



NISCC Technical note 09/03

Issued 19 November 2003

Understanding Intrusion Detection Systems

Key Points

- Introduction to intrusion detection technology
- Techniques used for detection
- Sensor types, and some principles of sensor placement
- Active responses and intrusion prevention

**National Infrastructure
Security Co-Ordination Centre**
PO Box 832
London, SW1P 1BG

Tel: 020 7821 1330 Ext 4511
Fax: 020 7821 1686
Email: enquiries@nisc.gov.uk
Web: www.nisc.gov.uk

NISCC Technical Note 09/03: Understanding Intrusion Detection Systems

Aim

1. This NISCC Technical Note is a revision of NISCC Technical Note 05/02. It is intended as an introduction to Intrusion Detection Systems (IDSs), but also explores possible security features of IDSs and their current state of implementation. It is vendor-independent and does not discuss features available on particular products. The intention is to increase technical awareness about IDSs in the NISCC constituency, and to enable potential purchasers to determine the security features of IDSs most appropriate to their networks. It is aimed at managers and security officers who wish to inform their decision on the choice of an IDS. A checklist of the issues raised is provided at the end of this note.

Summary

2. There are many types of IDSs, some more useful than others at detecting intrusions from particular classes of attackers. Each combination of options will have its own advantages and disadvantages.

3. There are a number of commercial and open source IDS products currently available, and despite the relative immaturity of intrusion detection technology in general and shortcomings in specific products, IDSs can be an important part of an organisation's computer security strategy as a second line of defence to other security devices.

Introduction

4. This note is not intended to be exhaustive in its coverage. The following URLs link to papers that provide alternative or more detailed coverage:

- <http://www.sans.org/resources/idfaq>
- <http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf>
- <http://www.securityfocus.com/infocus/ids>

5. An intrusion can be defined as “any set of actions that attempt to compromise the integrity, confidentiality or availability” [1] of a resource. This definition captures the notion of an intrusion as being a deliberate security violation, although it is arguable that unintentional unauthorised access to a resource would also count as an intrusion. In any case, intrusion detection in the context of this note is the detection of intrusions directed against computer systems.

6. An IDS is like a burglar alarm for computer systems and networks. Its function is to detect intrusions and take some appropriate action. Initially IDSs were limited to alerting the system administrators that an event had occurred, but most current systems offer the ability to take some action to defend against the attack, such as breaking the connection or amending the firewall rule-set to deny access to the perpetrator. The term Intrusion Prevention System (IPS) is often used to describe this class of IDS, but many common IDSs contain this functionality

7. The most common criticism of IDSs is the number of “false positives” they produce. A false positive occurs when the IDS identifies legitimate action as nefarious and takes inappropriate action. False positives occur primarily during the initial phases of an IDS installation and can be tuned down to a low level over time. Considerably more worrying are “false negatives” where nefarious action is classed as legitimate. These events are less obvious to the user, and result in less

criticism, but are more significant from a security point of view. It is better to deal with a few false positives than to miss a single compromise.

8. The scope of this note is restricted to detection of intrusion. Alternative approaches to improving overall levels of security are to limit the exposure of the system to attack and to limit the impact of attacks. Building dependable systems and network infrastructures are the subject of ongoing research [2], but this is not discussed further in this note.

IDS Categories

9. This note aims to help with understanding the types of intrusion detection systems that have so far been implemented in commercial or research systems. These can be categorised by the following:

- Techniques used for detection
- Sensor type
- Type of attacks identified
- Response

Techniques Used for Detection

10. Intrusion Detection Systems come in two broad categories: those that search for predefined patterns and those that search for unusual or anomalous activity. The former type is commonly called *signature detection* or *misuse detection*, while the latter type is known as *anomaly detection*.

Signature-Based Detection

11. Signature-based detection is the simplest to characterise of the intrusion detection techniques. A pattern or signature is used to identify an item of data as indicative of an intrusion and data items are examined against attack signatures. An example is the use of Unicode encoded characters present in a requested URL to take advantage of the directory traversal vulnerability present in a number of older web servers. To exploit this vulnerability the Unicode encoding of '/' is used instead of the actual character and the string './././.' is replaced with './.%c0%af.%c0%af.%c0%af'. As there is no legitimate reason why this string should appear in a URL its presence is enough to raise concern.

12. Signature-based detection techniques tend to be fairly simple to formulate and are easy to add to the rule set of the IDS. However, attackers can often obfuscate their activity by modifying their attack slightly so that it doesn't match the signature. In the above example, this could be as simple as adding an additional './.%c0%af' to the attack string. The problem for the IDS vendor is to write signatures that are stringent enough to capture all variants of an attack without producing false positives for legitimate traffic (such as someone discussing the attack in an email).

