System Security Policy & Practical Lockdown with Bastille

Jay Beale

Security Consultant
JJB Security Consulting, LLC

Tyler Easterling

Software Engineer
Hewlett Packard

HP WORLD 2003
Solutions and Technology Conference & Expo

Today's Agenda

- Why should you harden an operating system?
- What is hardening?
- How do I harden an operating system?
- Why should I use Bastille to harden a system?
- How is HP using Bastille?
- What does Bastille do, module by module?
- Hands-on with Bastille

Why do I need to harden?

Hardening is the process of tweaking system configuration settings for greater resilience to attack.

But why should **you** harden a system?

Why Should You Defend?

The first objection that we normally face to hardening is that people think they'll never be attacked.

They think they're not interesting enough or high-value enough to be targeted.

But they get attacked and compromised – why?

Why Do They Get Attacked?

Most of the crackers/hackers out there are low-skill “script kiddies.”

They download tools from the Internet, including, say, 10 exploits.

One or two of those exploits actually work. (Why?)

Why Do They Get Attacked?

Exploit creators often cripple an exploit so only someone with strong technical skills can use it.

So, our script kiddie gets one or two exploits working.

He then sets up automated scans of large swaths of the Internet, looking for vulnerable systems.

(Think 1-10 class B's, maybe 65,536 - 655,360 hosts)

He goes to bed. In the morning, he has 100-1000 hosts, easy, that he can compromise.

These are called "targets of opportunity."

Targets of Opportunity?

Our script kiddie can't hack just any site.

He has to attack one that is vulnerable.

Now, what about the skilled crackers, those who hit targets of choice?

He might hack us just to use us for bandwidth or to obfuscate his source from his real target.

Some attackers ocean-hop to avoid detection…

So We Will Be Targeted.

So we will be targeted at some point.

It would be best not to be vulnerable!

We can’t guarantee that, but we can definitely better our odds.

We can start by patching systems, but this isn’t enough.

Why is this not enough? Because it is reactive.

Reactive Security

Much of our security effort/time is spent reacting to security vulnerabilities:

- Patching hosts against new vulnerabilities
- Reactive firewalling
- Incident response

Patching

- We apply a huge number of patches each year to operating systems, applications and networking hardware.
- Even if we're diligent about patching, it's not good enough – we still had windows of vulnerability.

Lifecycle of a Vulnerability

- Step 1: Someone finds a bug in a program
- Step 2: Someone discovers that the bug is a security vulnerability.
- Step 3: Someone writes an exploit to compromise machines with this vulnerability.

The vulnerability AND/OR the the exploit **may** be released publicly after any of these steps.

Windows of Vulnerability

Window of Vulnerability (n):

The time period in which someone has a working exploit and our systems are still vulnerable.

Patching Isn’t Enough!

These windows of vulnerability provide times when attackers can compromise our systems.

It’s not enough to hope these aren’t too long. We should be working proactively to lessen our probability of being attacked.

Reactive Security?

A reactive security practice leaves you constantly playing the odds, hoping that your next window of vulnerability won’t be the one where you get attacked.

- Reactive firewall configuration
- Incident Response

Proactive Security

You can massively lessen your odds of being successfully compromised by:

- Configuring your hosts and your network to decrease their odds of being successfully hacked. (Hardening)
- Intelligently choosing policies ahead of time.

What is Hardening?

Hardening is the process of configuring a system for increased security.

It **does** involve deactivating unnecessary programs and auditing the configurations of those that remain.

It **does not** involve kernel-level modification of the system, along the lines of SELinux, Pitbull, or Trusted BSD/Solaris.

What is Hardening? 2/2

It **does** involve auditing the permissions and/or file access control lists and considering whether permissions are appropriate or too lax.

It **does** involve tweaking core operating system parameters to give users only what access they need, to the extent that the operating system allows this.

Let’s be more specific, though.

Principles of System Hardening

Basically, system hardening comes down to tuning an operating system and its applications for Least Privilege and Minimalism.

Least Privilege – each application or O/S component grants only what privilege each user type needs.

Minimalism – we configure the software for as few features as possible, to better our chances of not having vulnerable functionality active.

System Hardening: Practice

- Deactivate all system programs that aren’t being used. (minimalism)
- Configure all remaining system programs for least privilege and functionality minimalism.
- Audit permissions/ACL’s for least privilege.

