INEEL/EXT-05-02613

Vendor System Vulnerability Testing Test Plan

James R. Davidson

January 2005

Idaho National Engineering and Environmental Laboratory
Bechtel BWXT Idaho, LLC

INEEL/EXT-05-02613

Vendor System Vulnerability Testing Test Plan

James R. Davidson

January 2005

Idaho National Engineering and Environmental Laboratory
Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-99ID13727

Disclaimer

There are several mechanisms that allow the government and the private sector to contract work with the INL. These include Work-For-Others (WFO) agreements, Cooperative Research and Development Agreements (CRADAs), and non-disclosure agreements (NDAs). Whatever mechanism is used, there are certain key aspects of the work that must be addressed; project scope (including deliverables), project schedule, project funding, and protection of proprietary information.

This test plan covers the vulnerability testing of the SCADA portion of a SCADA/EMS system. It does not test for vulnerabilities in the highly complex EMS portion of the system.

This sample test plan presents only one possible method for testing.

No testing regime can assure that all Targets of Evaluation have been addressed and that all vulnerabilities have been discovered.

No testing regime can assure that a system is secure.

References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government, any agency thereof, or any company affiliated with the Idaho National Engineering and Environmental Laboratory.

ABSTRACT

The Idaho National Laboratory (INL) prepared this generic test plan to provide clients (vendors, end users, program sponsors, etc.) with a sense of the scope and depth of vulnerability testing performed at the INL's Supervisory Control and Data Acquisition (SCADA) Test Bed and to serve as an example of such a plan. Although this test plan specifically addresses vulnerability testing of systems applied to the energy sector (electric/power transmission and distribution and oil and gas systems), it is generic enough to be applied to control systems used in other critical infrastructures such as the transportation sector, water/waste water sector, or hazardous chemical production facilities.

The SCADA Test Bed is established at the INL as a testing environment to evaluate the security vulnerabilities of SCADA systems, energy management systems (EMS), and distributed control systems. It now supports multiple programs sponsored by the U.S. Department of Energy, the U.S. Department of Homeland Security, other government agencies, and private sector clients. This particular test plan applies to testing conducted on a SCADA/EMS provided by a vendor.

Before performing detailed vulnerability testing of a SCADA/EMS, an as delivered baseline examination of the system is conducted, to establish a starting point for all-subsequent testing. The series of baseline tests document factory delivered defaults, system configuration, and potential configuration changes to aid in the development of a security plan for in depth vulnerability testing. The baseline test document is provided to the System Provider,[a] who evaluates the baseline report and provides recommendations to the system configuration to enhance the security profile of the baseline system. Vulnerability testing is then conducted at the SCADA Test Bed, which provides an in-depth security analysis of the Vendor's system.[b]

a. The term *System Provider* replaces the name of the company/organization providing the system being evaluated. This can be the system manufacturer, a system user, or a third party organization such as a government agency.

b. The term Vendor (or Vendor's) *System* replaces the name of the specific SCADA/EMS being tested.

CONTENTS

FIGURES

ACRONYMS

CRADA	Cooperative Research and Development Agreement
CVSS	Common Vulnerability Scoring System
DHS	U. S. Department of Homeland Security
DOE	U.S. Department of Energy
EMS	Energy Management System
HMI	Human Machine Interface
ICCP	Inter-utility Control Center Protocol
INL	Idaho National Laboratory
NIAC	National Infrastructure Advisory Council
PI	principal investigator
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
TBD	to be determined
TOE	Target of Evaluation
VNC	Virtual Network Computing

Vendor System Vulnerability Testing Test Plan

1. TEST BED PROJECT OVERVIEW

The Supervisory Control and Data Acquisition (SCADA) Test Bed established at the Idaho National Laboratory (INL) is a testing environment where control systems, including SCADA systems, Energy Management Systems (EMS) and Distributed Control Systems, are tested for security vulnerabilities. The SCADA Test Bed supports multiple programs sponsored by the U.S. Department of Energy (DOE), U.S. Department of Homeland Security, other government agencies, and private sector clients. This sample test plan applies to the SCADA portion of a SCADA/EMS control system selected for testing at the INL SCADA Test Bed.

1.1 Vendor System Vulnerability Testing

Before performing a vulnerability test on a SCADA/EMS, an as delivered baseline[c] examination of the system is conducted to establish a reference point for all-subsequent testing. The series of baseline tests document factory delivered defaults, system configuration, and potential configuration changes to aid in the development of a security plan for in depth testing. The baseline test document is provided to the System Provider, who evaluates the baseline report and provides recommendations to the system configuration to enhance the security profile of the baseline system.

This test plan supports in depth vulnerability testing of the Vendor's SCADA/EMS, which also includes baseline scanning to validate the implementation the vendors' recommendations from the baseline report. The vulnerability testing will provide functional security testing through an in depth security analysis of the Vendor's system.

1.2 Disclaimer

Testing to determine the vulnerability of control systems is experimental work. As a result, there is no well defined and accepted testing method. Hence, the testing process is evolving and may deviate from this proposed plan during its implementation. Other factors that may affect plan implementation are the available resources, the funding organization's need, and vulnerability findings incurred during testing.

1.3 Customer

The System Provider is the Funding Organization[d] for vulnerability testing of the Vendor's system, and is having the vendor system tested to [*State the purpose/mission of the funding organization*].

1.4 Utility Profile

The INL SCADA Test Bed provides a sample utility environment where the Vendor's system can be tested. In the utility profile established for this test plan, the Vendor's system controls critical assets in the power transmission grid for an area. This portion of the transmission grid is a nexus for the movement

---

c. Baseline, in the context of this document, is the configuration management and testing of an "as delivered system" with all defaults settings left as delivered from the vendor.

d. The term funding organization refers to the program sponsor providing funding to the INL to evaluate the SCADA/EMS. This is typically a Government agency such as Department of Energy or Department of Homeland Security, but could be a private sector partner funding the activity as part of a Work-For-Others program.

of power between two major areas. The utility controls the transmission of generated power upstream to feed an area with inadequate generating capacity downstream. Any impact on the operations of this utility could have a significant effect on the power grid downstream from the control area.

