

Network Security



Assessment and Review of Enterprise Systems

How secure is your company's information? In this age of distributed computing and of client-server and Internet-enabled information access, computer security consistently raises to the top of most "important issues" lists. To answer this question with certainty is difficult. There are no absolutes with security. An important first step for most corporations is a security policy that establishes acceptable behavior. The next, and more critical step, is to enforce that security policy and measure its effectiveness.

Vision Technologies will assess your Network from multiple viewpoints for the best over all picture. These perspectives range from the physical security of the machines to the configuration of the firewalls to the trustworthiness of workers. The history of industrial espionage has been in the physical world and thus numerous practices have been developed to handle this portion of security assessment. The age of network based industrial espionage has a brief history and thus less developed security assessment practices.



Vision Technologies believes the security profile of a network of machines can be assessed from three principle vantage points.

- From the outside of the Enterprise - the view of the computer infrastructure through the firewall
- From the inside of the Enterprise - the view of computers from behind the firewall
- From the computer keyboard - the view from the actual operating system of the individual machine itself.

Each of these perspectives will reveal unique security vulnerabilities. Removing the vulnerabilities as seen from outside the enterprise is the first step to halt the efforts of the casual hacker and industrial espionage age. Removing the vulnerabilities as they appear from behind the firewall accomplishes two goals. It creates a second line of defense should the firewall become compromised. It also creates a defense for the attacks around the firewall through a modem or other non-protected entryway.

Finally evaluating security from the machines themselves will close vulnerabilities that could be exploited through a firewall or from other machines on the network. It also hardens the security of the machines, restricting the avenues of attack for the disgruntled worker or the co-opted contractor.

Vision Technologies will employ several lines of defense for the Corporate Information System.

Vision Technologies realizes that a successful security audit must be thorough; it can not leave out possible vulnerabilities. It must also be repeatable to provide a consistent perspective on the firm's security practice. By its very nature a security assessment will initially increase the workload for an MIS department. These seemingly conflicting goals can be met through the use of a security audit tools that can be provided by Vision Technologies thorough and repeatable process with an effective means of implementing corrective actions.

- *Firewalls*
- *Internal Defenses*
- *Denial of Service*
- *Source Porting*
- *Source Routing*
- *Stealth Scanning*
- *SOCKS*
- *Direct RPC Scan*
- *TCP Sequence Prediction*
- *Brute Force Attacks*
- *Anonymous FTP*

Vision Technologies, Inc.
530 J McCormick Drive
Glen Burnie, MD 21061
www.viontech.biz
(410) 424-2183
(410) 424-2208 fax



A SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS

Network Security



Assessment and Review of Enterprise Systems

Firewalls

Many enterprises erect a firewall as the first and often only line of defense for their information systems. A firewall is a device that controls the flow of communication between internal networks and external networks, such as the Internet. Many corporations assume that, once they have installed a firewall, they have reduced all their network security risks.

Internal Defenses

Even when properly configured, the firewall can only repel connection attempts that come through the firewall itself. An information attack can be mounted via modem on the internal network. If all of the enterprise's defenses are focused on the firewall then an attack that circumvents firewall through a modem or an internally based attack will have free reign over the information systems. Thus the security features of the internal computers must also be employed. The important balance between convenience for the users and security concerns must be considered. That is the computer systems must be allowed to be collaborative in nature with appropriate access to information and functions across systems. At the same time this access provides a wide open avenue for the industrial espionage attack. Often the elements of the enterprise's computer system must be updated to eliminate security risks introduced by bugs in operating systems and network service programs. If a bug creates a performance related problem then it is a "squeaky wheel" that will drive the upgrade. A functioning version of a program or service with the security bugs can be easily overlooked as an important item for upgrades. By the time a security related bug becomes the proverbial "squeaky wheel" - it's too late.

Source Porting:

Filter rules typically are based on source and destination port addresses. A TCP/IP-enabled machine has 65,535 possible virtual ports; some of them are defined for certain services; for example, e-mail is port 25. When one machine FTPs to another and wants to transfer a file back from the FTP server, typically the server opens source port 20 to connect to the FTP client and transfer data. Therefore, many firewalls allow source port 20 into a network. An intruder can modify telnet to make the connections come from source port 20, thereby penetrating the firewall. Firewall Scanner checks to see if source port 20 is allowed to connect to the network.

Source Routing:

Source routing is an IP protocol option that allows you to define how packets are routed. When source routing is on, many firewall filter rules are often bypassed. Many router-based firewalls allow source-routed packets to pass. Many hosts have source routing built into the kernel and do not allow it to be turned off. Firewall Scanner assesses susceptibility to source-routed packets.

SOCKS:

SOCKS is a library of proxy-application firewalls designed to allow certain services through and keep intruders out. The fundamental problem with SOCKS is the same as with many security tools: SOCKS is often miss-configured. Often the administrator establishes rules to allow certain services through the firewall, but the rules necessary for denying access to intruders are never implemented. Consequently, services seemingly work fine with the firewall, but the firewall's inability to keep intruders out is not recognized until an intruder breaks through. Even then, the cause of the problem may never be recognized. Firewall Scanner attempts to connect to important services through the SOCKS port, to see whether filter rules have been configured properly.

TCP Sequence Prediction:

TCP sequence prediction or IP spoofing - the technique that Kevin Mitnick used to break into many networks across the Internet - tries to trick a host that trusts another host. For example, if host A and host B are in a corporate network and host A is trusted by host B, then host A is allowed to log into host B based on this trust, without a password. An intruder who can make his host C look like host A will also be able to log into host B. Firewall Scanner determines a firewall's vulnerability to IP spoofing.



A SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS

Vision Technologies, Inc.
530 J McCormick Drive
Glen Burnie, MD 21061
www.visiontech.biz
(410) 424-2183
(410) 424-2208 fax

Network Security



Assessment and Review of Enterprise Systems

Direct RPC Scan:

The portmapper is a service, such as NIS, that allows you to identify the ports on which the RPC (Remote Procedure Commands) reside. Many filter-based firewalls may block the portmapper on port 111. The RPC commands themselves remain in place on various machine ports. It usually is hard to determine where the services are if the portmapper is blocked. However, if an intruder scans directly for the RPC services, the intruder could bypass this type of security. Firewall Scanner scans directly for the RPC services to determine whether they are exploitable.



Stealth Scanning:

In stealth scanning, an intruder does not attempt to establish a connection, but rather uses packets at a low level with the interface. These low level packets elicit different responses depending on whether or not a port is active. This technique allows TCP port scanning many times faster than a regular connect routine on UNIX and does not trigger alarms built into many SATAN detectors and tcp wrappers. While many firewalls block particular packets that would establish a connection, Firewall Scanner's stealth scanning packets do not attempt to establish a connection; therefore, they can bypass firewall security and identify services running on an internal network.

Denial Of Service:

A denial of service attempts to force the firewall into a failure condition, typically forcing a reboot of the machine. As an example, flooding a machine with sync packets or connections attempts can cause an overflow condition in buffers and log files. At this point the firewall can cease operation and close all connections; it can continue operations while stopping the logging operations or it can continue operations in a more open environment. Firewall Scanner has a battery of denial of service attacks to assess a firewall's durability.

Intranet

Vision Technologies will assess the Intranet security from the TCP/IP services perspective. Network devices might include a UNIX host, a Microsoft NT/Windows 95 system, a router, a web server, and even an X terminal. Network security is only as strong as the weakest link. Administrators may try to protect only machines that hold sensitive information. Intruders know this and look for machines that might not be protected, such as infrequently used print or fax servers. Then, once in the network, an intruder can set up sniffers to capture sensitive data, such as passwords, going over the internal network. If the intruder is using a machine that is already part of the internal network, sniffing and trust relationships usually allow spring boarding into access to sensitive machines. An administrator does not have time to identify the devices on the network that actually could be used as springboards. Our Security engineers can quickly find these weak links and identify the vulnerable services.

