Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Solaris 8 and Checkpoint NG FP3 install with SSH, JASS and Syslog

After determining the initial state of insecurity in an existing corporate firewall, the following discusses the process of building a hardened Solaris 8 Sun clone with SSH connectivity for remote firewall console access with Checkpoint NG FP1 firewall, an upgrade to FP3 then HF2, hardened further with JASS, and the last step remote syslog. Discussed below is the detailed account of the pre-existing insecurity, a brief note of the catalytic event precipitating the actual changes to the firewall, a discussion of the imp...

Copyright SANS Institute
Author Retains Full Rights

AD
Embed Security Into the Software Development Lifecycle
Sponsored By VERACODE
Download the Report by Securosis

Solaris 8 and Checkpoint NG FP3 install with SSH, JASS and Syslog

GIAC Security Essentials Certification (GSEC)
Version 1.4b (amended August 29, 2002)

Option 2, Case Study in Information Security

Submitted as Partial Completion
For GCEC Certification
7 September 2003

Mike Shannon

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

Table of Contents 2
Abstract: Topic of Discussion 3
Before: Recognizing and Evaluating the Risk 3
During: Implementing A More Secure Standard 4
Solaris 8 Installation 5
Secure Shell (SSH) Installation: 8
Checkpoint Installation: 11
FP3 Installation and Hot Fix 2: 12
AS400: 13
FTP fix. 13
Harden Solaris: 13
FW-1 Errors after JASS install: 14
Syslog setup 14
After: Enhanced Security 15
Impact: Does it Actually Work? 16
Appendix A: Core file listing [3]. 17
Appendix B: Files that can be removed [3]: 19
Appendix C: Startup scripts for sshd [8] 21
References 23

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract: Topic of Discussion

After determining the initial state of insecurity in an existing corporate firewall, the following discusses the process of building a hardened Solaris 8 Sun clone with SSH connectivity for remote firewall console access with Checkpoint NG FP1 firewall, an upgrade to FP3 then HF2, hardened further with JASS, and the last step remote syslog. Discussed below is the detailed account of the pre-existing insecurity, a brief note of the catalytic event precipitating the actual changes to the firewall, a discussion of the implementation, and the results and ultimate success of the procedure 'hardening' the corporate firewall.

Before: Recognizing and Evaluating the Risk

Shortly following the commencement of my employment at a multinational company, it came to my attention that the existing firewall required several security upgrades concurrently at a time that I needed to make a rule change on the existing Checkpoint firewall. Upon inquiry, I discovered the first potential flaw in the company's existing security measures, that the Checkpoint firewall was not maintained from within the company's IT infrastructure. It was handled by the company's ISP. This does not have to be a flaw. Electing to use an outside source for maintaining security is not an uncommon practice. Many ISP's also provide these services. Determining the choice of security maintenance is dependent upon a number of key factors, of which, first is finding a reputable, competent outside source. And, secondly, whether the company in question has a security professional on staff with a sufficient degree of expertise necessary to maintain an in-house firewall in appropriate and timely fashion. Ultimately, the company must make a decision as to which cost it is willing to bear.

In the matter in question, when the ISP's representative was asked some routine questions: what version of Checkpoint was on the firewall and what version of Solaris was installed on the Sun box, the representative did not know. The last and final question was how the firewall is maintained. The representative did have the answer, which was telnet. This was a rather obvious indication of a major security vulnerability. My concerns were mounting, and after further probing, I discovered that, contrary to standard security practices, the ISP had never patched either the Sun server or the Checkpoint firewall. It was chilling to discover that the very professionals relied upon, for a vital security function, were ignorant, and frankly, incompetent, when it came to our company's protection. Patching Solaris and Checkpoint on a regular basis is standard practice to reduce potential security risk and the procedure is strongly recommended by experts within the security community [1,2]. Additionally, it is never recommended to telnet to your firewall, internally let alone over the internet [1,2].

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Thus, upon investigation, there were several things contributing to the state of vulnerability and serious risk, stemming from the pre-existing state of the company's browsing firewall:

1. Solaris out of patch
2. Checkpoint out of patch
3. Security rules being managed by outside vendor with nobody able to see the rules internally
4. Management of the firewall over telnet, and
5. No firewall log reporting

At this point, it was obvious that the existing 'secure' state of the internet browsing firewall was completely inadequate and potentially open to malicious attack, which could result in serious consequences to the business. In fact, it was just such a malicious attack that brought all IT's attention to the serious lack of readiness on the part of the firewall. Due to the preceding circumstances, I took it upon myself to upgrade the firewall to bring it current with more acceptable standards of preparedness within the security community.

