Global Information Assurance Certification Paper

An Analysis of theSnort Network Intrusion Detection System

by

Mark D. Tollison

Submitted

December 10, 2000

Research PaperIndex

Overview

In today's world, everyone is increasinglydependent on the ability to have instant access to information. Theexplosion of the internet, along with wireless and broadband technologies,allow companies and individuals, unprecedented "Real Time" access to vastamounts of information. In our daily lives we are inundated withemail, voice mail, facsimile, pager and other types of information. In our personal lives, we use our computers to chat with friends, listento digitized music, make travel reservations and buy products. AsInternet access costs have plummeted, corporations are using the Internetas the media of choice for corporate data and, increasingly, voice communications. Any outage in any of these systems is not only a nuisance but a major eventto productivity. The Internet has and will continue to revolutionizethe way business is conducted.

Unfortunately, there is a dark sideto the use of the Internet. The many advantages, such as cost, opennessand flexibility of this vast computer network are heavily impacted by securityrisks. It is a daily occurrence to read about another malicious hackerwho has defaced a web site, gained unauthorized access to a large corporationsinformation resources, or shut down an Ecommerce site via a distributeddenial of service attack. The recent attack on Microsoft via a UnicodeBug or Web Server Folder Traversal Vulnerability, seemed to cause minormonetary damage to the company but this intrusion definitely raised credibilityissues with its information security program [1].

Virus or malicious code is distributedvia email and forces system administrators to scan for, and if found, removethe code from these systems. A recent report stated that about 50,000viruses had been created in the last 14 years [2]. Some of these attackersare initiated by novices who are just trying out one of the many new "HackerTools" available on the Internet. However, I believe a greater threat isfrom the dedicated individual who has a financial, theological, or personalreasons to disrupt a companies vital information flow. Espionageis a valid threat to the intellectual property of a company. Thereis no more cost effective way to gain a competitive advantage than to haveaccess to your rivals information.

These types of threats are just a fewof the reasons that information security is becoming increasingly important. Just as we lock our homes and offices to keep out intruders, we must protectour vital computing resources from unauthorized access. One part of anoverall information security initiative is the area of Intrusion Detection.

The focus of this research paper isto educate the reader about the need for an intrusion detection capability. Specifically, I examine the role of network intrusion detection and howone open source tool, Snort, can be used to establish a defense againstmany attacks. I will present some background information on the featuresof SNORT and list a some examples against a widely used vulnerability scanningtool, Nmap [3].

Index

Introduction

Before I examine the specifics of Snort,I believe that it is important to quickly review the concepts of intrusiondetection. As stated in the GIAC LevelOne Security Essentials Course,Intrusion Detection Systems (IDS) are separated into two main categories,network and host based systems. Each type of intrusion detection systemcomplements the other and both should be used in an effective informationsecurity program. Host based systems allow administrators to effectivelymonitor back doors into systems. Network Intrusion Detection Systems(NIDS) give administrators the ability to determine who is trying to gainunauthorized access to critical computing resources. Network intrusiondetection system are effective in learning about and monitoring the variousexploits that intruders can use. One open source network intrusiondetection system is Snort.

Index

Whatis Snort?

What is Snort? The followinginformation from the Snort web site [4] describes the system.

"Snort is a libpcap-based [PCAP94]packet sniffer and logger that can be used as a lightweight network intrusiondetection system (NIDS). It features rules based logging to performcontent pattern matching and detect a variety of attacks and probes, suchas buffer overflows [ALE96], stealth port scans, CGI attacks, SMB probes,and much more. Snort has real-time alerting capability, with alertsbeing sent to syslog, Server Message Block (SMB) "WinPopup" messages, or a separate "alert" file. Snort is configured using command lineswitches and optional Berkeley Packet Filter [BPF93] commands. The detectionengine is programmed using a simple language that describes per packettests and actions. Ease of use simplifies and expedites the developmentof new exploit detection rules. For example, when the IIS Showcode[IISBT99] web exploits were revealed on the Bugtraq mailing list [BTQ99],Snort rules to detect the probes were available within a few hours." [5]

In order to better understand whatthe description says, let's begin the analysis of Snort by examining someof the command line features.