1.5 Attacker Profile

In the attacker profile established for this test plan, the attacker has knowledge of the Vendor's system. Using various techniques, the attacker has penetrated the firewalls and has direct access to the primary network switch for the system.

The attacker's goals are to impact specific portions of the transmission system by taking control of critical components and assets (e.g., transmission grid breakers). By taking control of these breakers, the attacker can isolate the assets downstream from power generation upstream. This control can be obtained by direct manipulation of remote terminal units (RTU), a penetration of the system, or by causing the operator to control these breakers.

1.6 Projected Project Schedule

The sample overall vulnerability testing project schedule is detailed in Figure 1. The actual timeline will vary based on available resources and the funding organization's need.

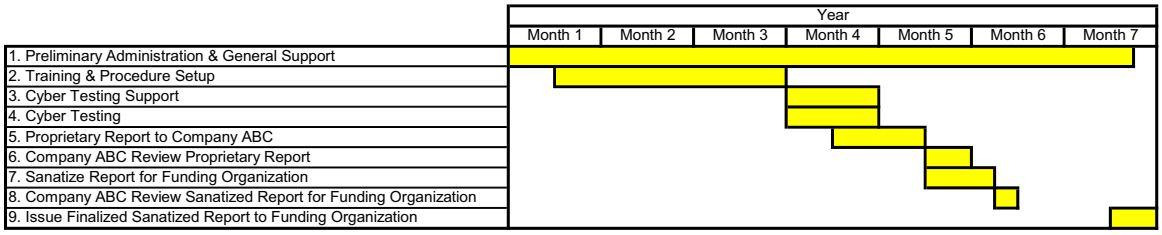

Figure 1. Timeline showing the overall project schedule.

The sample cyber security testing schedule is detailed in Figure 2. The actual timeline will vary based on available resources and the funding organization's need.

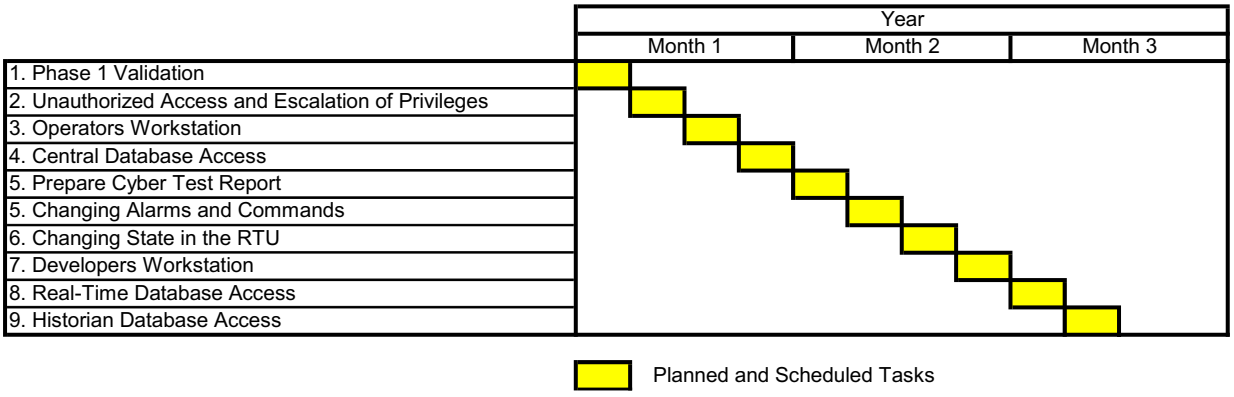

Figure 2. Timeline showing the stages of cyber security testing.

2. SYSTEM CONFIGURATION

The Vendor's system is the latest security enhanced version for the vulnerability testing. Prior to vulnerability testing, the system was configured and checked for proper operation; this activity was equivalent to a Factory Acceptance Test. this test configuration will include a security plan that should describe connections to RTU(s), and Inter-utility Control Center Protocol (ICCP) traffic (if possible).

The images in Appendix A, B, and C detail the Vendor's current test configuration.

2.1 Security Plan

A typical system installation should have an extensive security plan that includes physical, personnel, and cyber security. This includes the establishment of policies, procedures, and methods to protect SCADA/EMS assets, and how to deal with users, user groups, password management, password requirements, password expiration, data protection, data integrity, and disaster recovery. The security plan should also include policies for virus management and individual system component use. The "use" portion is important to preclude the system component from being configured to perform functions beyond its intended use.

In the baseline testing, no security plan was used in configuring the system. This was driven by the need to establish what the Vendor's system defaults were. In this way, we were able to test the system in its worst-case, most vulnerable state, and identify items that need to be changed in the default configuration. A security plan will be adhered to for this round of testing and documented in the final report.

2.2 RTU Connections

The Vendor's system will be connected to at least one RTU. The RTU(s) will be connected to relays and will receive multiple analog signals from distribution relays. This will provide live data traffic to the Vendor's system and allow for detailed testing of the system that was not available in the baseline testing. The amount and types of communication with the RTU and its availability will be limited and will therefore limit the amount of testing in this area.

2.3 ICCP Traffic

It is planned to connect to either another ICCP server on the Vendor's system or an ICCP server in the SCADA Test Bed, if available. This will allow for testing of the vulnerability of communications to and from the Vendor's system ICCP server.

3. TESTING STRATEGY

The main objective of Vulnerability testing is to demonstrate the ability of an attacker to compromise the operational aspects of the Vendor's system in an attempt to damage the system or cause disruption of service by trying to determine the susceptibility of the system to an organized and well thought out, funded, and prepared attack, including the possibility of an insider attack. The test cases outlined in Section 4 of this document are designed to address both types of attackers or threats.