13. Signature-based detection is also non-adaptive: from a set of attacks of similar types (e.g. buffer overflow attempts), the IDS will not be able to detect an instance of that attack for which it does not have a signature. It is therefore imperative that the signatures are kept up-to-date for the system to detect the latest exploits.

Protocol analysis

14. Protocol analysis of network data involves analysis of the data against a model for the correct and expected operation of the network protocol used, so that incorrect or unexpected behaviour can be detected. Protocol analysis has the advantage that it does not rely on attack signatures, but it is

limited by the completeness of the model's description of "normal behaviour" for the protocol and it is vulnerable to an attacker making an intrusion look like expected behaviour.

Anomaly Detection - Statistical Inference

15. Statistical inference is a common technique for detecting abnormalities in patterns. For example, a significantly larger than average data flow inbound to a network may indicate an attempted denial of service attack, while a gap in a log that is statistically significant may indicate deletion of records.

Anomaly Detection - Machine Learning

16. Machine learning approaches are designed to adapt to new attacks. This involves establishing a baseline of normal network activity, requiring a period of training. The system will then produce an alert when the current network activity changes unexpectedly.

17. In contrast to signature-based intrusion detection and statistical inference, machine learning approaches tend to be complicated to implement, and current implementations are mostly within the academic and research communities.

18. A number of machine learning techniques have been implemented in IDSs including Neural Networks, Rule-Based Learning and Expert Systems. They are less commonly used in production systems due to the additional complexity and associated processing overheads.

Sensor Type

19. Most modern IDSs comprise of a number of sensors connected to a central management console that is used to view alerts, tune rule sets and update sensors.

20. There are four common types of intrusion detection sensor that process data from different sources. They are as follows:

- Network-based intrusion detection sensors
- In-line Network detection sensors
- Host-based intrusion detection sensors
- Network node intrusion detection sensors

21. A good IDS installation will normally feature a number of different types of sensor, with network sensors placed to identify attacks entering or leaving networks and host-based sensors protecting sensitive servers.

Network-Based Intrusion Detection Sensors

22. Network-based intrusion detection is detection of attacks in network services, such as SMTP (email) or HTTP (web). Attacks of this kind are common, especially given the internet and extranet connectivity of many organisations.

23. Network-based IDSs employ sensors that listen to the network segments of the network and report to a central management console which is typically used for analysis and reporting. Network sensors can also be implemented on some routers. One sensor will be needed for each network segment if the packets are routed to the segments by a switch (unless the switch allows traffic on the same virtual local area network to be copied to a mirror Switch Port Analyser port).

24. Network-based IDSs suffer from two main limitations. Firstly, they cannot analyse encrypted packets. Secondly, they may not retain all packets relevant to an attack, so that it is not possible to verify that an alert is related to a real attack.

In-Line Network Intrusion Detection Sensors

25. An in-line network sensor is used to analyse all traffic travelling between two network segments. The sensor has a connection to each network and all traffic passes through in much the same way as it would through a firewall. As the sensor has complete control of the traffic, it can stop packets being passed between the networks if an alert is raised.

26. As each packet must be inspected before being passed on, there is the potential for in-line sensors to become a network bottleneck, in much the same way that a firewall can be. In deploying these sensors, it is necessary to check that they will be able to operate quickly enough to be able to handle the network traffic flow without dropping packets or causing an unacceptable performance load.

Host Based Intrusion Detection Sensors

27. Host-based intrusion detection sensors analyse activity on a particular computer by analysing system calls and operating system and application logs. As with network sensors, some host-based systems now have the ability to stop certain system calls that may be used in various exploits.

28. It is advisable to install a host-based IDS on each host that provides an essential service to the company or that is used to store sensitive data. Examples would be mail and web servers in the De-Militarised Zone (DMZ) and file and application servers on the internal network.

29. Host-based IDSs are very good at detecting intrusions on a particular host and for recording details of the intrusion. They do not in general obtain information on the origin of the attack.

Network node Intrusion Detection Sensors

30. Network node intrusion detection only analyses traffic to or from one particular host. The deployment of network node IDSs is therefore the same as for host-based IDSs, but the attack types that the IDS identifies are related to network attack. Because they report on network attacks relating to a host, network node IDSs can be combined with a host-based IDS to provide greater information on the cause of the attack

31. Network node IDSs require a security policy that identifies security critical hosts on the network (eg web servers, domain controllers), and as such have a different emphasis to network-based IDSs.

Response

32. When an IDS produces an alert, it will normally be forwarded to a management console and there will be a period of time between when the activity occurs and when it can be investigated. To ensure a more rapid response to certain types of intrusion, many IDSs now offer the ability to perform some form of active response to an identified attack. The type of response will vary between IDSs. They include:

- Connection Resetting

33. For TCP connections it is possible for the IDS to send a Reset packet to either or both of the attacking and attacked hosts, effectively breaking the connection.