Brute force Attacks

Many networked machines are shipped with default accounts that allow an administrator to gain immediate access to a machine and to configure it. If the administrator doesn't change the defaults, an intruder can use them to gain access to the network. When the administrator adds accounts to a machine, those accounts may get installed with an easy password. A brute force attack against a machine looks for common defaults and known accounts that might be vulnerable. If a default or login account becomes compromised, the services telnetd, ftpd, rsh, and rexec allow access to a machine. Intranet Scanner performs, through these services, brute force tests for default and vulnerable accounts.



A SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS

Vision Technologies, Inc.
530 J McCormick Drive
Glen Burnie, MD 21061
www.visiontech.biz
(410) 424-2183

Network Security



Assessment and Review of Enterprise Systems

Anonymous FTP

Anonymous FTP is a service that allows the easy transferring of files. The FTP server has many configuration issues. An improper configuration could allow unauthorized access to the rest of the machine. Intranet Scanner checks for these configuration flaws and determine whether the FTP site is vulnerable.

Networked File Systems

NFS allows many machines to have a virtual hard drive that operates over the network. If improperly configured, NFS may allow anyone to access this virtual hard drive. An intruder could then copy, modify, and possibly delete critical data from the NFS, and even gain full access to the machine. Intranet Scanner finds miss-configured NFS servers.

File Sharing

Windows NT and Windows 95 use a service called file sharing that allows for sharing files between networked computers. Unfortunately, many people do not realize that this may also allow access to their computers by anyone on the Internet. Intranet Scanner finds miss-configured file-shared machines and allow the administrator to take corrective action.

Rexd

Rexd, an old service from when UNIX was first being networked, was not developed with security in mind. It has little or no authentication to stop intruders from gaining access to a network. Intranet Scanner discovers this service. The administrator can then remove it from the machines on the network.

RSH and Rlogin

Both Rlogin and RSH vulnerabilities give an intruder instant access to the machine. The Rlogin vulnerability affects AIX and Linux machines. It allows anyone to rlogin as root without a password. An intruder issuing the command rlogin hostname.com -l -froot sees the login banner and a shell. Intranet Scanner locates these vulnerable services and enable the administrator to take corrective action.

X windows

Many users have xhost + in their configuration file. This permits access to the X Display by anyone, anywhere. An intruder who can access the X Display can obtain keystrokes and remotely execute commands as the user running the X Display. It is possible to configure the xhost to authorize only certain hosts, but even then any user from those remote hosts can use the X Display to compromise data. Intranet Scanner detects vulnerable X Displays.

File ownership and permission tests:

There are many potential vulnerability problems where the files are not owned by the proper accounts or the permission may not be set up correctly. There are two types of tests to check for:

Have a list of known permissions for certain files and directories, including home directories.

Build a baseline specific for the machine being tested and compare and contrast this library with future assessment tests of the machine.

Configuration and access file tests

Many system files can configure the machine insecurely and need to be checked. Users have certain files that allow access from certain services, these configurations should be checked against the security policy.

MD5 Signaturing

The best known method for checking if a file has the correct data content is through a md5 signature test. This digital signature is like a fingerprint. A database of fingerprints of good and bad programs can detect which files have been modified or which ones need to be upgraded to the latest version. There are three types of MD5 checksums tests to be considered:

- List of filenames with the good checksums and bad checksums to identify whether the machine is currently up to date.
- A list of only bad checksums and filenames that signify vulnerable versions of binary programs. This is for programs that do not have a specific location, such as a web browser.
- A baseline of md5 checksums for the machine currently being tested so that future scans can contrast the checksums to look for modifications to the machine's important files.

Hacker specific testing:

There are certain things that a hacker may do that can be detected. Checking if the machine is in promiscuous mode can detect whether a hacker is sniffing from that machine and catching passwords going across the network. There are also certain directories that hackers place files in that should be checked for odd files.



Vision Technologies, Inc.
530 J McCormick Drive
Glen Burnie, MD 21061
www.visiontech.biz
(410) 424-2183
(410) 424-2208 fax



A SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS