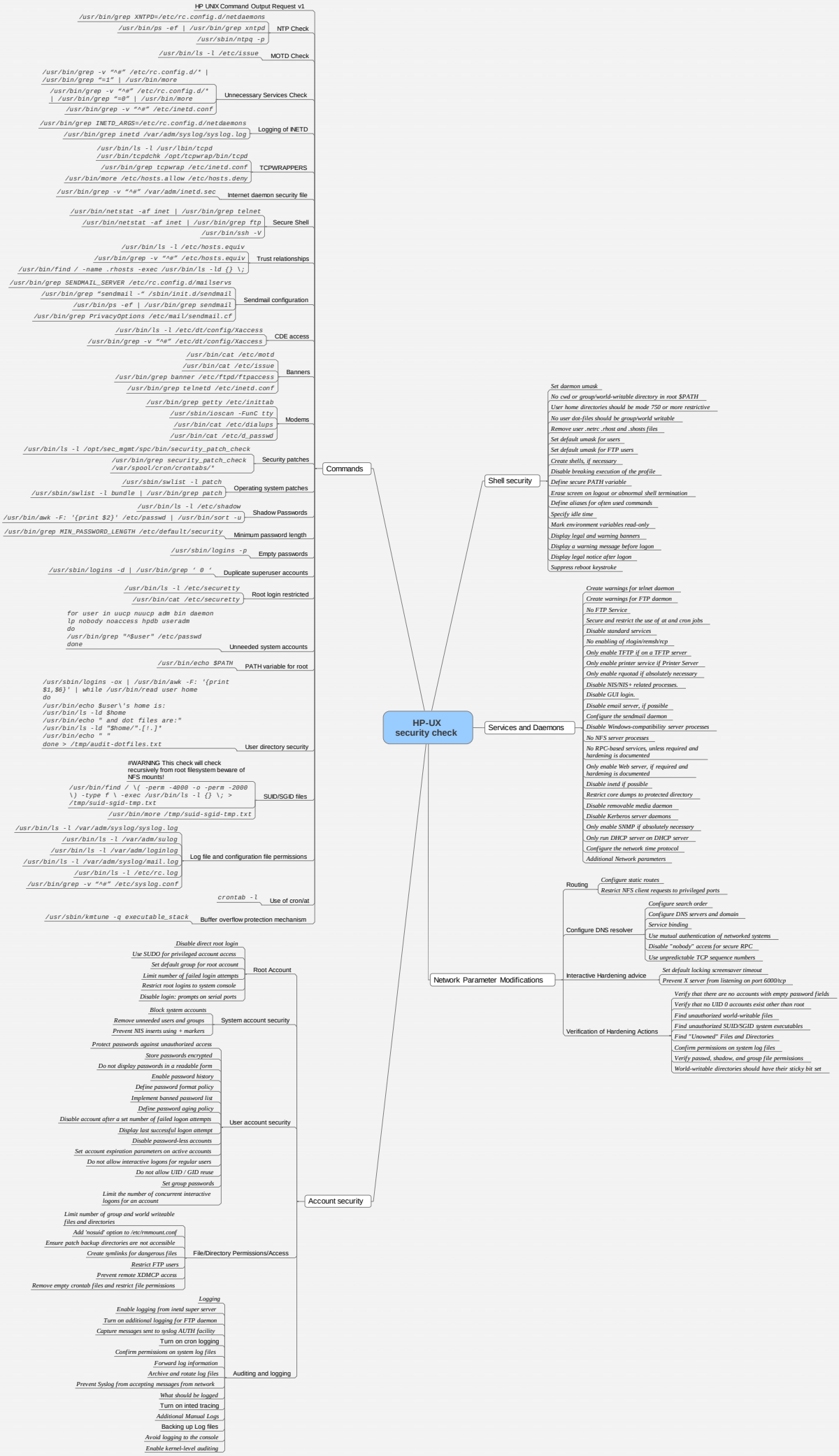
HP-UX security check
Commands
HP UNIX Command Output Request v1
/usr/bin/grep XNTPD=/etc/rc.config.d/netdaemons
/usr/bin/ps -ef | /usr/bin/grep xntpd
/usr/sbin/ntpq -p
NTP Check
/usr/bin/ls -l /etc/issue
MOTD Check
/usr/bin/grep -v "^#" /etc/rc.config.d/* |
/usr/bin/grep "=1" | /usr/bin/more
/usr/bin/grep -v "^#" /etc/rc.config.d/*
| /usr/bin/grep "=0" | /usr/bin/more
/usr/bin/grep -v "^#" /etc/inetd.conf
Unnecessary Services Check
/usr/bin/grep INETD_ARGS=/etc/rc.config.d/netdaemons
/usr/bin/grep inetd /var/adm/syslog/syslog.log
Logging of INETD
/usr/bin/ls -l /usr/lbin/tcpd
/usr/bin/tcpdchk /opt/tcpwrap/bin/tcpd
/usr/bin/grep tcpwrap /etc/inetd.conf
/usr/bin/more /etc/hosts.allow /etc/hosts.deny
TCPWRAPPERS
/usr/bin/grep -v "^#" /var/adm/inetd.sec
Internet daemon security file
/usr/bin/netstat -af inet | /usr/bin/grep telnet
/usr/bin/netstat -af inet | /usr/bin/grep ftp
/usr/bin/ssh -V
Secure Shell
/usr/bin/ls -l /etc/hosts.equiv
/usr/bin/grep -v "^#" /etc/hosts.equiv
/usr/bin/find / -name .rhosts -exec /usr/bin/ls -ld {} \;
Trust relationships
/usr/bin/grep SENDMAIL_SERVER /etc/rc.config.d/mailservs
/usr/bin/grep "sendmail -" /sbin/init.d/sendmail
/usr/bin/ps -ef | /usr/bin/grep sendmail
/usr/bin/grep PrivacyOptions /etc/mail/sendmail.cf
Sendmail configuration
/usr/bin/ls -l /etc/dt/config/Xaccess
/usr/bin/grep -v "^#" /etc/dt/config/Xaccess
CDE access
