SERVICE DESCRIPTION

Operational Technology Security Assessment

Service Scope

Trustwave's penetration testing services are delivered by SpiderLabs, an advanced security team within Trustwave focused on forensics, ethical hacking, application and network security testing. The team has performed thousands of forensic investigations, ethical hacking exercises and application security tests globally.

The broad experience of the team extends beyond regular corporate information technology environment to various operational environments including:

- Industrial Control Systems
- Smart Grid
- Building Management Systems
- Telecommunications Infrastructure
- Embedded Systems and Hardware

The SpiderLabs specialists deliver hundreds of ICS/OT security assessments each year to assist clients in various industry sectors across the US, Europe, Australia and Asia identify weaknesses in their industrial control systems and operational technology infrastructure including:

- Energy and Resources
- Transportation
- Telecommunications
- Mining

Our experience in the energy and resources sector includes multiple assessments across various core systems including:

- Transmission and distribution systems
- Bulk generation systems
- Usage and meter management systems including advanced metering infrastructure and Smart Grid systems.
- Individual PLCs and sensor infrastructure

Operational Technology Penetration Test

Approach and Methodology

Industrial Control System/SCADA Security Assessment

Approach

The Trustwave SpiderLabs ICS/SCADA penetration testing service results in an in-depth test of the entire target environment and provides a detailed deliverable with both tactical and strategic recommendations to improve the security posture of the target environment. These recommendations are both actionable and advisory in nature and are presented to the customer.

The approach to assessing the security of ICS/SCADA environments similar in many respects to our corporate infrastructure penetration testing there are considerations unique to ICS environments that must be accounted for.

Industrial networks utilize specialized systems and custom protocols that not only provide additional attack surface, require specialist skills and techniques to assess effectively. In addition, many systems are not available offline and can cause significant business impact should these systems be disrupted.

SpiderLabs ICS/SCADA penetration tests are designed to effectively assess the security risks facing these networks while minimizing the risk of system disruption.

Network Mapping and Reconnaissance

In the process of assessing the security of the ICS environment, building an accurate network map of the devices and systems in the environment is a critical task at the beginning of the penetration test. This typically includes:

- Network mapping
- Enumeration of network segments
  - Network mapping from various points in the ICS and corporate network to understand and identify segmentation controls
- Review external footprint (if applicable)
  - Remote access interfaces
  - VPN

System Identification and Classification

The network map would not be very useful if the systems located on the network were not identified and classified. Another probe is performed of the systems discovered to identify and classify systems and services. The data gathered is used to classify the systems by function. This phase typically includes:

- Port scanning
- Service enumeration of common ICS services
  - ICCP
  - Modbus
  - DNP
  - OPC UA

    - RPC
    - Ethernet/IP
    - Profnet
- Service enumeration of unknown or custom services
- System identification techniques including:
    - Sniffing Ethernet/IP traffic to obtain Critical Infrastructure Protection (CIP) device identifiers and attributes
    - Sweeping DNP3 requests that solicit a response (e.g., REQUEST_LINK_STATUS) to discover DNP3 slave addresses
    - Capture an EtherCAT frame or a SERCOS III Master Data Telegram to obtain all slave devices and time synchronization information

System Vulnerability Identification

Each in scope host and all associated listening services are probed to locate potential vulnerabilities. Using a large working knowledge of exploit techniques, public information, and extensive private vulnerability research, the Trustwave SpiderLabs consultants catalog all the potential attack vectors that may be exploitable.

Vulnerability Exploitation and System Compromise

Trustwave SpiderLabs consultants will then devise several attack strategies as planning step prior to the subsequent phases. As systems are compromised, key security contacts will be notified. When purpose-built exploits or potentially risky exploit code is required to exploit a system, the authorized point of contact(s) are given the opportunity to decide if the particular system should undergo additional tests.

Upon granting such permission Trustwave SpiderLabs will utilize additional techniques to further penetrate the target system and the environment as a whole. This may include:

- Exploiting known weaknesses in the systems and protocols used
- Exploiting poor segmentation controls to cross network boundaries
- Reverse engineering custom protocols and exploiting identified weaknesses
- Exploiting weaknesses in asset control and system hardening (e.g. USB attacks)
- Capturing credentials and exploiting authentication mechanisms
    - HMI Users
    - ICCP server credentials
    - Master node addresses
    - Historian database credentials

Smart Grid Security Assessment

Approach

Advanced Metering Infrastructure and Smart Grids offer many benefits to energy providers and their customers however the interconnectedness of key systems required in Smart Grid environments presents expanded attack surface that increases the risk of security vulnerability in the system.

SpiderLabs Smart Grid penetration tests are designed to effectively assess the security risks facing these systems while minimizing the risk of system disruption.

Methodology

The approach to testing Smart Grids builds on the standard ICS/SCADA penetration test methodology (see above) but is expanded to include elements unique to Smart Grid systems:

- Remote metering systems
- Remote billing systems
- Demand/response energy systems
- Remote connect/disconnect systems
- Payment systems
- Consumer face systems and applications (see Section A for our detailed application testing methodology).
- Physical smart grid devices (see below for our detailed hardware assessment methodology)

Hardware/Embedded Security Assessment

Approach

The approach to testing the security of devices embedded systems is broken down into three distinct components representing the key threat scenarios relevant to these devices.

1. Hardware Security Assessment
2. Firmware, OS and Application Assessment
3. Network Communications Assessment

Hardware Security Assessment

The hardware security assessment will determine how susceptible the device is to attacks against the physical hardware. This may include:

- Assessment of physical tamper protections
- Non-invasive tests/attacks
    - PCB reverse engineering
    - Data remnants
    - Fault injection/glitching
    - Power analysis
    - Acoustic analysis
    - Review of any available diagnostic interfaces
- Semi-invasive and invasive attacks (if permitted)
    - Decapping
    - Fault injection
    - Microprobing
    - Optical imaging

  - IC Modifications

Firmware, OS and Application Assessment

The firmware, OS and application assessment will review the software running at various layers on the device. This may include:

- Extracting the firmware from the device
- Reverse engineering and static analysis to identify vulnerabilities in the firmware
- Reviewing the hardening of embedded operating system running on the device
- Assessment of any binaries running on the device
- Assessment of any exposed web applications/interfaces including:
  - Data Protection
  - Information Disclosure
  - Account Policy
  - Session Management
  - Injection
  - Authentication & Authorization
  - Logic Flaws
  - Application Resource handling
  - Cryptographic controls
  - Bounds Checking (e.g. buffer overflows)

Network Communications Assessment

The network communications assessment will review the network interfaces, traffic and transport security controls on the device. This may include:

- Network interface and service analysis
- Passive traffic analysis
- Active traffic analysis
- Analysis of any custom network protocols (text based or binary):
  - Reverse engineering
  - Protocol fuzzing
  - Exploitation
- Analysis of the implementation and use of any open/documented protocols (e.g. IPv4/6, TCP, UDP, ARP, DNS, DHCP etc.)
- Review of any transport security controls (e.g. TLS, certificate pinning etc.)

Deliverables

Following the conclusion of the engagement, findings will be made available via the Trustwave SpiderLabs' Managed Security Testing Portal. The deliverables will be both strategic and tactical in nature, presented in a drill down format that will be highly accessible to both management and operational staff. Each finding will have a risk scoring associated with it as well as contain detailed technical information pertaining to the nature of the finding. Each finding will also be presented with clear guidance on how to remediate the issue.