

## Intrusion Detection Systems Terminology, Part Two: H - Z

A. Cliff 2001-07-19

### IDS Terminology, Part Two: H - Z

by A. Cliff

last updated July 19, 2001

---

This is the second of two articles intended to introduce readers to some IDS terminology, some of it basic and relatively common, some of it somewhat more obscure. (To see the first article, please click [here](#).) As a result of the speed of growth of IDSs, and the marketing prowess of some IDS vendors, some confusion has arisen about the proper meaning of certain terms: the same term may be used by different vendors to mean different things. Wherever possible, I have tried to include all terms except where I consider usage of the term to be inaccurate or misleading. This is a living document: if I'm missing any terms or you wish to discuss my interpretation please don't hesitate to contact [me](#).

### IDS Categories

Although we tend to talk about IDSs as though they are one thing, there are actually many different types of IDS. The following is a list of the various types of IDS, and a brief explanation of what differentiates them from other types.

#### IDS Category: Application IDS

Application IDSs are aware of the intrusion signatures for specific applications, usually the more vulnerable applications such as web servers, databases etc. However, many of the host-based IDSs that ordinarily look at operating systems, are becoming more application-aware. Many of the host-based IDSs that aren't application-aware by default can be trained to become so. For example, KSE (a host-based IDS) tells you everything that is going on from the event logs, including output from the event log reporting applications. Most of these events can be filtered by the operator because they have no security relevance, but those events with a security significance, such as viruses or failed access can be given a higher priority.

One example of an application-specific IDS is Enterscept Web Server Edition.

#### IDS Category: Consoles

In order to make an IDS suitable for the corporate environment, the dispersed IDS agents need to report to a central console. These days many central consoles will also accept data from

other sources, such as other vendors' IDSs, firewalls, routers etc. This information can be correlated to present a more complete attack picture. Some consoles will also add their own attack signatures to those supplied at agent level. Many consoles provide the facility of remotely administering the IDS.

Examples include Intellitactics Network Security Monitor and Open Esecurity Platform.

### **IDS Category: File Integrity Checkers**

When a system is compromised an attacker, it will often alter certain key files to provide continued access and prevent detection. By applying a message digest (cryptographic hash) to key files, the files can be checked periodically to see if they have been altered, thus providing a degree of assurance. Upon detecting such a change, the file integrity checker will trigger an alert. The same process can be employed by a system administrator after being successfully attacked, allowing him/her to ascertain the extent to which the system has been compromised. Previously, file integrity checkers detected intrusions long after the event; however, more products have recently been emerging that check files as they are accessed, thereby introducing a near real time IDS element.

Examples include Tripwire and Intact.

### **IDS Category: Honeypots**

As mentioned in the [first article](#) in this series, a honeypot is a system that can simulate one or many vulnerable hosts, providing an easy target for the hacker to attack. The honeypot should have no other role to fill; therefore, all connection attempts should be deemed suspicious. Another purpose is delay: the attacker wastes time on the honeypot while the original entry hole is secured, leaving the truly valuable assets alone.

Although one of the initial purposes of honeypots was to gather evidence for the prosecution of malicious hackers, there is much talk of entrapment when deploying honeypots; however, does the vulnerability of the honeypot give the hacker the right to attack it? In order to reach the honeypot an attacker would have had to circumvent at least one bonafide security device provided the honeypot is inside your network. In some countries law enforcement agencies cannot prosecute using evidence from a honeypot.

Examples of honeypots include Mantrap and Sting.

### **IDS Category: Host-based IDS**

This kind of IDS monitors sys/event logs from multiple sources for suspicious activity. Host-based IDSs (also known as host IDS) are best placed to detect computer misuse from trusted insiders and those who have infiltrated your network evading traditional methods of detection. What I've just described is really an event log viewer (with attitude). A true host IDS will apply some signature analysis across multiple events/logs and/or time. Many will also incorporate heuristics into the product. Some will introduce an added benefit: because they operate at near real time, system faults are often detected quickly, this makes them popular with techies as well as security personnel. The term host-based IDS has been applied to any kind of IDS sitting on a workstation/server. Vendors have tried this for various products from Network Node IDS to File Integrity Checkers, while I can understand their logic, this can be misleading to the buyer.

Examples include Kane Secure Enterprise and Dragon Squire.