To accomplish the objective we will (1) verify the Vendor's implementation of recommendations from baseline testing and (2) perform the system security test of the Vendor's system using the SCADA

Test Bed at the INL. Testing of the Vendor's system will occur from the switch level, meaning that the attacker has penetrated any firewalls and is operating on the same network segment as the SCADA/EMS system.

Although a portion of the testing is an evaluation of the security measures implemented as a result of the baseline recommendations, the majority of the testing is allocated to test specific targets or functional pieces of the Vendor's system. To accomplish this, the SCADA/EMS test team generated a list of Targets of Evaluation (TOEs). Each of these targets has a specific test case outlined in Section 4 of this document. Each TOE is given a priority based on the level of functionality it provides to the Vendor's system and its operational impacts to the system. Each test case is allocated an appropriate amount of testing time based on the priority level of the TOE. However, there are no guarantees that the targets will be achieved in the time frame allowed. If they are not, the status will be documented along with the steps accomplished and the suggested path forward. This will also include the estimated difficultly in completing the task and suggestions to prevent the attack.

Vulnerability testing will not include code reviews, such as looking for buffer overflow vulnerabilities and other insecure practices. It is expected that subsequent rounds of testing will include this level of scrutiny, but, due to the complexity of the source code, it is not expected that a full code review will be conducted in these tests.

Wireless connectivity to the Vendor's system will not be tested; the Vendor does not provide wireless capabilities as part of the delivered system.

4. PROPOSED TEST CASES

The testing period and time allocations for each test case discussed in this section are negotiated as part of the overall testing activity. Both the funding organization and the Vendor are involved in this negotiation.

Vulnerability testing and reporting is scheduled over a [TBD] period. Based on available resources, the testing and evaluation team develops a list of desirable test cases and allotted an appropriate amount of time for each. Total allotted testing time is [TBD] man-hours.

The proposed test cases begin with a validation of the vendor supplied, baseline recommendations and the implementation of a security plan followed by the functional testing contained in the TOEs list.[e]

4.1 Baseline Validation

Baseline testing identifies potential security vulnerabilities and offers suggestions for remediation to the Vendor in the baseline Test Report. The Vendor then provides configuration recommendations to their system to improve the security profile of the system. The system then undergoes configuration changes that implement the recommendations of the Vendor and implements the Security Plan. Baseline validation testing will compare the as delivered system to the security driven configuration to validate the effectiveness of these changes and document the results.

---

e. A TOE is a portion of the Vendor's system that is subject to testing. A TOE includes any combination and/or part of an IT technique, concept, method, product, system, or infrastructure and its associated administrator and user operational documentation. A TOE can be referred to as a product subset. A TOE is bounded by environmental assumptions. These assumptions are located in the Rules of Engagement.

Baseline validation testing is also essential to provide the testing team with the required information for further TOE testing. This validation test case provides the basic reconnaissance needed for enhanced testing and evaluation.

4.1.1 Allocated Testing Time

Baseline Validation testing is scheduled for the [TBD] period testing. System wide scanning and data analysis is scheduled to utilize [TBD] hours.

4.1.2 Test Procedure

A basic information technology (IT) assessment of the Vendor's system is the first step needed in gathering the required data to perform all subsequent tests. This basic IT assessment includes port scanning, vulnerability scanning, network mapping, password cracking, and network sniffing.

Vulnerability scans, including port scans, will be run on each of the computers. Vulnerabilities found will be compared to those found in baseline testing. All reported vulnerabilities will be verified as much as possible and included in the report to the Vendor.

The Vendor's principal investigator (PI) is responsible for the overall system configuration and operational status. During this test case, the PI's primary responsibility is to implement the test team's security policy and configure the system to Vendor's specifications. The Vendor's PI also assumes all responsibility for restoring the system to operational status, should the testing affect the system in any way.

The primary task for the testing team is to perform the system analysis tests needed to produce the data for Baseline validation. The goal is to perform the same tests as those performed in the baseline test and then provide detailed information on the changes implemented in Vendor's system.

For convenience, the following is a list of typical tools used during baseline testing; it is expected that most of these tools will also be used in the vulnerability testing so that the data from both phases of testing can properly be compared:

- Msinfo32.exe – A standard tool for scanning Windows computer's software and hardware
- AIDA3 – Provides supplemental information to the Windows System Configuration output
- Net Diagnostics – Windows XP network diagnostics tests
- Sys_check – Tru64 system configuration information tool
- Superscan 4.0 – A freeware program for scanning ports and IP address
- Cisco Assessment Tools – Used for detecting and configuration changes on network equipment
- STAT Scanner – A MS Windows vulnerability scanner
- John the Ripper – A multiplatform password-cracking tool
- Nessus – An open source multiplatform vulnerability scanner
- Nmap – An open source network and port scanner
- Ethereal/TCPDump – Network monitoring software.

4.1.3 Data Requirements

Prior to running this test case, the test team will receive complete network diagrams and detailed system configuration information.

Output data from the configuration, port, and vulnerability scans will be compared with output from the same scans performed on the original baseline system. This output data is also used in the subsequent TOE testing because it provides the detailed reconnaissance information needed by the testers.

A successful test will compare the enhanced security configuration against the findings documented in the baseline report. This will assess whether or not the recommended configuration changes implemented as a result of the baseline report have been addressed in the configured system, and test the overall security of the Vendor's system.

4.2 TOE – Unauthorized Access and Escalation of Privileges

Accessing a computer system without authorization is a common action of an attacker. Another attacker might be authorized to use a computer system (insider), but with restricted privileges. The intent of this TOE is to examine the possibility of accessing a system and/or escalating privileges such that an attacker can execute actions (i.e., become a "super user") on the SCADA/EMS system.

The ability for an attacker to obtain super user status on a machine is very dangerous because it gives the attacker total control of the system. With root or administrator level privileges, an intelligent attacker can take the necessary steps to corrupt the system, disrupt service, or act the part of a legitimate operator.

