SANDIA REPORT
SAND2005-2846P
Unlimited Release
Printed March, 2005

Penetration Testing of Industrial Control Systems

David P. Duggan

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

Penetration Testing of Industrial Control Systems

David P. Duggan
Michael Berg
John Dillinger
Jason Stamp

March 7, 2005

[Page intentionally left blank]

INTRODUCTION

Performing network penetration testing on Industrial Control Systems (ICS) should not be taken lightly. There are many things that can go wrong. These systems were designed and built to control and automate some real world process or equipment. Given the wrong instructions, they could perform an incorrect action causing waste, equipment damage, injury, or even deaths. These types of systems include systems also known as Supervisory Control and Data Acquisition (SCADA) systems, Electric Management Systems (EMS), Distribution Control Systems (DCS), or Process Control Systems (PCS). The next three paragraphs provide real examples of the danger.

While a ping sweep was being performed on an active SCADA network that controlled 9-foot robotic arms, it was noticed that one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated. Luckily, the person in the room was outside the reach of the arm.

On a PCS network, a ping sweep was being performed to identify all hosts that were attached to the network, for inventory purposes, and it caused a system controlling the creation of integrated circuits in the fabrication plant to hang. The outcome was the destruction of $50K worth of wafers.

A gas utility hired an IT security consulting company to conduct penetration testing on their corporate IT network and carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours. The outcome was the loss of service to its customer base for those four hours.

Identifying the vulnerabilities within a SCADA system requires a different approach than in a normal IT network. In most cases, systems on an IT network can be rebooted, restored, or replaced with little interruption of service to their customers. Their world is mostly virtual-based, connecting only peripherally to the physical world. SCADA systems control physical processes and therefore have real world consequences associated with their actions. Some actions are time critical, while others have a more relaxed timeframe. One shouldn't connect a test machine to the network and perform scans of a SCADA system without understanding the possible consequences of this testing.

APPROACH

The first question to ask is "Why is penetration testing necessary for this system?" First identify the threats of concern. Is the threat from people, rogue hosts, or something else? Is it malicious or accidental? Would this penetration test likely identify vulnerabilities that can be exploited by the threats of concern?

When performing a penetration test of an IT system, there are several steps that are generally used. Depending upon the tools used, one or more of these steps may be integrated together. They are:

1. Identify hosts, nodes, and networks.
2. Identify services available on items from #1, above.
3. Identify possible vulnerabilities for items found in #2, above.

There are usual actions associated with each step, above. In the table below, we provide the usual list of actions, along with other actions that may be taken instead, making the outcomes of any testing safer. These new techniques may make the job a little harder, but are intended to mitigate problems associated with active penetration testing.

Activity	Usual Actions for IT	Preferred Actions for SCADA
Identification of hosts, nodes, and networks	Ping Sweep (e.g. nmap)	1. Examine CAM tables on switches. 2. Examine router config files or route tables. 3. Physical verification (chasing wires). 4. Passive listening or IDS (e.g. snort) on network.
Identification of services	Port Scan (e.g. nmap)	1. Local port verification (e.g. netstat). 2. Port scan of a duplicate, development, or test system.
Identification of vulnerabilities within a service	Vulnerability Scan (e.g. nessus, ISS, etc…)	1. Local banner grabbing with version lookup in CVE. 2. Scan of duplicate, development, or test system.

The common theme of all the preferred actions is that there is no active component to put traffic on an operational network or against an operational system. The activities involved in an IT penetration test are only one way to obtain the information of interest. There are other less intrusive ways to gather most, if not all, of the same information. These other methods will allow collection of the information necessary for understanding the vulnerability of the SCADA system, without the risk of causing a failure, while testing.

While any assessment of the SCADA system is being performed, SCADA operations personnel must be aware that testing is occurring, and be prepared to immediately address any problems that arise. If manual control of the system is possible, personnel capable of performing manual control must be present during the security testing.

Some of the factors to consider when choosing active vs. passive testing of SCADA systems is that these systems have very limited resources as compared to normal IT systems. Since these

systems have longevity much greater than their IT counterparts, the CPU's are typically generations behind the state-of-the-art and can be easily overtaxed. They usually are run on legacy networks at slow speeds, which can be overwhelmed by the volume of traffic generated during active testing. Since they are special purpose, sloppy programming may go unnoticed through regular use and only be identified when scanned over a wide range of use as IT scanning tools provide. Network stacks on most SCADA systems fall into this category. While these flaws need to be identified and addressed, this should be done on test equipment and not on operational systems controlling critical processes.

Because of the limitations of these systems to defend themselves against attacks, there must be design considerations used to protect them from outside influences. Complete separation of the SCADA system from other IT systems and networks is the best method for accomplishing the protection. However, this is unpractical in a great number of cases since data from the SCADA system is used to provide input to business decisions and is needed on an almost instantaneous basis. Development of secure data exchange methods between components of the SCADA system and the IT system is required, with the goal of preventing any direct connection from the IT system to any SCADA system components.

A security examination of a SCADA system should not cause more problems for the operation of the system than absolutely necessary. Since these systems are different than regular IT systems, they require special handling when security, or any other, testing is performed. There isn't a security tester that wants to be known as the person that turned out the lights in a city, flooded a valley, or released a toxic cloud of chemicals into the air.

SCADA systems are in transition, as legacy systems are replaced with more modern systems vulnerability and risk assessment methods may need to change. However, with the diverse installations that currently exist, vigilance is required on the part of the auditor. The auditor needs to understand the SCADA system under test, the risk involved with the test, and the consequences associated with unintentional stimulus or denial of service to the SCADA system.