John Diamant
Hewlett-Packard
May 2001

HP-UX Security Hardening/Lockdown Management Tools/Resources

Contact Info:

John Diamant
Manageability Solutions Lab
Hewlett-Packard Company
Mail Stop 99
3404 East Harmony Rd.
Ft. Collins, CO 80528
(970)898-3528 (voice)
(970)898-2838 (fax)
john_diamant@hp.com

Hardening Lockdown Tools/Resources

- Building a Bastion Host using HP-UX - by Kevin Steves
  - Whitepaper
  - http://people.hp.se/stevesk/bastion.html
  - Versions for HP-UX 10.20 and 11.0
- **new** Security Patch Check tool
  - Assists with one of first hardening/lockdown steps you should take
  - http://software.hp.com, under "Internet & Security"
  - Free tool

Bastion Host Whitepaper Overview

- Useful for locking down machines (e.g. servers) that need to be protected, even if they don't meet the strictest definition of a Bastion host
- Describes a procedure for setting up such a system, including lockdown of security vulnerabilities
- Topics covered
  - Definition of Bastion host
    - Highly fortified machine at great risk of attack (e.g. reachable from public Internet)
  - Methodology
    - Limit machine to it's key functions,
    - reduce or eliminate all other exposures to the degree practical
  - Procedure
    - Described in subsequent slides

Bastion Host Whitepaper Procedure Outline

- Install HP-UX
- Install Additional Products
- Install Support Plus Bundle
- Install Security Patches
- First Steps
- Disable Network Services
- Disable Other Daemons
- Examine Set-id Programs
- Examine File Permissions
- Security Network Tuning
- Install Software and Test Configuration
- Create System Recovery Tape

Details in the whitepaper on the web

1 Install HP-UX

- Install only what you need

2 Install Additional Products

- Install needed drivers and software packages needed on this server.

3 Install Support Plus Bundl

- Install appropriate patch bundle

4 Install Security Patches

- Use Security Patch Check
- Review Advisories/Bulletins

5 First Steps

- Convert to a trusted system
- Set default umask
- Enable inetd logging
- More covered in paper

6 Disable Network Services

- Disable all services not required for this machine to function as desired

7 Disable Other Daemons

- Some daemons may not be required for normal operation

8 Examine Set-id Programs

- Find all setuid/setgid programs
- Remove setuid/setgid bit when not needed

9 Examine File Permissions

- Tighten some permissions

10 Security Network Tuning

- Check and set tuning parameters.

11 Install Software and Test Config

- Simulate a production environment
- Make adjustments as necessary

12 Create System Recovery Image

- Use make_recovery or make_net_recovery to save an image of the hardened system

Security Patch Check
Why stay current on security patches?

- Hackers monitor security email lists too.
- Some security weaknesses can only be fixed by patching.
- "Data from the Honeynet Project suggest that almost 80 percent of all un-patched servers wouldn't last more than three weeks before being compromised by Internet attackers"
- "Failing to responsibly patch computers led to 99 percent of the 5,823 Web site defacements last year, up 56 percent from the 3,746 Web sites defaced in 1999, according to security group Attrition.org"

http://www.zdnet.com/zdnn/stories/news/0,4586,2677878,00.html

- "The volume of reports describing successful attacks on systems with known security flaws, and whose vendors have already issued patches (often quite some time ago) is growing. Fast. The number of automated attacks--readily usable by the script kiddie demographic--that exploit these known and publicized vulnerabilities is on the rise as well."

http://www.zdnet.com/zdnn/stories/news/0,4586,2696130,00.htm

Security Patch Check
What is it?

- A Perl script that runs on HP-UX 11.X systems.
- Analyzes the file sets and patches on an HP-UX system.
- Generates a report of recommended security patches for the system.
- Warns about recalled patches present on the system.
- Free!
- Support is covered by HP-UX support contract
- Satisfies a significant pent-up demand
- Beta users have been enthusiastic

Security Patch Check Requirements

- Requires Perl, version 5.005 or higher. Perl is available at http://devresource.hp.com/OpenSource/Tools/Perl.html
- Requires lib_www_perl (LWP) module to download security patches. Comes with above.
- Security Patch Check
  - Download it from http://software.hp.com in “Internet & Security”

