2009

SCADA Forensics with Snort IDS

Craig Valli

Edith Cowan University

Snort IDS for SCADA Networks

Craig Valli
secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Mount Lawley WA, Australia

Abstract - *This paper is a research in progress paper outlining an approach using open source IDS (Snort) and honeypot (nepenthes, honeyd) technologies to create a resilient layered defensive approach for SCADA and control systems networks.*

Keywords: SCADA, Snort, nepenthes, honeyd, honeypot, forensics

1 Introduction

There is a growing discipline of network forensics with traditional Ethernet networks running TCP/IP. This is a discipline that utilizes networking science to investigate problems of network malfeasance both pre and ante incident. Packet capture and subsequent interpretation of the network dump files of packets and protocols whether this be in near real time or post incident provides invaluable insights into attacks. The capture files can be replayed and analysed until such time as a causation is found for a particular incident.

There are a range of commonly available packet capture and analysis utilities available for the modern network forensics practitioner. Most of these tools are dominated by the analysis of TCP/IP protocol suite and its inherent issues, whether these issues be at the actual packet level reaching through various protocols up to the final presentation of the network stream at the application layer. From this plethora of available open source and commercial tools there are a limited number of tools that natively tackle the protocols that are in the SCADA domain such as ModBUS, DNP3.
This research is aimed at utilizing relevant open source tools namely Wireshark, Etherape and Snort IDS to provide a platform for detecting, reporting, capturing, analyzing and ameliorating network borne threats to SCADA and control systems networks. An extension to this work is planned in that once these threats and modes of compromise are better known and understood then the development of customized detection modules for deployment in honeypots namely honeyd and nepenthes is planned.

Throughout the remainder of the paper the term SCADA will be used to encompass all protocols and systems used to control SCADA and industrial control system networks.

2 The need to protect SCADA

There is little argument that SCADA and control networks need protections from network borne attacks or malfeasance. There are a range of documented issues relating to SCADA or control system networks. The reports from various agencies indicate that SCADA systems as highly vulnerable to attack or compromise that would result in catastrophic failure of national critical infrastructures and ultimately the economic well being of that nation.

SCADA and control system networks drive much of the wealth generation processes of the modern industrial complex. Many of these systems are used to run the modern industrial complexes that supply modern Western nations with many of the services and goods that they take for granted. These systems are to be found in but not limited to petroleum complexes, power generation grids, water supply networks, sewerage networks and most other complex systems that require constant computer-based monitoring or control. Compromise or even minor disruption to these systems could have catastrophic outcomes and downstream consequences resulting in massive economic impact or significant loss of life[1-5].

Significant disruption to any one of these critical infrastructures through deliberate attack or inadvertent attacks such as the SQL slammer worm [4] can inflict catastrophic long term economic damage to that goes well beyond the cost of the material damage to the infrastructure itself. Disruption of gas services as result of an industrial mishap in Western Australia alone in 2008 almost saw that States economy grind to a halt [3]. The loss of capacity at ~ 40% was sufficient to have considerable downstream effects that for instance caused laundry for hospitals to be shipped in from other Australian states until increased supplies could be obtained.

SCADA devices/systems are built to run, monitor or control a particular process typically as a part of combined automated process that results in a "product". Many of these devices and systems in which they operate are intended to run for the life of the project, mine or product cycle which can be decades not weeks. As a result SCADA systems have a larger than expected level of legacy hardware and software installed, the old engineering adage if it is not broken do not fix it was a paragon in many of these systems. This was a perfectly acceptable paradigm in which to operate when many of these companies/entities did not connect to any network except their own production or engineering network, and were never connected to the corporate network that is then possibly connected to the Internet. This phenomenon has now changed as smaller companies merge and combine to become bigger entities as the pressure of globalisation and economic rationalisation increase. This leads to network infrastructures that are often comprised of different disjointed legacy network systems. Further adding to the entropy with respect to the security stability is the attachment of the corporate network and the increasing use of the Internet as a backbone network into the vanguard of SCADA networks.

Many older SCADA and control systems were proprietary systems with protected proprietary protocols and related processes. These legacy systems are now being upgraded and are being moved to open platform systems that utilise open protocols such as Distributed Network Protocol 3 (DNP3). New generation SCADA systems also use modern open standard communications protocols and networks to provide access to the SCADA systems for control and command. These networks even if totally private will almost atypically run the TCP/IP range of protocols and supporting services. Many providers due to costs are also replacing dedicated hard physical links to control/command interfaces commonly refererred to as HMI (Human Machine Interfaces) with ethernet or wireless links. Consequently, some of this SCADA or control traffic may actually travel on or rely upon open networks such as the Internet to provide these control conduits that were once private and fixed. Of greater risk is that some of these systems utilise open protocol wireless systems such as 2.4Ghz WiFi for these command and control conduits.