Index

SnortCommand Line Summary and Usage

Snort has an extensive set of featuresand command line options. These are documented fully in the accompanying"Readme" file which is included in the distribution. A sample ofthe basic command line options are summarized in the following table.

snort -[options] <filters>

COMMAND LINE OPTION	DESCRIPTION
-A <alert>	<alert> mode can be either Full,Fast or None. Type of alerting to the alert file Full mode, normal mode. Fast mode - Only Timestamp,Message, IPs, and P. None - No alerting.
-a	Display ARP packets
-b	Log packets in tcpdump format. FASTEST OPERATION
-c <cf>	Use configuration or rules file <cf>.
-C	Dump the ASCII characters in packetpayloads only. NO HEXDUMP
-d	Dump the application layer data
-e	Display/ and log the layer 2 packetheader data
-F <bpf>	Read BPF filters from file <bpf>. Can be used for complex filters
-i <if>	Use network interface <if>.
-l <ld>	Log packets to directory <ld>.
-N	Turn off logging. Alerts stillfunction normally.
-p	Turn off promiscuous mode sniffing.
-r <tf>	Read the tcpdump-generated file <tf>.
-v	Verbose output to console. Limiteduse. Will caused slowdown and possible packet loss.
-V	Show the version number and exit.
-?	Show the usage summary and exit.

Also, two very valuable features arethe support for filters and rules. Filters allow the program to betailored for specific needs such as monitoring a single host computer orsubnet. The use of rules allow Snort to be used as a fully functionalintrusion detection system. In the next sections I will run somesimple examples using a small computer network to show how Snort can beused in its two modes, as a packet sniffer and as an intrusion detectionsystem.

Index

Snortas a Packet Sniffer

For this example, I am running theWindows version of Snort on a small two computer network. The firstcomputer is running Windows 98 and is running the Snort system. Thesecond computer is a RedHat Linux system. To test Snort as a sniffer,I will use the ICMP Ping program to generate Echo packets.

In an MSDOS window, the command linefor Snort is the following.

D:\Snort\program\snort-1.6.3\Binary\snort.exe-l D:\Snort\TEMP -i 4 -a -e -d -A full

For this demonstration, I started Snort,sent Echo requests from the Linux computer, and terminated Snort usingCTRL C. Snort displayed the following statistics in the MSDOS window.

```
===============================================================================
Snort received 26 packets and dropped0(0.000%) packets
```

```
Breakdown by protocol:
    TCP: 0         (0.000%)
    UDP: 0         (0.000%)
   ICMP: 24        (92.308%)
  FRAGS: 0         (0.000%)
    ARP: 2         (7.692%)
   IPv6: 0         (0.000%)
    IPX: 0         (0.000%)
  OTHER: 0         (0.000%)
===============================================================================
```

Since I specified an ASCII data dump,instead of TCP dump format, the Snort program generated two IDS files underfolders, D:\Snort\TEMP\169.254.193.10 and D:\Snort\TEMP\169.254.17.196. Using a text editor, the following information is displayed. Forbrevity, I have only shown the first of twelve packets in each datafile.

Folder 169.254.193.10

```
12/10-07:25:19.157335 0:60:97:8A:F5:31-> 0:50:BA:A4:EA:97 type:0x800 len:0x62
169.254.193.10 -> 169.254.17.196 ICMPTTL:64 TOS:0x0 ID:90
ID:1297   Seq:0  ECHO
DE 36 33 3A 24 09 03 00 08 09 0A 0B0C 0D 0E 0F  .63:$...........
10 11 12 13 14 15 16 17 18 19 1A 1B1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                         01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

Folder 169.254.17.196

```
12/10-07:25:19.158583 0:50:BA:A4:EA:97-> 0:60:97:8A:F5:31 type:0x800 len:0x62
169.254.17.196 -> 169.254.193.10 ICMPTTL:128 TOS:0x0 ID:28672
ID:1297   Seq:0  ECHOREPLY
DE 36 33 3A 24 09 03 00 08 09 0A 0B0C 0D 0E 0F  .63:$...........
10 11 12 13 14 15 16 17 18 19 1A 1B1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                         01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

I am not going to discuss how to interpretall the packet information. This information can be obtained fromvarious references including "Using TCP/IP"[6]. It is important tonotice that Snort read the packets from network driver correctly and storedthe information in files in a very readable format. These files can beviewed manually or using one of many third party add-ons. Data miningor data filtering techniques could be used to find important events withinlarge data files.