Privilege escalation can be executed remotely or locally from a system console. Remote privilege escalation is generally accomplished through service or application exploitation. Local privilege escalation is similar in nature, but can utilize services and/or software that are not available remotely.

An example of a remote attack is exploiting a web sever (e.g., Apache or IIS) or file sharing service (e.g., Samba or network file system). Local privilege escalation could include password cracking or attacking a process that is running with elevated privileges.

The following is a list of typical computer systems in a Vendor's system configuration; this system list is ordered in priority of attack for this TOE:

- Application Server
- Active Directory Server
- Operator Console
- Data Acquisition Server
- Developer Console
- Historian Server
- ICCP Server.

4.2.1 Allocated Testing Period

Due to the priority of this TOE, testing is tentatively scheduled for [TBD] hours.

4.2.2 Test Procedure

The goal for this test case is to obtain administrator, root, or operator level access on the identified SCADA/EMS computer systems.

Figure 3 is a sample threat tree that outlines some of the typical steps in obtaining unauthorized access to an information system. This tree is not all-inclusive, but is used to demonstrate the many avenues that are available in an attempt to compromise a system. The paths in a threat tree are dependant upon the specific configuration of the system being attacked.

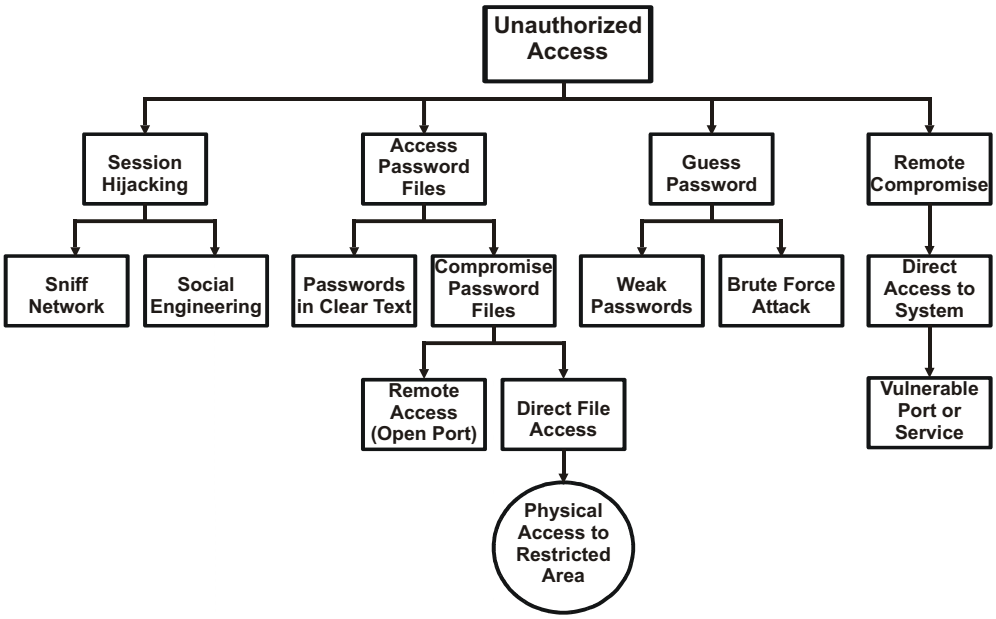

Figure 3. Unauthorized system access.

Utilizing the data from the Baseline validation test (reconnaissance), the testers will attempt to exploit known vulnerabilities to accomplish this test. The data gathered provides a clearer picture to the Test Team and allows for refinement of the threat trees. In particular, vulnerable services and ports as well as weak password implementation will be checked.

4.2.3 Data Requirements

The reconnaissance data from the Baseline validation test is essential information for the testers.

All exploit attempts, and their results, will be documented and published in the Vulnerability report. It is also understood that privilege escalation on a system may not provide the attacker with the ability to perform any actions on the SCADA/EMS system; therefore, each exploit attempt will also detail what type of SCADA/EMS level compromise was actually possible once the exploit was successful.

Successful tests are those that allow the attacker to gain access to a system as a user capable of performing SCADA/EMS operations.

4.3 TOE – Operators Workstation

The operator's consoles are the workstations used for command and control of the SCADA/EMS. These computers provide the human-machine interface (HMI) for the Vendor's system, making them a critical component in a SCADA/EMS system because it is the primary means of controlling the environment. In this configuration there is one operator's console.

The operators console has access to control the power grid, but does not have the resources to change the SCADA/EMS system. This is the function of the developer's console. In a typical SCADA/EMS system, physical access to the operator's console is often easier than the developer's console and is therefore targeted in this testing before the developer's workstation.

This test case examines the possibility for an attacker to gain unauthorized access to the system with the ability to issue commands using the HMI, thus having complete control of the SCADA/EMS system. For example, an attacker has direct access to all system functionality and HMI screens by using the XP Remote Desktop service.

4.3.1 Allocated Testing Period

Testing of this TOE is tentatively scheduled for [TBD] hours.

4.3.2 Test Procedure

The goal for this test case is to evaluate the multiple avenues by which an attacker can gain access to the operator's workstation. This can include physical access to the system or some other means of remote access.

The most desirable end result is to have an interactive desktop view of the operator's workstation. This will allow the attacker to see all of the HMI screens and to interact with the SCADA/EMS environment through the HMI. With this goal in mind, it is proposed that the testers attempt to gain physical access, or interactive remote access using tools such as Remote Desktop or Virtual Network Computing (VNC).

Figure 4 is a sample threat tree for unauthorized access to a PC or workstation. These are just some of the methods an attacker might use to compromise the system. This tree details the specific need for remote graphical access, not just remote shell access. This is due to the goal of the TOE to include interactive access with the HMI screens.