Security Patch Check
How To Run

- Requires ability to run swlist command (so you may want to limit this with swacl to only authorized systems/users)
- Uses a security patch catalog
  - Downloaded by security_patch_check automatically or
  - Manually before running.
- Can be run:
  - From the command line.
  - Automated via cron (recommended -- nightly)
  - Via Service Control Manager (cron or manual)

Security Patch Check Command Line Options

- -h Used to analyze a remote host.
  - Use a central server to examine many machines
- -r Used to retrieve the latest patch catalog.
- -o Alter the information that is printed.
- -c Location of the security patch catalog.
- -m Produce a machine-parsable output.
  - Allows adding your own automation
- -f Take input from a file
  - Used to analyze a depot
  - Used to analyze swlist output from a remote host.

Security Patch Check
Sample Output

- WARNING: ./security_catalog is group or world writable.
- WARNING: SG-Ext-SAP-R3.SG-SAP-TPL has a state of installed. The state should be "configured" or "available" (see swconfig(1M) or reinstall and configure SG-Ext-SAP-R3.SG-SAP-TPL).
- WARNING: Recalled patch PHCO_20443 is active on the target system. Its record, including the Warn field, is available from ./security_catalog, through the Patch Database area of the ITRC or by using the -m flag (security_patch_check -m ...).
- NOTE: Recalled patch PHCO_14044 is present, but superseded by PHCO_22096 on the target system. If patch PHCO_22096 is ever removed, patch PHCO_14044 will become active. Read the recall notice to make the right decision for your situation. Patch recall notices can be seen using the security_patch_check -m option, through the Patch Database area of the ITRC, or from within ./security_catalog.

Security Patch Check
Sample Output (continued)

List of recommended patches for most secure system:

#	Recommended	Bull(s)	Spec?	Reboot?	Pdep?	Description
1	PHCO_21534	113	No	No	No	patch for shutdown(1M)
2	PHCO_21993	130	No	No	No	auto_parms/set_parms
3	PHCO_22274	127	No	No	No	bdf(1M) cumulative
4	PHCO_22276	127	No	No	Yes	df(1M) cumulative
5	PHCO_22365	125	No	No	No	lpspool subsystem cumulative

.... Snipped....

Security Patch Check Catalog Retrieval

- Can be done manually if necessary but limits effectiveness.
  - ftp://ftp.itrc.hp.com/export/patches/security_catalog
  - Note that IE can be confused by files without extensions
- Automatic Download Preferred.
  - Patches announced daily
  - Patch catalog updated daily
- Security Patch Check can download through a firewall using $ftp_proxy.
  - Must set ftp_proxy environmental variable.
    - For Example:

```
ftp_proxy=http://proxy.company.com:8088
export ftp_proxy
security_patch_check –r
```

Security Patch Check
Checking Other Systems

- Security Patch Check can review other systems
  - Use the –h option
  - Must have permission to run swlist on the other systems (see man pages and README)
- Checking systems through a firewall
  - Need TCP access on port 2121
  - Need to configure swagentd for negotiated ports. HP Response Center or Application Support Engineer can help.
  - Make sure you aren't granting remote swagentd access to unintended parties, though.

Security Patch Check
Getting the Output

- Everything is sent to STDOUT or STDERR for versatility.
- Pipe the output where you want it to go.
  - > /home/secofr/patch_report.txt 2>&1
  - 2>&1 |mailx secofr@company.com
- Tip
  - Run Security Patch Check interactively the first time. You need to accept the disclaimer.

Security Patch Check
What It Will Not Do

- It will not make your system secure.
  - Though it will improve system security
- It will not avoid the need to review all relevant security bulletins and advisories for manual actions -- it only covers patches
- It will not reconfigure your system.
- It will not install patches automatically.
- It will not download patches automatically.
- It will not introduce insecurities into your system.

Security Patch Check Attributes

- Cost - free
- Effort – small
- Security – definite increase
- Disk space – minimal
- Performance Impact - none

Summary

- Tools and resources are available to lockdown/harden security of HP-UX systems
- Bastion Host Whitepaper
  - http://people.hp.se/stevesk/bastion.html
- **new** Security Patch Check tool
  - http://software.hp.com, under "Internet & Security"