

# 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.

# SANS GIAC Auditing Networks,Perimeters, and Systems GSNA Practical Assignment

Version 1.0  Current as of May 22,2001

Submitted By Ruangkrai Rangsiphol

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

## Checkpoint Firewall-1

**Part 1.** Research in Audit Measurement Practice, and Control

In this research project, the Checkpoint Firewall-1 is selected to be equipment for researching and auditing. Generally, Firewall is quite different from other tools in Information Security. Not only does Firewall need to protect the network, host, and data passing through, but the system itself must be configured and set up to be secure as well.

Firewall will use the Rule Base for controlling traffic, which will allow only some certain type of packets to be passing through. Normally, such rule is very much depending on the organization security policy. Certain rule will be adapted to some organization. Therefore, there is no solid standard to be widely applied for auditing the Firewall for all organization.

To verify whether Firewall reached level of standard security, the following criteria of auditing should be applied:

1. **Operating System Audit** In this research, Firewall is run on Solaris Operating System. As a result, the security of operating system could be easily effect to security of Firewall itself. Therefore, the operating system must be securely configured and dedicated to sever only for Firewall purpose.
2. **Firewall Audit** As nature of general software, there are vulnerabilities on product. As a result, the new patch always release for improving the security of Firewall itself. Therefore, there must be a procedure to audit whether the existing version is secured.
3. **Network Audit** The Rule Base must be verified whether relevant to the requirement. Even Rule Base is specified according to policy, there is a chance that the error could be caused by the set up of Administrator. The Rule Base, therefore, should be audited against what has been designed.

### Current State of Practice

In this research, the Audit Program is derived from Checkpoint Firewall Audit work Program by Terry Cavender. (terry.cavender@Vanderbilt.Edu, www.auditnet.org/docs/CheckpointFirewall.txt)
According to the questions of this Assignment:

- Why are current methods and techniques in need of improvement?
- What can be measured objectively?
- What must be measured subjectively? and
- How do you know when a system is out of specs?

In respond to the above questions, it can be classified into three criteria.

1. Improvement Needed
2. Objective Measurement
3. Subjective Measurement
4. Criteria

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

CHECKPOINT FIREWALL
AUDIT WORK PROGRAM - JANUARY 2000
Contributed January 16, 2001 by Terry Cavender (terry.cavender@Vanderbilt.Edu)

## FIREWALL LOGICAL ACCESS

STANDARD: Logical access to the various components (routers, firewall software) of the firewall solution is appropriately restricted to the individuals with an authorized need for such access.

1. Determine the individuals who have log in capability to the firewall components are appropriate.

**Improvement Needed :** The unnecessary accounts should be also included in the checklists.

**Objective Measurement :**

- By running "more /etc/passwd" command on Solaris

Sample Output

```
root:x:0:1:"Root at noah":/root:/sbin/sh
daemon:x:1:1::/:/sbin/noshell
bin:x:2:2::/usr/bin:/sbin/noshell
sys:x:3:3::/:/sbin/noshell
adm:x:4:4:Admin:/var/adm:/sbin/noshell
lp:x:71:8:Line Printer Admin:/usr/spool/lp:/sbin/noshell
uucp:x:5:5:uucp Admin:/usr/lib/uucp:/sbin/noshell
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/sbin/noshell
```

/sbin/noshell : This account have no shell , can not login . It is not user's account.
/sbin/sh : This account can login with the according shell type. It is user's account.

**Subjective Measurement :**

- After get user's account lists from objective measurement, it is needed to be determined which individual is the owner of the account and the job description of owner is appropriate or not.
- Obtain list of users who have log in capability then compare against current access authorization.

**Criteria :**

- Document of authorized users must exist.
- Current access authorization must not be against with document.
- Existing account must be only necessary for Firewall , whether they have login capability or not.

2. Determine password management features in place for the applicable firewall components and the shadow password file (etc/security/password) is used.

**Improvement Needed :** N/A

**Objective Measurement :** By running these following commands

```
# more /etc/default/passwd
# passwd -s XXXX
```

Sample output

```
# more /etc/default/passwd
# $Id: password,v 1.2 2000/03/15 06:29:14 chouanar Exp $
# Added by Titan defpwparams.sh on 200011292015
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MINWEEKS=1
MAXWEEKS=13
WARNWEEKS=4
PASSLENGTH=20

***# passwd -s XXXX***
XXXX PS 07/19/01 7 91 28
***# passwd -s YYYY***
YYYY PS 06/29/01 7 91 28

**Subjective Measurement:**
- Obtain password management policy and compare against current password management features.

**Criteria:**
- Password management policy must exist.
- Current password management features must not be against with password management policy.
- These guidelines for password management policy should be applied.

3. Determine logical connections to the firewall components are secured, e.g., encryption, IP restrictions for remote administration needs. Products such as ssh (encryption connection) and TCP wrappers (IP restrictions) may be appropriate. If TCP wrappers are used determine if the reverse look up (paranoid) option was activated (compiled). Second, determine if the advance configuration is used. This configuration keeps all the binaries in their original locations, which may be critical for future patches.

**Improvement Needed :** N/A
**Objective Measurement :**
Check whether Secured Shell running, use this command to obtain running process from host.
**# ps -ef |grep sshd**
Check whether Secured Shell running, use this command to obtain running process from host.
**# pkginfo |grep tcp_wrappers**

Check configuration of TCP Wrapper that restrict connection to firewall. Obtain host allow and host deny list on the server with the following commands.

***# more /etc/hosts.deny***
***# more /etc/hosts.allow***

4. Review for dial in access directly to the firewall server.

**Improvement Needed :** N/A
**Objective Measurement :** N/A
**Subjective Measurement :**
- Obtain list of users who have dial in capability then compare against current access authorization

**Criteria :**
If dial in to firewall is allowed:
- List of users who have dial in capability must be documented.
- Current access authorization must compile with the policy.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5. Are modems automatically disconnected by the system after a specified length of time of inactivity? After connection is broken?

**Improvement Needed :** N/A

**Objective Measurement :**

- Dial in to firewall and leave session inactivity for a period of time and see if it is automatically disconnected.

**Subjective Measurement :** N/A

**Criteria :**

If dial in to firewall is allowed:

- Modem must be disconnected automatically after ..... minutes of inactivity and after connection is broken.

## FIREWALL CONFIGURATION

STANDARD: The firewall configuration in place provides for an adequately maintained and effective firewall. Repeat each step as applicable for each firewall component.

1. Determine the firewall component logical/physical locations agree with the firewall strategy.

**Improvement Needed :** N/A

**Objective Measurement :** N/A

**Subjective Measurement :**

- Determine the physical location whether there is a appropriate protection of physical access such as location of server, location of data center, network, UPS, fire Suppression system, air conditioning system.
- Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness.

**Criteria:**

The following items must exist,

1.Secured Firewall Location, Physical network port.
2.Authenticated physical access
3.UPS
4.Fire Suppression System
5.Air Conditioner
6.Physical separation of network segment.

2. Determine the firewall components are on the latest possible version and security patches are current. Application of security patches - Is there a patch ID that equates to a certain level of applied patches. Expect patches to be applied bi-weekly, if less why.

**Improvement Needed :** N/A

**Objective Measurement :**

**Solaris** :

- The latest official Patch from Sun Microsystem can be found at http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access
- Besides, there is a Perl script for verify the patch "patchchk" which can be downloaded from ftp://sunsolve.sun.com/pub/patches/patchdiag.xref

Procedure:

At console of Solaris running theses commands

```
showrev -p > srp1
pkginfo -l > pil1
perl patchk -p pil1 srp1 <os> <arch> [<name>]
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Sample Output

```
INSTALLED PATCHES
Patch  Installed Latest   Synopsis
 ID   Revision  Revision
------ --------- -------- ------------------------------------------------------------
106327    08     CURRENT  SunOS 5.7: Shared library patch for C++
106541    12       16     SunOS 5.7: Kernel update patch
106793    05       07     SunOS 5.7: ufsdump and ufsrestore patch
106924    02       06     SunOS 5.7: isp driver patch
106925    02       07     SunOS 5.7: glm driver patch
106936    01     CURRENT  SunOS 5.7: /etc/cron.d/logchecker patch
106938    04     CURRENT  SunOS 5.7: libresolv patch
106940    01     CURRENT  SunOS 5.7: /usr/sbin/makedbm patch
```

**Firewall 1** : The Firewall 1 Latest bug report can be found at www.securityfocus.com in BugTraq Section (please see detail in Appendix A.)

a) Running command : fwver –K

Sample Output

```
This is Check Point VPN-1(TM) & FireWall-1(R) Version 4.1 Build 41814 [VPN + DES]
kernel: Version 4.1 [VPN + DES] Build 41814
```

**Subjective Measurement :** N/A

**Criterea :**
For Solaris OS, it needs to be verified as the following;

1. How many patches are not in the "Current" status.
2. How many "out-of-date" patches are security related patchs.

For Firewall-1

1. Compare actual running version against the vulnerable versions in appendix A.

3. Determine the security administrator solicits to Bugtraq and/others to be notified of the latest bugs and exploits.

**Improvement Needed:** N/A
**Objective Measurement:** N/A
**Subjective Measurement:**
Obtaining list of sources of information from administrators.
-Obtaining the bugs, exploit report last 3 months
-Verifying consistent of information form the sources versus the report.
**Criterea :**
- If there are sources of information, there must be evidences showing that the information had been reviewed

4. Identify the installation cluster used (core, end user, developer, entire distribution). Anything above end user should be explained, such as Developer, is adding potentially exploitable software (compile libraries).

**Improvement Needed:**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Firewall Server should be dedicated. Therefore any cluster that is not involved with Firewall's function should not be installed.

**Objective Measurement:**

- Verify current installed package by running "pkginfo" command on the Solaris console.

Sample Output

```
# pkginfo
application CPdtm-41      Check Point Policy Server
application CPfw1-41      Check Point VPN-1/FireWall-1
application CPgui-41      Check Point FireWall-1 GUI
system      GNUgzip       GNU gzip
system      GNUrcs        GNU rcs and diffutils
application IZzip         zip
system      PARCdaily     DailyCronJob
system      PRFtripw      tripwire
system      SECclean      Solaris 2.6, 7 and 8 Security Cleanup
```

**Subjective Measurement:** N/A

**Criteria:**

Compare pacakage list shown in the result with the recommend packaged in appendix B.

5. Obtain the /etc/inetd.conf file. Ftp and Telnet should be the only active services. If others are present determine why. Confirm what you have commented out with the following command (this will show you all the services that were left uncommented) #grep -v "^#" /etc/inetd.conf.

**Improvement Needed :**

- Actually both Telnet and FTP services are unsecured, they should not be running on the Firewall.
- This measurement shall not applicable

**Objective Measurement:** N/A
**Subjective Measurement:** N/A
**Criteria:** N/A

6. Obtain the /etc/rc2.d file. This file contains the startup scripts launched by the init(iation) process. Most of these are not needed. The following scripts are not needed and pose serious security threats:
/etc/rc2.d FILE
* S73nfs.client - used for NFS mounting a system. A firewall should never mount another file system.
* S74autofs - used for auto-mounting, a firewall should never mount another file system.
* S80lp - used for printing, your firewall should never need to print.
* S88sendmail - listens for incoming email. Your system can still send mail (such as alerts) with this disabled.
* S71rpc - portmapper daemon, a highly insecure service (required if you are running CDE).
* S99dtlogin - CDE daemon, starts CDE by default (GUI interface).