Difficulty

This work isn’t as difficult as it might sound.

- Bastille targets inexperienced sysadmins and does the “grunt work” for them.
- CIS’s Best Practices benchmarks are written for simplicity.
- There are week-long training programs that are comprehensive – you can do this by hand.

Is Hardening Effective?

Hardening can be extremely effective at avoiding vulnerabilities.

Examples:

- NSA’s Test of CIS’s Guides
- Bastille Linux’s test on Red Hat 6.0

Center for Internet Security

The Center for Internet Security produces system hardening guides. The NSA’s Information Assurance Directorate evaluated a system locked-down following CIS’s Windows 2000 guide. **90 percent** of all the vulnerabilities in this platform were mitigated by the guide.

CIS’s guides are simple industry best-practices – they’re not groundbreaking. They simply apply the same principles that you’ve seen here.

Bastille Linux/HP Bastille

Bastille is a programmatic solution that we’re showing you today.

Bastille was written right after the release of Red Hat 6.0, before any vulnerabilities were discovered and published.

It could stop or contain almost every publicly released exploit.

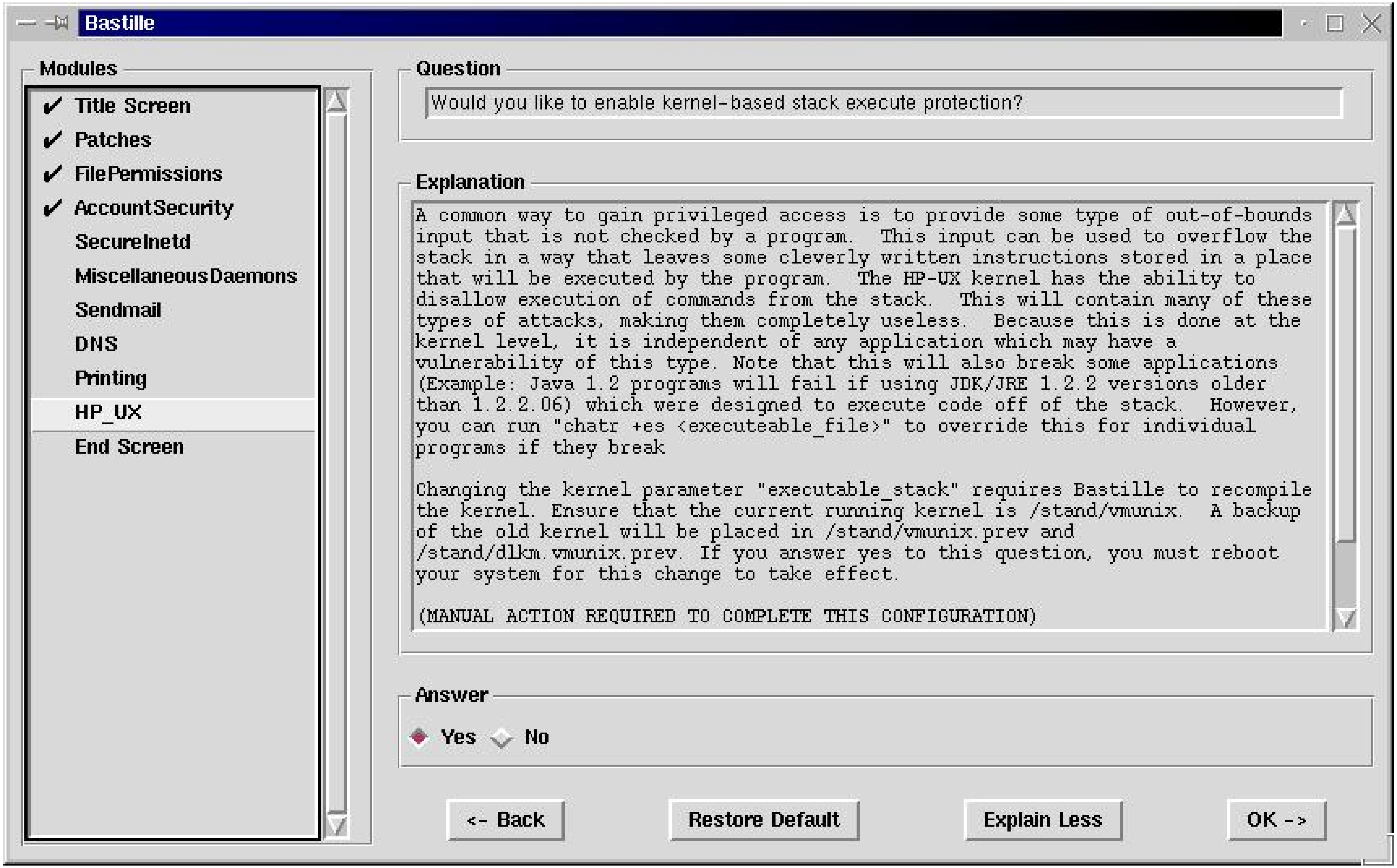
Bastille Effectiveness

Red Hat 6.0 Vulnerabilities Stopped or Contained:

- BIND – remote root hole
- WU-FTPd – remote root hole
- lpd+sendmail – remote root hole
- dump/restore – local root privilege escalation
- gpm – console root-level privilege escalation

We didn’t stop vulnerabilies in the man or nmh commands.

Bastille Screenshot



Question: Would you like to enable kernel-based stack execute protection?

Explanation:

```
A common way to gain privileged access is to provide some type of out-of-bounds
input that is not checked by a program.  This input can be used to overflow the
stack in a way that leaves some cleverly written instructions stored in a place
that will be executed by the program.  The HP-UX kernel has the ability to