/usr/bin/cat /etc/motd
/usr/bin/cat /etc/issue
/usr/bin/grep banner /etc/ftpd/ftpaccess
/usr/bin/grep telnetd /etc/inetd.conf
Banners
/usr/bin/grep getty /etc/inittab
/usr/sbin/ioscan -FunC tty
/usr/bin/cat /etc/dialups
/usr/bin/cat /etc/d_passwd
Modems
/usr/bin/ls -l /opt/sec_mgmt/spc/bin/security_patch_check
/usr/bin/grep security_patch_check
/var/spool/cron/crontabs/*
Security patches
/usr/sbin/swlist -l patch
/usr/sbin/swlist -l bundle | /usr/bin/grep patch
Operating system patches
/usr/bin/ls -l /etc/shadow
/usr/bin/awk -F: '{print $2}' /etc/passwd | /usr/bin/sort -u
Shadow Passwords
/usr/bin/grep MIN_PASSWORD_LENGTH /etc/default/security
Minimum password length
/usr/sbin/logins -p
Empty passwords
/usr/sbin/logins -d | /usr/bin/grep ' 0 '
Duplicate superuser accounts
/usr/bin/ls -l /etc/securetty
/usr/bin/cat /etc/securetty
Root login restricted
for user in uucp nuucp adm bin daemon
lp nobody noaccess hpdb useradm
do
/usr/bin/grep "^$user" /etc/passwd
done
Unneeded system accounts
/usr/bin/echo $PATH
PATH variable for root
/usr/sbin/logins -ox | /usr/bin/awk -F: '{print
$1,$6}' | while /usr/bin/read user home
do
/usr/bin/echo $user\'s home is:
/usr/bin/ls -ld $home
/usr/bin/echo " and dot files are:"
/usr/bin/ls -ld "$home/".[!.]*
/usr/bin/echo " "
done > /tmp/audit-dotfiles.txt
User directory security
#WARNING This check will check
recursively from root filesystem beware of
NFS mounts!
/usr/bin/find / \(-perm -4000 -o -perm -2000
\) -type f \ -exec /usr/bin/ls -l {} \; >
/tmp/suid-sgid-tmp.txt
/usr/bin/more /tmp/suid-sgid-tmp.txt
SUID/SGID files
/usr/bin/ls -l /var/adm/syslog/syslog.log
/usr/bin/ls -l /var/adm/sulog
/usr/bin/ls -l /var/adm/loginlog
/usr/bin/ls -l /var/adm/syslog/mail.log
/usr/bin/ls -l /etc/rc.log
/usr/bin/grep -v "^#" /etc/syslog.conf
Log file and configuration file permissions
crontab -l
Use of cron/at
/usr/sbin/kmtune -q executable_stack
Buffer overflow protection mechanism
Shell security
Set daemon umask
No cwd or group/world-writable directory in root $PATH
User home directories should be mode 750 or more restrictive
No user dot-files should be group/world writable
Remove user .netrc .rhost and .shosts files
Set default umask for users
Set default umask for FTP users
Create shells, if necessary
Disable breaking execution of the profile
Define secure PATH variable
Erase screen on logout or abnormal shell termination
Define aliases for often used commands
Specify idle time
Mark environment variables read-only
Display legal and warning banners
Display a warning message before logon
Display legal notice after logon
Suppress reboot keystroke
Services and Daemons
Create warnings for telnet daemon
Create warnings for FTP daemon
No FTP Service
Secure and restrict the use of at and cron jobs
Disable standard services
No enabling of rlogin/remsh/rcp
Only enable TFTP if on a TFTP server
Only enable printer service if Printer Server
Only enable rquotad if absolutely necessary
Disable NIS/NIS+ related processes.
Disable GUI login.
Disable email server, if possible
Configure the sendmail daemon
Disable Windows-compatibility server processes
No NFS server processes
No RPC-based services, unless required and hardening is documented
Only enable Web server, if required and hardening is documented
Disable inetd if possible
Restrict core dumps to protected directory
Disable removable media daemon
Disable Kerberos server daemons
Only enable SNMP if absolutely necessary
Only run DHCP server on DHCP server
Configure the network time protocol
Additional Network parameters
Network Parameter Modifications
Routing
Configure static routes
Restrict NFS client requests to privileged ports
Configure DNS resolver
Configure search order
Configure DNS servers and domain
Service binding
Use mutual authentication of networked systems
Disable "nobody" access for secure RPC
Use unpredictable TCP sequence numbers
Interactive Hardening advice
Set default locking screensaver timeout
Prevent X server from listening on port 6000/tcp
Verification of Hardening Actions
Verify that there are no accounts with empty password fields
Verify that no UID 0 accounts exist other than root
Find unauthorized world-writable files
Find unauthorized SUID/SGID system executables
Find "Unowned" Files and Directories
Confirm permissions on system log files
Verify passwd, shadow, and group file permissions
World-writable directories should have their sticky bit set
Account security
Root Account
Disable direct root login
Use SUDO for privileged account access
Set default group for root account
Limit number of failed login attempts
Restrict root logins to system console
Disable login: prompts on serial ports
System account security
Block system accounts
Remove unneeded users and groups
Prevent NIS inserts using + markers
User account security
Protect passwords against unauthorized access
Store passwords encrypted
Do not display passwords in a readable form
Enable password history
Define password format policy
Implement banned password list
Define password aging policy
Disable account after a set number of failed logon attempts
Display last successful logon attempt
Disable password-less accounts
Set account expiration parameters on active accounts
Do not allow interactive logons for regular users
Do not allow UID / GID reuse
Set group passwords
Limit the number of concurrent interactive logons for an account
File/Directory Permissions/Access
Limit number of group and world writeable files and directories
Add 'nosuid' option to /etc/rmmount.conf
Ensure patch backup directories are not accessible
Create symlinks for dangerous files
Restrict FTP users
Prevent remote XDMCP access
Remove empty crontab files and restrict file permissions
Auditing and logging
Logging
Enable logging from inetd super server
Turn on additional logging for FTP daemon
Capture messages sent to syslog AUTH facility
Turn on cron logging
Confirm permissions on system log files
Forward log information
Archive and rotate log files
Prevent Syslog from accepting messages from network
What should be logged
Turn on inted tracing
Additional Manual Logs
Backing up Log files
Avoid logging to the console
Enable kernel-level auditing