During: Implementing A More Secure Standard

Knowing that company IT security had become a priority, and after examining the options available, and ascertaining the IT budget for financial limitations, the decision was made to obtain and create an onsite managed firewall. Through the cooperation of several corporate and vendor contacts, I was able to acquire a new Fujitsu Sun Clone and Checkpoint NG FP1.

The actual set up process was straightforward. I commenced with a clean install of Solaris 8 from the point of booting with the Solaris CD. Of specific note is that the accessible version of Solaris 8 did not have the option of 64 bit installation for the Core install, thus for the purposes of this discussion, the install is based on 32 bit processes. In order to obtain the maximum benefit of the new security procedures I was implementing, I also researched to the method of hardening a Solaris system for firewall usage. I found that the most useful resource were Lance Spitzner's papers relating to Solaris Hardening [3]. In an additional effort to protect the company and create the highest level of security given the parameters given, I used Sun's JASS script to further harden the system [4]. After completion of the installation, I had a secure install of Solaris 8 fully patched and ready for Checkpoint installation.

Described in detail below are the steps taken to install Solaris 8, patch it, install SSH, install Checkpoint NG FP1, upgrade to NG FP3, apply hot fixes, harden Solaris using JASS and finally setup syslog to go to a remote syslog server:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Solaris 8 Installation

1. The following files need to be downloaded on a separate secured workstation:

    a. Latest Solaris patch (8_Recommended http://sunsolve.sun.com/pub-cgi/show.pl?target=home)
    b. openssh 3.4 or better (http://www.sunfreeware.com)
    c. openssl (SSL) (http://www.sunfreeware.com)
    d. prngd (Psuedo Random Generator Daemon) (http://www.sunfreeware.com)
    e. zlib (Z library) (http://www.sunfreeware.com)
    f. JASS (http://wwws.sun.com/software/security/jass/ choose .z file v4.0.0 as of 7/15/03)
    g. Checkpoint License file, if you have one. If you do not have a License file you can enter your license manually. Get the file from http://www.checkpoint.com with your user account
    h. Checkpoint NG FP3 files (http://www.checkpoint.com)

2. It is always recommended to build your firewall off line; i.e., not connected to the network [3].To that end, burn these files to a cdrom or put them on an isolated ftp server on a secure network.

3. Power up the Sun box and insert Solaris 8 CD 1 (Software 1) into your cdrom drive.

4. During boot up hit <stop>< a>, at ok prompt type boot cdrom1 or reboot cdrom1. The 1 at the end of cdrom was specific to my firewall.

5. Boot with cdrom, first option is: Select a Language, I chose 0 for English.

6. Select a locale, 45 for U.S.A (en_US.ISO8859-1)

7. Open Windows boots up.

8. The first GUI (Graphical User Interface) screen is a screen telling you that Solaris installation is broken up into short sections. Click Continue.

9. The installation procedure then tells that you need to identify the system. Click Continue.

10. Identify the system (on the following screens after you select your choice click Continue)

    a. Networked, yes
    b. DHCP, no
    c. Primary interface Qfe0 (assuming you have a Quad Ethernet card)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

d. Hostname, firewall (or something less conspicuous)
e. IP address x.x.x.x (internal address)
f. IPv6, no
g. Confirmation, continue or change
h. Kerberos, no
i. Continue
j. Name service, None
k. Continue or change
l. Part of a subnet, yes
m. Subnet mask, 255.255.255.0
n. Timezone, geographic region
o. US, pacific
p. Date and time
q. Continue or change

11. Next screen is asking if you want to upgrade or do initial install. Chose initial install.

12. It warns you that you will have to make some decisions and you can continue or go back, continue.

13. Next you select your geographic region again, choose your region, Continue.

14. Next you need to decide if you what type of system you are installing. For a firewall all you need is Core and then customize. Please see Appendix A for the file listing for a Core installation.

