Intrusion Detection

www.netsec.org.sa/int_det.htm

Network Security Center
NetSec
Internet Services Unit - King Abdulaziz City for Science & Technology

Introduction

With the evolvement of the Internet over the last few years, the need for security has been rising with it mainly due to the openness and connectivity nature of the web, people and organizations are faced with more challenges every day to secure their data and all other assets of value to them.

No system is totally secure. Any security procedures should be undertaken with that in mind. There will always be threats and actual intrusions. The ultimate goal should be minimizing the risk and not eliminating it.

What is an Intrusion?

Any attempt to compromise the integrity, confidentiality and availability of information and/or resources. There are two types of intrusion, Technical and non Technical. Technical intrusion involves using technical tools and expertise to perform the intrusion. Non technical (also known as social) intrusion involves using any non-technical means to perform the intrusion. Here we will focus on technical intrusion but its crucial to understand that non-technical intrusion methods can be as damaging as technical methods, if not more damaging.

Why do we need Intrusion detection?

1. There is no such thing as a totally secure system, this is due to:

- Software will always have bugs that compromise the system security
- The methods that are being used to develop software have not evolved much to reflect the need to minimize software bugs

2. The wide variety of hardware and software systems used will complicate the security process.
3. Cryptography as the most classical security method is source of concern in terms of the vulnerabilities that might be discovered in an algorithm or its implementation.
4. Users inside the environment are the biggest source of system abuses.
5. As more access control is enforced, users are more system friendly. Unfortunately, the opposite is quite true and in some environment tight access control is not an option.

Intrusion Methods

Most intrusion methods are based on three strategies:

1. *Targeting hardware and security system*: This method assumes the would-be intruder knows some information about the hardware and security methods used in the facility he's attacking.
2. *Exploitation of known weaknesses*: Software bugs are being brought attention quite frequently. Unfortunately sometimes, fixes for these bugs are not made available soon enough. This leads to exploits of these vulnerabilities.
3. *Brute force attacks*: In this method, the attacker attempts to break a system by trying to guess its security codes, such as attempting to guess the root password by trying possible combinations of characters.

Examples of known intrusion methods

Packet Sniffing

Packet sniffing is attempting to read information packets belonging to someone else to try to gain private information or illegal access. Packet sniffing is not a new technique, it has been around since Ethernet came about but it thrived on the internet. This is due to the fact that packet sniffing became easier over the web and packet sniffers are available via download from the web. This, coupled with the fact that packet sniffing is hard to detect, made packet sniffing very popular as an intrusion tool.

There are two main goals for packet sniffing on the commercial level, first to obtain user names and passwords and to gain sensitive and confidential data. The only way to guard against packet sniffing is by using encryption. There are three ways to apply encryption to packets:

1. *Link-level encryption*: packets are encrypted as they get on the transmission medium and decrypted as they arrive at the destination. This prevents sniffing since a sniffer gains access to packets while they are being transported on the medium and since they are already encrypted, no information is gained.
2. End-to-end encryption: packets are encrypted by the host transmitting the data, and are decrypted when they are received at the other end.
3. Application level encryption: here, encryption is done at the application layer instead of relying on hardware.

IP Spoofing

Spoofing an IP address means impersonate a trusted machine or a host by forging an IP address belonging to them. This is used for:

1. Reprogramming routers (SNMP frames within UDP packets)
2. Denial of service attack (TCP SYN flooding)

Firewalls are very effective in providing protection against IP spoofing.

What is Intrusion Detection?

Intrusion Detection is the active or continuous action(s) to detect intrusive acts.

Characteristics of a good intrusion detection system

- Continuous autonomous execution
- Fault tolerance
- Resistance to subversion
- Minimal overhead
- Observation of Deviations
- Easy customization to specific needs
- Dynamic behavior detection
- Not easily deceived

Types of Intrusion Detection

1. Anomaly intrusion detection: the intrusion is part of an anomalous behavior.
2. Misuse intrusion detection: the intrusion can be modeled and encoded.

Anomaly Intrusion Detection

Here, the system security administrator should have knowledge of what constitutes normal behavior and from there attempts to detect statistically significant deviations. Statistical approaches are an example of anomalous intrusion detection were intrusions are detected by analyzing user behavior patterns.

Its advantages are its adaptiveness to users behavior and its ability to detect new intrusion methods. All what is needed to know is what is the normal behavior.

However, it also has disadvantages since not all intrusive activities are anomalous and not all anomalous activities are intrusive.

Misuse Intrusion Detection

The requirement for this is the knowledge of known attack patterns and attempting to detect these patterns. An example of that is pattern matching. This method has the advantage of being difficult to subvert has a lower overhead. On the other hand, its as strong as the person encoding these patterns, can only detect known patterns and rely on the integrity of the audit trail so attacks that involve IP spoofing are not detected reliably.

Comparison

With anomaly intrusion detection, the system knows what is a normal behavior and attempts to search for other types of behavior that it will consider suspicious. While in misuse intrusion detection, the system knows what is a suspicious behavior and attempts to search for patterns that match its knowledge of suspicious behaviors. Combining the two methods will yield a better detection rate. Also having reactive intrusion detection as a second line of defense also improves security. And finally one must not forget that intrusion detection is a part of the big security picture and must be combined with other security system to have as close to a secure environment as possible.

Some Intrusion Tools

Crack

This program attempts to break a password file using brute force methods and depending on the strength of the password, it can take a long time to run. It can be rendered ineffective by shadowing the password file. It can obtain the password file through direct access or through an NIS attack.

Packet Sniffers

These are programs written by hackers, so there is a lot of them out there. Sniffers require a machine to be on the LAN of the attacked organization. They are usually hard to detect. One detection procedure is to scan local machine for suspicious acts.

Machine and Services Discovery Utilities

These tools help an attacker discover all the running machines and services on the network. This is usually is done through sending ping packets asynchronously to multiple hosts and scanning ports of known services. FPING is and example of a host discovery tool while STROBE is a service discovery tool.

Packet Spoofing Utilities

Again, these programs are written by hackers, so there a large variety of them available. They provide the ability to change the IP headers to anything the user wants. They are most effective on one's own LAN. In order for them to work outside, some routing changes are needed for the local router.

Packet flooding Utilities

Those are programs written by hackers to exploit software bugs for denial of service attacks. This includes ping floods, port overloading and broadcast storms and depending on how, when and where they are applied, they can be difficult to detect.

Some Intrusion Detection Tools

COPS (Computer Oracle and Password System)

This utility checks for file permissions and security parameters, devices, passwords and startup files. The checking is performed as a normal user (usually automated as a cron job). COPS then uses comparison do determine if any anomalies have occurred. COPS was presented by Dan Farmer and Gene Spafford at the 1990 Usinex Conference and can be obtained from: ftp://coast.cs.purdue.edu/pub/tools/unix/cops

Tripwire

Another security utility that monitors modifications made to files by keeping digital signatures. Each file has a digital signature in the Tripwire DB and all signatures are to be stored on a secure host. Using these signatures, tripwire checks file integrity. Tripwire is not automated (unless run as a cron job) and offers many digital signature algorithms and unlike COPS, tripwire runs as superuser. It was written by Gene Kim and Gene Spafford of the COAST project in Purdue university and can be obtained at: ftp://coast.cs.purdue.edu/pub/COAST/tripwire

Tiger

Similar to COPS, its comprised of a set of scripts that scan the Unix system for any security problems. It provides a wide range of settings and is slow while running. Tiger was written by Doug Schales of Texas A&M university, its can be obtained from: ftp://net.tamu.edu/pub/security/TAMU

ftp://coast.cs.purdue.edu/pub/tools/unix/tiger