

## Reducing False Positives using Vulnerability Assessment

by: Ramesh S and Elango K, 09/20/2004

<http://www.securitydocs.com/library/2563>

### Abstract

*Configuring Intrusion Detection System that suits the network is a tedious task for the security analyst. They need to be aware of the network topology and the hosts in the network in order to configure the correct set of signatures for detection. This paper explores a possibility of tuning IDS based on a Vulnerability Assessment tool (this paper deals with nessus). This will help avoiding false positives from triggering due to improper configurations.*

### Introduction

In IDS systems, the continuous growing problem is to manage the IDS effectively and reduce false positives. Tuning the IDS effectively is a tedious task for the security analyst. If the IDS are not configured correctly this may lead to lots of false positive alarms and the analyst needs to go through all these alarms to identify real events and false positive alarms. In order to tune the correct set of configurations in the IDS the security analyst need to be aware of the network topology and also needs the information of the all hosts monitored by the IDS. This will be a tedious task to the analyst to keep track of all the hosts in a large organization. The task becomes more tedious if the organization is managing hundreds of IDS. This paper tries to analyze a way by which the users can use a Vulnerability Assessment tool to study their network which would inform about any vulnerability based on which the security analyst can configure the IDS.

### Introduction to IDS

Intrusion detection system (also known as IDS) monitors the network promiscuously and analyzes the packets for possible presence of any attacks. The detection could be of Signature based or Anomaly. Anomaly tries to learn the behavior of the usage and then identifies the attacks based on this usage pattern. For Anomaly, anything deviating with the normal pattern is an attack. Signatures could be rule based (also known as mis-use). For every attack there exists a signature at the IDS. A signature is nothing but the profile of an attack. Some systems allow tuning the signatures. Careful tuning is required otherwise it may altogether change the definition of the signature itself.

There are two major types of Intrusion Detection systems that include network and host based intrusion detection systems:

#### **Network Based Intrusion Detection System (NIDS):**

These systems are placed on the network and sniff all packets destined to the network monitors. The sniffed packets are examined for any unauthorized activity.

#### **Host Based Intrusion Detection System (HIDS):**

These are installed on the actual system to be monitored. These monitor the system for any unauthorized changes or other anomalous activity.

### IDS Management Console

An IDS Management console is an application that manages the IDS. IDS Management Console configures and also receives the alarms generated by the IDS. The received alarms can be analyzed for forensic purpose and can be used for future attack predictions.

This is a simple application that knows the complexities of particular IDS that it is trying to configure and receive alarms. It should have the knowledge base of how to configure IDS for various signatures

suitably for individual networks.

### **IDS Configuration Issues**

The security team should have a detailed knowledge of all the hosts, their functions and their vulnerabilities. They need to configure the host based and network based intrusion detection systems granularly, based on each hosts unique functions and vulnerabilities. In most organizations, this is a manual process that involves using knowledge gained from different sources to generate rules for the Intrusion detection systems and is extremely cumbersome. If and when new vulnerabilities are detected, the Intrusion detection system signatures need to be updated. With the constant barrage of new vulnerabilities, it is becoming increasingly difficult for the security team in an organization to stay up-to-date with their IDS configurations. Organizations having a multitude of systems running many different applications, it is always a game to catch up and provide for up to date Intrusion Detection. As Intrusion Detection systems evolve, there is an increased need for automation to reduce human involvement.

Some issues with current IDS systems and their usage:

- False Positives due to default settings

If the default configuration provided by the vendor is used, the majority of the alerts produced by these systems tend to be false positives. This is because in many instances, what is normal activity for a particular organization could be an attack under certain circumstances for another network. The vendors provide rule-sets for all kinds of attacks and it is up to the organization to optimize the rule-sets to avoid false positives.

- False Positives due to Misconfigured Signatures

Security Analyst may enable/disable signatures for which they might have vulnerable hosts or might not have. Configuring such signatures without much knowledge about the network and hosts in the network would result in more false positives.

- Configuring IDS based on the hosts on the network is a challenging issue for the security analyst. Security analyst needs to be aware of all the information regarding all the hosts and its vulnerabilities and then should be able to configure the IDS effectively.

### **Vulnerability Assessment**

One of the first steps in securing a computer network is to assess the network's vulnerability. Vulnerability Assessment is a common security technique used to assess a network's vulnerability to attacks. Many products and services have been developed to aid the security engineer in making this assessment. Some of these freeware products are NMAP and Nessus.

### **NESSUS**

The "Nessus" Project aims to provide to the Internet community a [free](#), powerful, up-to-date and easy to use remote security scanner.