15. Select your boot disk, Continue.

16. Preserve data, continue will wipe the disk

17. Automatic Layout of file system? Choose Manual Layout.

18. File system and disk layout, Customize

19. Suggested disk partitions for a 9GB.

0	/	1024
1	swap	512
2	/opt	1024
3	/var	1024
4	/var/opt/	4608
5	/usr	1024

OK,
Continue

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

20. Mount Remote File Systems? Continue

21. Profile, Begin Installation (or Change or Exit)

22. Auto Reboot or Manual, Auto Reboot.

23. Installation begins.

24. The system will reboot when the installation is finished.

25. Login as root. No password.

26. Change password of root.

    a. Passwd root
       New password:
       Re-enter new password:
       Passwd (SYSTEM): passwd successfully changed for root

27. When I do a Core Installation with the above packages from my distribution of Solaris 8, I do not get gzip, SUNWter (required for Checkpoint installation) or bash. I have to add them separately from the Software Disk 2 of 2. They were in /cdrom/sol_8_sparc_2/Solaris_8/Product (/etc/init.d/volmgt start if needed).

    cd /cdrom/sol_8_sparc_2/Solaris_8/Product
    pkgadd –d . SUNWter
    pkgadd –d . SUNWbash
    pkgadd –d . SUNWgzip

28. Copy files from CDROM that you have downloaded and burned to a cd to a directory on the new system (/etc/init.d/volmgt start if needed). Copy to a directory of your choice (e.g., /usr/local)

    a. Solaris 8 patch
    b. JASS
    c. Open SSH and all associate files
    d. Any Checkpoint files (e.g., CPlicense.lic and hotfixes)

29. Remove un-necessary packages (See Appendix B for complete list of files that can be removed)

    a. Pkgrm is the utility to remove packages. Run the utility and select packages that are un-necessary like: Audio, SUNWaudd
    b. Scroll through the pkgrm list and write down your corresponding numbers to the list in Appendix B.
    c. Select the packages 1,2,3,4,20,24,.. etc. To do more than one at a time.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

d. Answer y to all the packages as they scroll by.

30. Patch Solaris 8

    a. Unzip 8_Recommended
    b. Creates a directory named 8_Recommended
    c. ./install_cluster from 8_Recommended dir.
    d. Reboot

31. Network [5]

    a. Netmasks file
        i. Add external net
            1. x.x.x.v 255.255.255.248
            2. x.x.x.y is the external subnet
    b. ifconfig
        i. ifconfig qfe1 plumb
        ii. ifconfig qfe1 x.x.x.x netmask 255.255.255.248 up
        iii. x.x.x.x is the external IP address that we will protect with Checkpoint.
    c. hostname
        i. echo x.x.x.x > /etc/hostname.qfe1
    d. default route
        i. echo x.x.x.z> /etc/defaultrouter
        ii. x.x.x.z is the next hop interface

32. Add Routes [6]:

    a. Edit /etc/rc2.d/S69inet with vi.
    b. At the end of the file put
    #Internal Routes
    route add net x.x.0.0 255.255.0.0 1
    c. x.x.0.0 is your internal subnet.

Secure Shell (SSH) Installation:

Prior to my upgrade the only way to manage the firewall was to telnet to it. This is considered extremely insecure. I did not want to telnet to the firewall but instead chose to use SSH as the means for remote administration of the firewall [7]. The following is a procedure to install SSH on Solaris 8 [8].

1. The following files are necessary and available at http://www.sunfreeware.com.

    a. openssh
    b. openssl (SSL)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

c. prngd (Psuedo Random Generator Daemon)
d. zlib (Z library)

2. **Installation:** Copy the files from your cdrom to the hard drive and expand, unzip, gzip –d, etc, for whatever format your files come in.

3. **#pkgadd -d openssl-0.9.6g-sol8-sparc-local**

4. **#pkgadd -d prngd-0.9.25-sol8-sparc-local**

5. **#pkgadd -d zlib-1.1.4-sol8-sparc-local**

6. **#pkgadd -d openssh-3.4p1-sol8-sparc-local**

7. Create Startup scripts: Startup scripts are located in Appendix C.

8. Start prngd: This never works the first time.

   # /etc/init.d/prngd start
   starting PRNG daemon
   Info: Random pool not (yet) seeded
   Could not bind socket to /var/spool/prngd/pool: No such file or directory
   If you get nothing try a reboot or try 9 then 16 below.

9. Try making a directory as follows:

   # mkdir -p /var/spool/prngd
   #/etc/init.d/prngd start
   starting PRNG daemon
   # Info: Random pool not (yet) seeded

10. I had to reboot a couple of times on one install to get prngd to work. If you still cannot get PRNG started try looking at 16 below.

