GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

An Explanation of "TCP Wrappers" for the Security Manager

Rick Branicki

November 21, 2000

Introduction:

Security Managers are often challenged with making decisions based upon presentations filled with technical terms and buzzwords. In today's small to large networked environments, it is common to have multiple platforms linked together within the organization. This has become a necessity as different business processes are automated outside of the organization, and these automated processes are only available on the platform of the vendor's choice. It is not always possible for any single Security Manager to have a working knowledge of the specific platform and its terminology. This paper attempts to assist the Security Manager in understanding the concept of TCP Wrappers, a tool often recommended for securing the Unix platform.

Simplification of terminology:

Anything that relates to a programmed set of instructions will be referred to as a *process.* Programs, scripts, and daemons are examples of processes. Anything that refers to a contained set of data or referenced information will be referred to as a *file.* The word *host* will be restricted to the single system that contains the business processes and related files that help comprise the value of your entity. The combination of these processes and files form your *system*, whether its purpose is billing, law enforcement records management, financial accounting and reporting, or product research and development.

A word on the importance of securing the host:

The field of Information Systems Security is often described in terms of military defense tactics. This helps in understanding how your network is secured. As an example, think of your network as the walled cities of earlier Mid-Eastern times. The walls were constructed around the perimeter of the city to keep the invaders out. Within these walls, dwellings were further fortified for individual protection. When the walls, or perimeter defenses, failed, families protected themselves by securing themselves inside their dwellings and fought off the invaders from their rooftops. This is a layered defense. Here, if constructed adequately, defenders could save the lives of their families. If your organization is protected from the Internet by perimeter devices such as routers and firewalls, you can think of your host as a dwelling inside the walled city. If your host is adequately configured for security, you could save the lives of your system family should your perimeter defense fail.

TCP Wrappers

TCP Wrappers is a process that was created by Wietse Venema in the early 1990's(1).

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Venema also co-authored the well-known SATAN vulnerability assessment process based upon a concept written in 1993(2). TCP Wrappers was created to help combat an intrusion by a destructive Dutch hacker at the university where Venema worked. They realized that someone from the outside was coming in, and their Unix systems did not have a way to record any information about who was coming in to their systems. TCP Wrappers was developed as an intermediate process to help record that information.

Access to Unix services from the Internet:

To understand how access to your Unix host from the Internet is accomplished, consider the example of a corporate receptionist. The receptionist's job is to answer the phones, find out what service the caller is requesting, and forward the call to the appropriate servicing department. When an Internet customer wants access to your Unix host, there is a receptionist process waiting, or listening, for the call, or request, for Unix services. The receptionist's Unix name is *inetd.* The inetd process manages the Internet requests on your Unix host, and is referred to as the Internet Super Server (3). The inetd process listens for a Unix service request and forwards it the requested Unix service. Note that in our description of the receptionist's job, there is no mention of writing down or recording any information about the caller or service being requested. This is what Venema encountered when investigating the Dutch intruder. There was no information recorded about the requestor or services requested.

What TCP Wrappers does:

It was mentioned that TCP Wrappers is an intermediate process. Using our receptionist example, consider that we hire a second receptionist that the first receptionist forwards the calls to. This second receptionist, or intermediate receptionist, writes down who the caller is and what servicing department the caller wants. The second receptionist then forwards the call to the requested servicing department. The second receptionist can also be assigned the responsibility of looking up the caller to see if the caller is a legitimate customer of the requested servicing department, and even verify the caller is who she says she is by calling her back at her number. TCP Wrappers, with a Unix name of *tcpd*, performs these functions. The tcpd process is inserted between the inetd process and the requested Unix services. Here the tcpd process can record the remote host and Unix service requested. It can also be configured optionally to look up the remote host in "allow" or "deny" files and do a reverse lookup to verify the identity of the remote host(4). The information is then recorded in your Unix host logs.

How this helps you:

By being able to record information on who is using your Unix host, you have an audit trail to follow should there be a need to investigate a possible intrusion into your system. With the optional TCP Wrappers functions configured, you can verify that the party that wants to get in to your system from the Internet has legitimate access to your system. There is a slight cost in overhead in terms of transaction processing and disk space, as

© SANS Institute 2000 - 2005 Author retains full rights.

well as the cost of labor to configure and verify TCP Wrappers. If your Unix System Administrator or vendor is not reviewing and managing your system logs, this will be an additional cost as well.