Unlike many other security scanners, Nessus does not take anything for granted. That is, it will not consider that a given service is running on a fixed port - that is, if you run your web server on port 1234, Nessus will detect it and test its security. It will not make its security tests regarding the version number; default port numbers of the remote services, but will really attempt to exploit the vulnerability.

Nessus is a powerful tool and a detailed comparative study is already made in the market and a report is

available at the following location:

<http://www.networkcomputing.com/1201/1201f1b1.html>

The reason that we chose Nessus as a tool to be integrated with IDS is that,

- it is powerful
- it allows to add plug-ins
- it allows to write new scripts for finding the weakness of network
- Nessus Attack Scripting Language support
- Up-to-date security vulnerability database
- Exportable reports

## NASL

NASL. The Nessus Security Scanner includes NASL, (Nessus Attack Scripting Language) a language designed to write security test easily and quickly. (Security checks can also be written in C)

## Signatures

Signatures are nothing but profiles of an attack. For every attack the IDS should have a signature tuned for it to detect. Snort is a publicly available IDS tool. A sample signature that looks for ICMP Echo Reply packet from snort IDS is given below. It specifically checks the ICMP packet header with the fields of ICMP TYPE = 0 and ICMP Code = 0 which signifies it is a ICMP echo reply packet.

SID	408	message	ICMP Echo Reply
Signature	alert icmp \$EXTERNAL_NET any - \$HOME_NET any (msg:"ICMP Echo Reply"; itype: 0; icode: 0; sid:408; classtype:misc-activity; rev:4;)		
Summary	This event is generated when a network host generates an ICMP Echo Reply in response to an ICMP Echo Request message.		
Impact	Information-gathering. An ICMP Echo Reply message is sent in response to an ICMP Echo Request message. If the ICMP Echo Reply message reaches the requesting host it indicates that the replying host is alive		
Detailed Information	ICMP Type 0 Code 0 is the RFC defined messaging type for ICMP Echo Reply datagram's. This type of message is used to determine if a host is active on the network.		
Affected Systems			
Attack Scenarios	A remote attacker may use ICMP Echo Request datagram's to determine active hosts on the network in prelude of further attacks.		
Ease of Attack	Numerous tools and scripts can generate this type of ICMP datagram.		
False Positives	None known		
False Negatives	None known		
Corrective Action	Use ingress filtering to prevent ICMP Type 0 Code 8 messages from entering the network.		
Contributors	Original rule writer unknown Sourcefire Research Team Matthew Watchinski (matt.watchinski@sourcefire.com)		

### **Configuring IDS with Vulnerability Assessment**

Most of the modern day attacks are automated and happen through automated scripts and worm based mechanisms. Recently there is sadmind/IIS worm that exploits a vulnerability in sadmind to compromise a Solaris machine and then uses the compromised host to attack IIS servers using the Unicode exploit. To counter automated attacks, it is absolutely essential that the tools used to secure and monitor networks communicated with each other in an automated, fashion. The VA tools provide a clear picture of all hosts on the network, the services that they provide and also information on the known vulnerabilities that exist in the network. This information would help the security analyst in configuring his network according the vulnerabilities existing in his network. Intrusion detection systems need data on, what needs to be monitored on the network. If there is automated interchange of information, where the data from the vulnerability assessment system is automatically used to generate filters for the Intrusion detection system, the number of false positives is greatly reduced. Most alerts on the IDS are genuine and will be taken seriously. This is an essential evolution for vulnerability assessment and the IDS systems in order for security professionals to keep up with the increasing sophistication of the attackers. In order for this marriage to work reliably, the vulnerability assessment systems should be kept up to date with any changes to the network and with the latest vulnerabilities.

Intrusion Detection Systems (IDS) are key components in actively policing and enforcing network and host policies. These policies are generally created with the aid or knowledge of vulnerability assessment. Many of the tasks of assessment and enforcement become labor intensive that requires specialized knowledge of the networks.

The next step in Vulnerability Assessment and IDS technology is to bring these two technologies together by automating the process of **assessment and enforcement**. The cooperation and automation of these two technologies takes security management to the next level. This level is an important step in automating security management

There are two approaches that can be taken in utilizing vulnerability data with IDS. The first approach is to use the vulnerability data to tune your IDS to reduce “false positives”. The analyst looks at the VA report and then configures the IDS based on the reported vulnerability. This process is labor intensive, requires manual configuration changes and requires specialized security knowledge. This approach could be useful if the number of IDS being managed is less and if the network being protected is small. If the number of IDS being managed is more than configuring the IDS manually based on the vulnerability can be tedious.

The second approach is to actively rise or lower the severity of an alert based on the vulnerability profile of the network. This approach is implemented on the management console side of an Intrusion Detection System. The management console system would relate the alarm (or alert) to a vulnerability database to change the severity.

#### **Major Features:**

For every attack, the common authority assigns a CVE id. This CVE (Common Vulnerability exposures) ID can be used to map the Signature ID and the NASL script. For every NASL script there is also a CVE ID associated with it by Nessus. Similarly every SigID might be associated with a CVE ID. Most of the IDS Vendors provide this feature. The analyst can identify the signatures that map with the CVE Ids and then configure those signatures that identified by the VA. Alternatively IDS Management console could map the SigIds with the CVE Ids and configure the corresponding signatures suitable for the IDS, by this approach the users can be able configure all the IDS automatically using the management console.

Nessus report also provides some solution to the vulnerability seen in the scanned network, this would allow the user to take the appropriate action other than configuring a IDS, like disabling the service.

#### Sample report in XML Format

```
<information>
  <severity>Sec urity Warning</severity>
  <id>10280</id>
  <data>
    The Telnet service is running.

    This service is dangerous in the sense that
    it is not ciphared - that is, everyone can sniff
    the data that passes between the telnet client
    and the telnet server. This includes logins and passwords.
    You should disable this service and use OpenSSH instead.
    (www.openssh.com)

    Solution : Comment out the 'telnet' line in /etc/inetd.conf.

    Risk factor : Low
    CVE : CAN-1999-0619

  </data>
</informa tion>
```

#### 1. Avoid False Positives:

Configuring the right set of signatures to the right set of IDS would avoid false positives. False Positives are nothing but, IDS thinks that it is an attack but actually it is not. It could have been a legitimate traffic. Also if that particular weakness does not exist for your network then raising an alarm for it is not necessary. This should save most of the time.

#### 2. Raise/Lower the Severity:

Severity for signatures comes with the factory defaults. This may not match one's security policy. Hence setting up the right severity (raising/lowering) based on the Nessus report would help.

#### 3. Self Generating Signatures:

For the weaknesses that don't match a signature, the IDS Management console could create a User defined signature (Self-generating signatures) for it. This requires a extensive knowledge of the IDS.

#### 4. Providing plug-in for non-CVE signatures:

For the signatures that don't match a Scanner's script the security analyst can write his own NASL scripts for it.

#### Steps to avoid False Positives

Scanning can be done periodically to get information for new vulnerability and information about new

hosts added in the network. This may subject to change according to the requirements of the security policy of a company.

Using the report from generated by the VA tool configuration of the IDS needs to be done. This report needs to be analyzed with the existing configuration of the IDS. Outcome of the analysis should include a recommendation for

- Signatures that needs to be disabled
- Signatures that needs to be enabled
- Signatures whose severity needs to be changed and to what level (raise/lower)
- User defined Signatures that needs to be created(Self Generating signatures)

### **Self Generating Signatures:**

Sample User Defined Signature for the attack: ICMP Destination Unreachable (Undefined Code!)

```
alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP Destination Unreachable (Undefined Code!)" ; itype: 3; sid:407; classtype:misc-activity; rev:4;)
```

Summary of the attack:

This event is generated when An ICMP Destination Unreachable datagram is detected on the network with an undefined ICMP Code.

Detailed Information:

This rule generates informational events about the network. Large numbers of these messages on the network could indication routing problems, faulty routing devices, improperly configured hosts, or an attempted DOS. ICMP Codes for Destination Unreachable datagram's are defined in RFC 792 and RFC 1812. The datagram that generated this event is not defined in either of these RFCs. This could be an indication of a DoS (Denial of Service) attempt against the network.

### **Conclusions**

An attempt is make to learn to use VA tool for configuring the IDS to reduce the false positives and avoid unnecessary signatures from firing. This can be done by manually configuring the IDS based on the VA report or provide the feature in the Management Console to automatically tune the signatures in the IDS based on the vulnerability finding. This proposal could save a lot of time for the forensic analyzer by avoiding time spent on the false positives. Also it makes the administrators to feel comfortable in configuring only the necessary signatures and thereby making the configuration even simple.

Integration of VA tool with the IDS has to be taken up to make the false positives to ZERO (can act as a added protection). Integration with Management Console will stop the signatures from firing and Integration with IDS will stop the alarms being forwarded to Monitoring stations.

### **References**

1. Network Intrusion Detection: An Analyst s Handbook by "Northcutt, Stephen"
2. Network Security Essentials -Applications & Standards by "Stallings, William"
3. Comparative study of VA scanners <http://www.networkcomputing.com/1201/1201f1b1.html>
4. Nessus tool, <http://www.nessus.org>
5. Common Vulnerability exposures <http://www.cve.mitre.org/>

