Global Information Assurance Certification Paper

TCP Wrapper; A Tool to Help Protect Your Data

Dan Gates

December 26, 2000

Introduction

In today's world of highly connected Information Systems, maintaining the confidentiality, integrity, and availability of data is a difficult job. Entrance into this connected world provides an organization with many benefits; unfortunately, increased data vulnerability is a very real side effect. This paper describes TCP Wrapper, a software tool which can be very effective in helping an organization to protect it's valuable Information System (IS) data by controlling network access.

What Is TCP Wrapper?

In the words of the developer, Wietse Venema, TCP Wrapper is a simple tool to monitor and control incoming network traffic. Dr. Venema developed the original version of TCP Wrapper in 1991, while at the Eindhoven University of Technology The Netherlands. The impetus for Dr Venema's effort was a Dutch computer cracker who repeatedly gained root access on the University's computers and destroyed data. A paper written by Dr Venema describing the development of the TCP Wrapper tool is located on his home page at http://www.porcupine.org/wietse/. You can also download the TCP Wrapper program, version 7.6 at the present time, from Dr Venema's home page. Other sources include ftp://ftp.porcupine.org/pub/security/ and http://ciac.llnl.gov/ciac/ToolsUnixNetSec.html#Tcpwrappers.

The Transmission Control Protocol/Internet Protocol (TCP/IP) is a series of protocols used to form the basis of Internet communications. The developers of TCP/IP were mainly concerned about enabling computers to communicate with each other, and although they aware of the problems, security was not a major concern. An excellent overview of TCP/IP Security can be found at http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html. The TCP Wrapper program provides a layer of security by intercepting calls to computer services (other programs) and determining whether or not the service will be allowed to run. The determinations made by the program are configurable by a system administrator. TCP Wrapper is analogous to a police officer directing traffic over an IS network, allowing some traffic into your

system, while blocking other traffic, all in accordance with your specifications. The program serves as an interface between TCP/IP and your computer services.

Features Of TCP Wrapper

- Monitors and filters incoming requests for network services such as: systat, finger, ftp, telnet, rlogin, rsh, exec, tftp, and talk.
- Provides extensive logging, as well as providing logging for services that are not normally logged.
- Passes control of a connection to the real associated network program, or to some other program of choice for further action.
- The installation does not modify existing software.
- There is no impact on system performance or authorized users.
- It comes with utilities that can examine it's configuration and that can predict how it would handle a specific request for service.
- It can optionally send a banner to a connecting client.

Limitations of TCP Wrapper

- It will not work on programs that are not using TCP/IP protocols.
- It will not work on programs that run all the time.
- It is not a panacea for security and is vulnerable to IP spoofing.

How Does TCP Wrapper Work?

Most UNIX versions have a program called inetd that is run at boot time as part of the start-up procedure. This program listens to the network ports and runs the appropriate server on demand when a connection is made. Basically, the TCP Wrapper program, tcpd, filters incoming requests for servers started by inetd and selectively allows or denies access to other programs through the use of two configuration files, /etc/hosts.allow and /etc/hosts.deny.

After installation of TCP Wrapper, the tcpd configuration files /etc/hosts.allow and /etc/host.deny are empty. Adding entries in these files is the method by which a system administrator defines access control over the host's servers. In other words, these entries are the rules that the aforementioned traffic cop uses when directing network traffic.

Dr Venema created a simple access control language based on client (host name/address, username), and server (process name, host name/address) patterns. This language, called hosts_options, is used when making entries in the /etc/hosts.allow and /etc/host.deny files. The hosts_options language allows for quite complex rule generation thus providing the system administrator considerable flexibility in configuring TCP Wrapper. Due to the possible complexity of rule definition, TCP Wrapper comes with a couple of utilities that can verify your rules. One utility, tcpdchk examines your TCP Wrapper configuration and reports all potential and real problems that it finds. The second utility, tcpdmatch, shows you what will happen when your rules are deployed, i.e., it predicts how the TCP Wrapper would handle a specific request for service.

When an incoming connection request is received, TCP Wrapper will first search the /etc/hosts.allow file to see if the host/protocol pair should be allowed. If no match is found, then the /etc/hosts.deny file is searched to see if the host/protocol pair should be denied. If a match is not found, then the connection is allowed.

This has been a rather simplistic description of how TCP Wrapper works, and there are many more features of the program. However, it should illustrate the power and flexibility provided by this software tool.

Conclusion

There are many advantages and benefits to be gained for an organization in being a part of the worldwide connectivity know as the Internet. There is also an inherent risk in being connected, in that your IS data becomes vulnerable to corruption and theft. Many organizations have discovered to their dismay that security should not be taken lightly.

Any system administrator charged with maintaining the security of a networked Information System should consider using TCP Wrapper. Good security is provided in layers, and TCP Wrapper can provide the user with a highly configurable security layer. This handy tool can provide firewall functionality by filtering and logging network service requests, thus providing another important layer to overall IS security.

Sources:

© SANS Institute 2000 - 2005 Author retains full rights.

Anonymous. (2000). Maximum linux security: A hacker's guide to protecting your linux server and workstation. Indianapolis: Sams.

Chamber, C., Dolske, J., & Iyer, J. "TCP/IP Security" URL: http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html (26 November 2000).

Garfinkel, S. & Spafford, G. (1996). Practical unix and internet security. Sebastopol, CA: O'Reilly & Associates, Inc.

McClure, S., Scambray, J., & Kurtz, G. (1999). Hacking exposed: Network security secrets and solutions. Berkley: Osborne/McGraw-Hill

Northcutt, S. (1999). Network intrusion detection: An analyst's handbook. Indianapolis: New Riders Publishing.

Server: ftp porcupine.org "Security" URL: ftp://ftp.porcupine.org/pub/security/ (4 December 2000).

Venema, W. Z. "Wietse's Home page" URL: http://www.porcupine.org/wietse/ (3 December 2000).

Zwicky, E., Cooper, S., & Chapman, D. (2000). Building internet firewalls. Sebastopol, CA: O'Reilly & Associates, Inc.

CIAC U.S. Department of Energy "Unix Network Security Tools" URL: http://ciac.llnl.gov/ciac/ToolsUnixNetSec.html#Tcpwrappers (5 December 2000)

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event