11. Start the ssh daemon,

    # /etc/init.d/sshd start
    starting SSHD daemon
    Could not load host key: /usr/local/etc/ssh_host_key
    Could not load host key: /usr/local/etc/ssh_host_rsa_key
    Could not load host key: /usr/local/etc/ssh_host_dsa_key
    Disabling protocol version 1. Could not load host key
    Disabling protocol version 2. Could not load host key
    sshd: no hostkeys available -- exiting.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

12. The errors here are due to not creating any key pairs for our ssh server. Create a public key pair to support the new, DSA-based version 2 protocol
    # /usr/local/bin/ssh-keygen -d -f /usr/local/etc/ssh_host_dsa_key -N ""
    Generating public/private dsa key pair.
    Your identification has been saved in /usr/local/etc/ssh_host_dsa_key.
    Your public key has been saved in /usr/local/etc/ssh_host_dsa_key.pub.
    The key fingerprint is:
    ef:c17d:56:39:66:0f:21:c3:9c:0a:32:22:78:62:e8 root@firewall

13. Create a public key pair to support the old, RSA-based version 1 protocol
    # /usr/local/bin/ssh-keygen -b 1024 -f /usr/local/etc/ssh_host_rsa_key -t rsa -N ""
    Generating public/private rsa1 key pair.
    Your identification has been saved in /usr/local/etc/ssh_host_rsa_key.
    Your public key has been saved in /usr/local/etc/ssh_host_rsa_key.pub.
    The key fingerprint is:
    ef:c17d:56:39:66:0f:20:c3:9c:0a:22:22:78:62 root@firewall

    # /usr/local/bin/ssh-keygen –t rsa1 –f /usr/local/etc/ssh_host_key -N ""
    Generating public/private rsa1 key pair.
    Your identification has been saved in /usr/local/etc/ssh_host_key.
    Your public key has been saved in /usr/local/etc/ssh_host_key.pub.
    The key fingerprint is:
    ef:c17d:56:39:66:0f:20:c3:9c:0a:22:22:78:62:ea root@firewall

14. Edit ssh daemon configuration file /usr/local/etc/sshd_config, enable protocol 2 and 1
    Uncomment the line, that says
    protocol 2,1

15. **# /etc/init.d/sshd start**
    starting SSHD daemon
    #

16. If there are issues try the following:

    a. mkdir /dev/urandom
    b. ln -s /var/spool/prngd/pool /dev/urandom/pool
    c. cat /var/adm/messages > /usr/local/etc/prngd/prngd-seed
    d. mkdir dir /var/spool/prngd
    e. /usr/local/sbin/prngd /var/spool/prngd/pool

    These directories are dependent on your own install.

17. Once you do those steps, go back and generate the keys (step 12) and start the services.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

18. I received the following error: “Privilege separation user sshd does not exist when the service starts”. To fix that error:

    a. Create a user called “sshd”. Passwd, make it a difficult password.
    b. Create a directory /var/empty

19. Once I did the following “/etc/init.d/sshd start” gives the following:

    Starting SSHD daemon

20. SSH was loaded and port 22 was open. You will have to create a rule in Checkpoint to allow this through to the firewall.

Checkpoint Installation:

1. Install Checkpoint NG. My Checkpoint install was from a NG FP1 cd. I found that Checkpoint installs cleaner if you install Checkpoint before JASS hardening.

   /etc/init.d/volmgt start (if it is not started)
   cd /cdrom/cp_ng_fpx (x = what ever fp you have I had fp1)
   ./UnixInstallScript

2. Hit N for next

3. Scroll through the License Agreement and hit y to accept the agreement.

4. The software does a quick check to see if your install meets minimum requirements for patches and then installs SVN Foundation.

5. Select what you are installing. I chose 1. [*] VPN-1 & Firewall-1, N for next

6. Choose the type of Installation: 1.(*) Enterprise Primary Management and Enforcement Module, N for next

7. Would you like to install backward compatability?

   1. ( ) Yes.
   2. (*) No.
   Hit N for next.

8. Your choices are valid. You have selected:
   VPN-1 & Firewall-1 Enterprise Primary Management and Enforcement Modules, N for next.

9. Installation of Checkpoint proceeds.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

10. The next screen that comes up is the Configuration screens.

11. It asks if you want to add licenses, I wait till it is done and add later.

12. Next is to add administrators: add an admin, and a password and give W, Write all. Confirm and add another if needed.

13. Gui clients: [A]dd or [D]elete one? A if you know the IP address or the resolvable name of the client station. You can always add one later.