Index

Snortas an Intrusion Detection System

For this next example, the small twocomputer network is again used. However, two configuration changesare made. The first is that Snort now uses a rules database. Being open source, the rules database is frequently updated by variousauthors. Also, various sites have downloadable rules files for Snort. The latest rules database can be obtained from the Snort web site.[] Oncedownloaded, the rules database must be configured with site specific information. It only took me a few minutes to added the required IP addresses information.

The second configuration change isthat I am used the Nmap port scanning utility to generate suspect datapackets. [7] This versatile and fully featured utility can be usedto map and identify hosts with networks. I am going to limit my Nmapscan to use TCP fingerprinting techniques to try to guess the operatingsystem on the computer running Snort. If all goes

well, I shouldbe able to obtain a good comparison of Snort operation and logging to theactual attack vector.

In an MSDOS window, the command linefor Snort is the following.

```
D:\Snort\program\snort-1.6.3\Binary\snort.exe-l D:\Snort\TEMP -c
D:\Snort\Rules\12062k.rules.txt -i 4 -a -e -d -A full
```

For this demonstration, I started Snort,ran Nmap with TCP/IP Fingerprinting option. Upon Nmap completion,I terminated Snort. The Snort system displayed the following statisticsin the MSDOS window.

```
===============================================================================
Snort received 3103 packets and dropped0(0.000%) packets

Breakdown by protocol:
    TCP: 3097      (99.807%)
    UDP: 1         (0.032%)
   ICMP: 3         (0.097%)
  FRAGS: 0         (0.000%)
    ARP: 2         (0.064%)
   IPv6: 0         (0.000%)
    IPX: 0         (0.000%)
  OTHER: 0         (0.000%)
===============================================================================
```

Investigating the D:\Snort\TEMP directoryrevealed that Snort had generated an alert file. This ASCII alertfile contained ten alert entries. One of the entries was the following.

```
[**] IDS05 - SCAN-Possible NMAP Fingerprintattempt [**]
12/10-10:05:07.959989 0:60:97:8A:F5:31-> 0:50:BA:A4:EA:97 type:0x800 len:0x4A
169.254.193.10:42856 -> 169.254.17.196:139TCP TTL:51 TOS:0x0 ID:4196
**SF*P*U Seq: 0xA5757576  Ack: 0x0   Win: 0x1000
```

This alert report that an Nmap TCP/IPFingerprinting attempt was made against the host computer. Snorteffectively generated an alert showing that this attempt had occurred.

Index

Conclusion

The Snort lightweight Intrusion DetectionSystem has all many features a system administrator needs to establishan efficient network based intrusion detection system. Through thirdparty add-ons, the system can be enhanced to make logs reviews and administratoreasier. This demonstration shows that Snort can be an effective partof intrusion detection architecture. Hopefully, this introductionwill peak your interest in this system and I invite you to explore Snortin more detail.

Index

References

[1] Delio,Michelle. "Hackers Crack Into MS System." 27 October 2000. URL: http://www.wired.com/news/culture/0,1284,39778,00.html (10 December2000)

[2] "Virus Woes Leadto New Tactics." Investors Business Daily. 30 November 2000.

[3] Fyodor. "GeneralInformation." URL: http://www.insecure.org/nmap/index.html#intro

(10 December 2000)

[4] Roesch, Martin"Snortorg Latest News" URL: http://www.snort.org/snortnews/news.asp (10 December 2000)

[5] Roesch, Martin"What is Snort?" URL: http://www.snort.org/what_is_snort.htm (10 December 2000)

[6] Ray, John. "UsingTCP/IP." January 1999. QUE Corporation.

Index

Linksof Interest

Snort 1.6.3 Source Code - http://www.snort.org/Files/snort-1.6.3.tar.gz

Snort 1.6.3-patch2 - http://www.snort.org/Files/snort-1.6.3-patch2.tar.gz

Snort-1.6.3-win32-source.zip - http://www.snort.org/Files/snort-1.6.3-win32-source.zip

Snort-1.6.3-win32-static.zip http://www.datanerds.net/~mike/binaries/snort-1.6.3-win32-static.zip

Snort Solaris Package - http://www.snort.org/Files/snort-1.6.3-sol-2.6-sparc-local

SnortWIN32 Graphic Interface for Snort - www.xato.net/downloadshttp://www.xato.net/downloads

Nmap Downloads - http://www.insecure.org/nmap/index.html#download

Index

Last Updated: July 22nd, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor