Intrusion Detection Systems: Securing a Network Environment

By Asha Bielewicz (9718446)

Traditionally, Web servers were connected directly to the Net without any protection. Today, it is highly unlikely to see a web server without screening routers or firewalls to block attacks. Screening routers, if configured right, will protect a network from IP spoofing. Some more advanced screening routers may protect the system from the Ping of Death and SYN floods. Firewalls can detect some hacker attacks, especially network probe attacks. However, if someone gets through the firewall, the firewall does not know what is happening. Malicious insiders will not be detected either. Furthermore, a firewall is effective when all network traffic passes through it. Many people use modems to connect to the outside world and unwanted traffic enters that the firewall does not see. Firewalls often do not work simply because someone does not configure the firewall properly. In addition, bugs that already exists in the firewall implementation can become exploited. By the time someone finds out about these problems, it may be too late. Intrusion detection is needed because firewalls and other network security mechanisms do not completely eliminate successful hacker attacks. For example, an internal web server uses a firewall to block bad protocols, but http traffic is allowed to travel through. Two well known hacks, *test.cgi* and *phf* , resulted from the way input data from HTML forms was processed by a CGI program. The user was asked to enter some text string, which the CGI script processed. With this setup, a hacker could remove all files in the current working directory of the Web server by adding ";rm *" to the input string. [2]

Intrusion Detection System (IDS)

Intrusion detection systems (IDS's) purpose is to monitor the system for attacks. There is a difference between misuse detection and intrusion detection. Misuse detection focuses on detecting problems from inside the trusted network by monitoring the activities of authorized users. [2] Intrusion detection is concerned with attacks from outsiders or intruders. The difference is that intrusion detection assumes that the intruder has no legitimate account and misuse detection presumes that the perpetrator has at least one valid account on the system. An attack can originate at an inside node, hop to an external node and come back into the trusted network. As a result, intrusion detection systems often deal with any misuse and intrusion that is unwanted. [2]

How does an IDS system work?

An IDS looks at all passing traffic on the network. It then stores the information, and compares the packets to a number of known attack patterns. (Branton, p.254) For example, a SYN flood will be noticed by an IDS when a particular host is sending SYN packets without ever attempting to complete the connection. The IDS would identify this and respond. "A good IDS may have well over 100 attack patterns saved in its database." [1] The action taken varies with IDS systems, and their different configurations. In addition, IDS systems log suspicious events. Raw packets can actually be saved so that they can be later analyzed by the network administrator. Some can be configured to send out a page or an e-mail alert of an intruder. Suspicious transmissions can be interfered by resetting both end of the connection. Finally, an IDS system, if advanced enough, can

work with a firewall or router to modify the passage rules blocking the attacking host. [1]

An IDS consists of an engine and a console. The engine is responsible for capturing and analyzing the traffic. The console is responsible for managing the engine and showing reports. It is possible to run multiple engines and monitor them from a single console. Consequently, it is effective to have the engine and the console run on separate systems. It should be mentioned that intrusion detection systems require a large amount of resources. It is recommended that the engine reside on a committed system with 128MB of RAM and an Intel 300MHz Pentium II or Pro processor or equivalent. [1] It is also recommended to have at least 100MB of disk space. The system logs all traffic, and depending on how busy the system is the database will need to be emptied with time. Therefore, a busy system will need more space. Running the console requires about the same requirements, plus enough disk space to store copies of each engines database. [1]

IDS Limitations

As with the screening router and the Firewall, there are limitations. The IDS works in real-time, and any countermeasure the system will take may be too late to prevent anything. For example, the Denial of Service attack is a common hack. By the time the IDS realizes it has been attacked, the DoS may be in full effect. For example, a Teardrop attack, causes a buffer to overflow and crash the receiving system. For some operating systems, it only takes one bad packet sent. By the time the IDS realized that a Teardrop attack has been launched the server has already shot down. [1]

In February 1998, a study was performed which discovered and documented vulnerabilities in IDS. One problem documented in this study was that some IDS systems were not verifying the checksum field with the IP header. Hackers manipulated this field causing the IDS to record different information than the receiving system. For example, an IDS looks for PHF CGI attacks by screening HTTP requests for the 'phf' string. Once this is detected, the IDS responds. An attacker could send a series of packets each containing one character of a string such as 'phoof'. If the attacker manipulated the checksum field of the packets containing characters 'o' to be invalid. The IDS, not checking the checksum field would process the string as 'phoof'. The received would process the 'phf' string and get hit without being detected. [1]

Direct attacks against IDS could cause the system to shut down and all attacks become undetected. However, there is no reason to have the intrusion detection system directly accessible from network hosts. As a result, making the IDS unreachable from the Internet makes it impossible to get hit.

Conclusion

By monitoring the system, one can be sure that the right security policy has been specified and that the policy is being implemented. Although there are limitations, once discovered the IDS system can be patched. IDS systems are not meant to be replacements for firewalls rather they are an additional source of security.

References

[1] Brenton, Chris, Mastering Network Security. Sybex: San Francisco, 1999.

[2] Excamilla, Terry, Intrusion Detection: Network Security Beyond the Firewall. Wiley Computer Publishing: Toronto, 1998.