

Implementing a network operations centre management console: Netmates

R.Bali and P.S.Dowland

Network Research Group, University of Plymouth, Plymouth, United Kingdom
email: info@network-research-group.org

Abstract

Network Management & Intrusion Detection Systems (NMIDS) are an important part of any network security architecture. They provide a layer of defense which monitors network traffic for predefined suspicious activity or patterns, and alert system administrators when potential hostile traffic is detected. Commercial NMIDS have many differences, but information systems departments must face the commonalities that they share such as significant system footprint, complex deployment and high monetary cost. Netmates - Network Monitoring & Attack Evaluation System, which is based on Snort was designed to address these issues. It features a near real-time snort alert monitor, providing many ways to indicate that the network may be experiencing an intrusion attempt including audio / visual warnings, email warnings, etc.

Keywords

Network Management Monitoring Intrusion Detection Console Real-time NMS NMIDS IDS

1. Introduction

Netmates is an implementation of a range of selected software to monitor (in real-time) the network and security breaches in the form of alerts generated by Snort. Other combinations of such tools like Snort (Snort, 2005) & ACID (Acidlabs, 2005) And Snort & BASE (BASE, 2005) lack something or other. Snort is great for identifying suspicious traffic and ACID is great for digging in to the details there was a need for something that was a little higher overview and able to sound alarms if certain conditions were met. For instance, if the network is attacked 50 times in a 2 minute period. Netmates does not replace Snort or ACID but rather it compliments them. This paper discusses Netmates, based upon Snort which is here being used as rules-based traffic collection engine, in turn as a NMIDS

Netmates fills an evident gap in the domain of network security: It is a robust implementation of cross-platform, lightweight network management and intrusion detection tools that can be deployed to monitor TCP/IP networks and detect a wide variety of suspicious network traffic as well as outright attacks. It can provide users with enough data to make informed decisions and take proper precautions and actions to face the suspicious activity. The beauty of the system is that it can be rapidly deployed to cover the potential hole in the security as and when it is detected,

while the commercial equivalents depend on OS or firmware update. This is possible due to its open source nature and wide user base of its core detection engine - Snort.

It is possible to easily deploy Netmats on any machine running windows as host operating system. Because Netmats is a pre compiled, pre configured and portable linux system which is an ideal NMIDS solution that is available as a virtual machine based on Microsoft Virtual Machine Technology (Microsoft Corporation, 2004). This makes deployment of such a powerful tool quick and easy where other propriety solutions strive to score anywhere closer. It can comfortably fit on a CD, or can be downloaded over the network. Its ready and working is just five minutes, only needs Microsoft Virtual Machine installed and configured to use Netmats as a virtual hard disk. Also the Netmats console to view the alerts with audio visual aids.

2. Architecture

Netmats fulfills its objectives i.e. light weight Network Monitoring, Intrusion detection and wireless sniffing by deploying the following key techniques in the form of add-ons to snort which come as a separate package or as a plug-in. These can be either installed together to form a single software or multiple instances on one single machine or in a distributed environment logging to same database.

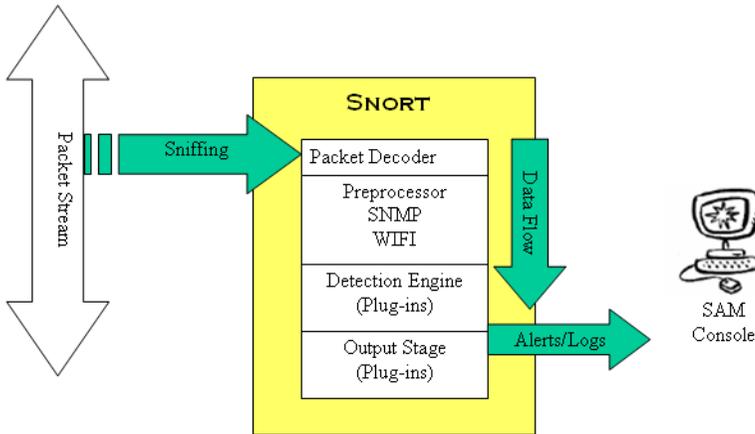


Figure 1: Netmats Data Flow

2.1 Snort

At its most basic level, Snort is a simple sniffer which means that it captures the network traffic for further analysis. It does so by listening to the network traffic in 'promiscuous mode' which allows it to capture all the data that passes over the network regardless of its destination address. Inherently, if a packet of information is addressed to another computer all other network cards will reject this data, which saves system resources.

Snort emerges more powerful when it is properly configured to detect intrusion using a combination of rules and pre-filters. It can also recreate data streams and analyse

them for any number of signatures that give some indication of a possible network attack

Most of the intruder activity has some sort of bit pattern also called signature. Information about these known patterns can be used to create Snort rules. There are many known vulnerabilities that attackers want to exploit. But at the same time these can be used as weapons to find out if someone is trying to exploit them. These bit patterns can be found in the header parts of a packet or in the payload. Snort's detection system is based on rules which in turn are based on intruder bit pattern. Snort rules can be used to check various parts of a data packet. Rules are applied in an orderly fashion to all packets depending on their types. The detection engine is programmed using a simple language that describes per packet tests and actions. Snort rules are written in an easy to understand syntax. Most of the rules are written in a single line but can be extended to multiple lines using backslash character at end of the line.