**Improvement Needed:** N/A
**Objective Measurement:**

Running following command on Solaris console.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

***# ls /etc/rc3.d***

**Subjective Measurement:** N/A

**Criteria:**

The mentioned scripts should not be found on the file .

7. Obtain the /etc/rc3.d file. More startup scripts launched by the init process are contained within. Two of these scripts are not needed.
/etc/rc3.d
* S15nfs.server - used to share file systems, which should not be done with firewalls.
* S76snmpdx - snmp daemon

**Improvement Needed:**

**Objective Measurement:**

Running following command on Solaris console

***# ls /etc/rc2.d***

**Subjective Measurement:** N/A

**Criteria:** The mentioned scripts should not be found on the file

8. If the following files are not present on the system request that they be created:
* The file /etc/issue. This file will be an ASCII text banner that appears for all telnet logins . This legal warning will appear whenever someone attempts to login to your system.
* The file /etc/ftpusers. Any account listed in this file cannot ftp to the system. This restricts common system accounts, such as root or bin, from attempting ftp sessions. The following command should create this file:
cat /etc/passwd | cut -f1 -d: > /etc/ftpusers

**Improvement Needed:**N/A .

**Objective Measurement:**

**# ls -al /etc/issue ftpusers**
**# more /etc/issue**
**# more /etc/ftpusers**

**Subjective Measurement:**
- Consider the appropriateness of the content in the banner.

**Criteria:**
- File should exist and contains proper legal warning.

9. Determine that root cannot telnet to the system. This forces administrators to login to the system as themselves and then su to root. This is a system default, but always confirm this in the file /etc/default/login, where the console command (console=/dev/console) is left uncommented.

**Improvement Needed:**

**Objective Measurement:**

Running following command,

**# more /etc/default/login |grep CONSOLE**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**Subjective Measurement:** N/A
**Criteria:**
The CONSOLE should be set to ensure that root can only login from console.

10. Determine the telnet OS banner has been eliminated and suggest creating a separate banner for ftp. For telnet, create the file /etc/default/telnetd and adding the statement:
BANNER="" # Eliminates the "SunOS 5.6" banner for Telnet

For ftp, create the file /etc/default/ftpd and add the statement:
BANNER="WARNING:Authorized use only" # Warning banner for ftp.

**Improvement Needed:**
- Actually both Telnet and FTP services are unsecured, they should not be running on the Firewall.
- This measurement shall not applicable

**Objective Measurement:**
**# more /etc/default/telnetd | Grep BANNER**
**# more /etc/default/ftpd | Grep BANNER**

**Subjective Measurement:**
- Consider the appropriateness of the content in the banner.

**Criteria:**
- File should exist and contains proper legal warning.

11. Determine if there are any compilers on the Solaris box and the need. Generally there should not be any compilers.
**Improvement Needed:**
**Objective Measurement:**
**# pkginfo**
**Subjective Measurement:**
**Criteria:**
Compiler package can be found on the 3rd column in the "pkginfo" command result. The required compiler for Firewall-1 is only SUNWlibC SPARCompilers Bundled libC. Others complier is not necessary and considers as a inappropriateness

12. Determine if these files: .rhosts, .netrc, and /etc/hosts.equiv are secured. The r commands use these files to access systems. To lock them down, touch the files, then change the permissions to zero. This way no one can create or alter the files. For example,
/usr/bin/touch /.rhosts /.netrc /etc/hosts.equiv
/usr/bin/chmod 0 /.rhosts /.netrc /etc/hosts.equiv

**Improvement Needed:**
-Any remote services should not allowed on the Firewall , this measurement would rather check whether rlogin and other "r" services are running by checking the etc/inetd.conf.

**Objective Measurement:**
**# ls -al /.rhosts /.netrc /etc/hosts.equiv**

**Subjective Measurement:** N/A

© SANS Institute 2000 - 2002, Author retains full rights.

**Criteria:**

13. Determine if the TCP initial sequence number generation parameters is randomized. This is done by setting TCP_STRONG_ISS=2 in the file /etc/default/inetinit.

**Improvement Needed:**

**Objective Measurement:**

**# more /etc/default/inetinit | grep TCP_STRING_ISS=**

**Subjective Measurement:** N/A

**Criteria:**

If TCP_STRONG_ISS parameter is set to 1, it considers as not secure. There is risk of ISN predictable and spoofed packets

14. Determine if the following lines are in /etc/system:
set noexec_user_stack=1
set noexec_user_stack_log=1
The settings protect against possible buffer overflow (or stack smashing) attacks.

**Improvement Needed:**

**Objective Measurement:**

**# more /etc/system | Grep noexec_user_stack**

Sample Output

set noexec_user_stack = 1

set noexec_user_stack_log = 1

**Subjective Measurement:** N/A

**Criterea :**

-The buffer overflow attack is a high risk, if there is no parameters setting for protect the OS. It is considerable as unsecured.

15. The rpc.cmsd subsystem of OpenWindows/CDE has been identified as a security risk. This daemon is required for the GUI interface. RPC.CMSD DAEMON should be removed.

**Improvement Needed:** The RPC service contains a lot or vulnerabilities and it is well known threat. It must be totally disabled from Firewall by getting of the portmapper services in the "rc" and the "inetd.conf".

**Objective Measurement:**

**# ps -ef|grep rpc.cmsd**

Sample output

daemon 8597 8588 0 14:42:09 pts/9 0:00 /usr/dt/bin/rpc.cmsd

root 8599 8588 0 14:42:29 pts/9 0:00 grep rpc.cmsd

**Subjective Measurement:** N/A

**Criteria:**

- If there is RPC process running on the Firewall, the output from the command will showing as indicate in the sample output.

16. Determine if the following commands have been placed in one of the start up scripts for the IP module:
### Set kernel parameters for /dev/ip

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ndd -set /dev/ip ip_respond_to_echo_broadcast 0
ndd -set /dev/ip ip_forward_directed_broadcasts 0
ndd -set /dev/ip ip_respond_to_timestamp 0
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
ndd -set /dev/ip ip_forward_src_routed 0
ndd -set /dev/ip ip_ignore_redirect 1

**Improvement Needed:**
**Objective Measurement:**

**Command and Sample output**

```
# ndd -get /dev/ip ip_respond_to_echo_broadcast
0
#  ndd -get /dev/ip ip_forward_directed_broadcasts
0
# ndd -get /dev/ip ip_respond_to_timestamp
0
# ndd -get /dev/ip ip_respond_to_timestamp_broadcast
0
```

**Subjective Measurement:** N/A
**Criteria:**
Result form running each command "0" is mean , it already running in the system.

## O/S LOGS

17. Obtain the firewall operating system configuration (/etc/syslog.conf) for rejection and logging of activities.

**Improvement Needed:**
**Objective Measurement:**
**# more /etc/syslog.conf**
**Subjective Measurement:** N/A
**Criteria:**

- From the result of the command , review the content in log file and find out security related activities such as, Unauthorized login , drop are rejected packets, daemon startup and terminated.
- Obtain the report of the response to suspects activities .

18. Document the logging results are monitored and follow up actions is performed.

**Improvement Needed:**
**Objective Measurement:** N/A
**Subjective Measurement:**

- Obtain the report of logging review.
- Verify whether any errors on log had been fixed.

**Criteria:**

- If there is no evidence showing the activities , it assumable that there is no action performed.
-

19. Determine how the system and firewall logs are rotated to reduce disk space problems. Rotation should be automatic. Document how long they are kept.

**Improvement Needed:**
**Objective Measurement:** N/A
**Subjective Measurement:**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Obtain the procedure of logs rotation.
- Obtain the report of logs backup.
- Obtains the media of backup and according report.

**Criteria:**

-There must be backup equipment, process, procedure and documents.

20. Checkpoint FireWall-1 comes with several ports open (default), such as 256, 257, and 258, and ICMP service. These ports are for administration, and found in the control properties. They should disable and rules in the database established to allow access to the server.

**Improvement Needed:**

**Objective Measurement:**

- Running this command to obtain current allowed client .

**# $FWDIR/bin/cpconfig**

-Open Firewall-1 Administration client and review current rule base.

**Subjective Measurement:** N/A

**Criteria:**

The client IP address will be showing in the output, verify that it is consistent with the authorized administrator clients.

## TEST THE FIREWALL

21. Attempt to port scan the firewall(s), from both the internal network and the Internet, scanning for ICMP, UDP and TCP. There should be no open ports and should not be able to ping it.

**Improvement Needed:**

**Objective Measurement:**

Procedure

Inbound Scan

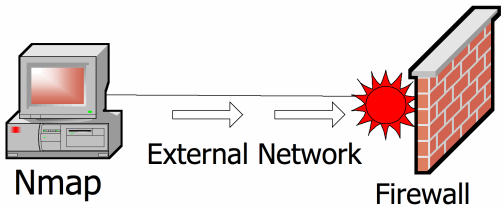
a). Install Nmap's machine at the external network

b). Fill in Nmap with the IP address of Firewall the Nmap parameter should be as followed

Nmap –v –g53 –P0 –SA –T Aggressive FirewallAddress ( For TCP)

c). Running Nmap Scan

d). Compare scanning result with the Firewall's port in Appendix C.

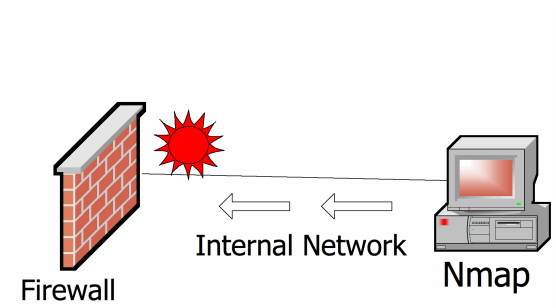



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Outbound Scan

a). Install Nmap's machine at the external network

b). Do the same as Inbound scan




**Subjective Measurement:** N/A

**Criteria:**

- Compare the result with the expected opened ports on Firewall in Appendix C.

## REVIEW & TEST THE RULE BASE DESIGN

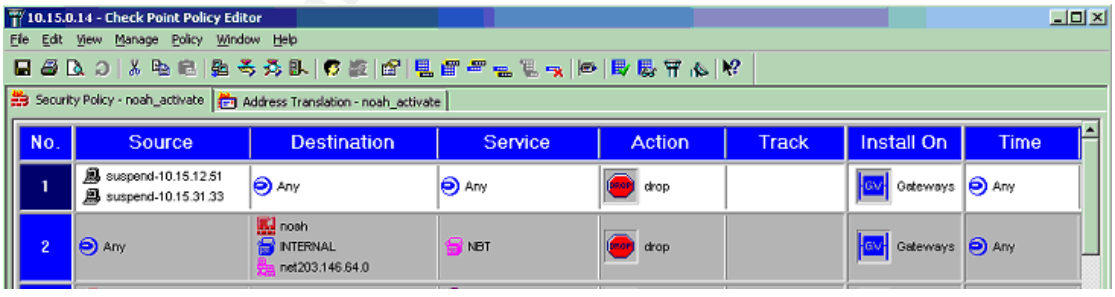
22. Determine a lockdown rule has been placed at the beginning of the rule base. The lockdown rule protects the firewall, ensuring that whatever other rules you put in later will not inadvertently compromise your firewall. If administrative access is required then a rule should be placed before the lockdown rule. All other rules should go after the lockdown rule going from most restrictive to general rules. Review the remaining rules.