14. Add a group if you want, or do it later.

15. Configuring Random Pool… Just keep typing till you fill the bar….

16. Configuring Certificate Authority…Press Enter.

17. Configuring Certificate Fingerprint… Save to file.

18. Would you like to reboot the machine [y/n]: y, system reboots and firewall is installed.

19. You will get some warnings the first reboot because there is no license or rules installed.

FP3 Installation and Hot Fix 2:

1. The version of Checkpoint that I had was pre-FP3. Patch Checkpoint with the FP3 patch.

   After expanding gzip –d then tar –xvf:
   Pkgadd –d . CPshrd-53 (from the directory right above CPshrd-53)
   Pkdadd –d . CPfw1-53 (from the directory right above CPshrd-53)

2. Hot fix 2 (after expanding)

   a. ./cpshared_HF2_53957_4
      It will ask: "Do you wish to proceed with installation of Check Point SVN Foundation NG FP3 Hotfix2 for Check Point SVN NG FP3 on this computer? If you choose to proceed, installation will perform CPSTOP.
      (y-yes, else no): y"
   b. ./fw1_HF2_53945_1
      It will ask: "Do you wish to proceed with installation of Check Point VPN-1/Firewall-1 NG FP3 Hotfix2 for Check Point VPN-1/Firewall-1 NG FP3 on this computer? If you choose to proceed, installation will perform CPSTOP.
      (y-yes, else no): y"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

It will remind you to reboot. Reboot.

3. Add license and management stations. Use cpconfig. I copied the .lic file to the same cdrom that had the other files (SSH, JASS, etc). Using the [F]etch method is much easier than typing in the key.

4. Add rules using the management client for Checkpoint NG FP3, default and ssh through the gui. Nothing allowed inbound. Allow only what is needed outbound; e.g., http, https, ftp, ssh…etc.

AS400:

In order to allow our AS400 out to the internet using ICMP, I had to open up the ICMP packet size from the default 64byte to 260 byte size. Located under Policy/Smartdefense settings/IP and ICMP/Max Ping Size. Change to 260 bytes.

FTP fix.

My company has requirements to FTP to servers that do not send the newline at the end of each line. Because of this, certain ftp sites (e.g., ftp.compaq.com) will not allow you to connect. The following will fix the requirement for a newline at the end of each line [9].

Modify the $FWDIR/lib/base.def file.
Close all open GUI clients.
Open the file $FWDIR/lib/base.def in vi.
Find the line
#define FTP_ENFORCE_NL
Comment it out:
// #define FTP_ENFORCE_NL
Save the file. The fix will not work until you re-apply rules.

Harden Solaris:

I chose the JASS [4] hardening script from Solaris as my way of a final hardening process. The main objective of the Solaris Security Toolkit, JASS is to simplify and automate the process of securing Solaris systems. It implements the recommendations in the Sun BluePrints Online security articles. The script goes through the Solaris system and hardens and minimizes services in the Solaris Operating Environment [10]. I do this as a final step in the build of the firewall.

1. After expanding the JASS package

2. ./jass-execute –d secure.driver

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3. Test the firewall by attaching to it using the management tools.

4. Vulnerability/Port scan, on all interfaces.

FW-1 Errors after JASS install:

> "FW-1 driver could not be informed. This may be due to the driver being removed from the system, or a failure of the fw bootd process. If this message keeps appearing after rebooting the machine, please contact Check Point technical support. This message can be safely ignored in the following cases: FW-1 has just been uninstalled or upgraded and has not been rebooted yet or the machine is now in single user mode. This message will be suppressed for the next 127 times."

This error is due to the hardening portion of JASS that modifies the way syslog starts. It starts with the –t option. If you edit /etc/init.d/syslog and take the –t out of the line that starts syslogd this error goes away [11]. According to the Unix man pages the –t "disables the syslogd UDP port to turn off logging of remote messages" [12]. Since the firewall is not allowing UDP port 514 connections to the firewall this should not be a security issue.

Syslog setup

It is more secure to save the system log files from the firewall off to another server [2]. Solaris has a facility to send the syslog logs to a remote host.

1. Edit /etc/syslog.conf file with vi

2. Uncomment or put in the following lines

3. *.alert @loghost

4. *.emerg @loghost

5. *.debug @loghost

6. Edit /etc/hosts file with vi

7. Modify the line that has loghost or add the following

8. x.x.x.x loghost

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

9. x.x.x.x should be a secure machine on the inside network with some form of syslogd running on a secured pc. For example, Kiwi Syslog Deamon from http://www.kiwisyslog.com.

After: Enhanced Security

Initially, the implementation was a by the book, straightforward use of standard security concepts and measures that I gleaned from my personal research of current, available, well respected resources. However, since that time, I have continued to maintain the firewall at its current level, and I have modified it further to suit the company's purposes. IT security is an ever changing environment, and is a priority for companies wishing to do business internationally, effectively, and efficiently.

Following the successful implementation of the proposed creation and internally maintained Solaris 8 system with Checkpoint NG FP3 installed, patched, hardened, and ready for rule base installation, it was my welcome task to maintain, and monitor the firewall. Thus, I set up hiding NAT, basic rules, and set the system so that there is no ICMP allowed to the firewall. Prior to this installation, you could ping the firewall from the internet, rendering it potentially vulnerable to Denial of Service attacks.