A word of caution:

TCP Wrappers can be downloaded at no cost from the Internet. In January of 1999, an advisory was published that stated that someone had modified and inserted a Trojan Horse into copies of the TCP Wrappers code found in various sites on the Internet (5). If the only way for you to obtain TCP Wrappers is from the Internet, ensure that your administrator or vendor verifies the authenticity of the code. This can be accomplished with encrypted numerical "hashes" compiled on the code itself and with public key identifiers. A verifiable copy of TCP Wrappers can be obtained at ftp//ftp.porcupine.org/pub/security/.

The future of TCP Wrappers:

Wietse Venema stated in his paper that he did not have access to the inetd source code. This is why the intermediate TCP Wrappers process was necessitated. In June of 2000, a replacement process for inetd, *xinetd*, was made available(6). This has promise to incorporate the same functionality as TCP Wrappers (and more) in to the Unix Internet management process that inetd now performs. The xinetd process is new and currently is being tested for bugs and vulnerabilities.

Conclusion:

This paper has been written with the intention of giving the Security Manager an explanation of TCP Wrappers that the manager can understand. It is with hope that the paper has accomplished its purpose.

References:

(1)Venema, Wietse. "TCP Wrapper". 15 July 1992
URL:http://ltpwww.gsfc.nasa.gov/ltpcf/about/unix/Depotdoc/tcp_wrappers/index.html. (21 Nov. 2000).

(2)Kemer, Edwin. "What SATAN is". 24 April 1995.
URL:http//www.cs.ruu.nl/cert-uu/satan.html. (21 Nov. 2000).

(3)delorie software (based upon documentation by Lotter, Mark). "INETD". 5 July 2000.
URL:http//theoryx5.uwinnipeg.ca/gnu/inetutils/inetd.8.html (21 Nov. 2000).

(4)Quinn, Stephen. "Unix Host and Network Security Tools". 16 May 1996.
URL:http//cs-www.ncsl.nist.gov/tools/tools.htm#access (20 Nov. 2000).

(5)Carnegie Mellon University. "Cert® Advisory CA-99-01-Trojan-TCP-Wrappers". 22

© SANS Institute 2000 - 2005 Author retains full rights.

Jan. 1999. URL:http//www.cert.org/advisories/ca-1999-01.html (21 Nov. 2000)

(6)Braun, B. "xinetd". (undated). URL:http//www.synack.net/xinetd. (20 Nov. 2000).

© SANS Institute 2000 - 2005, Author retains full rights.

Last Updated: April 21st, 2018

Upcoming Training

SANS Seattle Spring 2018	Seattle, WA	Apr 23, 2018 - Apr 28, 2018	Live Event
Mentor Session - AW SEC401	Detroit, MI	May 01, 2018 - May 17, 2018	Mentor
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VA	May 20, 2018 - May 25, 2018	Live Event
SANS Atlanta 2018	Atlanta, GA	May 29, 2018 - Jun 03, 2018	Live Event
Community SANS Bethesda SEC401	Bethesda, MD	Jun 04, 2018 - Jun 09, 2018	Community SANS
Community SANS New York SEC401	New York, NY	Jun 04, 2018 - Jun 09, 2018	Community SANS
SANS London June 2018	London, United Kingdom	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, CO	Jun 04, 2018 - Jun 09, 2018	Live Event
Community SANS Madison SEC401	Madison, WI	Jun 18, 2018 - Jun 23, 2018	Community SANS
SANS Crystal City 2018	Arlington, VA	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, Japan	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Oslo June 2018	Oslo, Norway	Jun 18, 2018 - Jun 23, 2018	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 18, 2018 - Jun 23, 2018	Community SANS
Minneapolis 2018 - SEC401: Security Essentials Bootcamp Style	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	vLive
Community SANS Nashville SEC401	Nashville, TN	Jun 25, 2018 - Jun 30, 2018	Community SANS
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Cyber Defence Canberra 2018	Canberra, Australia	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Vancouver 2018	Vancouver, BC	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, Singapore	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NC	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, Malaysia	Jul 16, 2018 - Jul 21, 2018	Live Event
SANSFIRE 2018 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
Mentor Session - SEC401	Jacksonville, FL	Jul 17, 2018 - Aug 28, 2018	Mentor
Community SANS Bethesda SEC401	Bethesda, MD	Jul 23, 2018 - Jul 28, 2018	Community SANS
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event
San Antonio 2018 - SEC401: Security Essentials Bootcamp Style	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS August Sydney 2018	Sydney, Australia	Aug 06, 2018 - Aug 25, 2018	Live Event