4.3.3 Data Requirements

The reconnaissance data from the Baseline validation test and the results from the privilege escalation tests are critical information for the testers.

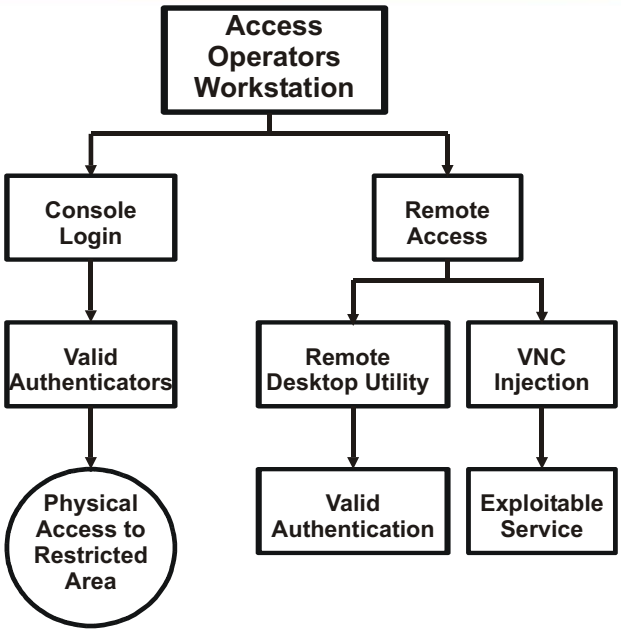

Figure 4. Access the operations workstation.

The output data for this test case is the successful or unsuccessful control of the SCADA/EMS system though the operator's workstation. This will include the details of how access was gained. For example, Remote Desktop may not be enabled by default, but an Administrator level compromise may allow the attacker to enable Remote Desktop and then accomplish this goal.

A successful test is determined by the ability of the test team to gain an interactive remote logon session. This session should include more than shell access and should mimic that of a Remote Desktop session or a VNC session. The goal is to have access to the HMI screens and functionality.

4.4 TOE – Central Database Access

The Central database typically contains all the information about the SCADA/EMS system network including configuration information, EMS data, system maps, and all information tying the data gathered from the RTU (in the real time database) to the descriptive data used in the HMI.

The Central database is of particular interest due to the complete system information contained therein. For example, the HMI only contains simple information that is used by an operator familiar with the SCADA/EMS. The Central database, however, contains information on the SCADA/EMS components shown on the HMI screens. Due to these facts, the Central database is the primary target for this test.

Keeping the information in the SCADA/EMS databases confidential is a high priority because it is what allows for a coordinated, intelligent, and perhaps stealthy attack. This information could be used to identify critical assets for a cyber and/or physical attack.

4.4.1 Allocated Testing Period

Testing is tentatively scheduled for [TBD] hours.

4.4.2 Test Procedure

The goal for this test case is to evaluate the multiple avenues by which an attacker can gain access to the Central database. The attack can include direct access to the database system after remotely accessing the machine or access using "trusted" systems that normally connect to or receive data from the Central database. The main objective is to mine information from the Central database.

The Central database contains critical system information, raw data, real-time information and information for constructing some of the other databases in the SCADA/EMS system.

Central database systems can be configured in a variety of ways with regards to authentication. Typically there are two methods of authentication:

1. Directory service, network or operating system authentication

2. Database authentication using Central database user accounts and passwords

The test team will attempt to authenticate to the database server and access the database information using Active Directory and/or Operating System authentication. The team will also attempt to establish a connection to the server via the central database port and authenticate using default Central database user accounts and passwords.

Another process for accessing the Central database is to compromise the developer's workstation. The developer's workstation is likely to have access to the Central database because a SCADA/EMS developer is the person creating, updating, or modifying that information. Figure 5 is a sample threat tree for compromising a Central database system and outlines some of the possible paths for gaining unauthorized access to the data.

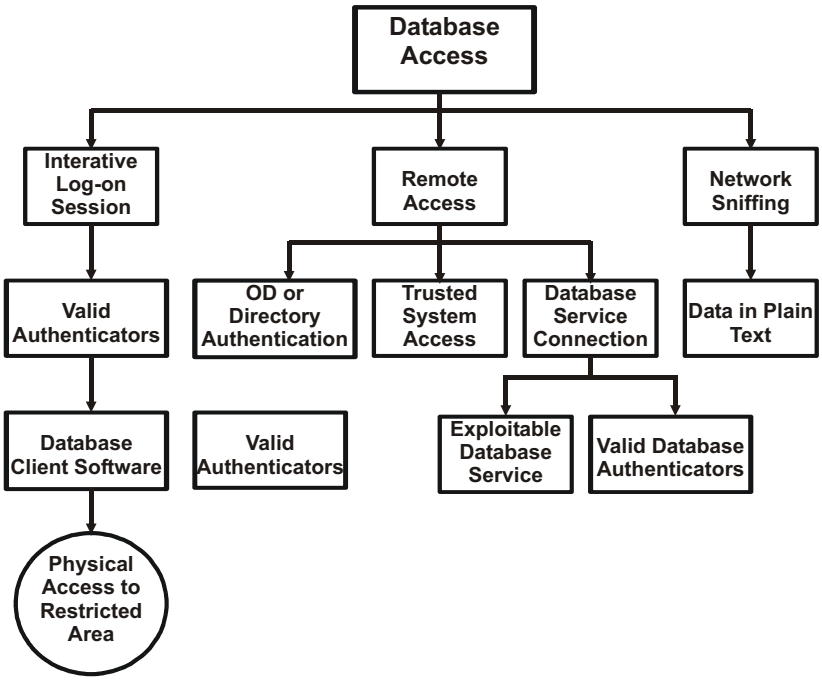

Figure 5. Central database.

4.4.3 Data Requirements

The reconnaissance data from the Baseline validation test and the results from the privilege escalation tests are critical information for the testers.