An additional precaution was taken which is that all ports were blocked outbound, with the exceptions of permissible traffic (HTTP, HTTPS, FTP, Telnet, etc). This is a marked departure to the standard procedure of the preceding firewall in which all ports were open outbound. By reducing the number of ports allowed outbound we reduced the risk of Trojans being used as backdoors to our network. This additionally, effectively eliminated Peer-2-Peer file trading as well as eliminating various IRC channels.

Additional procedures set into place relate to rules, remote administration, and logs. Now, rules are controlled by an internal security engineer whose reporting structure is within the company's IT division; the remote administration of the firewall is performed over a secure channel (SSH) internally, which is in direct contrast to the previous method of remote administration which was over clear channel telnet, over the internet; and system logs are sent to a secured syslog server off of the firewall, which is more secure in that if the firewall is compromised, the attacker would have to attack an additional system to cover their tracks.

Prior to the upgrade we suffered a detrimentally effective Code Red II attack which caused the firewall to cease functioning [13]. In fact, it was the Code Red II incursion that precipitated the changes leading to our current state of preparedness. Among the numerous companies recently affected by the multi-pronged attacks, our network experienced an MSBlast/Welchia worm attack on August 20, 2003. The firewall withstood a heavy beating from this malicious worm from numerous internally infected hosts that attempted connections to random hosts on the internet. However, despite the worms' extensive attempts at connecting to more hosts on the internet and before

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

we could get a handle on the worm, the firewall withstood the attack with no decrease in performance. There were some errors on the firewall (errors sent to the remote syslog), but we were still able to get out to the internet and continue the daily operation of the company, without detriment.

Unfortunately, there are some security implications with the FTP fix I applied in which there exists a potential vulnerability on un-patched Solaris systems that have Tooltalk installed [14]. Fortunately, Tooltalk is not installed on this firewall which eliminates the potential vulnerability.

Impact: Does it Actually Work?

The decision to create the Checkpoint firewall and physically house and maintain the system has had a significantly positive impact. In contrast to the previous firewall in use: this firewall is more stable and up to date; the rules are now maintained internally; and, logs are viewable by security engineers within the company. We have been successfully using this firewall for two years, since its implementation. Our bandwidth has been increased to 6Mb and the firewall has experienced no issues in keeping up with the increased bandwidth. We have no internal services going through this particular firewall and only perform internet browsing through it therefore, do not need to worry about passing traffic internally. I do weekly vulnerability scans on the firewall to look for new potentially vulnerable open access points in a continuing security presence.

It is worthwhile to note that regardless of the time and energy security professionals spend in protecting systems and building, maintaining, updating, patching, and hardening firewalls there still exist those malicious enough to spend their time, effort and energy in inventing and seeking methods in which to destroy those things that others build and protect. It is always easier to destroy a thing than it is to build and maintain it. I prefer to work on the side that builds something to be safely used and to that end, it is of paramount importance to continue to learn, study, and create effective methods of customizing the firewall that guards a company's network systems.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix A: Core file listing [3].

The following are the files that were the final file selection on my version of Solaris. Most come with the Core install of Solaris. Some were selected for firewall functionality. I chose to add some additional files for ease of firewall management.

system	SUNWcar	Core Architecture, (Root)
system	SUNWcarx	Core Architecture, (Root) (64-bit)
system	SUNWcsd	Core Solaris Devices
system	SUNWcsl	Core Solaris, (Shared Libs)
system	SUNWcslx	Core Solaris Libraries (64-bit)
system	SUNWcsr	Core Solaris, (Root)
system	SUNWcsu	Core Solaris, (Usr)
system	SUNWcsxu	Core Solaris (Usr) (64-bit)
system	SUNWkvm	Core Architecture, (Kvm)
system	SUNWkvmx	Core Architecture (Kvm) (64-bit)
system	SUNWdoc	Documentation Tools
system	SUNWesu	Extended System Utilities
system	SUNWfns	Federated Naming System
system	SUNWfnsx	Federated Naming System (64-bit)
system	SUNWswmt	Install and Patch Utilities
system	SUNWnamos	Northern America OS Support
system	SUNWman	On-Line Manual Pages
system	SUNWpd	PCI Drivers
system	SUNWpdx	PCI Drivers (64-bit)
system	SUNWtoo	Programming Tools
system	SUNWtoox	Programming Tools (64-bit)
system	SUNWqfed	Sun Quad FastEthernet Adapter Driver
system	SUNWqfedx	Sun Quad FastEthernet Adapter Driver (64-bit)
system	SUNWlibC	Sun Workshop Compilers Bundled libC
system	SUNWlibCx	Sun WorkShop Bundled 64-bit libC
system	SUNWlibms	Sun WorkShop Bundled shared libm
system	SUNWlmsx	Sun WorkShop Bundled 64-bit shared libm
system	SUNWhmd	SunSwift SBus Adapter Drivers
system	SUNWhmdx	SunSwift SBus Adapter Drivers (64-bit)
system	SUNWadmc	System administration core libraries
system	SUNWadmfw	System & Network Administration Framework
system	SUNWloc	System Localization
system	SUNWlocx	System Localization (64-bit)
system	SUNWvolr	Volume Management, (Root) (optional for cdrom access)
system	SUNWvolu	Volume Management, (Usr) (optional for cdrom access)
system	SUNWCvolx	Volume Management (64-bit) (optional for cdrom access)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Optional packages for firewall functionality that even though they are selected did not get installed with the core install of Solaris that I had.

