

The Use of Network Intrusion Detection System

by: YY Ngai, 10/25/2004

<http://www.securitydocs.com/library/2650>

About the author:

YY Ngai is responsible for the Corporate network and server operations of a mobile operator. Prior to this, she was a solution architect with Digital Equipment and Compaq Computer. She started her career as a system engineer in the Telecom industry. Security is an area that she devotes her times in recently. She is a CISSP. Perimeter defense, patching up holes in IT devices, and sniffing for tell tale signs of intrusions are becoming more and more important in network guys' profile.

To the readers

This paper is written for IT managers. The techies can get an understanding of the objectives (some are reasonable, some not quite) of their management out of the paper, and get some tips to cut corners to achieve the objectives.

Along with the paper, the fundamental security defense mechanisms that are strongly recommended have been highlighted in **bold**.

Foreword

Network Intrusion Detection System(NIDS) has been outsourced to vendor who installed and managed the system the past 3 years. NIDS alerts were received from the service provider about 1 to 3 times a day, and a monthly report that showed thousands of intrusion attempts. None of these alerts turned out to be security crisis. However, there were 2 occasions of attack, both started from employee's infected Laptops. Disappointed to say that the NIDS failed to detect the incidents.

Then the questions raised were: What is the use of NIDS? Did the vendor send a few alerts a day to remind us their presence? Did I pay to receive these false alarms to feel good that we have NIDS? Is NIDS useful?

Not satisfied with the few daily alerts and an after-the-matter monthly report, I started a drive to get more values out of my new NIDS provider this time round. I am going to share with you the pain and gain in implementing a useful NIDS.

Introduction

There are many terms about intrusion systems, IDS, HIDS, NIDS, IPS, and more being invented in the pipeline. To elaborate, they mean Intrusion Detection System, Host Intrusion Detection System, Network Intrusion Detection System, and Intrusion Prevention System respectively. All these terms point to one thing, there are invisible intrusions coming off the network wire lying on your desk, at the corner of the office, hiding in the cabling closet in the building riser. Having mentioned the above terms, I owe it to my readers the definitions of the terms and why am I not adopting those other systems. IDS is a generic term for intrusion detection system. HIDS and NIDS are 2 types of IDS. NIDS is like a CCTV that is installed at various corners in the building to capture activities in the building. An alarm is triggered when abnormal activities are captured. The short coming of NIDS is that it is not able to tell whether the abnormal activities are harmful or benign by the appearance. You do not know what that guy peeping into the meeting room is up to without further investigation, right? Unlike HIDS which is

like a security guard in the room. He guards only his room but he guards better than NIDS. NIDS and HIDS complement one another.

IPS does more than an IDS, the word prevention suggests that the system is more reactive compared to IDS. An IPS detects abnormal activities; for example, there is a suspicious TCP connection, the IPS can inject a TCP packet to drop the connection to prevent further damages to the target. Such reaction can be harmful if the suspicious TCP connection turns out to be a normal transaction.

After 3 years into NIDS, I still stick to NIDS. HIDS requires some administration effort to set up and maintain. I have a small team and responsible for many servers. It is more efficient to use a CCTV (NIDS) rather than a guard in each room (a HIDS in each server). The down side is that NIDS is blinded of what is going in the server. To counter this, patching is the ultimate solution to attacks.

IPS is an in-line device like that of a Firewall. Malfunction of an IPS will cripple the network. Moreover, a secure and reliable device should have the least software components with least changes. But an IPS will have intrusion definitions updated regularly.

The Wish List For NIDS

Ideally, NIDS should fulfill the following requirements:

1. Sniff out all the bad traffic and alerts administrators of the events. There will be lots of bad traffic, and hence lots of alerts. So, NIDS should
2. Suppress casual attempts. Such attempts are part of the Internet highway traffic from script kiddies. Unlikely they will succeed if (1) perimeter defense are put in place and (2) servers are properly patched. What if someone is seriously and determined to get you?
3. Alert if the attempt is persistent, it could be an intentional hacker targeting the company, the industry, or the country. For zero day prevention, NIDS should
4. To detect abnormal behaviors like extraordinary high volume of mails and high traffic at firewalls.
5. Though we are less concerned with malicious codes not targeting at us, the implication is that the sources, i.e. your systems, are infected. The sources need to be traced and cleaned.