The key data to capture in this test is the amount of information mined from the Central database. Likewise, it is assumed that some custom software may be needed in order to mine useful information from the system. The custom software used for this process will be part of the reporting data.

A successful test is one in which the attacker retrieves data from the Central database that can be used to provide a detailed view of the SCADA/EMS environment.

4.5 TOE – Changing Alarms and Commands

Alarms and commands are the method for communication between the HMI and the Data acquisition server. Commands are sent by the HMI to take an action in the SCADA/EMS system. Alarms are sent by the data acquisition server to alert the operator of various events. The integrity and timely delivery of alarms and commands is critical in a SCADA/EMS system.

4.5.1 Allocated Testing Period

Testing is tentatively scheduled for [TBD] hours.

4.5.2 Test Procedure

One method of attack might be to analyze the network traffic among the data acquisition server, the developer's workstation, and the operator's workstation (HMI), and to develop a man-in-the-middle (MITM) style of manipulation.

Two suggested attempts are:

1. Place an additional computer on the SCADA/EMS network that Address Resolution Protocol (ARP) poisons the switch and then manages the traffic between the console and the real-time server

2. Inject software on the console or the real-time server that analyzes network traffic prior to allowing it to be processed by the application layer of the system

If time allows, another attack or test is to perform security analysis on communication traffic protocol used by the data acquisition server and the HMI. Analysis of this protocol might discover potential vulnerabilities in the protocol handlers.

Delete and/or change alarm or command traffic between the real-time server and the operator console. Change the state (or spoof) of the operator console so that the operator has the wrong picture of the system status.

4.5.3 Data Requirements

A detailed composition of the message format and the complete process for changing both an alarm and a command is valuable information for obtaining this TOE. This includes documentation on communication traffic protocol, used by the Vendor's system to communicate with the operator consoles.

A communications map of how the data acquisition server and the HMI transmit messages may also be built to help with this effort.

A successful test is one that disrupts normal command and alarm traffic by deleting messages from the network or changing the content of the message. Another successful test would be the creation of bogus command or alarm messages.

4.6 TOE – Changing State in the RTU

A RTU is a hardware device used in SCADA/EMS systems for interfacing with various analogue and digital signals. RTU's are often used for controlling equipment such as substation breakers. Changing the state of an RTU could send a command to the connected components of the electrical grid and control them (e.g., opening a closed breaker).

A man-in-the-middle attack between the communication output of the SCADA/EMS and the RTU will be attempted in this TOE.

4.6.1 Allocated Testing Period

Testing is tentatively scheduled for [TBD] hours.

4.6.2 Test Procedure

The goal for this test case is to analyze the communication link between the SCADA/EMS communication port and the RTU and develop a means to send a message to change state in the RTU. The COM port will be used to attempt to attack this target. This will be done on a serial port connection and a TCP/IP connection if available.

4.6.3 Data Requirements

The reconnaissance data from the Baseline Validation test and the results from the privilege escalation tests are critical information for the testers.

Detailed information on the communication format between the system and RTU must be obtained in order to perform the man-in-the-middle attack.

A successful test is one that changes the state of the RTU.

4.7 TOE – Developers Workstation

The developer's workstation is a workstation used for system development of the SCADA. It is a tempting target because it usually has direct access to system resources (e.g., the central database) that are not accessible to other operator consoles or workstations.

This test case will examine the possibility for an attacker to gain unauthorized access to the system with the ability to access other portions of the SCADA/EMS system, acting in the role of a SCADA/EMS developer.

4.7.1 Allocated Testing Period

Testing is tentatively scheduled for [TBD] hours.

4.7.2 Test Procedure

The goal for this test case is to evaluate the multiple avenues by which an attacker can gain access to the developer's workstation. This can include physical access to the system or some other means of remote access (e.g. Remote Desktop, VNC, etc.).

Figure 6 is an abstract Threat Tree for unauthorized access to a PC or workstation. These are just some of the methods an attacker might use to compromise the system.

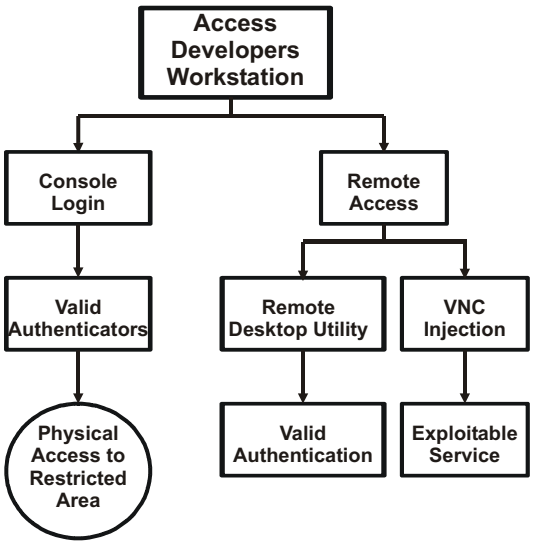

Figure 6. Access the developer's workstation.

The most desirable end result is to have an interactive desktop view of the developer's workstation. This will allow the attacker to see all of the HMI screens and to interact with the all of the other SCADA/EMS systems. With this goal in mind, it is proposed that the test team attempt to gain physical access, or interactive remote access using tools such as Remote Desktop or VNC.

4.7.3 Data Requirements

The reconnaissance data from the Baseline Validation test and the results from the privilege escalation tests are critical information for the testers.

The output data for this test case is the successful or unsuccessful control of the SCADA/EMS system though the developer's workstation. For example, Remote Desktop may not be enabled by default, but an Administrator level compromise may allow the attacker to enable Remote Desktop and then accomplish this goal.

A successful test is determined by the ability of the test team to gain an interactive remote logon session. This session should include more than shell access and should mimic that of a Remote Desktop

session or a VNC session. The goal is to have access to the developer's resources (e.g. development environment, database access, HMI, etc.).