**Improvement Needed:**

**Objective Measurement:**

- Running Firewall Administration Client to obtain current rule base setting.

Screen shot.




**Subjective Measurement:**

**Criteria:** The action in the first rule must be "drop", Source and Destination must be appropriate setting.

23. Obtain and review the connections table for time out limits and number of connections.

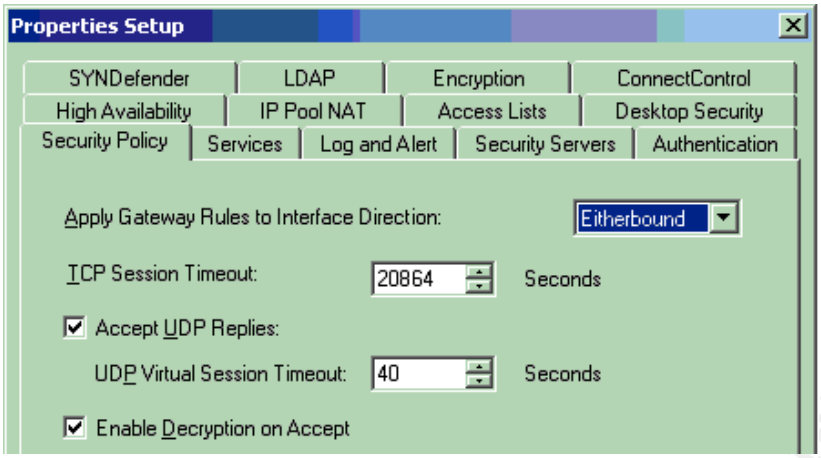
**Improvement Needed:**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**Objective Measurement:**

For determine connection time out.

- Running Firewall Administration Client to obtain current rule base setting .




For determin connection limitation,

- Running "**more table.def | grep "hashsize" "** command

**Subjective Measurement:** N/A

**Criteria:**

-The high TCP Session Time out setting will lead the high risk from being Denial of Services by fill connection table. Consider the appropriate time out according to the nature of traffics (900 sec is recommend)

- The actual connection limitation will appear in the result of the "more…" command, Consider the appropriate limitation according to the nature of traffics (50,000 connection is recommend)

24. Attempt to test the rulebase by scanning secured network segments from other network segments.

**Improvement Needed:**

**Objective Measurement:**

Procedure

a). Install Nmap's machine at the external network.

b). Select a host in internal network to be target of the scan.

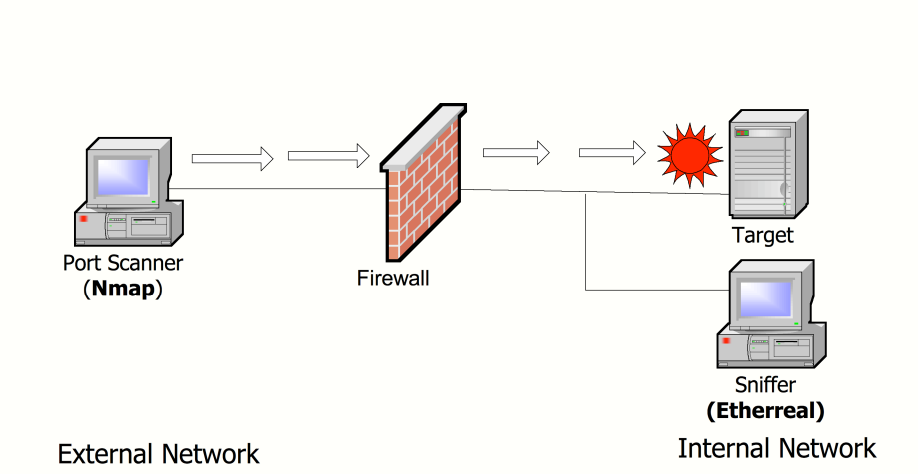
c). Determine the rulebase that control traffic to that host and created expected result from ther rulebase.

d) Fill in Nmap with the IP address of Firewall the Nmap parameter should be as followed

Nmap –v –g53 –P0 –SA –T Aggressive TargetHostAddress ( For TCP)

e) Running Nmap Scan

© SANS Institute 2000 - 2002, Author retains full rights.




**Subjective Measurement:** N/A

**Criteria:**

-Compare the scanning result with the predetermined expected result , it must be the consistent result . There might be something wrong either rulebase design or firewall itself.

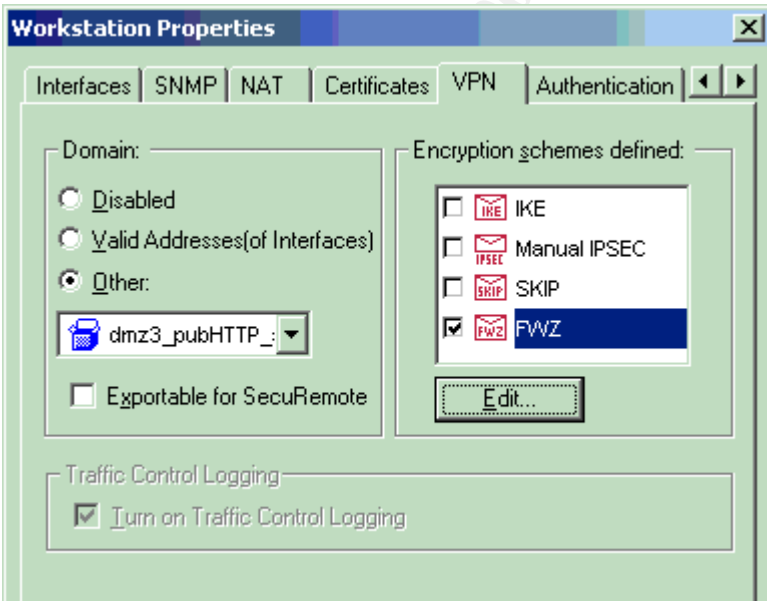
25. Identify accessible resources behind the firewall that are to be encrypted and determine the connections are encrypted. This may entail using a sniffer to capture log in data to the firewall and traffic going through the firewall.

**Improvement Needed:**

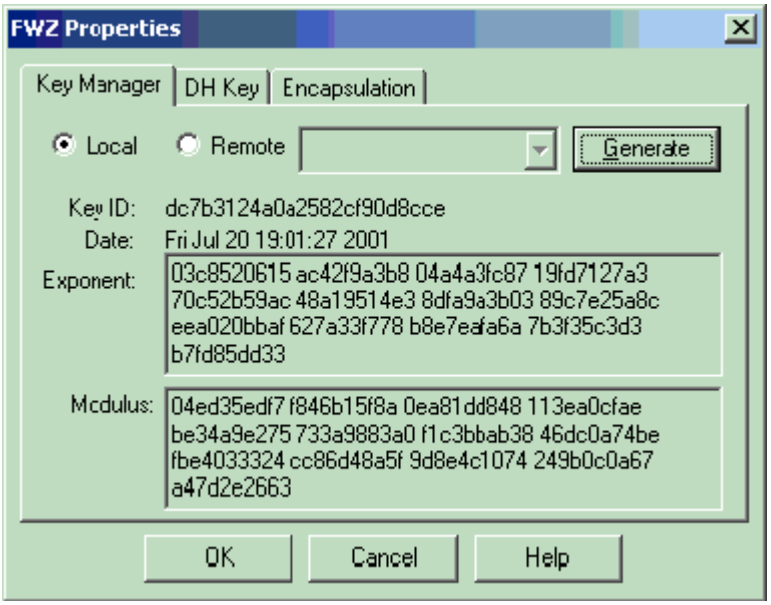
**Objective Measurement:**

- Running FW-1 Admin client , check the workstation properties which is using encryption .
- Put the TCPdump host to sniff the packets in-out the selected workstation
- Try to running "clear text" application such as Telnet within to that workstation.

Sample screen shots.




© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.




**Subjective Measurement:** N/A
**Criteria:**

- If the traffic are encrypted the results from the sniffer must be unreadable.

26. Determine if there is a change control process in place for the rule base.

**Improvement Needed:**
**Objective Measurement:** N/A
**Subjective Measurement:**

- Obtain Change Control Policy
- Verify if the following information is included in the rule:
  * Name of person modifying rule
  * Date/time of rule change
  * Reason for rule change.
- Reconcile change control record against the current rule base.

**Criteria:**

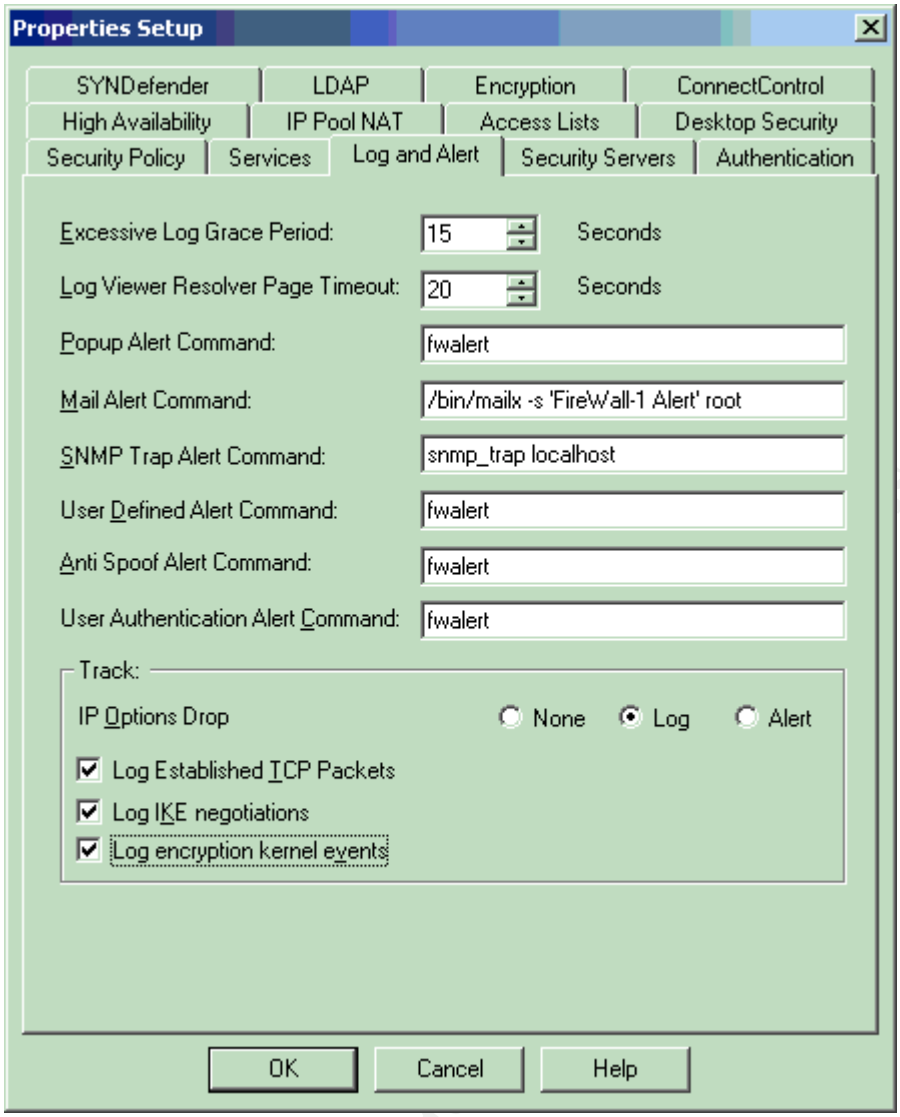
- The reconcile results must be consistent.