The rules are then used to generate an alert message, which is logged to the Snort MySQL (MySQL AB, 2005) database. The database can be simultaneously accessed by Snort Alert Monitor SAM (LookAndFeel, 2002) to produce a real-time output. The database grows quite rapidly if the rules are incorrectly configured or specifically in attempt to gather more packets for later analysis.

2.2 SNMP: Network Management Integration

The SnortSNMPplugin (Cyber Solutions 2005) which has been used here enables snort to send Simple Network Management Protocol (SNMP) alerts to Snort alert database. The alerts can be traps – information broadcasts which do not get any acknowledgements or informs where the alert will be acknowledged by the receiver. This adds significant power to the NMS by allowing it to monitor the security of the network. This makes it possible for the snort sensor to exploit the features that are built into existing network management systems.

An SNMP notification carries information in the form of a set of name-value pairs. The names are, Object instance Identifiers (OID). Managed Objects (MO) are observables that are used by NMSs. To report any network link or status update (e.g. sensor location, alert message, attack source etc). MOs are uniquely identified by their OIDs. The MOs and their OIDs are defined in Management Information Base (MIB) modules.

The OIDs are organised in the form of a tree - the "global naming tree". Each node in this tree has an identifier and a label. The identifier is unique among the siblings of a node. The concatenation of the identifiers of the nodes on the arch starting at the root and ending at a node is the OID of that node. The organisation that has been assigned a node in the "global naming tree" is in charge of the sub tree rooted at that node. Organisations in turn may delegate the administration of sub tree(s) of the tree in their charge.

Snort.org has been assigned the unique node numbered *10234* under the enterprises node of the global naming tree. The OID of this node is 1.3.6.4.1.10234, the

concatenation of the identifiers of the nodes on the arch starting from the root node to the node assigned to snort. (Going by the labels of the nodes the OID will look like iso.org.dod.internet.private.enterprises.snort). All Snort related MIBs can be defined under this node.

2.2.1 The MIB implementation

In the simple case we just want to send SNMP alerts to a NMS or a Network Security Manager. This is simple because snort does the detection and calls the SNMPplugin module to generate the corresponding SNMP alert packet with the appropriate OID-value pairs. The SNMP alert packet is then logged to the database.

2.2.2 The Actual communication

The actual communication between the snort and the NMS will use the Simple Network Management Protocol. Both the versions of SNMP are supported i.e. SNMPv2C and SNMPv3. In order to set up Snort for generating SNMP alerts it is required to set up the snort.conf with the appropriate parameters for SNMP alert generation. The SNMPTrapGenerator output plug-in requires several parameters. The parameters depend on the SNMP version that is used. More information on setting up Snort can be obtained from Cyber Solutions SNMP Snort Guide. (Keeni, 2005)

2.3 Wireless Sniffing

Another add-on is Snort-Wireless (Snort Wireless, 2005) which is an attempt to make a scalable 802.11 intrusion detection system that is easily integratable into an IDS infrastructure. It is completely backwards compatible with Snort 2.0.x and adds several additional features. Currently it allows for 802.11 specific detection rules through the new "wifi" rule protocol, as well as rogue AP, AdHoc network, and Netstumbler (NetStumbler.com, 2005) detection.

2.3.1 WiFi Protocol Rules

Snort at present does not contain direct support for rule based detection of anything below the IP layer. It is possible in Snort 2.0.x to match byte patterns in a packet, but it is not very straightforward and is very time-consuming to write detection rules this way. Rules for detecting particular 802.11 frames are specified using the following syntax:

```
<action> wifi <src mac> -> <dst mac> (<rule options>)
```

2.3.2 RogueAP Preprocessor

The RogueAP preprocessor detects both rogue APs and AdHoc networks. To configure it, for the APs BSSIDs and channels it has to be specified that they operate on in the snort.conf file using the ACCESS_POINTS and CHANNELS variables.

2.3.3 The AntiStumblerPreprocessor

NetStumbler is a tool for Windows that detects Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g. It is potentially used for war-diving. The AntiStumbler preprocessor attempts to detect Netstumbler like traffic. It does this by keeping track of probe request frames sent with NULL SSID fields.

2.4 Console

Data is useless without some manageable method for review. If we simply expect to be able to sit down and read each entry in a log file, we will be quickly overcome with pages and pages of alerts, warnings, and even regular user activity. With Netmates console, one can quickly and easily target the important information.