system	SUNWbash	GNU Bourne-Again shell (bash)
system	SUNWbzip	The bzip compression utility
system	SUNWbzipx	The bzip compression library (64-bit)
system	SUNWgzip	The GNU Zip (gzip) compression utility
system	SUNWzip	The Info-Zip (zip) compression utility
system	SUNWter	Terminal Information

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix B: Files that can be removed [3]:

system	SUNWatfsr	AutoFS, (Root)
system	SUNWatfsu	AutoFS, (Usr)
system	SUNWauda	Audio Applications
system	SUNWaudd	Audio Drivers
system	SUNWauddx	Audio Drivers (64-bit)
system	SUNWcg6	GX (cg6) Device Driver
system	SUNWcg6x	GX (cg6) Device Driver (64-bit)
system	SUNWdfb	Dumb Frame Buffer Device Drivers
system	SUNWdtcor	Solaris Desktop /usr/dt filesystem anchor
system	SUNWfcip	Sun FCIP IP/ARP over FibreChannel Device Driver
system	SUNWfcipx	Sun FCIP IP/ARP over FibreChannel Device Driver (64 bit)
system	SUNWfcp	Sun FCP SCSI Device Driver
system	SUNWfcpx	Sun FCP SCSI Device Driver (64-bit)
system	SUNWfctl	Sun Fibre Channel Transport layer
system	SUNWfctlx	Sun Fibre Channel Transport layer (64-bit)
system	SUNWftpr	FTP Server, (Root)
system	SUNWftpu	FTP Server, (Usr)
system	SUNWi15cs	X11 ISO8859-15 Codeset Support
system	SUNWi1cs	X11 ISO8859-1 Codeset Support
system	SUNWkey	Keyboard configuration tables
system	SUNWluxdx	Sun Enterprise Network Array sf Device Driver (64-bit)
system	SUNWluxop	Sun Enterprise Network Array firmware and utilities
system	SUNWluxox	Sun Enterprise Network Array libraries (64-bit)
system	SUNWm64	M64 Graphics System Software/Device Driver
system	SUNWm64x	M64 Graphics System Software/Device Driver (64-bit)
system	SUNWmdi	Sun Multipath I/O Drivers
system	SUNWmdix	Sun Multipath I/O Drivers (64-bit)
system	SUNWnamow	Northern America OW Support
system	SUNWnisr	Network Information System, (Root)
system	SUNWnisu	Network Information System, (Usr)
system	SUNWpcelx	3COM EtherLink III PCMCIA Ethernet Driver
system	SUNWpcmci	PCMCIA Card Services, (Root)
system	SUNWpcmcu	PCMCIA Card Services, (Usr)
system	SUNWpcmcx	PCMCIA Card Services (64-bit)
system	SUNWpcmem	PCMCIA memory card driver
system	SUNWpcser	PCMCIA serial card driver
system	SUNWpl5u	Perl 5.005_03
system	SUNWpsdpr	PCMCIA ATA card driver
system	SUNWrmodu	Realmode Modules, (Usr)
system	SUNWses	SCSI Enclosure Services Device Driver
system	SUNWsesx	SCSI Enclosure Services Device Driver (64-bit)
system	SUNWsndmr	Sendmail root
system	SUNWsndmu	Sendmail user