27. Determine the use of the firewall's automatic notification/alerting features and archiving the detail intruder information to a database for future analysis.

**Improvement Needed:**
**Objective Measurement:**

- Running Firewall Administration Client to obtain current rule base setting .

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.




- Determine alert condition, testing simulated condition and checking the alert result .

**Subjective Measurement:**

- Determine the alert condition is practical and appropriate.

**Criteria:**

- The alert command must be properly set in the Firewall set up,
- There must be alert in simulation test.

## FIREWALL APPLICATION LOGS

28. A separate partition for the firewall logging should be considered. For Checkpoint Firewall 1, all logging by default happens in /etc/fw/log and /var/opt/CKPfw/log for ver 4.0. Expect to see a second drive. If its not mirrored suggest using it for firewall logging.

**Improvement Needed:**

**Objective Measurement:**

***# df -k |grep /var/opt/CPfw1-41/log***

/dev/dsk/c0t1d0s0 8705501 3242616 5375830 38% /var/opt/CPfw1-41/log

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

***# df -k***

```
Filesystem            kbytes    used   avail capacity  Mounted on
/proc                      0       0       0     0%    /proc
/dev/dsk/c0t0d0s0    5602359  329103 5217233     6%    /
fd                         0       0       0     0%    /dev/fd
/dev/dsk/c0t0d0s3    1018382   78793  878487     9%    /var
/dev/dsk/c0t0d0s4    1018382   46970  910310     5%    /export/home
/dev/dsk/c0t1d0s0    8705501 3242616 5375830    38%    /var/opt/CPfw1-41/log
swap                  102400      24  102376     1%    /tmp
```

**Subjective Measurement :** N/A
**Criterea :** N/A

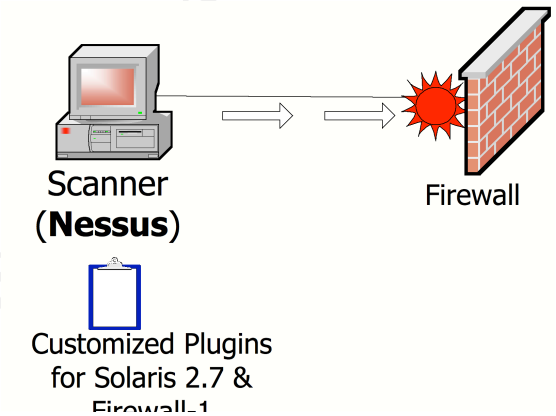
## Additional Checklist

***** The additional Checklist is recommended by Author which are not part of original checklist.*

1. Vulnerability Scanning, Vulnerability Scanning is to scan the vulnerability cause by installed configuration or administration of the OS itself. The tool for auditing is "Nessus" version 1.8 which can get from www.nessus.org and customize plugins for scanning the Solaris and Firewall 1 as shown in the Appendix D.

**Objective Measurement:**
Procedures

a). Install Nessus on Linux machine to be scanner
b). Config plugins to scan only Solaris & Firewall-1 Vulnerabilities and Denial of service as show in Appendix D.
c). Connect Nessus machine to Firewall
d). Perform Solaris scanning by Nessus
e). Get the scanning result aftter scanning finish.



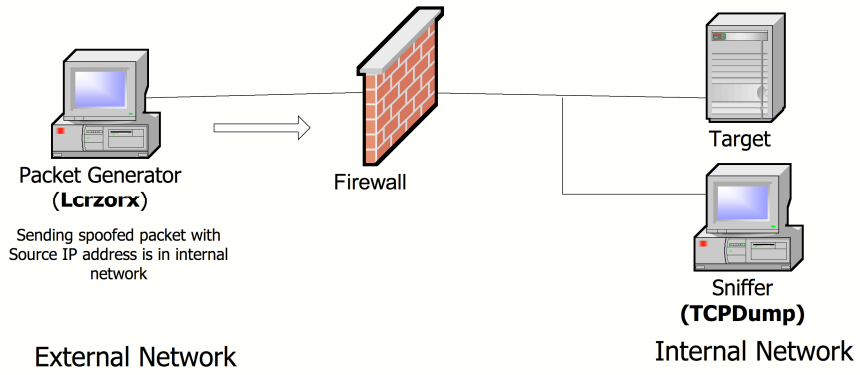

**Subjective Measurement:** N/A
**Criteria:** The scanning result from Nessus should not found any vulnerabilities remain on the Solaris and it should still be able to running as usual after being Denial of Services attacked from Nessus.

2. Spoofed Address Filtering Spoofed packets is intrusion technique which widely uses by hacker. So, Firewall must be configured properly to protect internal network from such technique.

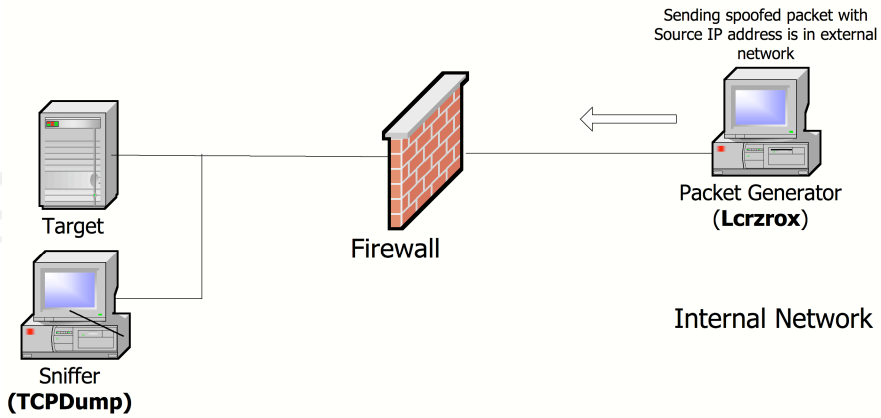
**Objective Measurement:**
Procedures

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

a). Discover network diagram , obtain valid IP and invalid IP address for each network .
b) Install Lacrzoex to be packet generator .
c) Install TCP Dump as a sniffer to detect scanning packets from Lacrzoex
d) Select destination host in internal network that allow inbound packets pass through firewall.
e) Install sniffer in the same segment with target's host .
e) Connect Lacrzoex's machine to external network
f) Running Lacrzoex to generate packet contain Invalid source IP Address to target host with the allowed port.
g) Record the result of scanning on TCPdump host




h) Select destination host in external network.
i) Install sniffer in the same segment with target's host.
j) Connect Lcrzoex's machine to internal network.
k) Config Firewall's rulebase to allow outbound packets form Lcrzoex 's host.
l) Running Lcrzoex to generate packet contain Invalid source IP Address to target host.
m) Record the result of scanning on TCPdump host.




## Output

.....

Criteria

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Spoofed IP address packets should be dropped at firewall in any interface regardless to the rulebase.

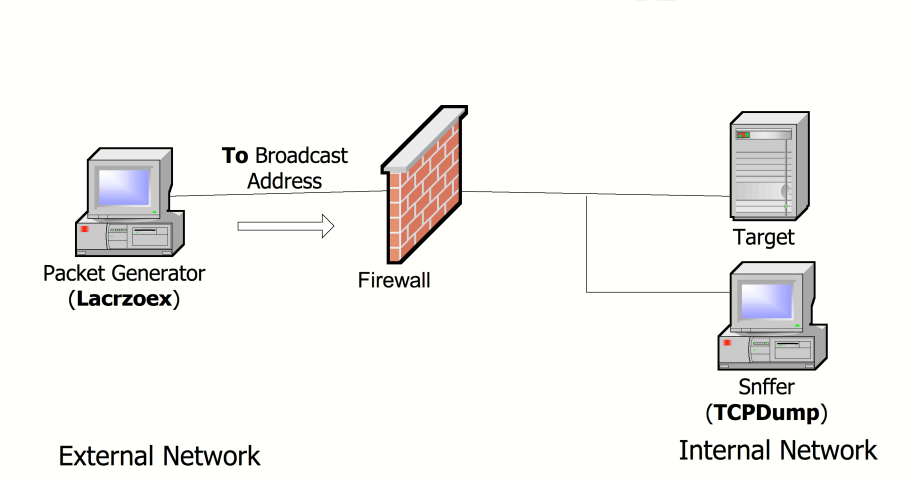
3. Broadcast Address Filtering

Broadcast packets always be used to Denial of Services or network enumeration such as Smurf Attack , Network Scanning Firewall must be configured properly to protect internal network from such packets.

**Objective Measurement**

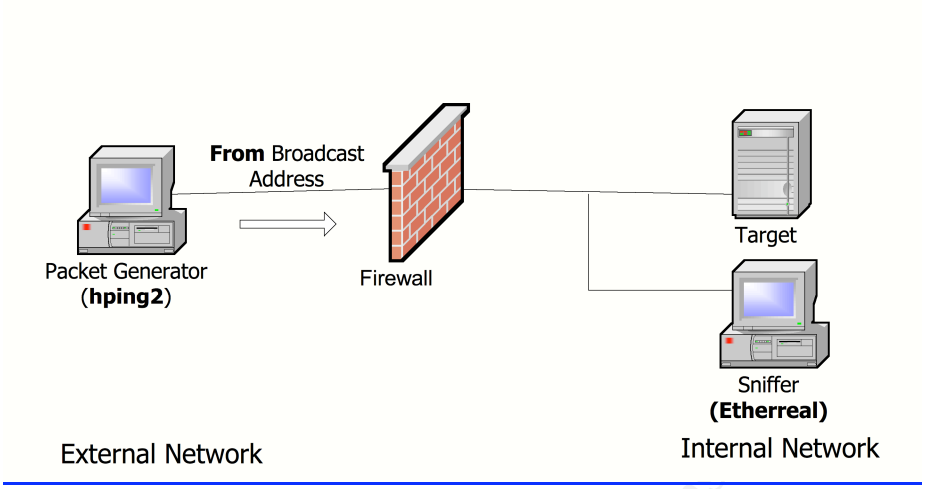
Procedures

a) Install Lacrzoex on External network
b) Select host in the internal network to be target of scanning
c) Install sniffer ( TCPDump ) machine in the same segment with target host and can sniff any in-out packets from the target host .
d) Running Lacrzoex to generate packet **to** broadcast address located in internal network , the command and parameters will be
e) Record the result of scan packets detected at TCP Dump.




f) Running Lacrzoex to generate packet **from** broadcast address located in external network, the command and parameters will be
g) Record the result of scan packets detected at TCP Dump.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.




**Subjective Measurement**

.....

**Criteria**

**There should no broadcast address packets traverse through Firewall either incoming or outgoing.**

## 4.Port Scanning with Firewalk

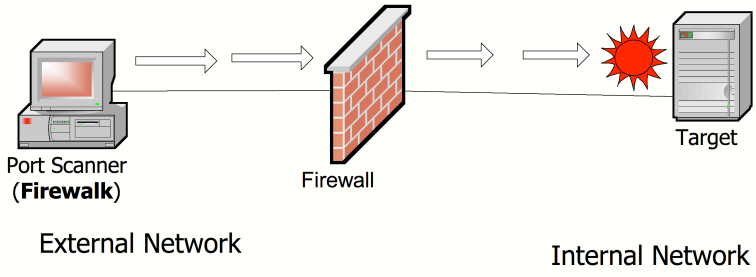
There are various techniques to penetrated the firewall. Almost (of) all Firewalls can block directed scanning such as SYN scan or FIN Scan. However the new technique always developed, using TTL is an example of advanced scanning technique. Firewalk is the Firewall scanning tools that apply TTL technique to scanning host behind Firewall.

*** Program Firewall can be searched from http://www.packetfactory.net/Projects/Firewalk/ Authors Mike D. Schiffman and David E. Goldsmith

**Objective Measurement.**

Procedures

a) Install Firewalk's machine at the external network
b) Select the target host to be scanned from Internal network
c) Create expected scanning result from the Rule Base that relate to target host.1
d) Fill in Firewalk with the IP address of Firewall and Target
e) Running Firewalk Scan
f) Compare scanning result with the expected result




© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**Subjective Measurement :** N/A
**Criteria :**

Scanning result should not different from any scanning. If there are rules to block certain type of services, Firewall should block all traffic regardless which protocol are using.

© SANS Institute 2000 - 2002, Author retains full rights.

**Part 2.** Application of Audit Technique to a Real World System

**Conduct and Evaluate the Audit**

** From the full audit checklist in assignment 1,there are 11 tests have been selected as a sample of this assignment.

**1**. Determine the individuals who have log in capability to the firewall components are appropriate.

**Result:**

```
# more /etc/passwd
root:x:0:1:"Root at noah":/root:/sbin/sh
daemon:x:1:1::/:/sbin/noshell
bin:x:2:2::/usr/bin:/sbin/noshell
sys:x:3:3::/:/sbin/noshell
adm:x:4:4:Admin:/var/adm:/sbin/noshell
lp:x:71:8:Line Printer Admin:/usr/spool/lp:/sbin/noshell
uucp:x:5:5:uucp Admin:/usr/lib/uucp:/sbin/noshell
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/sbin/noshell
listen:x:37:4:Network Admin:/usr/net/nls:/sbin/noshell
nobody:x:60001:60001:Nobody:/:/sbin/noshell
noaccess:x:60002:60002:No Access User:/:/sbin/noshell
nobody4:x:65534:65534:SunOS 4.x Nobody:/:/sbin/noshell
thirada:x:101:101::/export/home/thirada:/bin/ksh
patrol:x:102:101::/export/home/patrol:/sbin/noshell
```

**Evaluation :**

There is only user "thirada" can log in to this Firewall. With the information obtain from organization chart , he is firewall administrator, therefore it is appropriate assignment.

However ,ther are a lot of unnecessary accounts found ( lp, uucp, nuucp, listen, patrol). These accounts must be removed. It is considerable as a inappropriate administration.

**2.** Determine logical connections to the firewall components are secured, e.g., encryption, IP restrictions for remote administration needs.

**Result:**

```
#ps –ef |grep sshd
root     29277      422   0 11:48:45 ?           0:01 /usr/local/sbin/sshd
root       422        1   0      Jul 10 ?        0:00 /usr/local/sbin/sshd
root     29435   29304   0  11:52:56 pts/0       0:00 grep sshd
#pkginfo |grep tcp_wrappers
system          Wvtcpd          [Wiets Venema]  tcp_wrappers
# more /etc/hosts.deny
ALL: ALL
# more /etc/hosts.allow
sshd: 10.15.14.4 10.15.14.28
```

**Evaluation:**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The "Secured Shell" and "TCP_Wrappers" are found on the Firewall. There are restriction found in "hosts.deny" , this is evidence of restriction and encryption have been applied to this host.

**3.** Determine the firewall components are on the latest possible version and security patches are current. Application of security patches - Is there a patch ID that equates to a certain level of applied patches. Expect patches to be applied bi-weekly, if less why.

**For Check Point Firewall-1**

**Result :**

```
# fw ver -k
This is Check Point VPN-1(TM) & FireWall-1(R) Version 4.1 Build 41862 [VPN + DES]
kernel: Version 4.1 [VPN + DES] Build 41862
# 
```

**Evaluation:**

The current version of this Firewall is "Check Point VPN-1 & Firewall-1 Version 4.1 Build 41862 [VPN+DES]". This version is the latest and not vulnerable.

**For Solaris 2.7**

**Result:**

```
# perl ./patchk.pl -p pil1 srp1 5.7 sparc noah -x patchdiag.xref > result.txt
```

INSTALLED PATCHES

| Patch ID | Installed Revision | Latest Revision | Synopsis |
|---|---|---|---|
| 106327 | 08 | CURRENT | SunOS 5.7: Shared library patch for C++ |
| 106541 | 12 | 16 | SunOS 5.7: Kernel update patch |
| 106793 | 05 | 07 | SunOS 5.7: ufsdump and ufsrestore patch |
| 106924 | 02 | 06 | SunOS 5.7: isp driver patch |
| 106925 | 02 | 07 | SunOS 5.7: glm driver patch |
| 106936 | 01 | CURRENT | SunOS 5.7: /etc/cron.d/logchecker patch |
| 106938 | 04 | CURRENT | SunOS 5.7: libresolv patch |
| 106940 | 01 | CURRENT | SunOS 5.7: /usr/sbin/makedbm patch |
| 106942 | 07 | 17 | SunOS 5.7: libnsl, rpc.nisd and nis_cachemgr patch |
| 106944 | 03 | CURRENT | SunOS 5.7: /kernel/fs/fifofs and /kernel/fs/sparcv9/fifofs patch |
| 106948 | 01 | CURRENT | SunOS 5.7: /kernel/drv/qe and /kernel/drv/sparcv9/qe patch |
| 106950 | 13 | CURRENT | SunOS 5.7: Linker patch |
| 106960 | 01 | CURRENT | SunOS 5.7: Manual Pages for patchadd.1m and patchrm.1m |
| 106963 | 01 | CURRENT | SunOS 5.7: /kernel/drv/esp and /kernel/drv/sparcv9/esp patch |
| 106978 | 10 | 11 | SunOS 5.7: sysid patch |
| 106980 | 07 | 16 | SunOS 5.7: libthread patch |
| 106982 | 01 | CURRENT | SunOS 5.7: /kernel/drv/fas and /kernel/drv/sparcv9/fas patch |
| 106985 | 01 | CURRENT | SunOS 5.7: /usr/sbin/uadmin and /sbin/uadmin patch |
| 106987 | 02 | 03 | SunOS 5.7: /usr/sbin/tar patch |
| 107018 | 02 | 03 | SunOS 5.7: /usr/sbin/in.named patch |
| 107038 | 01 | 02 | SunOS 5.7: apropos/catman/man/whatis patch |
| 107059 | 01 | CURRENT | SunOS 5.7: /usr/bin/sort and /usr/xpg4/bin/sort patch |
| 107147 | 05 | 08 | Obsoleted by: 106541-14 SunOS 5.7: pci driver patch |
| 107148 | 04 | 08 | SunOS 5.7: /kernel/fs/cachefs patch |
| 107171 | 06 | 08 | SunOS 5.7: Fixes for patchadd and patchrm |
| 107185 | 01 | CURRENT | SunOS 5.7: Miscellaneous Russian KOI8-R problems |
| 107187 | 01 | 02 | SunOS 5.7: Miscellaneous Eastern European locale problems |
| 107285 | 02 | 03 | SunOS 5.7: passwd & pam library patch |
| 107316 | 01 | CURRENT | SunOS 5.7: localeconv() returns wrong results for French |
| 107330 | 01 | 02 | SunOS 5.7: /usr/sbin/ntpdate patch |
| 107332 | 02 | CURRENT | SunOS 5.7: libadm patch |
| 107401 | 01 | CURRENT | SunOS 5.7: /usr/bin/iostat patch |

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
107403  01    CURRENT  SunOS 5.7: rlmod & telmod patch
107432  03    CURRENT  SunOS 5.7: CTL printing patch
107441  01      02     SunOS 5.7: /usr/bin/mailx patch
107443  12      13     SunOS 5.7: packaging utilities patch
107448  01    CURRENT  SunOS 5.7: /usr/lib/fs/cachefs/cachefsd patch
107451  05      06     SunOS 5.7: /usr/sbin/cron patch
107453  01    CURRENT  SunOS 5.7: Ultra-80 platform patch
107454  05    CURRENT  SunOS 5.7: /usr/bin/ftp patch
107456  01    CURRENT  SunOS 5.7: /etc/nsswitch.dns patch
107458  04      13     SunOS 5.7: dad, sd, ssd, uata kernel drivers patch
107459  01    CURRENT  SunOS 5.7: qec driver patch
107460  03      09     SunOS 5.7: st driver patch
107462  01    CURRENT  SunOS 5.7: /kernel/sched/TS patch
107465  02    CURRENT  SunOS 5.7: /kernel/fs/hsfs and /kernel/fs/sparcv9/hsfs patch
107474  01    CURRENT  SunOS 5.7: ifp adb macro patch
107475  01      02     SunOS 5.7: /usr/sbin/in.telnetd patch
107477  02      03     SunOS 5.7: /usr/lib/nfs/mountd patch
107544  03    CURRENT  SunOS 5.7: /usr/lib/fs/ufs/fsck patch
107551  01    CURRENT  SunOS 5.7: /usr/bin/date and /usr/xpg4/bin/date patch
107589  03      06     SunOS 5.7: se, zs, kbd and kbio.h patch
107624  01    CURRENT  SunOS 5.7: /usr/lib/fs/ufs/df patch
107680  01    CURRENT  SunOS 5.7: /kernel/sys/msgsys and /kernel/sys/sparcv9/msgsys patch
107738  01    CURRENT  SunOS 5.7: Estonian locale uses incorrect codeset (QU)
107744  01      02     SunOS 5.7: /usr/bin/du and /usr/xpg4/bin/du patch
107746  03    CURRENT  SunOS 5.7: Croatian locale hr_HR corrections
107792  02    CURRENT  SunOS 5.7: /usr/bin/pax patch
107796  01      03     SunOS 5.7: /kernel/fs/lofs patch
107799  01      02     SunOS 5.7: compress/uncompress/zcat patch
107809  03
107836  01    CURRENT  SunOS 5.7: /usr/sbin/format patch
107841  01      03     SunOS 5.7: rpcsec patch
107843  02    CURRENT  SunOS 5.7: /sbin/init and /usr/sbin/init patch
107865  01    CURRENT  SunOS 5.7: /kernel/sys/shmsys patch
108068  03    CURRENT  SunOS 5.7: Manual Page updates for Solaris 7
108089  02      03     SunOS 5.7: /usr/bin/tail patch
108148  01    CURRENT  SunOS 5.7: prtconf patch
108158  01    CURRENT  SunOS 5.7: /usr/lib/fs/nfs/share patch
108162  01      03     SunOS 5.7: jsh, rsh, sh patch
108170  01    CURRENT  SunOS 5.7: showrev patch
108175  01    CURRENT  SunOS 5.7: DSR Upgrade patch for localization packages
108203  01      05     SunOS 5.7: adb macro & headers for fibre channel transport layer
108224  01    CURRENT  SunOS 5.7: envctrl driver patch
108244  01      02     SunOS 5.7: libaio patch
108263  01      07     SunOS 5.7: hme driver patch
108285  01    CURRENT  SunOS 5.7: /etc/init.d/MOUNTFSYS patch
108301  02    CURRENT  SunOS 5.7: /usr/sbin/in.tftpd patch
108482  02    CURRENT  SunOS 5.7: /usr/sbin/snoop patch
108662  01    CURRENT  SunOS 5.7: Patch for sadmind
108798  01      02     SunOS 5.7: /usr/bin/tip patch
108838  02    CURRENT  SunOS 5.7: allocate/mkdevmaps/mkdevalloc patch
109104  04    CURRENT  Obsoleted by: 106541-14 SunOS 5.7: /kernel/fs/sockfs patch
109253  01    CURRENT  SunOS 5.7: /usr/bin/mail patch
109744  01    CURRENT  SunOS 5.7: /usr/lib/nfs/nfsd patch
```

**Evaluation:**

There are total 85 patches found on this server , 50 patches are the latest patches , 35 are out-of-date patches .

Some out-of-date patches are security related and need to be installed.

**4.** Identify the installation cluster used (core, end user, developer, entire distribution). Anything above end user should be explained, such as Developer, is adding potentially exploitable software (compile libraries).

**Result :**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
# pkginfo
application CPdtm-41      Check Point Policy Server
application CPfw1-41      Check Point VPN-1/FireWall-1
application CPgui-41      Check Point FireWall-1 GUI
system      GNUgzip       GNU gzip
system      GNUrcs        GNU rcs and diffutils
application IZzip         zip
system      PARCdaily     DailyCronJob
system      PRFtripw      tripwire
system      SECclean      Solaris 2.6, 7 and 8 Security Cleanup
application SMCgzip       gzip
application SMCunzip      unzip
system      SUNWadmc      System administration core libraries
system      SUNWadmfw     System & Network Administration Framework
system      SUNWcar       Core Architecture, (Root)
system      SUNWcsd       Core Solaris Devices
system      SUNWcsl       Core Solaris, (Shared Libs)
system      SUNWcsr       Core Solaris, (Root)
system      SUNWcsu       Core Solaris, (Usr)
system      SUNWdfb       Dumb Frame Buffer Device Drivers
system      SUNWdoc       Documentation Tools
system      SUNWesu       Extended System Utilities
system      SUNWhmd       SunSwift SBus Adapter Drivers
system      SUNWkey       Keyboard configuration tables
system      SUNWkvm       Core Architecture, (Kvm)
system      SUNWlibC      SPARCompilers Bundled libC
system      SUNWlibms     Sun WorkShop Bundled shared libm
system      SUNWloc       System Localization
system      SUNWman       On-Line Manual Pages
system      SUNWntpu      NTP, (Usr)
system      SUNWos86u     Platform Support, OS Functionality (Usr)
system      SUNWpd        PCI Drivers
system      SUNWploc      Partial Locales
system      SUNWploc1     Supplementary Partial Locales
system      SUNWqfed      Sun Quad FastEthernet Adapter 32bit Driver
system      SUNWscpu      Source Compatibility, (Usr)
system      SUNWswmt      Install and Patch Utilities
system      SUNWter       Terminal Information
system      SUNWudfr      Universal Disk Format 1.50
system      TSIgfxdrv     GFX drivers for Solaris 2 (v2.1)
system      WVtcpd        [Wietse Venema] tcp_wrappers
#
```

**Evaluation:**

Comparing result with the Firewall-1 required packages ,there are only additional 3 packages ( GNUgzip ,GNUrcs , Izzips) found . However these packages are essential utilities, and acceptable.

**5**. Determine that root cannot telnet to the system. This forces administrators to login to the system as themselves and then su to root.

**Result:**

```
# more /etc/default/login |grep CONSOLE
CONSOLE=/dev/console
```

**Evaluation:**

The console device has been set properly.

**6.** Determine if the TCP initial sequence number generation parameters is randomized. This is done by setting TCP_STRONG_ISS=2 in the file /etc/default/inetinit.

**Result:**

```
# more /etc/default/inetinit |grep TCP_STRONG_ISS=2
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

TCP_STRONG_ISS=2

**Evaluation:**

The parameter has been configured properly.

**7.** CheckPoint FireWall-1 comes with several ports open (default), such as 256, 257, and 258, and ICMP service. These ports are for administration, and found in the control properties. They should disabled and rules in the data base established to allow access to the server.

**Result:**

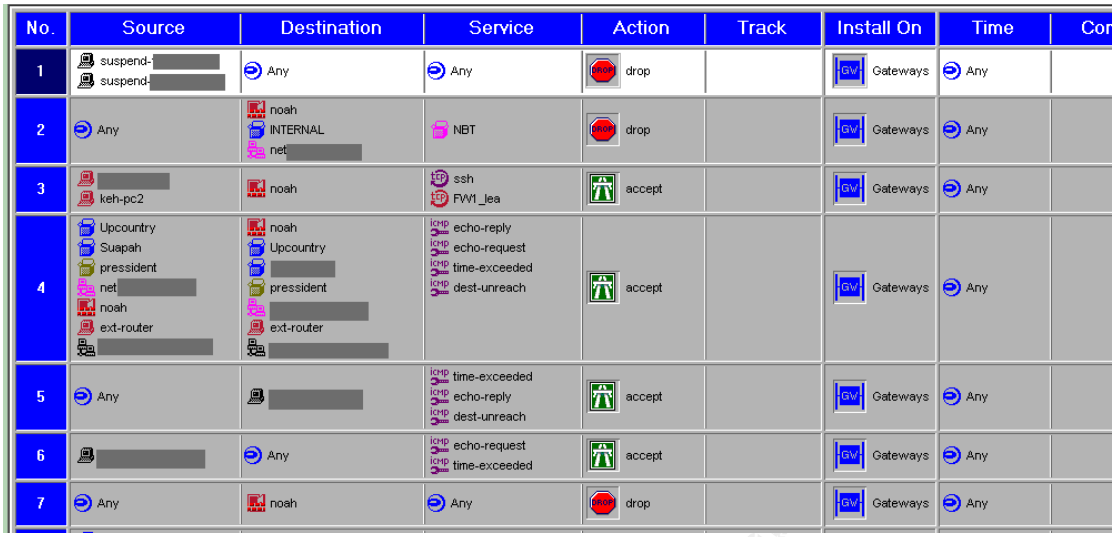
```
# $FWDIR/bin/cpconfig
Configuring GUI clients...
============================
GUI clients are trusted hosts from which
Administrators are allowed to log on to this Management Station
using Windows/X-Motif GUI.
you have selected the following hosts to be GUI clients:
10.15.14.4
10.15.14.28
```

- Review rule base screen shot from FW-1 admin client

| No. | Source | Destination | Service | Action | Track | Install On |
|---|---|---|---|---|---|---|
| - | FW1 Host | FW1 Host | FW1 | accept | | Gateways |
| - | FW1 Host | FW1 Host | FW1_log | accept | | Gateways |
| - | gui-clients | FW1 Management | FW1_mgmt | accept | | Gateways |
| - | FloodGate-1 Host | FW1 Management | FW1_ela | accept | | Gateways |
| - | Any | FW1 Host | FW1_topo | accept | | Gateways |
| - | Any | FW1 Host | FW1_key | accept | | Gateways |
| - | Any | FW1 Host | IKE | accept | | Gateways |
| - | FW1 Host | Any | IKE | accept | | Gateways |
| - | Any | Any | RDP | accept | | Gateways |

Implied rule base.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



| No. | Source | Destination | Service | Action | Track | Install On | Time | Con |
|---|---|---|---|---|---|---|---|---|
| 1 | suspend-[redacted]<br>suspend-[redacted] | Any | Any | drop | | Gateways | Any | |
| 2 | Any | noah<br>INTERNAL<br>net[redacted] | NBT | drop | | Gateways | Any | |
| 3 | [redacted]<br>keh-pc2 | noah | ssh<br>FW1_lea | accept | | Gateways | Any | |
| 4 | Upcountry<br>Suapah<br>pressident<br>net[redacted]<br>noah<br>ext-router<br>[redacted] | noah<br>Upcountry<br>[redacted]<br>pressident<br>[redacted]<br>ext-router<br>[redacted] | echo-reply<br>echo-request<br>time-exceeded<br>dest-unreach | accept | | Gateways | Any | |
| 5 | Any | [redacted] | time-exceeded<br>echo-reply<br>dest-unreach | accept | | Gateways | Any | |
| 6 | [redacted] | Any | echo-request<br>time-exceeded | accept | | Gateways | Any | |
| 7 | Any | noah | Any | drop | | Gateways | Any | |

Rule base.

**Evaluation:**

- The result from testing showing that the Firewall configuration allowed only 2 IP address to be administration clients, these 2 IP addresses are belong to administrator.

- In the rule base review, there are 2 rule base are applied to the firewall,

1. Implied rules , these are system rules that must be set in order to administrate firewall properly , these rules will be processed prior to normal rule base. There are rules specify to allow connection from administration client to connect to the Firewall.(Rule in line no.3)

2. Normal rules , these are rules that set up by administrator to control traffic pass through Firewall. There are rules to control connection to the Firewall as following,

   -No.2 : Drop all traffic from any hosts that using NBT services. **This rule is not necessary because it would be covered by Firewall lock down rule.**

   -No.3 : Allow connection from 2 Gui clients using ssh and FW1_lea services. **This rule is acceptable but must be first rule.**

   -No.4 : Allow hosts to Ping to Firewall. **This rule is inappropriate, Firewall should not response to ICMP.**

   No.7: Drop all traffic from any host to Firewall in any service. **This rule is Firewall lockdown rule it should be set before another rules , for this audit, it should be second rule.**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**8.** Attempt to port scan the firewall(s), from both internal network and the Internet, scanning for ICMP, UDP and TCP. There should be no open ports and should not be able to ping it.

TCP scanning

```
[root@furies /root]# nmap -n -sS -sR -g53 -P0 -O -t aggressive 10.15.0.14

Starting nmap V. 2.54BETA26 ( www.insecure.org/nmap/ )
Adding open port 265/tcp
Adding open port 264/tcp
Interesting ports on  (10.15.0.14):
(The 1537 ports scanned but not shown below are in state: filtered)
Port       State       Service (RPC)
113/tcp    closed      auth
264/tcp    open        bgmp
265/tcp    open        unknown
500/tcp    closed      isakmp
6699/tcp   closed      napster
20005/tcp  closed      btx
22273/tcp  closed      wnn6
22289/tcp  closed      wnn6_Cn
22305/tcp  closed      wnn6_Kr
22321/tcp  closed      wnn6_Tw
22370/tcp  closed      hpnpd