- Packet Filtering

34. With in-line sensors, in addition to sending Reset packets to break the connection, it is possible to block the packet that contains an identified exploit to stop it reaching the host being attacked.

Access-List Modification

35. Some IDSs can interact with a firewall to block access from a given host if that host is identified as being the origin of an attack or port scan.

36. With all forms of active response there is a risk that an attacker could use a badly configured IDS to deny service to legitimate users by forging nefarious packets to look like they originated from an accepted source IP address.

37. For the same reason, active responses should only be used in a system that has a low occurrence of false positives.

Type of Attacks Identified

38. The type of IDS is also determined by the type of attacker that an IDS needs to identify. Broadly there are two types of attacker:

- External attackers
- Legitimate system users

External Attackers

39. To identify attacks by external attackers, it is important to have adequate physical security measures in place and to have a firewall controlling all remote access. The firewall should be configured to log all traffic, especially that which does not meet the expected business functions. A network-based intrusion detection sensor could be placed on the external side of the firewall if it is important to assess the potential level of threat. However, an external sensor will produce a disproportionate amount of alerts due to the large amount of indiscriminate scanning present on the Internet. Differentiating between this “Internet noise” and any directed attacks is extremely difficult.

40. It is advisable to place a network-based intrusion detection sensor on the internal interfaces to the firewall (including any De-Militarised Zones, where mail servers and web servers are typically located). The sensor would report detected intrusions to the management console, which would alert the system administrator

41. It is also important to have host-based operating systems sensors in place for any computers that are exposed to the external network. If the network-based intrusion detection sensors fail to detect an attack (e.g. if the exploit was sent to a web server over an encrypted SHTTP channel), vulnerabilities in the services offered could lead to compromise of the host offering the vulnerable service.

Legitimate System Users

42. Legitimate system users may misuse their privileges to gain access to data to which they are not permitted access, modify or corrupt data, cause the system to crash or otherwise violate the terms of the system security policy. It is much harder to counter the threat from system users than from external attackers. It is essential to have good procedures for personnel security so that the level of trust appropriate to the user can be identified.

43. It is also essential to confirm that the system security policy permits monitoring of email, web and other network services offered by the organisation, and that users have signed the appropriate agreements. From a technical perspective, one can then pass internal network traffic through content filtering programs in order to identify abuses of the system security policy.

Protecting the IDS

44. IDSs themselves are often the target of attack because it is in an attacker's interest to prevent detection of attacks. For this reason the operating systems on which the IDS run, and the operating system of the data collection unit and the management console, should be hardened as far as possible. Furthermore, in the case of a network-based IDS, it is often advisable to deploy a passive tap that listens on the network without producing network traffic of its own, to avoid being detectable by network monitoring software. Examples of passive taps are hardware taps (e.g. shimiti) or ethernet cards in promiscuous mode with no IP address.

45. For network sensors, communication between the sensors and management console can be made over the network that is being protected (in band) or on a separate IDS network (out of band). By adopting the second approach, the console is isolated from attack, and sensors can be run in promiscuous mode. The transition of data between network segments is also simplified as no additional firewall rules are required.

Checklist

46. A checklist of the issues to take into account when planning deployment of an intrusion detection capability is listed below.

Is the main threat from outside or in? [Emphasis on sensor placement]
Do you offer network services outside your organisations? [Emphasis on network based IDS and host based sensors for external facing servers]
Do you have a switched network? [Emphasis on network node IDS]
Is the IDS signature-based? If so:
Does the vendor supply regular signature updates? [If signature-based IDS]
Can you write your own signatures? [If signature-based IDS]
Does the IDS perform misuse detection or anomaly detection? If so:
How well does the IDS perform on a well-known sample of test data?
How much tuning does the IDS require?
Can you tune out persistent false alarms? [If misuse detection IDS]
How much training does the IDS require? [If anomaly detection IDS]
How much packet information does the IDS store when it identifies an event as an incident?
Does the IDS offer host and network-based intrusion detection?
Can the IDS be integrated with firewalls and routers to provide a centrally managed solution?
Can the IDS correlate across hosts? [If host based IDS]
Can the IDS export logs and alerts in a common format?
Does the IDS block intrusions?

References

[1] Quoted from R. Heady, G. Luger, A. Maccabe and M. Servilla “The architecture of a network level intrusion detection system” Technical Report, Computer Science Department, University of New Mexico, August 1990.

[2] See, for example, the work of Carnegie Mellon University, http://www.cert.org/nav/index_purple.html, in the US and the MAFTIA project, <http://www.research.newcastle.ec.org/maftia/index.html> in Europe.