Various reports as far back as the late 1990s have indicated the need for better diligence when dealing with these systems. The knowledge of SCADA vulnerability is now spreading into the hacker or blackhat communities with systems such as the Metasploit framework having several specific SCADA exploits now installed for use and available publicly. One of the problems is that the SCADA community still believes that security via obscurity, the keeping of a secret in this increasingly inter-connected and global world is a viable and sustainable option.

3 The research approach

This research is aimed at providing a working framework for testing, modifying and where possible providing remedy for known and published vulnerability of SCADA and control systems. It does not seek nor does it not intend to provide a platform for exploit development. This quasi-experimental research is aimed at producing systems hardened against incursions from would be attackers using known vulnerability or exploit to penetrate systems or simply to disrupt systems. Later on when combined with honeypot technologies the ability to track or capture zero day exploits will also be a possibility.

The two main protocols that will be initially examined in this research are ModBUS and DNP3. It is not the intent of this paper to provide an in depth analysis of DNP3 or ModBUS protocols. These types of open protocol will be used increasingly as a result of the growing convergence of technologies and the business imperatives to have these types of supporting systems for billing and asset control. It should be noted that in the SCADA and control systems space there is the use of various proprietary protocols and they are not well represented at this stage in the open source community. The research approach is to produce a robust method and architecture for forensic examination of network borne threats using DNP3 and ModBUS as vectors and then apply lessons learned over other less known protocols in the space.

Experimental Procedure for Snort SCADA

1. **Environmental Scanning**

   This will include scanning of blackhat, hacker, vendor and CERT sites for vulnerability announcements or trace. The only restriction is that the exploit be network borne, it does not specifically have to attack the underlying network protocol but could also be malicious payload or instructions for a PLC.

2. **Production of Replay/Replication of vulnerability**

   This stage will involve the production of the vulnerability for replay via a script or code base preferably. This also allows for easy testing and verification of the exploit.

3. **Analysis of vulnerability**

   This is the extended analysis of the *modus operandi* of the exploit. Seeing what limits or bounds are contained in the vulnerability/exploit itself.

4. **Creation of IDS rulesets**

   There are 3 sub-stages for this stage. At some stages of the process it may only be able to achieve identification i.e the attack is unstoppable

   a. to identify
   b. to reduce/stop attack
   c. extensive logging

5. **Testing of the ruleset**

   Testing of the ruleset for resilience when under sustained attack.

Unlike IDS rule development that we currently use for reducing or eliminating risk the SCADA or control systems space has some unique requirements. In conventional IDS/IPS a perfectly acceptable paradigm is the denial access for the malicious packets either by dropping them or dropping the routing for the packets. This *modus operandii* for a number of reasons is not acceptable in the SCADA environment. Due to the requirement for most SCADA systems need to have regular and continual communication between devices and controllers a denial of route or packet may cause a system to fail or shutdown at best. Failure to communicate to a device in a SCADA network may have catastrophic downstream consequences.

4 Experimental Environment

For each identified attack the attack is perpetrated against a simple experimental network as designed below. The 100Mb hub and use of the same subnet in this case 192.168.1.0/24 allowing for the promiscuous sniffing of network traffic by various utilities. The network machines are a combination of VMWare instances and physical hardware that as previously mentioned could be rapidly redeployed. All machines are time synchronized by ntp services to the same timestamp before the start of an experimental run.

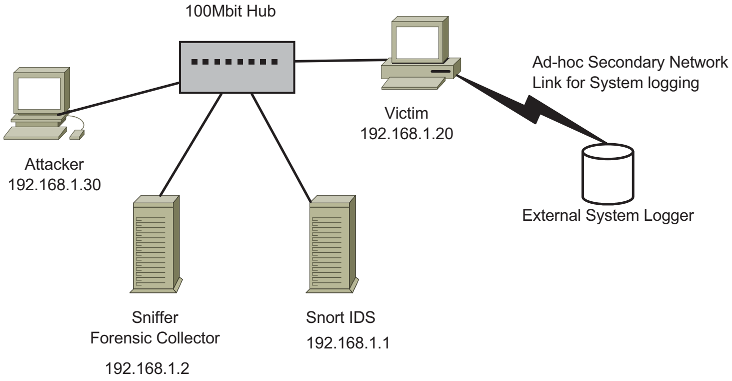


Figure 1: Network Design

Victim/Target Machine

This is constructed as a raw default installed machine but where possible live configurations will be obtained from SCADA and control systems users/operators. Failing the availability of sample live configurations then the default configuration from the software vendors will be deployed for testing.

For each victim or target machine where possible performance logging and monitoring will be gathered to aid forensic analysis, but not at the expense of experimental situation reflecting operational realities. Preferably all logging or system logging will go out on another network interface separate to the one being sniffed as indicate in the network design.

