Chapter 33

IDENTIFYING AND RESPONDING TO SECURITY VIOLATIONS

INTRODUCTION

It is imperative for Internet and security administrators to know exactly what is going on in their network. With a complete, real-time picture of the network, administrators can proactively protect their resources and quickly resolve any security incidents to strengthen their network security posture. Without proper visibility, administrators can be blindsided by attacks that they didn't even know they were vulnerable to and waste valuable resources researching, containing and responding to successful exploits [1].

Just obtaining a complete, on-demand picture of what is on the network, however, represents a significant challenge for most organizations:

- How does an administrator learn what servers, applications and devices have been added to the network?
- How do they find out about someone from finance suddenly accessing the R&D servers?
- How do they know when an employee downloads a new application from the Internet?
- How do they keep track of which software versions are loaded on each system?
- The answer to most of these questions is they often don't, until it is too late [1].

Generally this is because the person responsible for security may not be the same person who is responsible for the network, which may be separate from the IT administrator. Without tight integration and rigorous checks, it is highly probable that a new user, application, server or protocol will be introduced to the network without the security administrator knowing. Anything on the network that a security administrator doesn't know about represents a vulnerability [1].

Anything on the network, particularly changes to resources or activity, needs to be considered in the context of what it does to the organizations' overall Internet security posture. For example, someone connecting to a server that they have never connected to before may indicate a policy violation; a new application, such as P2P file sharing or Instant

Messaging, may open up holes that an attacker can use to get into the network; and desktops may be a risk until they receive the latest patch for a software version they are running. The security administrator needs to keep track of everything that is actively participating in or being used on the network to identify potential violations of the organization's policies or compromises in the organization's overall security stance [1].

To get this information, a security administrator has traditionally had to correlate disparate data derived from multiple sources and solutions. This often includes the manual aggregation and analysis of information from routers, firewalls, IDSes, IPSes and vulnerability scanners, which is a daunting, time consuming exercise that is virtually impossible to keep current. As a result, Internet security administrators regularly operate in a mode of catch up or spend their time researching and trying to resolve the most pressing Internet security incidents [1].

To give administrators the insight they need to understand what is going on in their network, they need an Internet security tool that passively monitors network activity and stores the data in a network profile. This profile can be used to provide administrators a comprehensive, on-demand view of network activity, for example what hosts, servers, applications and operating systems are currently on the network. This chapter very briefly describes this Internet security tool technology (as part of Internet security management solutions and future directions); and demonstrates how it can help administrators identify potential problems and make well-informed security decisions that strengthen the Internet's security posture [1].

THE PROFILER

An Internet security tool that passively monitors network activity and stores the data in a network profile should be designed to provide administrators the tools they need to identify changes to the network to ensure appropriate security policies are in place to enable the swift resolution of anomalies and exploits. This Internet security tool (IST) should also be an on-demand, searchable database that an administrator can use to quickly see the level of detail they need to understand what is going on in the network [1].

The database should also be integrated right into the log viewer to help administrators investigate and resolve security incidents. The database should also be available through the "profiler view," which an administrator can use to explore their network to help them predict where problems may arise, so they can make proactive security decisions [1].

There should also be at least three different views in the profiler to help administrators zero in on the information they need; as well as, a security violation view for pseudo firewall policies that help pinpoint what an administrator may not know about the network [1]. The IST should also passively monitor network activity and store the data in a network profile. Knowing where to look for important, relevant data that make up an interaction, IST should be provided with a record of all key network activity. The IST then stores this information, which includes any unique attempts, probes and successful connections, including the start, relevant service field information and end of the connection, in its searchable database. An