

PORTUS™ SMTP Application Defenses

September 29th, 2004



Overview

The PORTUS Application Protection System functions as an in-line Network Intrusion Prevention System and firewall. PORTUS delivers in-depth protection against known and unknown forms of attack. Protocol Anomaly Detection (PAD) detects and blocks previously unknown forms of attack without the need for signatures. PAD provides Zero-Hour™ protection, which means new forms of attack are blocked the instant they reach the PORTUS gateway. One does not have to wait days for the latest attack signature to be identified and downloaded for use. Even unknown viruses and worms are stopped.

Detect, Report and Repel attacks via e-mail: smwrap is designed to detect and report suspicious and malicious activity using SMTP. With the wrapper in place an attacker cannot use your mail server to access or modify data on your protected hosts. Smwrap prevents attackers from obtaining information required to attack a private network, including host names, user IDs etc. Attempts to use SMTP sub-commands for this purpose are logged. The wrapper also detects and reports spoofed host names and addresses and prohibits communications with such systems. The system administrator is alerted whenever mail is received that is directed to a file instead of a user or when parameters are being passed to sendmail.

PORTUS provides comprehensive defenses for hundreds of applications. This paper is meant to specifically discuss the PORTUS SMTP defenses.

Smwrap provides

Protocol Anomaly Detection to provide Zero-Hour defenses against SMTP attacks that violate SMTP protocols.

Real time identification and blocking of executable file attachments provides Zero-Hour defenses against viruses and worms without waiting for the downloading of new virus signatures.

SPAM Blocking using a series of defenses including: Extensible Mail filter that uses heuristic and statistical analysis to identify SPAM; DNS Black Listing; Configurable SPAM thresholds; Deny by e-mail address of domain; Client DNS lookups; Deny of executable file attachments; Use of real-time collaborative spam-tracking data bases to block SPAM identified by others.

Blocking of mail that contains specific keywords or phrases. Reduces the amount of offensive mail. Reduces risk of transmitting e-mail containing sensitive information.

Blocks offensive pictures contained in SPAM sent from porn sites.

Works with multiple virus scanners to identify and block known viruses and worms.

smwrap

The smwrap program is a small secure application designed to receive mail from protected and unprotected hosts. Smwrap's primary purpose is to defend against all form of e-mail attack. However in order to reliably perform this task it must be capable of defending itself from direct attack. Other products designed to protect e-mail, including leading virus scanners, have fallen subject to direct attacks which have disabled their defenses. Smwrap runs on a hardened OS, in a non-privileged state in a chrooted directory. This architecture prevents an attacker from exploiting any coding errors that might exist to circumvent the security and integrity of the system itself. The architecture of PORTUS including smwrap has successfully defended itself from all forms of attack for more than 10 years, a remarkable and unequaled record.

Smwrap prevents direct IP connectivity between external and protected systems. This further increases the level of security far beyond that provided by ordinary e-mail filters used in conjunction with stateful packet filters. Some of the Trojan horses communicate with the attackers external system using ports that packet filters permit traffic. In one case, the Trojan horse used UDP port 53, which fooled the stateful packet filter. The SPF treated the hackers communications as normal DNS traffic. With PORTUS all direct IP traffic is denied and this attack would not work.

Block SMTP based Attacks

Smwrap protects against multiple attacks directed at mail servers and mail clients. This includes checks for unauthorized use, requests to obtain access to private information and multiple Denial of Service (DoS) attacks.

Smwrap guards against: Unauthorized sender/receiver, Bogus Helo command, use of VRFY and EXPN commands, anonymous mail relaying, commands imbedded in Header fields, password file access, Root user access, sendmail debug exploits and address spoofing.

DoS Attacks blocked: Helo buffer overflow, SMTP command buffer overflow, SMTP header overflow, SMTP Header Parsing Attack, Maximum number of recipients exceeded, Maximum message size exceeded, harmful header address characters, MIME header buffer overflow, MIME field overflow, and more.

Mail Blocking

Smwrap can be configured to run any script to process complete e-mail messages. These scripts can be used to run SPAM filters, virus scanners, content filters or a combination to eliminate undesirable e-mail.