disallow execution of commands from the stack.  This will contain many of these
types of attacks, making them completely useless.  Because this is done at the
kernel level, it is independent of any application which may have a
vulnerability of this type. Note that this will also break some applications
(Example: Java 1.2 programs will fail if using JDK/JRE 1.2.2 versions older
than 1.2.2.06) which were designed to execute code off of the stack.  However,
you can run "chatr +es <executeable_file>" to override this for individual
programs if they break

Changing the kernel parameter "executable_stack" requires Bastille to recompile
the kernel. Ensure that the current running kernel is /stand/vmunix.  A backup
of the old kernel will be placed in /stand/vmunix.prev and
/stand/dlkm.vmunix.prev. If you answer yes to this question, you must reboot
your system for this change to take effect.

(MANUAL ACTION REQUIRED TO COMPLETE THIS CONFIGURATION)
```

Answer: ● Yes ○ No

What is Bastille?

- Bastille can lock down these operating systems:
  - Red Hat Linux
  - HP-UX
  - Mandrake Linux
  - Debian Linux
  - SuSE Linux
  - TurboLinux
  - Mac OS X

Why educate the sysadmin?

One of Bastille's real differentiators was that you could run it in interactive mode.

Bastille educates the sysadmin. Why?

Example: telnet

Example: we want to deactivate telnet.

If we do so without asking, we might “break” their remote administration interface.

We need to explain why telnet is bad: password stealing and session takeover.

We need to tell them that SSH is an alternative.

Now they’ll make the right decision.

Why Should I Use Bastille?

- Bastille is an automate-able solution, allowing you to create one policy file that you can apply to a huge number of similar systems.
- Even if you've only got one or two systems to configure, this policy file idea can be very useful, because it gives you consistency.
- You only have to choose your hardening steps once per major release of the operating system, at most.

