
Network and Host-based Vulnerability Assessment

A guide for information systems and network security professionals



**6600 Peachtree-Dunwoody Road
300 Embassy Row
Atlanta, GA 30348
Tel: 678.443.6000
Toll-free: 800.776.2362
Fax: 678.443.6477
E-mail: sales@iss.net**

Introduction:

With the advent of open systems, intranets, and the Internet, information systems and network security professionals are becoming increasingly aware of the need to assess and manage potential security risks on their networks and systems. Vulnerability assessment is the process of measuring and prioritizing these risks associated with network- and host-based systems and devices to allow rational planning of technologies and activities that manage business risk. These tools allow customization of security policy, automated analysis of vulnerabilities, and creation of reports that effectively communicate security vulnerability discoveries and detailed corrective actions to all levels of an organization.

Implementing network- and host-based scanning products together offers powerful security protection against the three types of risks: vendor, administrative, and user introduced. This paper examines the appropriate uses of network- and host-based vulnerability assessment tools, unique strengths of each type of solution, and how they complement each other to provide a comprehensive security assessment and correction solution.

What types of security vulnerabilities do I need to be aware of?

A security risk analysis of corporate computing devices allows quantification of the risks associated with open computing. Risks fall into three main categories:

Risks associated with vendor-supplied software – includes bugs, missing operating system patches, vulnerable services, and insecure choices for default configurations

Risks associated with administration – includes options available but not used correctly, insecure requirements for minimum password length or unauthorized changes to the system configuration

Risks associated with user activity – includes risky “shortcuts,” such as sharing directories to unauthorized parties, policy avoidance such as failure to run virus scanning software or using modems to dial in past the corporate firewall, and other, more malicious, activities

These types of risks can be present in and apply to network services, architecture, operating systems, and applications.

Network Scanning Strengths

A network scanner should be the first tool used in the vulnerability assessment process. It provides a quick snapshot of the highest risk vulnerabilities that require immediate attention. A network-based scanning assessment might detect extremely critical vulnerabilities such as misconfigured firewalls or a vulnerable web servers in a DMZ that could provide a stepping stone to an intruder and allow them to quickly compromise an organization's security. Network-based scanning performs quick, detailed analyses of an enterprise's critical network and system infrastructure from the perspective of an external or internal intruder trying to use the network to break into systems.

Network-based scanner strengths fall into two main categories:

1) **Centralized access to enterprise security information**

- Network-based scanners analyze network based devices on an organizations network, quickly providing detailed repair reports to allow quick corrective action. The resulting data and reports allow prompt attention for vulnerable systems, accelerating the process of reducing security risk.
- Network-based scanners discover unknown or unauthorized devices and systems on a network, helping determine if there are unknown perimeter points on your network, such as unauthorized remote access servers or connections to insecure networks of business partners. Has a department set up an insecure Linux-based web server on their own? Are there curious, unknown systems on the network that warrant further investigation?
- Network scanners provide a comprehensive view of all operating systems and services running and available on your network, as well as detailed listings of all system user accounts that can be discovered from standard network resources. This data and corresponding reports give administrators a clear picture of what types of services are actually being used on their network. In addition, this information can be used by a network scanner for further vulnerability evaluation, such as using user accounts to test for password strength, or services detected to check for vulnerable services.
- Because they require no host software to be installed on the systems being scanned, network-based scanners can be set up and used quickly, without requiring the deployment, planning and installation of traditional host software. In other words, network-based scanners are organizationally non-intrusive to individual systems and their systems administrators, and provide a rapid return on an organization's security investment. By means of comparison, a host-based scanning product can only scan the systems on which it is supported and installed.

2) Unique “Network-centric” view of an organization’s security risks

- Network-based scanners assess network-based vulnerabilities by replicating techniques that intruders use to exploit remote systems over the network. The first detailed vulnerability assessment report from a scanner often provides an eye-opening experience to an information systems staff when they realize their true, documented security posture.
- Many network-based vulnerabilities are more efficiently investigated over the network. These include vulnerable operating system services and daemons, DNS servers, “denial of service” exploits (i.e., “teardrop” and “land”), and low-level protocol weaknesses. Advanced network-based attacks such as protocol spoofing can only be tested thoroughly from the network.
- Network-based scanners test vulnerabilities of critical network devices that don’t support host-scanning software, including routers, switches, printers, remote access servers and firewalls. Network scanners can include advanced features such as stealth scanning for firewalls, specific router vulnerability checks and “brute force” checks to test default user ID and password back doors built in by network device manufacturers.
- Network-based scanners provide “real-world” testing of systems that have already been locked down with host-based assessment tools, such as critical file, database, web and application servers, and firewalls. In addition to testing standard security features, it may also detect critical configuration errors that have left these devices open to intruders.