Black Listing: Smwrap can be configured to use DNS Black Listing to block incoming mail based on the IP address of the sending server by looking them up in one or more DNSBL databases. This feature will block the majority of the SPAM found on the Internet.

Extensible Mail Filter: Smwrap can be used to activate Spam Assassin to examine in-bound e-mail. Its rule base uses a wide range of advanced heuristic and statistical analysis tests on mail headers and body text to identify SPAM. Each e-mail message is given a score. The disposition of the message can be controlled via an adjustable threshold, that determines if the mail should be deleted, re-routed or passed to the user.

Collaborative spam-tracking database: SPAM Assassin can be configured to use a collaborative spam-tracking data base to identify new forms of SPAM in real-time. As new forms of SPAM appear their signature is entered into the data base. Typically more than 97% of the SPAM is blocked by the first two methods.

Deny rules can be coded to block mail from specific e-mail addresses or domains. The Administrators can enter a list of senders, addresses, sites, or domains they want to target for blocking. Like Call Blocking on your telephone Smwrap allows you to choose who you want to get e-mail from. Blocked e-mail can be deleted, sequestered or redirected to a specified recipient. If the mail is sequestered or redirected it can be kept as evidence along with the log information.

Archiving

The smwrap program allows selected e-mail messages to be archived. The messages will be sent as usual and a copy will be stored in the archive directory.

Information hiding

Smwrap hides internal network information by automatically translating e-mail addresses and by scrubbing selected header information from outbound mail. Smwrap uses high speed table lookups to translate external e-mail addresses to internal addresses. A reverse translation is made for outbound mail. When outbound mail is directed to multiple users using "Cc:" each internal e-mail address is translated to an external name.

Multiple domain support

The aliases data base used by smwrap supports e-mail for multiple domains. This can be done using several different options. For example, one can explicitly code each user's external address and their associated internal address. This method would be used when mail for a single domain is to be delivered to more than one internal system. If all the mail for a domain is to be delivered to a single mail server then it is possible to specify a single entry that will route all mail for a domain to a single server.

Other SMTP mail servers

smwrap works with other SMTP compatible mail servers such as sendmail, HP's Open Mail, Microsoft Exchange Server Internet Mail Connector, Microsoft Outlook, and others.

Additional Features

The aliasreq command permits control of who is allowed to send mail outbound through the firewall. If a user is not registered in the alias data base then any attempt to send mail through the firewall will be rejected and a Security Alert will be issued.

The Secure Mail Wrapper translates internal e-mail addresses to external e-mail addresses. This translation includes all internal addresses that are part of a Carbon Copy (Cc:) or To: addresses. Translation support for addresses generated by Novell's GroupWise and MS Mail Exchanger is also provided.

Smwrap supports translation of out-bound headers generated by Microsoft Outlook. Smwrap will not translate the e-mail addresses that Outlook encloses within double

quotes on out bound mail.

The MS Internet Mail Exchange program can be configured to produce non-standard e-mail addresses in To: and Cc: fields. Smwrap can accommodate translations of several new forms of To: and Cc: addresses on out-bound e-mail.

Protocol Anomaly Detection (PAD)

In order to safeguard and secure various applications and their related programs, servers and clients PORTUS utilizes Protocol Anomaly Detection. Protocol Anomaly Detection (PAD) works by analyzing application-level traffic, commands and behavior, blocking and denying undesirable or otherwise inappropriate commands.

Protocol Anomaly Detection has successfully detected and blocked many forms of e-mail attack using code that was in place years before the first instance of the attack. The following example, demonstrates the effectiveness of PAD in blocking previously unknown forms of attack.

Protocol Anomaly Detection in Action

On March 3, 2003 a CERT Advisory warned of a new application level attack aimed at sendmail. Invalid header data was used to overflow a buffer allowing the attacker to gain root control of the system. This attack passed undetected through stateful packet filters and other firewalls. However, the Protocol Anomaly Detection code inserted into smwrap in the year 1995, more than 7 years before the attack, detected the invalid header data and blocked the attack. In fact, PORTUS contained three independent checks each of which would have blocked the attack if the others had not. The following description gives shows some of the in-depth defenses provided by PAD.