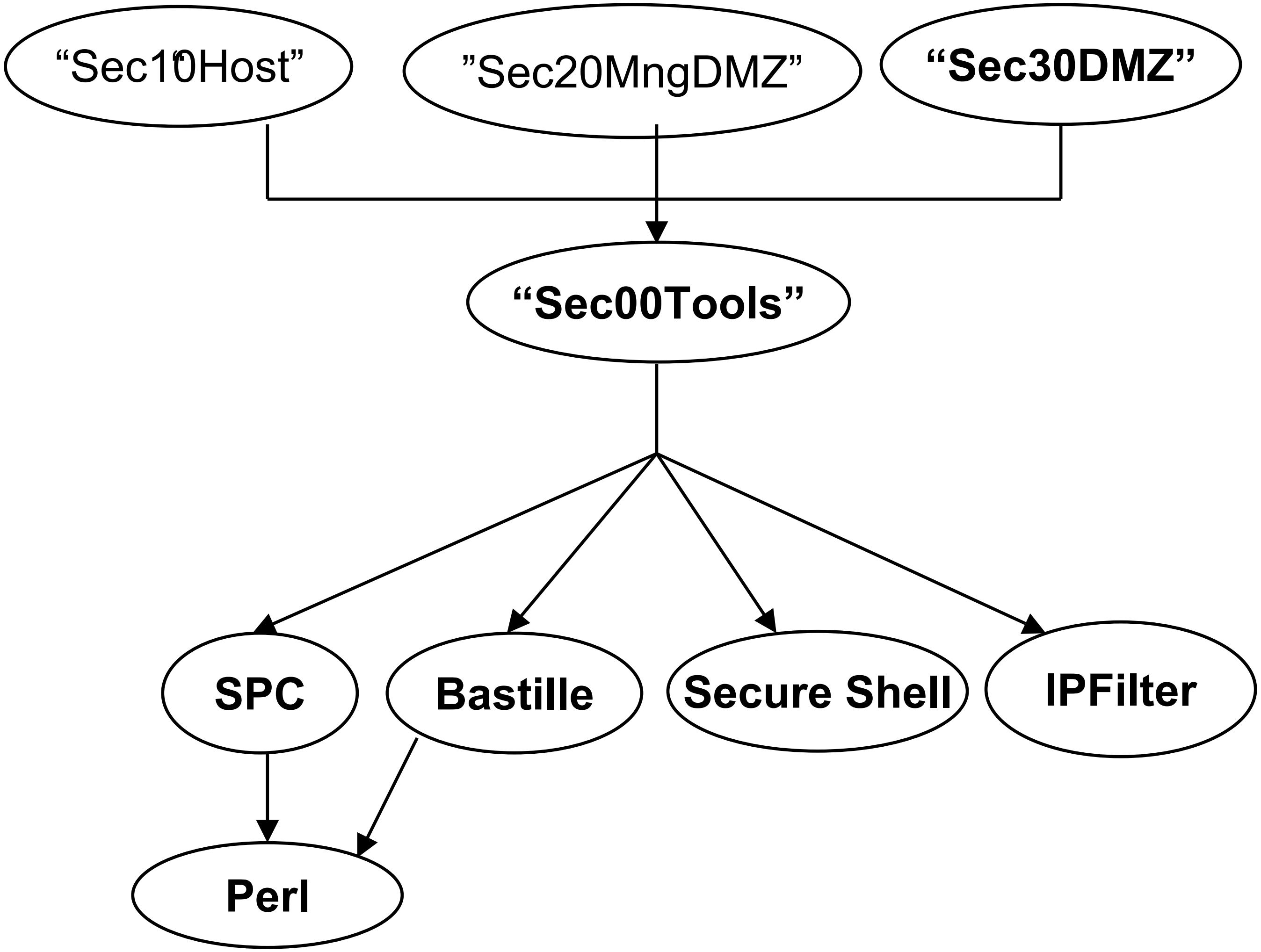
Install Time Security

- Deploy HP-UX into high threat environments quickly
  - make security or compatibility decisions suited to your needs
  - security tradeoffs no longer configured for the “generic user”
- Customers can be “secure-by-default,” at installation,
  - Can later revise settings with Bastille

Install Time Security Options

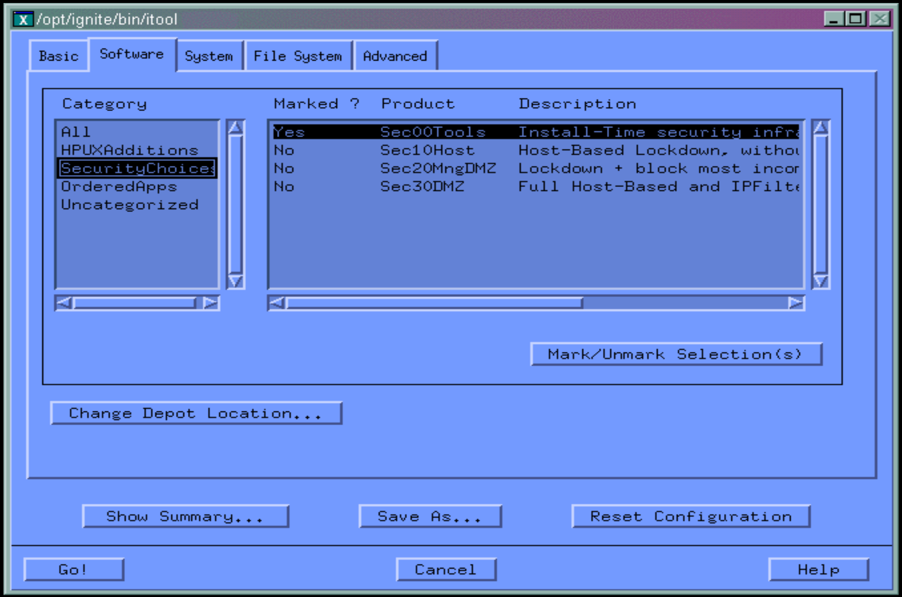
Security Level	Description
Sec00Tools	The install-time security infrastructure; no security changes
Sec10Host	Host-based lockdown: no firewall; networking runs normally, including non-root Telnet and FTP
Sec20MngDMZ	Lockdown uses IPFilter firewall to block incoming connections except common, secured, management protocols
Sec30DMZ	Full lockdown: IPFilter blocks all incoming connections except Secure Shell

ITS "Under the Hood"



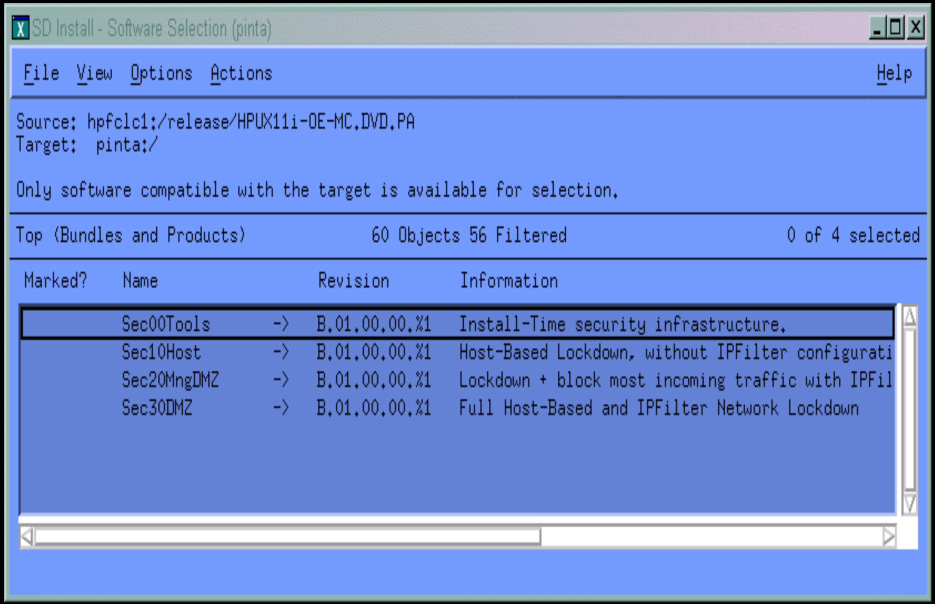
Four Ways to Use Install-Time Security

1) Ignite/UX



```
Category             Marked ?  Product      Description
All                  Yes       Sec00Tools   Install-Time security infra
HPUXAdditions        No        Sec10Host    Host-Based Lockdown, withou
SecurityChoices      No        Sec20MngDMZ  Lockdown + block most incor
OrderedApps          No        Sec30DMZ     Full Host-Based and IPFilte
Uncategorized
```

2) Software Distributor



```
Source: hpfclc1:/release/HPUX11i-OE-MC.DVD.PA
Target:  pinta:/

Only software compatible with the target is available for selection.

Top (Bundles and Products)            60 Objects 56 Filtered            0 of 4 selected

Marked?  Name               Revision         Information
         Sec00Tools    ->   B.01.00.00.%1    Install-Time security infrastructure.
         Sec10Host     ->   B.01.00.00.%1    Host-Based Lockdown, without IPFilter configurati
         Sec20MngDMZ   ->   B.01.00.00.%1    Lockdown + block most incoming traffic with IPFil
         Sec30DMZ      ->   B.01.00.00.%1    Full Host-Based and IPFilter Network Lockdown
```