Snort IDS

A VMWare based image based on Debian was developed. The Snort IDS system used the base network install for i386 platform. Then the Snort IDS with PostgreSQL database extensions was installed. In addition Wireshark, tcpdump and Etherape were installed. Several Snort IDS analysis frontends were installed with the primary interface being the ACID/BASE hybrid frontend. The system also had X Windows installed although strictly not used on secure production servers its use and installation enabled faster analysis of the experiments. The final system is used as a baseline system for each experimental run undertaken. This has allowed a consistent approach to the experimentation and a reduction of compounding variables in that the experiments all start with same software and configurations. Where a Snort IDS ruleset was in existence this was utilized to initially detect the attack upon replay of packets that should be addressed by the IDS ruleset. Where no rule existed rule development is taken as per stage 4 of the experimental procedure which is produce a ruleset to identify, then extend (where possible) a ruleset to ameliorate or stop, and then an extended ruleset to observe and document the attack more thoroughly.

Network Sniffer/Forensic Collector

This is a VMware instance that is a forensic collector designed to forensically capture all network traffic and response generated. The system simply creates a tcpdump binary capture file of the network sessions for later analysis via various tools and techniques.

Attacker

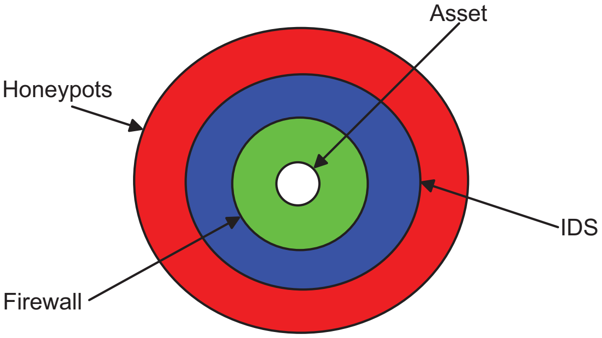
This is typically a simple Debian base installation with scripting languages and appropriate attack tools installed to realize the attack. On occasion the use of bootable Linux CD security implementations such as Backtrack will be used as the attack platform. All attacks are preferably executed from a script or compiled code base for consistency of attack profile or mode of operation.

5 Discussion

This is a research project that is in progress. The aim of the project is to produce a reliable technological framework for the investigation of network borne threats to SCADA and control system environments. The framework will allow for production of Snort signatures for the SCADA and control systems environments using open source tools as the platform. This is the first stage in the development of a hardened network architecture for SCADA and control systems.

From these forensically verified signatures the development of emulation scripts for deployment in the honeyd honeypot system will be undertaken. Honeyd also has a tarpitting capability that can be used to slow down or resource exhaust an attacker. The principle *modus operandii* for this honeypot will be competent emulation of a SCADA system with vulnerability.

In addition it is planned to where applicable to create specific vulnerability modules for use with the nepenthes honeypot system as well. Nepenthes honeypot is designed to principally collect malicious codes in the form of shellcode or custom built binaries. It does this by fooling an attacker into believing they have exploited the machines vulnerability and can "oWn" the machine by the download and execution of malicious code. Nepenthes via its emulation of actions makes the attacker or bot surrender the malcode. These two honeypots will allow a significant opportunity to provide a defence in depth approach to protecting these networks and network protocols from known attacks and vulnerabilities. It will also provide the ability to track zero day exploits or vulnerabilities.



By producing the honeypot layers and IDS they will take load off of the systems and also isolate response away from critical assets. The integration and layering of defence from the firewall to IDS to honeypot should produce a highly resilient architecture to attacks on SCADA systems.

6 Conclusion

There is strong evidence that the installation of a hardened, up to date IDS system that is placed at the network perimeter or intersection can yield significant protection for networks. The problem is manifest in making sure that the IDS is current and hardened against known exploits.

This research aims to provide a reliable system for the rapid production of IDS rulesets for amelioration of threat to SCADA and control networks. It will extend the resilience by combining firewall – IDS – honeypot integration and awareness of exploits and vulnerability. These three technologies should provide a hardened series of barriers by chaining and tight integration of defensive technologies.

The further research to use the identified attacks in honeypot technology should allow significant protection from would be attackers or mishap principally as a tarpit technology but also as a collector of attack modes and motivations. These can then be examined and used to further harden network defences by the production of new IDS rules.

This combination of open source technologies, SCADA operator knowledge and targeted vulnerability and exploit research should produce a hardened resilient infrastructure for use by the SCADA community with the end result being critical infrastructures better protected from cyber attack.

7 References

[1] T. Claburn, "CIA admits cyber attacks blacked out cities, ," in *informationweek*, 2008.

[2] S. Gorman, "Electricity grid in US penetrated by spies," The Wall Street Journal, 2009.

[3] E. Gosch, "West Australian gas shortage to continue all year," perthnow.com.au, 2008.

[4] K. Poulsen, "Slammer worm crashed Ohio nuke plant network," SecurityFocus, 2003.

[5] T. Smith, "Hacker jailed for revenge sewage attacks.," 31st October ed: The Register, 2001.