First, it blocks invalid addresses in header lines.

Second, the exploit involves embedding object code in the e-mail header. If the attacker manages to guess a valid recipient address for your system, then smwrap will block the message due to the invalid characters. Almost all binary codes contain characters that will be blocked by smwrap. The current attack program has invalid header characters near the beginning of the program so detection is immediate.

Third, if the attacker modified the program in a manner to enable it to get past the smwrap checks it could get installed and executed on an internal system. While this is highly unlikely, it might be possible. Even so the program will be defeated by PORTUS. The attacker program tries to connect back to the attackers computer. This connection will automatically be blocked unless the administrator codes a rule to let it through.

Use of Protocol Anomaly Detection means PORTUS will block new forms of attack without requiring the downloading of a new attack signatures as is required by virus scanners and IDS programs. An rarely does PORTUS require patches or updates to block new attacks that rely on protocol violations.

Standards violations: Many programmers too often assume that clients or servers will abide by the application standards they were developed and designed upon. Unfortunately it is too often the case that these programs perform no internal checks to watch for or prevent inappropriate commands and behavior. In general many clients and their servers provide an insufficient level of checking for compliance, which leaves them open to exploitation by malicious code and attacks.

For SMTP PAD is employed to block certain types of attacks, commands and other behavior which either violates the standards, or which is otherwise insecure. Attacks and exploits against SMTP servers can cause the server to become overloaded and overworked, or even crash (DoS). Other exploits and attacks can cause the SMTP server or system to execute malicious commands or code, this form of exploit for example is often possible with various buffer overrun forms of attack. The following list is a small sample of all the attacks and exploits that are blocked.

Long text lines: Lines longer than 1000 bytes can overrun E-mail servers buffer with unpredictable results. Some attacks have been used to insert worms and trojan horses on to mail server and others have been used to crash virus scanners.

Long filenames in MIME Attachment: Buffer overruns in Netscape Communicator, MS Outlook and other SMTP clients, can cause a Denial of Service (DoS).

SMTP commands longer than 512 bytes: Buffer overrun attack/exploit.

HELO buffer overrun: This exploit and attack is used by SPAMMERS to hide their trail. If the HELO command is longer than 1200 characters the SMTP server will crash.

MAIL FROM buffer overflow: Long MAIL FROM command can overflow the SMTP servers buffer causing Denial of Service.

Sendmail buffer overflow converting invalid characters to integer: Insufficient range checking before conversion can cause a buffer overrun.

Mail Header Size > 32 KB: An excessive header size could Span hundreds of lines and scores of packets, and is capable of causing a buffer overrun of the SMTP server. Smwarp permits a configurable maximum header size.

Sendmail parsing Redirection DoS: Excessive address length invokes a buffer overflow allowing execution of arbitrary code at the privilege of the sendmail daemon (usually root).

Excessive number of Recipients: This is a DoS exploit and attack wherein an excessive number of 'SMTP RCTP TO:' commands are sent to and received by the SMTP server.

Excessive number of TO: lines in header: Used to send a large number of invalid TO: addresses that consumes the processor trying to resolve errors. Results is a CPU DOS attack.

Bogus Helo: This exploit attempts to hide the sender's identity. The *bogushelo* directive can permit or deny e-mails that contain "bogus helo" SMTP commands.

Mail Server Exploits: The ability to pass parameters to the machine or SMTP server is blocked. This prevents the execution of commands imbedded in the header information, as well as imbedded programs or code. Attackers often try to mount attacks by inserting executable (binary) code into mail headers. This code overruns the buffers and modifies the stack, permitting the imbedded code to be executed. Attacks of this nature are typically used either to destroy or erase data upon the server, or to implant a trojan horse or otherwise compromise the security of the machine.

Use of VRFY & EXPN: These commands are often used to gather information to mount an attack

External Mail relay: This prevents someone from 'bouncing' mail off of your system to attack another, often used as a means of delaying discovery or making the attack seem to originate from another source or host.

MS Word Macros: Macros imbedded in MS Word attachments can be used to run arbitrary code.

Executable attachments: More than 190 executable file types exist in the MS environment. It is possible for an attached file to hide its true nature from the end-user. The user may for example, see a file with a name like "myphoto.gif" but the actual filename is fully "myphoto.gif.vbs"!

