



Absolute Security Assurance: A white Paper

Teknotrends software Pvt Ltd
info@teknotrends.com

Vulnerability Assesment:

Vulnerability assessment (VA) is the process of detecting security holes/gaps in your system. There are two kinds of ways of doing VA - host-based and network-based. A host-based VA tool sits on the host (or target) whose holes need to be detected, while a network-based VA tool remotely detects the holes in your system. Obviously, a host-based VA tool can detect holes in services/executables, which are not network-bound while the network-based VA tool can only detect holes in services that are network-bound. Alternatively, a network-based VA tool can be considered to be more relevant at one level, since it mimics a hacker sitting at a remote location and trying to hack into the system. Vulnerability assessment tools basically embody the philosophy that it is better for one to detect security holes in one's system before the hackers do. VA is a growing market today estimated to reach around \$1 billion by 2006.

Shortcomings of Current VA solutions:

There are several shortcomings of network-based vulnerability assessment the way it is done currently.

1. Because of the way VA tools are designed, to run in a batch mode, the system check has to be done again and again. Thus, companies have to do initiate the VA tool once a day or a week or some such time period according to company policy. Since VA tools will detect the vulnerabilities in a network system at the time they are run, vulnerabilities that are manifested during other times --- that is when the VA tools are not on --- can go undetected.
2. The way VA tools are designed, it has generally to be an "all" or "no" run for a VA tool. This can take a substantial amount of time to complete its run. For instance, a full run of Nessus --- a popular open source VA scanner --- on a single system takes about 15 to 30 minutes to run, and requires to transfer 1 to 2 MB of data each way. Suppose you have 100 systems, the time as well as the bandwidth required will add up to significant systems constraints. Add to it the fact that suppose you do VA on all your machines every day, the time and the bandwidth required are enormous. Your network could be potentially clogged for a substantial amount of time. Even when the VA tool may have the facility not to run in an all or no mode but (running only specific tests), there is no easy way to determine what would be a sufficient enough test suite to be run to detect all your vulnerabilities.
3. You may have other security devices in your infrastructure. These could be firewalls, intrusion detection systems, and others. A network-based VA tool does a port scan first to find out which are the open ports on your target machine. This, plus the inordinate amount of traffic on your system due to the VA tool can trigger alerts on your security

devices to the point that the VA traffic can be blocked. Thus, to run an effective network based assessment, you will have to coordinate with your other security personnel (firewall, intrusion detection system maintenance) and ensure that they know that the VA tool is being run. They also need to ensure that devices such as firewalls and intrusion detection systems are disabled or are appropriately configured to allow for VA related traffic to take place. This is a cumbersome process not to mention a big drain on time and other resources of your personnel. Having to do this time and again only adds up to significant resource constraints.

4. Current VA tools require that IP addresses of the target systems for the assessment tool be given a priori. This limits their usefulness severely. For instance, if you plug in a laptop and connect to your ISP through a dial-up or through a wireless interface which gives you a dynamic IP, there is no easy way that interface can be checked for assessment. It is quite possible that some spyware appears on that particular interface and not on your other interfaces, and there is a need to run an assessment on that interface as well.

5. Finally, VA tools have to be explicitly scheduled to run. This involves a resource overhead not to mention that there are no thumb-rules or ways to determine when or how often these tools ought to be run.

Teknotrends Software solves all of the above problems and more through its patent pending technology and gives you the best returns on your VA investment.

For more details on Teknotrends Software's solution for vulnerability management, please fill the form at http://teknotrends.com/contact_us.htm