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

system	SUNWsolnm	Solaris Naming Enabler
system	SUNWssad	SPARCstorage Array Drivers
system	SUNWssadx	SPARCstorage Array Drivers (64-bit)
system	SUNWtleux	Thai Language Environment user files (64-bit)
system	SUNWudf	Universal Disk Format 1.50, (Usr)
system	SUNWudfr	Universal Disk Format 1.50
system	SUNWudfrx	Universal Disk Format 1.50 (64-bit)
system	SUNWusb	USB Device Drivers
system	SUNWusbx	USB Device Drivers (64-bit)
system	SUNWwsr2	Solaris Product Registry & Web Start runtime support
system	SUNWxwdv	X Windows System Window Drivers
system	SUNWxwdvx	X Windows System Window Drivers (64-bit)
system	SUNWxwmod	OpenWindows kernel modules
system	SUNWxwmox	X Window System kernel modules (64-bit)

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix C: Startup scripts for sshd [8]

Startup Scripts:
Create a startup script for the ssh daemon.
/etc/init.d/ssh

```
#! /bin/sh
#
# start/stop the secure shell daemon

case "$1" in

'start')
# Start the ssh daemon
if [ -f /usr/local/sbin/sshd ]; then
echo "starting SSHD daemon"
/usr/local/sbin/sshd &
fi
;;

'stop')
# Stop the ssh deamon
PID=`/usr/bin/ps -e -u 0 | /usr/bin/fgrep sshd | /usr/bin/awk '{print $1}'`
if [ ! -z "$PID" ] ; then
/usr/bin/kill ${PID} >/dev/null 2>&1
fi
;;

*)
echo "usage: /etc/init.d/sshd {start|stop}"
;;

esac
```

Make the script executable and create a startup script on run level 2.

#**chmod +x /etc/init.d/sshd**
#ln –s /etc/init.d/sshd /etc/rc2.d/S99sshd

Create a startup script for the pseudo random generator daemon.
/etc/init.d/prngd

```
#! /bin/sh
#
# start/stop the pseudo random generator daemon
```


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
case "$1" in

'start')
# Start the ssh daemon
if [ -f /usr/local/bin/prngd ]; then
echo "starting PRNG daemon"
/usr/local/bin/prngd /var/spool/prngd/pool&
fi
;;

'stop')
# Stop the ssh deamon
PID=`/usr/bin/ps -e -u 0 | /usr/bin/fgrep prngd | /usr/bin/awk '{print $1}'`
if [ ! -z "$PID" ] ; then
/usr/bin/kill ${PID} >/dev/null 2>&1
fi
;;

*)
echo "usage: /etc/init.d/prngd {start|stop}"
;;

esac
```

Make the script executable and create a startup script on run level 2.

#**chmod +x /etc/init.d/prngd**
#ln –s /etc/init.d/prngd /etc/rc2.d/S99prngd

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

1. SANS Top 20 List. http://www.sans.org/top20/

2. E. Cole, J. Fossen, S. Northcutt and H. Pomeranz. SANS, GSEC Course Material. SANS Security Essentials with CISSP CBK, Version 2.1. February, 2003.

3. Lance Spitzner. Guide to Armoring Solaris II, 20 July 2002. http://www.spitzner.net/armoring2.html

4. Solaris Security Toolkit (JASS). http://wwws.sun.com/software/security/jass/

5. Lance Spitzner. Configuring Network Interface Cards, 17 August 1999. http://www.spitzner.net/interfaces.html

6. Lance Spitzner. Routing with Solaris, 9 March 2000. http://www.spitzner.net/routing.html

7. Krisni Naidu. SANS Firewall Checklist. http://www.sans.org/score/checklists/FirewallChecklist.pdf

8. SSH Installation for Solaris 8. http://www.unixguide.net/sun/ssh_installation.shtml

9. The Shmoo Group. FTP problems to some sites, 8 August 2000. http://www.shmoo.com/mail/fw1/aug00/msg00095.shtml

10. Solaris Security Toolkit (JASS) Documentation. http://www.sun.com/solutions/blueprints/0601/jass_internals-v03.pdf

11. Phoneboy. fwip messages, 7 March 2002. http://www.phoneboy.com/wizards/200203/msg00119.html

12. Netsys The Intelligent Hacker's Choice. Solaris syslog Man Page. http://www.netsys.com/cgi-bin/man2html?syslogd(1M)

13. Mike Shannon. CODE RED II: Caught Without a Plan. GIAC Certified Incident Handler Practical, January 2003. http://www.giac.org/practical/GCIH/Mike_Shannon_GCIH.pdf

14. Checkpoint. Passive FTP Vulnerability, 11 February 2000. http://www.checkpoint.com/techsupport/alerts/pasvftp.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced