needed anymore and can be identified for removal.

5. Do not rely on proprietary protocols to protect your system

The Passive Vulnerability Scanner and Nessus scanner can both be used to identify several SCADA clients and servers. The protocols for SCADA devices have been published in several different computer security venues and more information is being disclosed as time goes on.

With Tenable's solutions, a security manager for a SCADA network can easily discover all of their active SCADA devices and identify when new devices are added.

6. Implement the security features provided by device and system vendors

Many core operating systems and network devices include fairly good auditing, securing and logging options. The Security Center and Nessus vulnerability scanner can be used to "log into" these devices and ensure that basic security parameters have been enabled. Tenable calls these checks "compliance checks".

Tenable has many customers who use these checks to ensure their devices are configured according to a corporate policy. For example, all event logging should be enabled on all Windows 2000 servers and all passwords should be changed every 30 days. Policies to take advantage of the basic security features of underlying operating systems can be used to harden SCADA networks.

7. Establish strong controls over any medium that is used as a backdoor into the SCADA network

The "compliance checks", which have been alluded to in the previous step, can be used to ensure that servers have been "locked down". Modern operating systems can be configured such that non-admin users do not have access to insert CDs, USB drives or PCMCIA devices with modems on them.

8. Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring

The Security Center can correlate events from a wide variety of NIDS. The correlation includes real-time vulnerability to event correlation, such that only IDS events which target vulnerable servers are alerted on.

It also includes "per-asset" analysis such that all IDS events going to or from a particular asset group are considered. This makes analysis of any threat to a specific SCADA network much easier.

Lastly, the Log Correlation Engine (LCE) can also accept logs from many different NIDS as well as other sources of data including netflow, network monitoring, firewall logs and application logs. The LCE can perform anomaly detection on the logs and search for changes in behavior which traditional NIDS may miss.

9. Perform technical audits of SCADA devices and networks and any other connected networks to identify security concerns

The Security Center can be used with distributed Nessus and Passive Vulnerability Scanner devices to identify a wide variety of security concerns in any network which connects to the SCADA network.

For the actual SCADA devices themselves, the ideal method to discover them without any impact to operations is to monitor the network with a Passive Vulnerability Scanner. This allows 24x7 continuous discovery of current and new SCADA devices.

Once these devices are "discovered", a manual analysis of their configuration can be used, or if the devices are modern, a direct vulnerability scan can be launched with Nessus. These scans include several dozen SCADA-specific checks written for Tenable Network Security by Digital Bond.

10. Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security

Although the Security Center and each of its managed devices do not specifically perform physical inspections, it can gather a great deal of information which can make a physical inspection much easier. For example consider how useful the following pieces of information can be before a remote site is visited:

- Having a good understanding of the Internet and Intranet traffic usage
- Knowing which computers are managed (part of a domain) and which may have been part of the network unchanged for years
- Having a good idea of the usernames, accounts, and frequency of use of various administrator and end user activity

- Knowing the operating system and running applications of all active nodes on a remote network
- Understanding if the remote network is a source of network attacks, worm outbreaks, or unauthorized activity such as P2P file sharing

In addition to gathering such useful knowledge, the Log Correlation Engine can also be used to gather logs from a variety of physical access control devices.

11. Establish SCADA "Red Teams" to identify and evaluate possible attack scenarios

For an existing Red Team, having the knowledge of what actually is in use on the network can help them identify more realistic attack scenarios. In the last step, we showed how Tenable solutions can be used to gather intelligence about a remote network prior to physical inspection. Those same methods can be applied to gather information about the entire network. For example, consider how useful the following pieces of information can be to a Red Team:

- Knowing the frequency devices are patched or upgraded
- Knowing what ports firewalls are allowing though
- Identifying trust relationships between separate asset groups
- Seeing where real hackers and worms have broken out inside or outside the SCADA network
- Having a list of all software in use on the network
- Knowing which computers are used for administration

12. Clearly define cyber security roles, responsibilities and authorities for managers, system administrators and users

The Security Center is ideally suited to provide the correct level of access to vulnerability, log, compliance and patching information. Almost any hierarchy of security roles and responsibilities can be configured to ensure the right level of attention, reporting and monitoring is given to security issues.

13. Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection

Through active and passive analysis, the Security Center can be used to identify the network architecture. The combination of groups of like devices into business-level assets as well as knowing how the network is connected, makes the Security Center ideal for disseminating this information.

In addition, once "critical" assets are either discovered or manually added into the Security Center, they can be monitored at a closer level. For example, the Security Center could be used to identify all computers as a "control center" for a coal burning power plant. Any changes to these devices or new types of security threats and vulnerabilities can be highlighted specifically for the "control center".

14. Establish a rigorous, ongoing risk management process

A key element of risk management is to monitor the network for new vulnerabilities or evidence of intrusions. The Security Center is ideally suited to gather this sort of information and produce asset based risk management reports.

Once the various types of assets are added into the Security Center, many different types of assets can be reported on. For example, one view can show how all physical buildings as part of a SCADA network compare against each other. Another view can highlight how various devices such as desktops, SCADA clients and servers compare. The Security Center can present this trend data in such a way that small changes can be used to identify increased risk to key assets.

15. Establish a network protection strategy based on the principle of defense-in-depth

When deploying defense in depth, most solutions will employ different types of security and access control technology. The Log Correlation Engine is ideally suited to gather logs from many different devices and report on how that information affects each asset.

16. Clearly identify cyber security requirements

For organizations which have outlined their specific cyber-security requirements, solutions from Tenable can be used to implement a variety of policies. Tenable has helped customers implement a wide variety of programs that reflected an organization's overall desire for a uniform security policy. At an extremely high level, Tenable's products can help identify:

- Unauthorized devices, applications and, networks
- Network activity which is harmful
- Unauthorized information access
- Devices which are not configured to a gold standard

17. Establish effective configuration management processes

The Security Center and Nessus vulnerability scanner can be used to log into a variety of systems to audit their configuration. Tenable includes many of these audits out of the box with Security Center, but they are also flexible enough to create new policies particular to any organization's needs. Non-compliance devices can have their specific configuration issues reported on.

And for general network configuration management, the Security Center, repeated network scanning and continuous network monitoring with the Passive Vulnerability Scanner can be used to detect changes. Changes include new hosts, new applications and new vulnerabilities.

18. Conduct routine self-assessments

As with step 11 and 14, organizations which have the Security Center deployed with log analysis, passive monitoring, or active scanning solutions can perform a wide variety of routine self assessments. These include:

- Identification of all "new" devices and applications
- Performing patch audits of all operating systems
- Identifying changes in communication behavior of SCADA networks
- Identifying new trust relationships between various asset groups

19. Establish system backups and disaster recovery plans

The Security Center can be used to ensure that systems are configured correctly to participate in backup and fail-over operations. Any type of data storage or fail-over technologies will also need their vulnerabilities and security events managed. The Security Center can accomplish this with existing technologies.

20. Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance

The Security Center can be used to display a variety of security data. The data can be presented by business unit, technology, physical locations, protocols and many other ways. By using the Security Center to distill information out of raw security data, senior management can be better informed about what is occurring on their SCADA networks.

21. Establish policies and conduct training to minimize the likelihood that organizational personal will inadvertently disclose sensitive information regarding SCADA systems design, operations, or security controls.

Tenable has made partnerships with companies like Reconnex that can monitor communications for sensitive information. These devices can be configured to detect when inappropriate communications containing human resources, customer data, SCADA configuration information, etc. has been sent outside of the network. The Log Correlation Engine can correlate these events with known asset groups or intrusion detection events.

Conclusion

Tenable Network Security is ready to help answer any of your questions regarding your specific SCADA security concerns. Our solutions offer a very robust and accurate way to discover and report about all security issues on your SCADA network, without any adverse effect.

About Tenable Network Security

Tenable, headquartered in Columbia, Md., USA, is the world leader in Unified Security Monitoring. Tenable provides agent-less solutions for continuous monitoring of vulnerabilities, configurations, data leakage, log analysis and compromise detection. For more information, please visit us at http://www.tenablesecurity.com.

TENABLE Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
TEL: 410-872-0555
http://www.tenablesecurity.com