

Unix Security Checklist

Prepared by: Rob Mallory
Date: Mar 20, 2003 Rev E

Machine Name: _____

security: **Restricted Distribution**
department/company:

Description

The purpose of this checklist is to raise the security level on the UNIX platforms at MedImpact. The checklist is a result of the work associated with the Hardened Solaris Jumpstart and is used as part of a "build sheet to document specific machines.

Columns in the checklist

- Priority** Every statement has a priority whose value depends on the importance to fulfill the statement from a security point of view. 1= High priority.
- True/False** The points in the checklist are normally formed as statements. One should strive for the system to fulfill the respective statement. To the right there are 2 columns, True and False, where True shall be specified if the statement is fulfilled and False shall be specified if the statement is not fulfilled. The optimal is if all points are true.
- Exceptions** Last in this document are "Priority lists". Here, the cause of a mark in the "False" square is to be given. These are indicated with a "-" priority and more information must be provided under the sub-category A1, A2, A3.

ID	Prio.	Action	True	False
1.	1	Recommended patches are installed.		
2.	1	The password file is shadowed		
3.	1	All user accounts are password protected.		
4.	1	All default accounts are password protected and any default passwords are changed.		
5.	2	All user accounts have unique user-ID (UID).		
6.	3	All UNIX groups have unique identity (GID).		
7.	1	There exist personal agreements about responsibility for each user account.		
8.	3	All user accounts not used for 2 months should be blocked automatically.		
9.	2	Password validity is limited to 3 months.		
10.	1	Passwords shorter than 8 characters are not allowed.		
11.	2	There is a delay period between unsuccessful login attempts.		
12.	2	Inactive user's screens are locked after 30 min.		
13.	1	Root is automatically logged out after 30 min.		
14.	3	A warning message about unauthorized access is given upon login.		
15.	1	All persons with access to the root password are registered on a list. This list is constrained to only Unix Sysadmins, and Security Admins.		
16.	1	There are no .rhosts file in the root directory.		
17.	1	There are no root owned files that have write permissions for normal users.		
18.	2	There are no root owned core files. Such files are cleaned once a day with cronjob.		
19.	1	"." Does not exist in the search path for root.		
20.	1	None of root's initiation files executes files owned by anyone else except root.		

ID	Prio.	Action	True	False
21.	1	Root is only allowed to log on via console, not via the network		
22.	1	No files referenced from cron, at or batch have write permissions for anyone else but the owner.		
23.	-	NFS is not used		→A1
24.	-	NIS+ is not used.		→A2
25.	-	NIS is not used.		→A3
26.	-	Sendmail is turned off.		→A4
27.	-	FTP is turned off.		→A5
28.	-	TFTP is turned off.		→A6
29.	-	The file hosts.equiv does not exist.		→A7
30.	-	No user has .rhosts files in their home directory (Alt. The file is owned by root). NOTE: all r-commands should be disabled, and replaced with ssh rsa/rhosts.		→A8
31.	1	No user has .netrc files in their home directory.		
32.	2	All unnecessary services are commented out of the inetd.conf file		
33.	2	The inetd.conf file has permissions 444.		
34.	2	The services file has permissions 444.		
35.	2	“xhost +” is not used in any script or .xsession files.		
36.	-	Uucp is not used and the account uucp is password protected.		
37.	-	No system development is performed on this machine.		
38.	1	The application does not give the user a unix shell.		
39.	2	Sticky bit is set on all directories where “world” has write permissions.		
40.	1	The machine does not give root shell without root password if it is brought down to monitor level.		
41.	1	Important log information is sent to a special log machine.		
42.	2	Files for network services, passwords and file system export are backed up.		
43.	2	SUID and SGID set files are documented and have no write permission for anyone else but the owner.		
44.	1	Responsible system administrator applies the routines in “Checklist for secure UNIX”.		
45.	2	SSH (secure shell) is used for all logins from other hosts. (including sudo)		
46.	2	All network services that the host provides are protected by TCP-wrappers.		
47.	2	Tripwire is used to fulfill the earlier requirements e.g. points 42-43.		
48.	1	Root has at least umask 022.		
49.	2	Protect the lastdb file from users.		
50.	2	Give information about the latest login upon startup		
51.	1	SNMP agent is not in use on the system		
52.	2	Unnecessary startup files have been renamed or removed		
53.	1	dtlogin is disabled.		
54.	2	The OS kernel is secured		

Basic check A1 NFS

ID.	Prio.	Action	True	False
1.	1	User and group-id are consistent between the NFS server and clients.		