If we look back to our original description of the three types of security risks, you’ll notice from the examples above that *network-based scanners are excellent tools for evaluating security risks associated with two types: risks associated with vendor-supplied software, and risks associated with network and systems administration.*

Host Scanning Strengths

Host-based scanning's strengths lie in direct access to low-level details of a host's operating system, specific services, and configuration details. While a network-based scanner emulates the perspective that a network-based intruder would have, a host-based scanner can view a system from the security perspective of a user who has a local account on the system. *This is a critical difference, since a network-based scanner can not, by definition, provide sufficient insight into potential user activity risks.*

Accessing these user-driven security risks is critical not only to the specific host affected, but to the security of the entire network. Once a user has access to local account (even just a "Guest" account) it opens up a whole range of possibilities for exploiting and taking control of the local system. An intruder who has accessed a specific host might be a legitimate user misusing an account, or it could be an account taken over by an intruder who guessed or cracked a password. For both situations, a host-based scanner helps ensure that a given system is properly configured and that vulnerabilities are patched so that a local user doesn't gain access to administrator or root privileges.

Host-based Scanner strengths fall into three main categories:

1) Identifies Risky User Activities:

- Risky user activities range from user ignorance to behavior that intentionally violates an organization's security policy for the convenience of the individual user. All types of risky user behavior within this spectrum can potentially compromise the security of all systems in the organization.
- Users selecting easily guessed passwords or using no passwords at all are a classic example of risky user activities. Another significant network security exposure is the sharing of entire hard drive over the network, either because it is easier than learning the secure method of sharing information, or accidentally, through a default setting for a Windows 95/98 or Windows NT system.
- Host-based scanners detect installed devices such as modems and determine if that modem is connected to an active phone line. This type of hardware setup could indicate an unauthorized remote access server that circumvents the organization's firewall and secure dial-in procedures.
- Host-based scanners detect the presence of a "remote control" applications such as Carbon Copy or pcANYWHERE that may be used by employees calling in from home to access resources after hours or through an unknown network perimeter point, such as an unauthorized remote access server.

2) Hacker identification and intrusion recovery (internal or external intruders):

- Host-based scanners detect signs that an intruder has already infiltrated a system. These hacker traces include suspicious file names, unexpected new files, device files found in unexpected places and unexpected SUID/SGID privileged programs that have potentially gained “root” privilege.
- Host-based scanners can create cryptographically secure MD5 baselines of critical files, allowing administrators to compare the current files on a system to a previously known secure state. This process allows detection of any unauthorized changes in these critical system files, such as a “login” program that may have been replaced by a “Trojan horse” back-door. In addition, host-based scanners on Windows NT systems can use baselining to notify administrators of unauthorized changes to Registry entries, which contain critical security settings.
- Host-based scanners detect signs that an intruder is still currently active on a system, including locating “sniffer” programs actively looking for passwords and other critical information, or unauthorized services popular with hackers currently running on the system, such as IRC chat and FSP file transfer servers.
- Host-based scanners detect well-known hacker back-door programs such as “Back Orifice” from the Cult of the Dead Cow. They also detect local host services vulnerable to “local buffer overflow” exploits from hacker web sites. Without a host-based scanning regimen, these exploits can be easily downloaded from popular hacker web sites like www.rootshell.com, compiled, then run by a low-level user to gain immediate access to full “root” level privileges.

3) Security checks that are impossible or difficult for a network scanner perform, or are extremely time consuming over a network:

- Examples of security checks that can be performed significantly faster or more reliably using host-based scanning include password guessing and policy checks, searches for Windows 95/98 password hash files (.PWL), and active file share detection.
- Host-based scanners are ideal for performing resource-intensive baseline and file system checks, which are impractical with network-based scanners and would require that entire contents of hard drives be transferred over the network to the scanning system.
- Host-based scanners can check network services to ensure they been correctly configured and implemented, including NFS, HTTPD, and FTP. For example, an incorrectly configured trust relationship under NFS could allow an intruder that has broken into one system to have an open door to all other NFS systems on the entire network.