4.8 TOE – Compromise the Communication Processor

A RTU should only change state when a command is received from the Vendor's communication processor. If an attacker can directly control the RTU, or control the RTU from the communication processor, they then have the power to control a portion of the SCADA/EMS system.

In this test-bed configuration, simulated analogue signals are sent from the RTU connected to a relay board (simulator), to the data acquisition server. Commands to open or close a breaker are typically sent from the HMI. In this test, we will try to send a command directly to the RTU from another host on the network.

4.8.1 Allocated Testing Period

Testing is tentatively scheduled for [TBD] hours.

4.8.2 Test Procedure

The goal for this test case is to compromise the communication processor and send messages directly from the communication processor to the RTU. By penetrating the communication processor, the attacker would not need a specific definition of RTU type, communications connection type, or RTU protocol used. With the Vendor's system, if you could penetrate the communication processor and act as the SCADA/EMS system, you only need to talk the Vendor's default RTU protocol.

This test case will analyze the network traffic between the communication processor and the RTU and develop a means to send a message to change state in the RTU. This will involve network traffic analysis.

4.8.3 Data Requirements

Detailed information on how the communication processor operates in the Vendor's system.

Detailed information on the format of messages sent to the communication processor and messages sent from the communication processor to the RTU.

A successful test is one that spoofs the communication processor into sending messages to the RTU or direct control of the communication processor with the ability to generate and send messages to RTU.

4.9 TOE – Data Acquisition Database Access

The Data Acquisition database contains all the information gathered from the SCADA/EMS system in real time. For example, this database contains the latest values reported by a RTU for a particular segment in the grid.

4.9.1 Allocated Testing Period

Testing is tentatively scheduled for [TBD] hours.

4.9.2 Test Procedure

The goal for this test case is to evaluate the multiple avenues by which an attacker can gain access to the Data Acquisition database. The attack can include direct access to the database system after remotely accessing the machine or access using trusted systems that normally connect to or receive data from the database. The main objective is to mine information from the Data Acquisition database.

The test team will attempt to authenticate to the database server and access the database information.

4.9.3 Data Requirements

The reconnaissance data from the Phase 1 Validation test is essential information for the test team. In addition, the results from the privilege escalation tests area critical information for the testers. Along with the reconnaissance data, the test team requires detailed information on the operations and configurations or the real-time database (i.e. identification of the files used, communication channels, etc.).

A successful test is one in which data is retrieved or changed in the real-time database. It might also include the denial of service of the real-time server so that updates are neither transmitted nor received.

4.10 TOE – Historian Database Access

The Historian database contains all the information from the central database selected for archive.

4.10.1 Allocated Testing Period

Testing is tentatively scheduled for [TBD] hours.

4.10.2 Test Procedure

The goal for this test case is to evaluate the multiple avenues by which an attacker can gain access to the Historian database. The attack can include direct access to the database system after remotely accessing the machine or access using “trusted” systems that normally connect to or receive data from the database. The main objective is to mine information from the Historian database.

The test team will attempt to authenticate to the database server and access the database information.

4.10.3 Data Requirements

The reconnaissance data from the Phase 1 Validation test is essential information for the testers. In addition, the results from the privilege escalation tests area critical information for the testers. Along with the reconnaissance data, the test team requires detailed information on the operations and configurations or the historian database (i.e. identification of the files used, communication channels, etc.). It is assumed that some custom software may be needed in order to mine useful information from the system. The custom software used for this process will be part of the reporting data.

A successful test is one in which the attacker retrieves data from the historian system that can be used to provide a detailed view of the SCADA environment.

5. VULNERABILITY SCORING

While conducting vulnerability assessments, it is important to define a set of metrics with which to score or rank the importance of the discovered vulnerabilities. The Department of Homeland Security's National Infrastructure Advisory Council (NIAC) developed a common scoring system to evaluate vulnerabilities found in a variety of information systems. Their goal is to provide a set of metrics for evaluating vulnerability's threat to an information system. This scoring system, which is still in draft form, is known as the Common Vulnerability Scoring System (CVSS). At the time of writing this test plan, the current CVSS version was Draft 0.2.

The INL Test Team does not endorse any single tool or method for scoring or ranking vulnerabilities, but it does recognize the importance of defining a set of metrics that are used, and can be reused, to quantify the finding of a vulnerability assessment. Due to this need, (enter scoring method here) has been selected for scoring the vulnerabilities found during vulnerability testing.

As a special note, it is not the intent of any testing conducted by the SCADA Test Bed to provide and overall security ranking of a SCADA/EMS system. The ranking of vulnerabilities found in Vulnerability testing is solely for the use of the Vendor in directing future improvements to the Vendor's system.

The abstract found in the (enter scoring method here) Document states:

(Enter scoring method abstract here)

Appendix D contains an example matrix from CVSS 0.2. This example shows how the different metrics of vulnerability contribute to an overall base score, temporal score, and environmental score. The explanation of these scores is found in the Common Vulnerability Scoring System document.

6. RULES OF ENGAGEMENT

Outlines of the assumptions that the test team can make and a definition of the environmental conditions in which all parties are to operate are contained in this section. The INL Test Team and the site test team established these rules of engagement as a foundation for how the Vulnerability testing will be performed. At a minimum, all activities conducted during Vulnerability testing will adhere to the following agreements and assumptions:

Agreements

- All information will be protected from unauthorized access in accordance with the data security agreement.
- The INL will suspend testing at the request of the site Vendor's PI, or if there are legitimate safety, security, or operational concerns.
- Maintain frequent communications with the site Vendor's PI on the status of testing activities.