Snort Alert Monitor: Snort Alert Monitor (SAM) which has been modified and bug fixed for this project is a Java-based console that can be used to get a quick look at the Snort alerts in MySQL database. It runs as a Java-console, so it's platform independent. The frequency of the updates from snort's MySQL database can be tweaked to get a near real-time view of incoming Snort alerts. SAM is freely available under LAF General Public License. (lookandfeel, 2002)

The console has many ways of grabbing attention. The first is the rather large stop light in the top left corner of the screen. The second is by playing a specific sound when a particular threshold is reached. The third way we can be notified is that an email can be sent to a specific person or group of people.



Figure 2: Network Monitoring & Attack Evaluation System Console

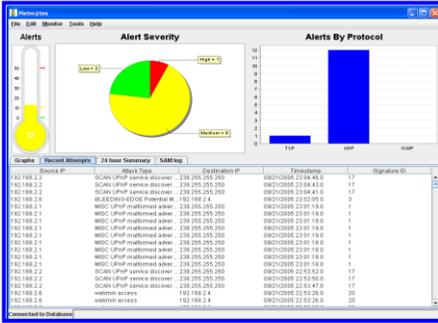


Figure 3: Snort Alert Monitor Recent Attack Attempts

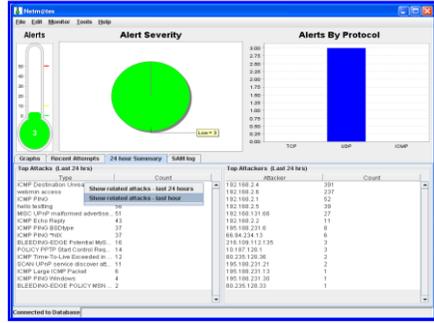


Figure 4: Snort Alert Monitor Summary

2.4.1 Alert Severity

Sometimes it's difficult to predict how serious the alert is. To help us determine the severity of the outage, the reasons administrator may be alerted have been divided into three basic categories: Green, Yellow, and Red alerts:

Green Alerts are OK. They are a result of a less than ten alerts in last five minutes. This threshold value can be altered by changing the value of `alertlevel.medium=x` to desired number of alerts per five minutes. Any value below this number will be considered to be of low sensitivity.

Yellow Alerts are cause for concern. Yellow alerts are characterised by ten or more but less than 50 alerts (these default threshold values can be changed). The idea is that when the number of alerts (in the past five minutes) is equal to or above this value, the alert level is then set to medium, and the traffic light will flash yellow.

Red Alerts are serious outages. This is a numerical field (`alertlevel.high=x`) that represents the threshold for the medium alert level. The idea is that when SAM receives more than fifty alerts in five minutes, the alert level is then set to high, and the traffic light will flash red.

SAM will warn the administrator if the connectivity to the snort database server is lost, but it can not tell why. Some research might be needed to determine the failure of the link or server.



Figure 5: External Stoplights interfaced with Netmats

2.4.2 Stoplights

It is possible to connect the some kind of external visual alarm system in the form of spot lights. As seen in the Figure 5, a multi colored alarm can indicate the current status of the attacks, the color or level of the attack can be determined on the same principles discussed in section 2.4.1. This has to be done by using some kind of low level program. This feature has not been implemented yet, but there are many possibilities of further developing the alert and alarm system.

3. Conclusion

Netmates would be the most admirable tool for security professionals, powered by Snort which is an icon of intrusion detection software, proves how effectively it can implemented using its modular approach in which Snort applies rules and preprocessors, this program can be enhanced by anyone with even a basic understanding of security.

The uniqueness of Netmates is that it puts together a working model that features the functionality of Network Management and Intrusion Detection in a single box, complemented with a java based Console which is so robust and just the right desirable for network security personnel.

4. References

- Acid Lab (2005), “Analysis Console for Intrusion Databases (ACID)”, <http://acidlab.sourceforge.net>, (Accessed 01-Aug-05)
- BASE (2005), “Basic Analysis and Security Engine”, <http://sourceforge.net/projects/secureideas>, (Accessed 25-Aug-05)
- Cyber Solutions (2005), “SnortSNMP”, <http://www.cysols.com/contrib/snortSNMP/index.shtml>, (Accessed 01-Aug-05)
- Keeni G.M. (2005), Cyber Solutions, “Snort-SNMP Guide”, <http://www.cysol.co.jp/contrib/snortsnmp/snortSnpmpGuide.html>, (Accessed 22-Aug-2005)
- LookAndFeel (2005), “Snort Alert Monitor”, <http://sourceforge.net/projects/snortalertmon>, (Accessed 01-Aug-05)
- Microsoft Corporation (2004), “Microsoft Virtual PC 2004”, <http://www.microsoft.com/windows/virtualpc/default.mspx>, (Accessed 23-Aug-2005)
- MySQL AB (2005), “The World's Most Popular Open Source Database”, <http://www.mysql.org>, (Accessed 25-Aug-05)
- NetStumbler.com (2005), “NetStumbler”, <http://netstumbler.com>, (Accessed 25-Aug-2005)
- Snort (2005), “Snort - the de facto standard for intrusion detection/prevention”, <http://www.snort.org>, (Accessed 01-Aug-05)