The Reality of NIDS

In reality, NIDS sniff out all network packets that transmit over the IP network. Three mechanisms are used to inspect a packet:

- Pattern matching

NIDS detect malicious codes by matching the patterns of network packets of known intrusions like Windows Spyware and slammer worm. An attack is flagged if the matching pattern is found.

- Protocol behavior

Network packets are expected to behave as defined in the RFC. A simple example is that SMTP uses port 25, a SMTP packet that use ports other than 25 will be flagged as attempting to inject non-standard codes to the target server.

- Heuristic

This is a big word used by vendors. It means that a NIDS has the intuitive to detect a bad packet based on intelligence other than the 2 mechanisms mentioned above. I have seen a couple of basic rules that vendor input to their NIDS product for differentiation.

Are these mechanisms of NIDS capable of detecting intrusions as efficient as anti-virus software? Below are my findings:

1. NIDS picked up the bad traffic as well as the noise. Users aka Windows desktops contribute the most noise to the bad traffic. First, Windows use available ports to communicate if the defined port is used. This violates the protocol behavior. Second, instant messaging, music and movies download, spyware and peer-to-peer shareware are considered illegal activities by NIDS. Instant messaging alone contributes to 30% of the total NIDS alerts.

These noise masks the real attacks. The administrator faces the dilemma of tracking or ignoring the traffic from Windows, the most vulnerable OS. One golden rule to eliminate the noise is to ignore known Windows virus alerts that target mail servers. Don't panic, mails are a popular carrier of virus, **the mail servers would and should have anti-virus software and virus definitions up to date.**

The server LAN is very much under control, the alerts indicates 2 possibilities, either someone is doing troubleshooting or some cracker is trying to get at the target.

2. Script kiddies's pastime is to pop around the Net to look for easy targets. With **proper perimeter defense and up-to-date security patching for servers**, these kiddies are unlikely to spend long time on a target and unlikely to succeed. These are noise that we can ignore. We can set thresholds for frequency and duration of incidents to filter the noise.
3. One way to tell an intentional cracker from a causal hacker is the persistency. If someone hangs around your DMZ for more than 30 minutes, we should trace the source, block the source IP if the company has no business relationship with the source.
4. **An administrator should have the baseline volume of Firewall reject logs and email.** Large volume of emails is a common symptom of virus attack. Large volume of firewall rejections indicates a possible DOS, or infected internal systems by virus or worms that send packets out to a wide range of IPs. Note that monitoring of Firewall logs is beyond the NIDS capability. This service can be extended to a managed security service provider since the vendor is already providing 24 x 7 NIDS monitoring service.
5. The utmost concern for administrators is internal system being the targets of attack coming from Internet. Do we care when the attack targets are external systems? Yes when the attacks are sent from your network. One or more of your systems could have been compromised and become the victims or robots that are used by the hackers to achieve their goals.

Summary

We started out with a wish list. NIDS will alert only when necessary. We had a security response and escalation procedure nicely laid down. There are 2 levels of alerts, the first level is email notification for non-critical events, the second level is SMS notification where staff will respond immediately. A ticket

will be opened, staff is to investigate and close the loop.

From the security aspect, 95% of the alerts were found either false positive or non-threatening due to the noise from Windows platform, office users, and the script kiddies. Having observed the NIDS performance for a month, the reality was most alerts do not require immediate attention from administrators. Only when the intrusions persist then we should investigate immediately.

So we now have 4 critical alerts: (1) high reject volume from Firewall, (2) high volume of emails, (3) persistent attempts, and (4) network availability affected, symptom of DDOS. With appropriate thresholds set for events (1), (2), and (3), we reduce the false positive rate. Event (4) will be detected by server and network monitoring tools.