Remote operating system guess: Solaris 2.6 - 2.7 with tcp_strong_iss=2
Uptime 8.534 days (since Tue Jul 10 22:08:02 2001)
```

UDP Scanning

```
[root@furies /root]# nmap -n -sU -sR -P0 -O -t aggressive 10.15.0.14

Starting nmap V. 2.54BETA26 ( www.insecure.org/nmap/ )
Skipping host   (10.15.0.14) due to host timeout

Nmap run completed -- 1 IP address (1 host up) scanned in 300 seconds
[root@furies /root]#
```

ICMP (Ping)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
[root@furies /root]# ping -c 10 10.15.0.14
PING 10.15.0.14 (10.15.0.14) from 10.15.12.91 : 56(84) bytes of data.
64 bytes from 10.15.0.14: icmp_seq=0 ttl=254 time=932 usec
64 bytes from 10.15.0.14: icmp_seq=1 ttl=254 time=916 usec
64 bytes from 10.15.0.14: icmp_seq=2 ttl=254 time=854 usec
64 bytes from 10.15.0.14: icmp_seq=3 ttl=254 time=856 usec
64 bytes from 10.15.0.14: icmp_seq=4 ttl=254 time=938 usec
64 bytes from 10.15.0.14: icmp_seq=5 ttl=254 time=875 usec
64 bytes from 10.15.0.14: icmp_seq=6 ttl=254 time=932 usec
64 bytes from 10.15.0.14: icmp_seq=7 ttl=254 time=910 usec
64 bytes from 10.15.0.14: icmp_seq=8 ttl=254 time=928 usec
64 bytes from 10.15.0.14: icmp_seq=9 ttl=254 time=1.411 msec

--- 10.15.0.14 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.854/0.955/1.411/0.156 ms
[root@furies /root]#
```

**Evaluation:**

The result from TCP scanning showing that only port 264 and 265 are open, these ports are intentionally opened by for VPN services. The related rules can be found in rule number 7 and 8 or implied rules. This is all right.

The result from UDP scanning showing no UDP ports open.

The result from ICMP (ping) showing that Firewall response with icmp echo request. This is not secure to allow this type of packets and must be fixed. ICMP response will introduce another threats to Firewall.

**9.** Scan the vulnerability cause by installed inappropriate configuration or administration of the OS and Firewall itself. The tool for auditing is "Nessus" version 1.8 which can get from www.nessus.org and customize plugins for scanning the Solaris and Firewall 1 as shown in the Appendix D.

**Result:**

```
==================================================
Scanned hosts:

Name                    High  Low   Info
--------------------------------------------------
10.15.0.14               0    2     2
Host: 10.15.0.14
Open ports:
  unknown (264/tcp)
  unknown (265/tcp)
Service: unknown (264/tcp)
Severity: Low
The remote host seems to be a Checkpoint FW-1 running SecureRemote.
Letting attackers know that you are running FW-1 may enable them to
focus their attack or will make them change their attack strategy.
You should not let this information leak out.
Furthermore, an attacker can perform a denial of service attack on the
machine.
Solution:
Restrict access to this port from untrusted networks.
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Risk Factor: Low
For More Information:
http://www.securiteam.com/securitynews/CheckPoint_FW1_SecureRemote_DoS.html
Service: general/tcp
Severity: Low
QueSO has found out that the remote host OS is
* Standard: Solaris 2.x, Linux 2.1.???, Linux 2.2, MacOS
CVE : CAN-1999-0454
==========

**Evaluation:**

Status of this Firewall from Nessus showing that there is only low risk on ports openend on the Firewall . There is no known vulnerabilities related to Solaris or Firewall-1 found.

**10.** Spoofed Address Filtering Spoofed packets is intrusion technique which widely uses by hacker. So, Firewall must be configured properly to protect internal network from such technique.

**Result:**

Running Lacroex to spoofed packets from internal host using external IP address as a source address . ( Firewall Rule allow all outbound traffic)

```
# lcrzoex 138 eth0 00:C0:4F:BC:83:44 00:03:6B:D0:EC:40 203.xx.xx.xx 203.yy.yy.yy 555 30
Closing spoof (received : SIG2)
Closing sniff (received : SIG2)
Terminated

Result :

# tcpdump -ln ip dst host 203.yy.yy.yy and dst port 555
Kernel filter, protocol ALL, datagram packet socket
tcpdump: listening on all devices

0 packets received by filter
```

**Evaluation:**

There is no packets captured on TCPdump , Firewall could detect and drop all spoofed packets.

**11.**Port Scanning with Firewalk

There are various technique to penetrated the firewall. Almost of Firewall can block directed scanning such as SYN scan or FIN Scan. However the new technique always developed, using TTL is an efficient technique. Firewalk is the Firewall scanning tools that use technique.

**Result:**

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
[root@furies /root]# fwalk -S1-1024 -s53 -pTCP -T1 203[redacted] 203.[redacted] > /tmp/.fw.
[root@furies /root]# grep ": open" /tmp/.fw.scan ;tail -2 /tmp/.fw.scan
port  80: open
port 443: open
2 ports open, 0 ports unknown
1027 probes sent, 5 replies received
[root@furies /root]#
```

**Evaluation:**

The result showing that Firewalk found 2 TCP ports open (80,443) that is for HTTP and HTTPS server. This result is consistent with the rule base that allow these 2 inbound services. But Firewalk did not found another ports on the server that actually also open such as SMTP, FTP, NetBIOS. It is ensure that Firewall can block port scanning using TTL technique.

© SANS Institute 2000 - 2002, Author retains full rights.

## Conclusion

| Checklist | Pass | Fail |
|---|---|---|
| **1**. Determine the individuals who have log in capability to the firewall components are appropriate. | | X |
| **2.** Determine logical connections to the firewall components are secured, e.g., encryption, IP restrictions for remote administration needs. | X | |
| **3.** Determine the firewall components are on the latest possible version and security patches are current. | X | |
| **4.** Identify the installation cluster used (core, end user, developer, entire distribution). | | X |
| **5**. Determine that root cannot telnet to the system. This forces administrators to login to the system as themselves and then su to root. | X | |
| **6.** Determine if the TCP initial sequence number generation parameters is randomized. | X | |
| **7.** CheckPoint FireWall-1 comes with several ports open (default), such as 256, 257, and 258, and ICMP service. These ports are for administration, and found in the control properties. They should disabled and rules in the data base established to allow access to the server. | | X |
| **8.** Attempt to port scan the firewall(s), from both internal network and the Internet, scanning for ICMP, UDP and TCP. | | X |
| **9.** Scan the vulnerability cause by installed inappropriate configuration or administration of the OS and Firewall itself. | X | |
| **10.** Spoofed Address Filtering Spoofed packets is intrusion technique which widely uses by hacker. So, Firewall must be configured properly to protect internal network from such technique. | X | |
| **11**.Port Scanning with Firewalk | X | |

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**Direction for the future work**

1. **Time synchronization,** Time synchronization is pretty important for security especially for investigation and computer forensic. If Firewall's log has been appropriate configured, there are a lot of evidences could be found on this log. However without synchronized time, the materiality of this record might not be reliable. Therefore, in the audit checklists must be including the measurement of time synchronization maintaining process on the Firewall.
2. **High availability Firewall testing ,** as a gateway to the internet , now the availability of the Firewall is also important issue. There are a lot of High Availability products such as Stone Beat that integrate with the Firewall-1 to make it more reliable. However more components will introduce more vulnerability. There should be some certain measurements and methodology to audit this function.
3. **Integration with Intrusion Detection System,** There is a feature that allows Firewall-1 to integrate and interoperate with another security tools also IDS via the OPSEC. This will make Firewall-1 to be more "active and dynamic" defense. However, this feature needs more co-operations between firewall and other equipment, which is IDS. Thus, it needs more measurement to ensure that implementation of interoperation between firewall and IDS system is consistent and reliable. Moreover, network base IDS sometimes detect false positive events, the event that is not really malicious action; some audit measurement should be defined to test firewall in responding false positive events.
4. **Automatic Rule Base testing,** Firewall is protect the network regard to what design in Rule Base, but the Rule Base itself can be unintentionally misconfigured by the administrator. There should be some tools that can import the Firewall Rule Base and generate the scanning traffic to test against all of the rules. Therefore the result will show all condition of traffic that could pass Firewall to the protected network. Firewall-1 store the Rule Base in text file , there might be somehow to using script to enumerate all the rules and generate the scanning packets with Nmap through the Firewall to test whether each rule is protect as expectation.
5. **Performance monitoring & testing ,** In this research, there is no subjective measurement to ensure that performance of the Firewall has been properly tuned and monitored . There is also no objective measurement that can be used to measure the current performance indicator. The additional auditing criteria should be developed to cover this area. There should be some tools to perform "stress test" on the Firewall to make sure that it complies with the minimum specification.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

## Appendix A. Firewall-1 Vulnerability list .

** From BugTraq www.securityfocus.com ***

### Table 1. List by Vulnerability.

| Bugtraq ID | Details | Vulnerable |
|---|---|---|
| 2001-07-09:2952 | RDP Header Firewall Bypassing | FW-1 [ VPN+DES+STRONG] 4.1 SP2 Build 41716<br>FW-1 [ VPN+DES+STRONG] 4.1 Build 41439<br>FW-1 [ VPN+DES] 4.1 |
| 2001-01-17::2238 | Denial of Service | FW-1 4.1 SP3 + Solaris 2.6<br><br>FW-1 4.1 SP3 + Solaris 2.5.1<br>FW-1 4.1 SP2<br>FW-1 4.1 |
| 2001-01-14:2143 | Fastmode TCP Segment | FW-1 4.1 SP2 |
| 2000-11-01:1890 | Valid Username | FW-1 4.0<br><br>FW-1 3.0 |
| 2000-08-15:1662 | Session Agent Dictionary Attack | FW-1 4.1<br><br>FW-1 4.0<br>FW-1 3.0 |
| 2000-08-02:1890 | Unauthorized RSH/REXEC connection | FW-1 4.1<br><br>FW-1 4.0<br>FW-1 3.0 |
| 2000-07-05:1419 | Spoofed Source Denial of Service | FW-1 4.1<br><br>FW-1 4.0<br>FW-1 3.0 |
| 2000-06-30:1416 | SMTP Resource Exhaustion | FW-1 4.1<br><br>FW-1 4.0 |

### Table 2. List by Firewal version

| Version | Vulnerability |
|---|---|
| 4.1 SP3 + Solaris 2.6 , 2.5.1 | Denial of Service<br>Fast Mode TCP Fragment |
| 4.1 SP2 Build 41716 | RDP Header Firewall Bypassing<br>Fast Mode TCP Fragment |
| 4.1 Build 41439 | RDP Header Firewall Bypassing |
| 4.1 | RDP Heaser Firewlll Bypassing<br>Session Agent Dictionary Attack<br>Unauthorized RSH/REXEC<br>SMTP Resource Exhaustion<br>Fragmented Packet Dos |
| 4.0 | Vaild Username Vulnerability |

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

| | |
|---|---|
| | RDP Heaser Firewlll Bypassing<br>Session Agent Dictionary Attack<br>Unauthorized RSH/REXEC<br>SMTP Resource Exhaustion<br>Fragmented Packet Dos |

© SANS Institute 2000 - 2002, Author retains full rights.