### **IDS Category: Hybrid IDS**

Modern switched networks have created a problem for intrusion detection operators. By default, switched networks don't allow network interface cards to fully operate in a promiscuous fashion (although some allow spanning ports or link mode Terminal Access Points (TAPs), whereby a certain TAP will see the traffic on all other TAPs.) However, some switches will not allow it at all, making the installation of a traditional network IDS difficult. Furthermore, high network speeds mean that many of the packets may be dropped by a NIDS. A solution has arisen in the form of Hybrid IDSs, which takes delegation of IDS to host one stage further, combining Network Node IDS and Host IDS in a single package. In my experience, while this solution gives maximum coverage, consideration should be given to the amount of data and cost that may result. Many networks reserve hybrid IDS for critical servers.

Some vendors refer to any IDS that fills more than one role as being Hybrid IDS; however, I feel this is more out of marketing greed than genuine honesty. The term "Hybrid IDS" was flavor of the month circa mid-2000 and many vendors wanted to jump on the bandwagon.

Examples of hybrid IDS include CentraxICE and RealSecure Server Sensor.

### **IDS Category: Network IDS (NIDS)**

Monitors all network traffic passing on the segment where the agent is installed, reacting to suspicious anomaly or signature-based activity. Traditionally these were promiscuous packet sniffers with IDS filters, though these days they have to be far more intelligent, decoding

protocols and maintaining state etc. They come in the guise of appliance-based products that you just plug in to software that can be installed on off-the-shelf computers. They analyze every packet for attack signatures, though under network load many will start to drop packets.

Many Network IDS have the facility to respond to attacks, which was covered under 'Automated Response' in [part 1](#). There was some hype in late 2000 about how Network IDS had seen its day pass due to high speeds and switched networks, but some Network IDS can cope with gigabit speeds with minimal dropped packets, and switched networks can be overcome with spanning ports or TAPs such as those supplied by Shomiti.

Examples of Network IDS include SecureNetPro and Snort.

### **IDS Category: Network Node IDS (NNIDS)**

Switched and/or high-speed networks have brought with them a problem: some Network IDS are unreliable at high speeds, when loaded they can drop a high percentage of the network packets. Switched networks often prevent a network IDS from seeing passing packets promiscuously. Network Node IDSs delegate the network IDS function down to individual hosts, alleviating the problems of both high speeds and switching.

While Network Node IDSs are closely related to personal firewalls, there are differences. For a personal firewall to be classed as an NNIDS, event analysis would have to be applied to the attempted connections. For instance, rather than "attempted connection to port \*\*\*\*\*" as you find on many personal firewalls, a NNIDS should identify a "whatever" probe, applying a signature for the "whatever" attack. A NNIDS would also pass events received at the host to a central console. Despite these differences, I suspect that many personal firewall vendors will start to push their products as NNIDS.

Examples of an NNIDS include BlackICE Agent and Tiny CMDS.

### **IDS Category: Personal Firewall**

Personal firewalls sit on individual systems and prevent unwanted connections, incoming or outgoing. While not infallible, they are very effective in protecting hosts from attack. Not to be confused with Network Node IDS.

Examples include ZoneAlarm and Sybergen.

## **IDS Category: Target-Based IDS**

This is one of those ambiguous IDS terms, which means different things to different people. One definition may refer to them being File Integrity Checkers, while an alternative is a network IDS that only looks for signatures of attacks to which the protected network may be vulnerable. The objective of the latter definition is to speed up the IDS by not looking for unnecessary attacks. Personally, I want to know about every attack regardless of its chance of success. My point of view is that because the term has meant very different things, its use should be avoided for a few years - in effect, quarantining the term to avoid confusion.

## **Intrusion Detection Working Group (IDWG)**

The purpose of the Intrusion Detection Working Group is to define data formats and exchange procedures for sharing information of interest to intrusion detection systems and response systems, and to management systems which may need to interact with them. The Intrusion Detection Working Group will coordinate its efforts with other [IETF](#) working groups.

## **Incident Handling**

Detecting an intrusion is just the beginning. More often than not, the console operator will be receiving alerts almost constantly, therefore he/she cannot spare the time to follow up each potential incident in person. The operator will tag events of interest for further investigation by the incident handling team. After the initial response the event then needs to be handled, looking at issues such as investigation, forensics and prosecution. Chris Jordan's paper "[Analyzing IDS Data](#)" covers first and second level analysis of IDS alerts

## **Incident Response**

The initial reaction to a detected potential incident, which is then handled according to incident handling procedures.

## **Islanding**

Cutting the network off from the Internet, islanding is a drastic action, almost a last resort. It is occasionally used by some organizations faced with a large virus outbreak, or even when the threat of an attack is considered significant enough.

## **Promiscuous**

By default, the IDS network interface only sees information to or from the host - this is termed non-promiscuous. By making the interface promiscuous, you can see all the network traffic on your segment regardless of the source or destination. This is essential for a Network IDS, but

by the same token can be used by packet sniffers to monitor your network traffic. Switched hubs go a long way to prevent this and many have span ports where you can see all the traffic.

## **Routers**

A router is a device for connecting sub-networks. They operate at the Transport and Network layers of the OSI 7 layer model. More basically, routers help to navigate network packets to their destinations. Many also have Access Control Lists (ACLs) that will allow you to filter out undesirable packets. Many routers can feed their logs into an IDS, providing valuable information about blocked attempts to access a network.

## **Scanners**

Scanners are automated tools that will scan network for hosts and/or vulnerabilities. Like intrusion detection systems, these also come in a variety of guises. I have included a list of scanners below, along with a description of each. (For a full list of available products visit [my website](#).)

### **Scanner Category: Network Scanners**

Network scanners are designed to map a network, finding all the hosts on that network. Traditionally they would use an ICMP ping, but this is too noisy and can be detected with ease. As the network scanners had to become a lot stealthier, they began to use a variety of other methods, such as ack scans and fin scans, to achieve their goal undetected. The other advantage in using these more obscure methods is that different operating systems will respond to these scans in different ways giving the attacker more valuable information.

One example of such a tool is nmap.

### **Scanner Category: Network Vulnerability Scanners**

Taking the network scanner a stage further, a network vulnerability scanner will check the target host(s), highlighting any vulnerabilities that can be exploited by the hacker. They are used by attackers and security professionals and are very noisy - they make the Network IDS go ballistic. Some vulnerability scanners such as [Whisker](#) look for vulnerabilities in web servers, it even has an anti-IDS setting, making it difficult for a Network IDS to detect.

Retina and CyberCop Scanner are examples of network vulnerability scanners.

### **Scanner Category: Host Vulnerability Scanners**

Operating as a privileged user, these tools will scan the host from the inside, checking a wide range of things from password quality and security policy to file permissions. It can be detected by a Network IDS and, particularly, by a Host IDS. SecurityExpressions is a remote Windows vulnerability scanner that will also auto fix. Some tools such as ISS database scanner will scan a database for vulnerabilities

### **Script Kiddies**

Rather than do it the hard way, a script kiddie will use exploit scripts written by others to achieve their aims. There is much talk about belittling a Script Kiddies capability, even the name sounds a little derogatory. However, tread carefully they are a force to be reckoned with, as [grc.com](http://grc.com) know only too well. An analogy given to me by a Policeman from the Royal Air Force CERT; script kiddies are like kids with guns, they don't need to understand ballistics or be able to build the gun to make them a formidable foe, at no time should they be under estimated.

### **Shunning**

Shunning is the practice of configuring border devices to reject any packets from objectionable sources. Some networks have been known to shun IP addresses from a specific country. More often than not ISP's with a poor clean up rate will be shunned.

### **Signatures**

At the heart of the IDS is the attack signature, this is what makes the IDS trigger on an event. Too short and it triggers (too often creating false positives,) too long and it slows the IDS down. Some people see the number of signatures that an IDS supports as a benchmark of the IDS's quality. However, while one vendor has one signature covering many attacks another vendor may list the signatures separately, giving the impression (to some) that because it appears to include more signatures, it's a better IDS.

### **Stealth**

Stealth interfaces allow an IDS to be invisible to the outside world while still being able to detect attacks. They are most used outside the DMZ, beyond the protection of firewalls. There are drawbacks such as automated response.

## Relevant Links

[IDS Terminology, Part One: A-H](#)

*A. Cliff*

[Talisker's Network Security Tools](#)

[Privacy Statement](#)

Copyright 2006, SecurityFocus