- Host-based scanners frequently provide more detailed security information from Windows 95/98 hosts than can be detected over a network. These investigations are important due to the large number of “back door” and “sniffer” programs available for these operating systems.

If we look back to our original description of the three types of security risks, you’ll notice from the examples above that *host-based scanners are excellent tools for evaluating security risks associated with all types of user risks. These include risks caused by ignorant users, malicious users, and all users in between. They also provide additional coverage for a variety of risks associated both with vendors and administrators.*

Host based scanners are also great tools for helping to “lock down” a critical system such as file, database, web and application servers, and firewalls. In addition to testing standard security features, they may also detect configuration errors that have left these devices open to intrusion.

What systems should I scan with network- and host-based scanning products?

A network-based scanner can discover unknown or unauthorized devices and systems on a network, as well as help point out unknown perimeter points on your network, such as unauthorized remote access servers. Network-based scanning identifies devices on your network, and evaluates the configurations and strengths of systems such as firewalls, routers, and corporate web servers living outside the firewall. Because of these capabilities, it is recommended that a network-based scanning product should be used to scan an entire network. An intruder will take advantage of any access point he or she can. An unprotected Windows 95/98 or NT desktop or departmental server could provide the needed stepping stone to gain control of the entire domain.

Host-based scanning products are a clear choice for securing servers that run critical file, email, web, directory, remote access, database, and other application services. These systems often contain critical business data, and host-based scanning can find high-risk vulnerabilities and provide fix information to make sure that local users don't have inappropriate access to these services and resources. Host-based scanning should also be a priority for securing firewall products, which usually run on standard Unix and NT operating systems and frequently contain well-known vulnerabilities and default configurations as they ship from the vendor. A properly configured firewall does not provide a secure perimeter defense if administrator or root privileges on the firewall itself can be compromised by any uncorrected exposure.

Keep in mind that the term "Host" doesn't just apply to servers, but to any network-based computer in an organization. Critical strategic business information resides on the desktops of every organization's key knowledge workers. Each of these systems may introduce as much business risk from one of those desktop systems being compromised as from a hacked server. This information is stored, transferred and communicated every day via email, spreadsheets, presentations, and documents between senior management, Finance, business partnerships, Engineering, Marketing and Sales. Organization face serious business risks if a competitor could gain access to these critical plans, strategies, and corporate assets.

It is worth considering network- and host-based scanning for desktop systems as well as servers for the following reasons:

- Desktop users are not typically security aware, and often act in ways that can compromise an organization's security. Examples of this sharing an entire hard drive, using easily guessed passwords, and running insecure personal web servers on the desktop.
- Desktop users can compromise security of the entire network by setting up unprotected and unauthorized remote access connections for personal convenience using a modem. Without realizing it, these users have created a new network access point not protected by a firewall. It is crucial to know if a desktop system on your

network is connected to a live phone line or running a remote control application. Host-based scanning products provide this information.

- On a Windows based network, the security of a Windows NT domain is only as strong as its weakest link. A compromised desktop can quickly lead to more severe intrusions. An attacker typically finds a weak machine, gains local administrator privilege, leverages this toehold to gain domain credentials, then uses that base to jump to new NT systems. NT Servers are usually set up with greater attention to security, so initial attacks are frequently launched against desktop machines.

Which products best cover the 3 categories of security vulnerabilities?

From the analysis and examples discussed previously, we come to the following conclusions:

Risks associated with vendor-supplied software, including missing operating system patches, vulnerable services, bad choices for default settings and services, or issues such as an outdated Java Security Manager in a web browser, **are best addressed by both network- and host-based scanning products.**

Risks associated with administration, including insecure values for Registry Keys, insecure requirements for minimum password length or unauthorized changes to the system configuration, **are easier to identify with a network-based scanning product, and most thoroughly analyzed by both host and network-based scanning applications.**

Risks associated with user activity, including sharing directories with unauthorized parties, failure to run virus scanning software, and using modems to circumvent the corporate firewall, **are best detected by a host-based scanning product.**

Conclusions: While both network- and host-based scanning technologies have their unique strengths, using both tools in a coordinated fashion provides the best vulnerability assessment for measuring an organization's security risks. Network-based scanners allow information security professionals to assess and correct network-based vulnerabilities, secure network perimeter points on an ongoing basis and strengthen initial lines of defense against intrusion. Host-based scanners provide an additional level of security by locking down individual hosts to prevent critical resources from being accessed by internal misuse or external intruders using compromised accounts.