Sendmail decode flaw: This exploit allows EXPN command to overflow the buffer enabling the overwriting of sensitive files on the mail server.

Mailing to programs: This exploit and method of attack is used to send commands to and execute programs already upon the targeted machine. For example:

```
MAIL FROM: root@this.host
RCPT TO: |testing
```

This attack sends the mail directly to a program, which is a serious threat, since this allows anyone to execute arbitrary commands on the host.

MS SMTP DoS: Malformed data transfer (BDAT) requests causes DoS for service in Microsoft Windows 2000, Windows XP, and Exchange 2000. For example:

```
RCPT TO: Administrator
BDAT4
```

Mailing to a file: This attack sends mail directly to files, which is a serious threat, since this allows anyone to overwrite any file on the remote server.

```
MAIL FROM: root@this.host
RCPT TO: /tmp/test_file
```

Sendmail ETRN DoS: An attacker can cause a denial of service by sending a series of ETRN (remote queuing) commands then disconnecting from the server, while Sendmail continues to process the commands after the connection has been terminated.

Excessive invalid recipients: Sometimes attackers will send e-mails with multiple recipients in hopes of guessing a valid e-mail address. Smwrap keeps track of the number of invalid recipients and when the threshold is exceeded it blocks the mail.

Blocking E-mail Attachments

There are many different types of file attachments, and it is all too easy to attach one to any piece of outgoing mail. Machines that have already succumb to a viral infestation could easily attach files to a users outgoing mail without them even being aware. Though there are perfectly legitimate reasons to send various files as e-mail attachments, document or data files for example perhaps, other file types pose a security risk, such as files that can be executed on a users machine, and should not be allowed. The following table shows 70 of the 190 filename extensions that should be considered for blocking at the firewall.

File Extension Name	Description and reason for blocking
386	Device Driver. You should beware of e-mail sending you device drivers.
ade	
adp	
app	Application file. This is an executable file and should be blocked.
asp	Active Server Page. The active server page can contain code that can execute on the client system.
avi	Audio Video Interleave. This is a movie page.
bas	Basic File. This is an executable file and should be blocked.
bat	batch file.
bin	binary file.
bmp	Bitmap file.
btm	??
chm	A Compiled HTML Help File. This is an executable file and should be blocked.
cla	A JAVA class file. This is an executable file and should be blocked.
class	A JAVA class file. This is an executable file and should be blocked.
cmd	A command file similar to a bat file. This is an executable file and should be blocked.
com	A MS DOS application program. This is an executable file and should be blocked.
cpl	A Control Panel File. This is an executable file and should be blocked.
crt	A Security Certificate. This file can change your security certificates and should be blocked.
css	A Cascading Style Sheet for webpages.
dat	A data file. This can contain video data or program data required to support another executable program.

dll	A dynamic Loadable Link program. This is an executable file and should be blocked.
dot	A Document Template.
drv	A device Driver. This is an executable file and should be blocked.
eml	E-mail File. ???
exe	A executable program that should be blocked.
flc	A flick (video) file.
fli	A flick (video) file.
fon	A font file.
hlp	A Help File. This could replace an existing file on the client system . So it should be blocked.
hta	HTML application file.
htm	Hypertext Markup Language file.
inf	Setup Information.
ini	Configuration Settings
ins	Internet Communication Settings (windows). Install Shield Setup Information.
isp	Internet Communication Settings.
js	A Javascript file.
jse	A Javascript extensions file.
lnk	A windows symbolic link also known as a shortcut. This could be used to change a link to point at a different file.
mdb	One of the Files made my MSVC++
mde	One of the Files made my MSVC++
mov	Quicktime Movie
mp3	MPEG Layer 3 Audio
mpe	MPEG Video, Audio, Or Movie
mpeg	MPEG Video, Audio, Or Movie
mpg	MPEG Video, Audio, Or Movie
msc	Microsoft Common Console Document
msi	Microsoft System Installer