- Upon completion of testing, the INL will work with the site Vendor's PI and provide detailed information on how to return computer systems to their original configuration so that no systems are left in a compromised condition.
- In the unlikely event that performance testing adversely affects an information system, the INL will work with the site Vendor's PI to determine the nature of the problem and restore the system to its desired state of operation.
- The INL Test Team may exclude some cyber systems from performance testing activities

Assumptions

- All cyber testing is performed from the same network segment as the Vendor's SCADA/EMS (the attacker is plugged into the same switch).
- The vulnerability tester will operate as if all items listed in the security document are indeed implemented.
- The servers are located in a separate, physically secure, area from the developer and operator consoles. The attack team will not have physical access to these servers.
- The attack team will perform some testing directly on the operator and developer consoles. These tests will demonstrate some of the insider threat capabilities.
- The operator and developers consoles have no removable storage. This includes floppy disk drives, CD/DVD drives, or USB ports. All have been physically removed from the consoles.

6.1 Security Plan Adherence

The INL Test Team will test the Vendor's system under the assumption that all security measures outlined in the security plan are implemented. This will allow the site Vendor's PI to prepare the system for operations without worrying about controls and procedures that are impractical to implement (e.g., some physical security protection measures).

6.2 Equipment Assumptions

INL Test Team will test the Vendor's system under the assumption that the system is not in production use and there are no real world consequences for any operational downtime (the lights are not going to turn off when the system shuts down).

INL Test Team is planning on testing the Vendor's system while live data is available, at a minimum, between Vendor's system and a single RTU. This live data is critical in performing the enhanced operational tests.

6.3 Software Assumptions

Although the Vendor's software source code is available to the INL, the INL Test Team will not examine the source code prior to performing any security tests. Software code review is well beyond the scope of this set of tests.

7. STAFFING

Staffing will be varied depending on the expertise required to fully implement this plan and the resources available to meet these needs. The table below attempts to provide the key personnel for this test plan.

Name	Responsibility	Clearance Requirements
	PI on Vendor's system	"Secret"
	Co-PI on Vendor's system	"Secret"
	Cyber PI - Vulnerability testing and reporting	"Secret"
	Windows security scans and analysis	"Secret"
	Vulnerability testing support as needed	"Secret"

8. INFRASTRUCTURE PLAN

The test environment is the Vendor's donated system. Vulnerability testing will be conducted from computers connected to the system switch. Testers will provide their own machines and tools for testing the system.

8.1 Software Requirements

The Vendor has supplied the system to be tested and the cyber research group will supply the software, hardware, and operating systems required for testing.

8.2 INL Owned Testing Hardware

The following table lists the testing hardware owned by the INL.

Hardware Description	Manufacturer	Model
Remote Telemetry Unit		
Distribution Relays		
Communications Processor		
Signal Generator		
Relays and Displays		

8.3 Test Bed Environment

Test personnel will have access to the Vendor's test cubical after signing the Vendor's security requirements document. A table and connection to the Vendor's network switch will be available for use during testing.

9. REPORTS

A log will be kept of all the tests performed and their results. An internal cyber security testing report is due at the end of the testing period. This report will be used to create a report for the Vendor that includes vulnerabilities and suggested mediation for the Vendor's system. Other required deliverable external reports are a Vulnerability Report protected at an agreed upon level and a Sanitized Report for public release.

10. RISKS AND CONTINGENCIES

The following table lists the risks and contingencies associated with this test plan.

Risk #1	The Vendor's system is not fully configured and ready for testing on January 3, 2005.
Contingency #1	Baseline validation testing will begin even if the Vendor's system has no live data. Baseline validation testing does not require live data. During this period, it is expected that the site Vendor's PI's will continue to work on bringing the Vendor's system into operational status.
Contingency #2	All live data testing (TOE testing) will be suspended until the Vendor's system is in operational status.

11. MILESTONES AND DELIVERABLES

The following table outlines major milestones and deliverables for this phase of testing.

Milestone Task	Start Date	End Date	Deliverables
Test Plan			Test Plan Approval
Cyber Test Report			Test Result Summary
Vendor's Test Report			Test Results & Recommendations
Sanitized Final Report			Sanitized Report for public release

Appendix A

Physical Components

Place diagram of the Vendor's Physical Components here

Appendix B

Vendor's System

Place Vendor's system Process Flow Chart Here

Appendix C

INL's SCADA Test Bed

Place Diagram of INL's SCADA Test Bed here.

Appendix D

Common Vulnerability Scoring System

(Note: this is an example of a scoring matrix; the matrix for the scoring system used should be used to replace the example below)

Common Vulnerability Scoring System (CVSS) Version 0.2

	Vulnerability	Microsoft Outlook Express Scripting vulnerability	Microsoft LSASS vulnerability	BGP potential DOS	
	CVE number	CAN-2004-0380	CAN-2004-0533	CAN-2004-0589	
	URL				
Invariant Metrics	Access Vector	REMOTE	REMOTE	REMOTE	LOCAL
	Access Complexity	HIGH	LOW	HIGH	HIGH
	Authentication	NOT-REQUIRED	NOT-REQUIRED	NOT-REQUIRED	REQUIRED
	Confidentiality Impact	COMPLETE	COMPLETE	NONE	NONE
	Integrity Impact	COMPLETE	COMPLETE	NONE	NONE
	Availability Impact	COMPLETE	COMPLETE	COMPLETE	NONE
	Impact Bias	NORMAL	NORMAL	AVAILABILITY	NORMAL
	(invariant score)	**8.0**	**10.0**	**4.0**	**0.0**
Temporal Metrics	Exploitability	FUNCTIONAL	FUNCTIONAL	UNPROVEN	UNPROVEN
	Remediation Level	OFFICIAL-FIX	OFFICIAL-FIX	UNAVAILABLE	OFFICIAL-FIX
	Report Confidence	CONFIRMED	CONFIRMED	CONFIRMED	UNCONFIRMED
	BASE SCORE	**6.6**	**8.3**	**3.4**	**0.0**
	Collateral Damage Potential	NONE	NONE	NONE	NONE
	Target Distribution	HIGH	HIGH	HIGH	NONE
	ENVIRONMENTAL SCORE	**6.6**	**8.3**	**3.4**	**0.0**