## Appendix B.

*** From Armoring Solaris , Preparing solaris for firewall by Lants Spitzner , www.enteract.com/~lspitz/core7.txt

Core Packages

| | | |
|---|---|---|
| system | SUNWcar | Core Architecture, (Root) |
| system | SUNWcsd | Core Solaris Devices |
| system | SUNWcsl | Core Solaris, (Shared Libs) |
| system | SUNWcsr | Core Solaris, (Root) |
| system | SUNWcsu | Core Solaris, (Usr) |
| system | SUNWdfb | Dumb Frame Buffer Device Drivers |
| system | SUNWesu | Extended System Utilities |
| system | SUNWhmd | SunSwift SBus Adapter Drivers |
| system | SUNWkey | Keyboard configuration tables |
| system | SUNWkvm | Core Architecture, (Kvm) |
| system | SUNWlibC | Sun Workshop Compilers Bundled libC |
| system | SUNWlibms | Sun WorkShop Bundled shared libm |
| system | SUNWloc | System Localization |
| system | SUNWos86u | Platform Support, OS Functionality (Usr) |
| system | SUNWpd | PCI Drivers |
| system | SUNWploc | Partial Locales |
| system | SUNWploc1 | Supplementary Partial Locales |
| system | SUNWqfed | Sun Quad FastEthernet Adapter 32bit Driver |
| system | SUNWswmt | Install and Patch Utilities |
| system | SUNWter | Terminal Information |
| system | SUNWudfr | Universal Disk Format 1.50 |

Optional Packages

| | | |
|---|---|---|
| system | SUNWdoc | Documentation tools |
| system | SUNWman | Online Manual Pages |
| system | SUNWfns | Federated Naming System |

Security Packages

System SECclean : The core package
System GNUrcs : RCS 5.7 and diff 2.7 [GNU]
System GNUgzip : gzip 1.2.4a [GNU]
System PARCdaily
System GNUgzip and GNUrcs
System WVtcpd : tcp_wrappers 7.6 + rpcbind 2.1 [Wietse Venema]
System PRFtripw : Tripwire 1.2 [Purdue Research Foundation of Purdue University]
System OPENssh : OpenSSH 2.3.0p1 [OpenSSH.com]

Firewall Packages

| | | |
|---|---|---|
| application | CPdtm-41 | Check Point Policy Server |
| application | CPfw1-41 | Check Point VPN-1/FireWall-1 |
| application | CPgui-41 | Check Point FireWall-1 GUI |

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

**Appendix C. Firewall Ports**

***** From Which ports does Firewall-1 use ?, By Dameon D. Welch , www.phoneboy.com/faq/0105.html

- **TCP Port 256** is used for three important things:
  - Exchange of CA and DH keys in FWZ and SKIP encryption between two FireWall-1 Management Consoles
  - SecuRemote build 4005 and earlier uses this port to fetch the network topology and encryption keys from a FireWall-1 Management Console
  - When instaling a policy, the management console uses this port to push the policy to the remote firewall.
- **TCP Port 257** is used by a remote firewall module to send logs to a management console.
- **TCP Port 258** is used by the fwpolicy remote GUI.
- **TCP Port 259** is used for Client Authentication.
- **UDP Port 259** is used in FWZ encryption to manage the encrypted session (SecuRemote and FireWall-1 to FireWall-1 VPNs).
- **UDP Port 260** and UDP Port 161 are used for the SNMP daemon that Check Point FireWall-1 Provides.
- **TCP Port 264** is used for Secure Client (SecuRemote) build 4100 and later to fetch network topology and encryption keys from a FireWall-1 Management Console
- **TCP port 265**, Check Point VPN-1 Public Key Transfer Protocol. ThIs is used by FireWall-1
  to exchange public keys with other hosts.
- **UDP Port 500** is used for ISAKMP key exchange between firewalls or between a firewall and a host running Secure Client.
- **TCP Port 900** is used by FireWall-1's HTTP Client Authentication mechanism.
- **TCP Ports above 1024** are generally any Security Servers that are active. The actual ports used by these servers will vary.
- **TCP Port 18181** is used for CVP (Content Vectoring Protocol, for anti-virus scanning).
- **TCP Port 18182** is used for UFP (URL Filtering Protocol, for WebSense and the like).
- **TCP ports 18183** is used for SAM (Suspicious Activity Monitoring, for intrusion detection).
- **TCP ports 18184** is used for Log Export API (lea) .

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

## Appendix D. Solaris 2.7 and Firewall-1 Plugins for Nessus

| Id | Name |
|---|---|
| 10335 | Nmap tcp connect() scan |
| 10330 | Services |
| 10126 | in.fingerd \|command@host bug |
| 10269 | SSH Overflow |
| 10073 | Finger redirection check |
| 10675 | CheckPoint Firewall-1 Telnet Authentication Detection |
| 10676 | CheckPoint Firewall-1 Web Authentication Detection |
| 10264 | Default community names of the SNMP Agent |
| 10688 | Obtain network interfaces list via SNMP |
| 10582 | HTTP version spoken |
| 10472 | SSH Kerberos issue |
| 10337 | QueSO |
| 10550 | Obtain processes list via SNMP |
| 10068 | Finger |
| 10551 | Obtain network interfaces list via SNMP |
| 10265 | An SNMP Agent is running |
| 10223 | RPC portmapper |
| 10268 | SSH Insertion Attack |
| 10244 | ypxfrd service |
| 10243 | ypupdated service |
| 10242 | yppasswd service |
| 10241 | ypbind service |
| 10209 | X25 service |
| 10240 | walld service |
| 10239 | tooltalk service |
| 10238 | tfsd service |
| 10281 | Detect Server type and version via Telnet |
| 10237 | sunlink mapper service |
| 10236 | statmon service |
| 10249 | EXPN and VRFY commands |
| 10235 | statd service |
| 10234 | sprayd service |
| 10233 | snmp service |
| 10159 | News Server type and version |
| 10280 | Telnet |
| 10232 | showfhd service |
| 10231 | selection service |
| 10072 | Finger dot at host feature |
| 10267 | SSH Server type and version |
| 10230 | sched service |
| 10229 | sadmin service |
| 10263 | SMTP Server type and version |
| 10228 | rusersd service |
| 10227 | rstatd service |
| 10226 | rquotad service |
| 10225 | rje mapper service |
| 10653 | Solaris FTPd tells if a user exists |
| 10224 | rexd service |
| 10222 | nsemntd service |
| 10090 | FTP site exec |
| 10195 | Usable remote proxy |
| 10194 | Proxy accepts POST requests |

© SANS Institute 2000 - 2002, Author retains full rights.

10260 HELO overflow
10221 nsed service
10220 nlockmgr service
10219 nfsd service
10218 llockmgr service
10092 FTP Server type and version
10217 keyserv service
10070 Finger backdoor
10216 fam service
10087 FTP real path
10215 etherstatd service
10214 database service
10082 FTPd tells if a user exists
10607 SSH1 CRC-32 compensation attack
10213 cmsd service
10212 automountd service
10081 FTP bounce check
10211 amd service
10210 alis service
10208 3270 mapper service
10201 Relative IP Identification number change
10193 Usable remote proxy on any port
10198 Quote of the day
10069 Finger zero at host feature
10107 HTTP Server type and version
10168 Detect talkd server port and protocol version
10158 NIS server
10640 Kerberos PingPong attack
10114 icmp timestamp request
10113 icmp netmask request
10061 Echo port open
10663 DHCP server info gathering
10052 Daytime
10043 Chargen
10651 cfinger's version
10652 cfingerd format string attack
10031 bootparamd service
10192 Proxy accepts CONNECT requests
10028 Determine which version of BIND name daemon is running
10029 BIND vulnerable
10038 Cfinger's search.**@host feature
10539 Useable remote name server
10125 Imap buffer overflow
10605 BIND vulnerable to overflows
10423 qpopper euidl problem
10275 Systat
10608 OpenSSH 2.3.1 authentication bypass vulnerability
10157 netstat
10185 POP3 Server type and version
10130 ipop2d buffer overflow
10021 Identd enabled
10044 Checkpoint FW-1 identification
10617 Checkpoint SecureRemote detection
10203 rexecd
10245 rsh
10205 rlogin
10407 X Server

© SANS Institute 2000 - 2002, Author retains full rights.

10452 wu-ftpd SITE EXEC vulnerability
10464 proftpd 1.2.0preN check
10634 proftpd exhaustion attack
10084 ftp USER, PASS or HELP overflow
10086 Ftp PASV on connect crashes the FTP server
10088 Writeable FTP root
10083 FTP CWD ~root
10332 ftp writeable directories
10380 rsh on finger output
10329 BIND buffer overrun
10684 yppasswdd overflow
10279 Teardrop
10692 ftpd strtok() stack overflow
10687 Too long POST command
10271 stream.c
10544 format string attack against statd
10338 smad
10515 Too long authorization
10266 UDP null size going to SNMP DoS
10319 wu-ftpd SITE NEWER vulnerability
10320 Too long URL
10318 wu-ftpd buffer overflow
10191 ProFTPd pre6 buffer overflow
10133 Land
10190 ProFTPd buffer overflow
10074 Firewall/1 UDP port 0 DoS
10030 Bonk
10189 proftpd mkdir buffer overflow
10620 EXPN overflow
10085 Ftp PASV denial of service
10648 ftp 'glob' overflow
10374 uw-imap buffer overflow after logon
10625 IMAP4rev1 buffer overflow after logon
10197 qpopper LIST buffer overflow

© SANS Institute 2000 - 2002, Author retains full rights.

## Reference


1. Securing a Solaris Check Point Firewall , Lee R. Baker , www.sans.org/infosecFAQ/firewall/solaris_check.htm
2. Armoring Solaris , Preparing solaris for firewall By Lants Spitzner , www.enteract.com/~lspitz/amoring.html
3. Hardening Solaris, Secure installation of Bastion hosts By Sean Boran , sean@boran.com www.securityportal.com/topnets/solaris_hardening20000523.html
4. CheckPoint Firewall Audit Work Program by Terry Cavender (terry.cavender@Vanderbilt.Edu ) www.auditnet.org/docs/CheckpointFirewall.txt
5. [BugTraq ] From www.securityfocus.com
6. Auditing Routers and Firewalls By David Rhoades From SANS 2001 , Baltimore , Maryland
7. Which ports does Firewall-1 Use ? By Dameon D welch http://www.phoneboy.com/faq/0105.html
8. Solaris 7 Recommended Patch http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access


## Tools

1. Nmap download from www.insecure.org/nmap
2. Nessus by Renuad Deraison, download from www.nessus.org
3. Lacroex by Laurent Constantin, download from www.laurentconstantin.com
4. Firewalk by Mike D.Schiffman and David E.Goldsmith, download from http://www.packetfactory.net/firewalk
5. Patchcheck by Sun Microsystem inc, download from ftp://sunsolve.sun.com/pub/patches/patchdiag.xref

© SANS Institute 2000 - 2002, Author retains all rights.