Network Intrusion Detection Proposal

Erin Jamroz University of Puget Sound
1500 N. Alder St.
Tacoma, WA
ejamroz@ups.edu

Jacob Fuhrman University of Puget Sound
1500 N. Alder St.
Tacoma, WA
jfuhrman@ups.edu

ABSTRACT

Keywords

IDS: Intrusion Detection System
IPS: Intrusion Prevention System

1. INTRODUCTION

1.1 Host-Based Audit Systems

Host based audit systems are audit systems that rest on the host that they monitor, and thus analyze the activity on only one computer. They are primarily used due to the extremely high granularity of analysis they provide, as they can observe and monitor every aspect of a running system, from running processes and services, to who launched them and when. In the case of many attacks on an individual system, this finely detailed analysis is essential, as it allows host-based systems to detect attacks that cannot be observed from anywhere but the host itself (such as network traffic in a network-based system, which will be explained in the next section). Host-based audit systems are also compatible with systems that converse using encrypted traffic, if configured properly, as the traffic needs to be decrypted at some point before reaching the user, at which point the host-based system can intercept it. This way the traffic can remain secure within a layer of encryption, and the host can remain secure and analyzable by the audit system, creating a solid series of defense mechanisms that do not conflict with one another. Similarly, host-based audit systems can operate without handicaps of any kind in switched networks, as the physical layout of the network does not affect the host system, a point that will also be made more relevant once network-based audit systems are explained.

However, host-based audit systems do lend themselves to several key flaws. The first flaw, and arguably the most regrettable considering the impressive list of strengths listed above, is the fact that host-based systems are vulnerable to attack. Simply, the host-based system resides on the system it monitors, and thus a clever attacker, if they can locate where the software sits on the system, can disable or perhaps even destroy a host-based audit system if they gain access to the computer it rests on. The second flaw is that host-based systems, by design, have only the resources of the host system they reside on and monitor available to perform their analysis with, and cannot be supplemented in this task. Thus in the perhaps rare scenario in which one possess an important system that needs to be protected at the host-level, but the system is composed of low-performance hardware, a host-based solution is simply not feasible. Moreover, on systems with reasonably powerful hardware, one could imagine the scenario in which the system, if it is acting as a webserver or providing services to a large number of clients, may experience a large enough request for said services that its resources could become tied up in managing server-client interactions to the extent that a host-based system is unable to perform its analysis. This, of course, is a critical flaw in the system's design, as the behavior of the increasingly prevalent Denial of Service attack exploits just this sort of resource-binding potential. Thus the efficacy of host-based systems is predicated by the amount of resources a system has to work with, making such systems incredibly vulnerable to Denial of Service attacks.

1.2 Network-Based Audit Systems

1.3 Application-Based Audit Systems

1.4 Signature Detection

1.5 Anomaly Detection

2. RELATED WORK

2.1 Probes

2.2 Privilege Escalation

Privilege Escalation attacks are described in two general categories in this paper: Remote to User Attacks and User to Root Attacks. In the broadest sense, Remote to User Attacks are when an attacker seeks to gain local user access to a machine that they have network access to. A User to Root Attack, as one may infer from its name, is when an attacker who already possesses local user access seeks to escalate their privileges to those of a root user, IE gain root user access. In the following sections, both types of attacks are explained in detail.

2.2.1 Remote to User

A Remote to User attack is when an attacker who has network access to a system but does not have an account on that machine exploits a vulnerability on the system to gain unauthorized local access as a user of the target system. These types of attacks come in many forms, and can be as simple as getting valid user authentication information through guessing a user's password with a dictionary attack. However, just as common are attacks that exploit a vulnerability in a common and innocuous system service, such as FTP to gain local user access. These exploits can change system settings to allow an attacker remote access, but they can also trigger buffer overflows, which in many circumstances allow an attacker to execute arbitrary code on the remote host (which is often used to gain root access, as we will discuss later).

2.2.2 User to Root

User to root attacks

2.3 Denial of Service

3. METHODS

4. EVALUATION

5. DISCUSSION

6. CONCLUSIONS

7. REFERENCES