msp	Microsoft System Installer Patch
mst	mst
nls	National Language System? For setting code pages for keyboards... (this is old DOS info might not fit any longer)
obj	Compiled Includeable Object File
ocx	ActiveX Control.
pcd	Type of Graphics
pif	Program Information File. A DOS Program LNK that also holds program settings
qic	Backup Data??
ra	RealAudio File
ram	RealMedia File
reg	Registry Settings
rm	ReaLMedia File or RV RealVideo File
rts	Real Time Stream ?
scr	Screen Saver
sct	Windows Script Component
shb	Shortcut into a Document
shs	Scrap Object -like and OBJ file
sys	System File/Device Driver
url	Internet Shortcut
vb	Visual Basic File
vbe	Visual Basic Extension?
vbs	Visual Basic Script
vxd	Device Driver
wav	Waveform Audio File
wmf	Windows Metafile (Typically just graphics)
wsc	Windows Script Component
wsf	Windows Script File
wsh	Windows Script Host Settings File

Smwrap can be configured to block attached files of any extension type. The following list is a sample set of denyx rules that could be used to block various file attachments.

denyx from * to * ext = 386 sequester denyx from * to * ext = ade sequester denyx from * to * ext = adp sequester denyx from * to * ext = app sequester denyx from * to * ext = asp sequester denyx from * to * ext = avi sequester denyx from * to * ext = bas sequester denyx from * to * ext = bat sequester denyx from * to * ext = bin sequester denyx from * to * ext = bmp sequester denyx from * to * ext = btm sequester denyx from * to * ext = chm sequester denyx from * to * ext = cla sequester denyx from * to * ext = class sequester denyx from * to * ext = cmd sequester denyx from * to * ext = com sequester denyx from * to * ext = cpl sequester denyx from * to * ext = crt sequester denyx from * to * ext = css sequester denyx from * to * ext = dat sequester denyx from * to * ext = dll sequester denyx from * to * ext = dot sequester denyx from * to * ext = drv sequester denyx from * to * ext = eml sequester denyx from * to * ext = exe sequester denyx from * to * ext = flc sequester denyx from * to * ext = fli sequester denyx from * to * ext = fon sequester denyx from * to * ext = hlp sequester denyx from * to * ext = hta sequester denyx from * to * ext = htm sequester denyx from * to * ext = inf sequester denyx from * to * ext = ini sequester denyx from * to * ext = ins sequester denyx from * to * ext = isp sequester denyx from * to * ext = js sequester denyx from * to * ext = jse sequester denyx from * to * ext = lnk sequester	denyx from * to * ext = mdb sequester denyx from * to * ext = mde sequester denyx from * to * ext = mov sequester denyx from * to * ext = mp3 sequester denyx from * to * ext = mpe sequester denyx from * to * ext = mpeg sequester denyx from * to * ext = mpg sequester denyx from * to * ext = msc sequester denyx from * to * ext = msi sequester denyx from * to * ext = msp sequester denyx from * to * ext = mst sequester denyx from * to * ext = nls sequester denyx from * to * ext = obj sequester denyx from * to * ext = ocx sequester denyx from * to * ext = pcd sequester denyx from * to * ext = pif sequester denyx from * to * ext = qic sequester denyx from * to * ext = ra sequester denyx from * to * ext = ram sequester denyx from * to * ext = reg sequester denyx from * to * ext = rm sequester denyx from * to * ext = rts sequester denyx from * to * ext = scr sequester denyx from * to * ext = sct sequester denyx from * to * ext = shb sequester denyx from * to * ext = shs sequester denyx from * to * ext = sys sequester denyx from * to * ext = url sequester denyx from * to * ext = vb sequester denyx from * to * ext = vbe sequester denyx from * to * ext = vbs sequester denyx from * to * ext = vxd sequester denyx from * to * ext = wav sequester denyx from * to * ext = wmf sequester denyx from * to * ext = wsc sequester denyx from * to * ext = wsf sequester denyx from * to * ext = wsh sequester
---	---

For more information on smwrap or PORTUS please contact us at:

Freemont Avenue Software, Inc.
1830 S. Kirkwood Suite 205
Houston, TX 77077
Phone: 281-759-3274
Fax: 281-759-8558
e-mail: portus@lsli.com
Web: www.lsli.com