2.	2	No file systems are exported outside the subnet of the NFS server.		
3.	1	The NFS server is not included in it's own access list for mounting permissions.		
4.	1	The NFS server accepts no requests from ports above 1024.		
5.	1	Only absolutely necessary file systems are exported.		
6.	1	All file system exports are made with restrictions.		
7.	2	All file systems exports are made with option "read only".		
8.	2	All file systems are mounted with option "nosuid".		
9.	1	No file systems are exported with root-access (anon=0)		
10.	1	The file for NFS export (dfstab) is owned by root with permissions 640.		
11.	1	Check of the export file (dfstab) is performed.		

Basic check A2 NIS+

ID	Prio	Action	True	False
1.	1	NIS+ is run in security level 2.		
2.	1	The network is divided into netgroups (If NFS is used).		
3.	1	All NIS+ tables are owned by root with permissions 640.		
4.	1	The library of NIS+ tables is owned by root with permissions 744.		
5.	1	Ciphered passwords in passwd.org_dir are not accessible for all users.		
6.	3	There exists a script for security backup of the NIS+ maps.		

Basic check A3 NIS

ID	Prio	Action	True	False
1.	1	All hosts in the NIS domain belong to the same subnet or to some allowed net that is pointed out.		
2.	1	The hosts are divided into netgroups (if NFS is used).		
3.	1	All NIS maps are owned by root with permissions 640.		
4.	1	This host is either a NIS client and has a line starting with + in /etc/passwd and /etc/group or it is a NIS server and does not have that.		
5.	1	All lines in /etc/passwd starting with "+" has "*" in the password field.		
6.	1	The password information of the NIS master is not included in the passwd map.		
7.	1	The information in the password map and local password file is kept consistent at password changes.		
8.	1	The NIS domain name is not easily guessed (Easy to derive from the DNS domain).		
9.	1	Specify uniquely which NIS server to use for each client. (/var/yp/binding)		

Basic check A4 sendmail

ID	Prio	Action	True	False
1.	1	The latest version of sendmail is installed		
2.	1	Sendmail log level should be at least 9		
3.	1	All programs executed from the alias file are owned by root		
4.	1	Decode is commented out		
5.	1	Root owns /etc/mail/aliases.pag & aliases.dir with permissions 644		
6.	1	Expn option turned off. Sendmail 8.12 security features used.		

Basic check A5 ftp

ID	Prio	Action	True	False
1.	1	All users which are not allowed to login via ftp, are included in the proper file		
2	1	All ftp sessions are logged on the server side		
3	1	ftp accounts are blocked from using shell		
4	1	Anonymous ftp is not used		
5	1	ftp is used with chroot		
6	1	ftp is using tcpwrappers		

Basic check A6 tftp

ID.	Prio	Action	True	False
1.	1	The safety option is set		

Basic check A7 hosts.equiv

ID.	Prio	Action	True	False
1.	1	The file is owned by root with permissions 600.		
2.	1	A net group with allowed hosts is defined and is the only reference in the file.		
3.	1	All allowed hosts belong to the same subnet as this host.		
4.	1	No line in the file begins with "#".		
5.	1	The file does not begin with "-".		

Basic check A8 \$HOME/.rhosts

ID	Prio	Action	True	False
1	1	The file is owned by root with permissions 600		
2	1	No users in .rhosts file contains a "+"		
3	1	There are only a limited amount of host names in the file		
4	1	All hosts in the file belong to the same subnet as this host.		
5	1	No line in the file begins with "#"		
6	1	The file does not begin with "-"		

Basic check A9 uucp

ID	Prio	Action	True	False
1.	1	There exists a separate account for each host that is allowed to login via uucp.		
2.	1	/usr/lib/uucp/uucico is used as login shell.		
3.	1	No files that are owned by the uucp user gives write permissions to "world".		
4.	1	The uucp user is only given access to the commands needed to perform the job.		

Basic check A10 System development environment

ID	Prio	Action	True	False
1	1	This system is not used as a production system with the same software that is developed on this machine.		
2	1	This system is not connected to any production LAN.		
3	1	This system is connected to a LAN behind a firewall.		

Basic check A11 Poroduction environment

ID	Prio	Action	True	False
1	1	The application does not give the user a UNIX shell		

Basic check A12 SNMP

ID	Prio	Action	True	False
1	1	Write is inactivated (if write has to be possible, see point 2).		
2	1	Default community name for write is substituted with a stronger one.		
3	2	Default community name for read is substituted with a stronger one.		
4	1	Possibly platform specific sub agents are identified and securely configured.		

DO NOT COPY -- Proprietary Information