2) Manual

```
# swinstall –s <depot> -x autoreboot=true <level>
```

4) Update/UX

```
# update-ux –s <depot> <OE> <level>
```

Bastille Linux's Modules

- Looking at Linux functionality
  - Linux modules list
    - File Permissions
    - Account Security
    - Boot Security
    - Secure Inetd
    - Disable User Tools
    - Configuring PAM
    - Miscellaneous Daemons
    - Sendmail

Bastille Linux’s Modules

- More Linux functionality
  - Linux modules list continued.
    - DNS
    - Apache
    - Printing
    - FTP
    - TMP Directory
    - Firewall
    - PSAD

Bastille Linux's File Permissions Module

- Administration Utilities
  - Privilege reduction for management applications via the removal of world executable permissions
- Disabling SUID root permissions
  - "mount" and "umount"
    - File system activation and deactivation tools
  - "ping"
    - Network connectivity testing utility
  - "dump" and "restore"
    - file system backup and restoration utilities
  - "cardctl"
    - PCMCIA device control utility

Bastille Linux’s File Permissions Module

- Disabling SUID root permissions (continued)
  - “at”
    - Individual task scheduling
  - “DOSEMU”
    - DOS emulation software
  - “inndstart” and “startinnfeed”
    - INN news server tools
  - “rsh”, “rcp”, and “rlogin”
    - Remote connection client utilities
  - “usernetctl”
    - Network interface control utility

Bastille Linux's File Permissions Module

- Disabling SUID root permissions (continued)
  - "traceroute"
    - General network configuration test utility
  - "Xwrapper"
    - X windowing system wrapper script for X binaries
  - "XFree86"
    - X server binary

Bastille Linux’s Account Security Module

- Disable clear-text r-protocols (rlogind, rshd, and
  - Removes execution permission from server binaries
  - Removes r-protocol service entries in inetd/xinetd configurations
  - Modifies system PAM configuration
- Enforce password aging
  - 180 day default cycle in “/etc/login.defs”
  - Handles removal of inactive accounts

Bastille Linux's Account Security Module

- Restrict "cron" to administrative accounts
  - "cron" scheduling can be useful, for legitimate and illegitimate ends
- Default system "umask"
  - Default configurations for bash, csh, ksh, and zsh.
- Restricting root login on tty's
  - Restricts root login on console

Bastille Linux’s Boot Security Module

- Grub configuration
  - Boot prompt password protection
- Lilo configuration
  - Boot prompt password protection
  - Removes boot all boot prompt delay
- Securing the “inittab”
  - Disables “ctrl-alt-del” rebooting
  - Password protects single-user mode

Bastille Linux's Secure Inetd Module

- TCP Wrapper configuration
  - Default deny settings for inetd, xinetd and TCP Wrapper aware services
- Services using clear text protocol
  - Disables telnetd
  - Disables ftpd
- "Authorized Use Only" messages
  - Login time banner serves as an unwelcome mat
    - Possibly helpful in the prosecution of system crackers.

Bastille Linux's Disable User Tools and PAM Modules

- Disable User Tools
  - "gcc" complire
    - Removes user execution privileges from the "gcc" binary
- Configure PAM
  - The number of allowed core files is reduced to zero
  - Individual users are limited to 150 processes each
  - Individual files are limited to 100MB each
  - Console access is limited to a small group of users, including but not limited to the "root" user

Bastille Linux’s Logging Module

- Logs status messages to the 7th and 8th virtual terminals
- Adds two addition log files to the basic setup
  - “/var/log/kernel” logs kernel messages
  - “/var/log/loginlog” logs all user login attempts
- Adds sensitivity to current system logs
  - “/var/log/syslog” will contain messages of severity “warning” as well as severity “error”
- Sets up remote logging
- Enables process accounting

Bastille Linux's Miscellaneous Daemons Module

- Disables apmd
  - Battery power monitor used almost exclusively by laptops
- Disables NFS
  - Network file system transfers data in clear-text and uses IP based authentication
- Disables Samba
  - CIFS server which transfers data in clear-text
- Disables PCMCIA services
  - Allows the use of easily removable credit-card-sized devices used almost exclusively by laptops

Bastille Linux's Miscellaneous Daemons Module

- Disables DHCP daemon
  - Used to distribute temporary IP (Internet) addresses to other machines.
- Disables GPM daemon
  - Used in console (text) mode to add mouse support
- Disables the news server daemon
  - Provides news services to outside machines
- Disables routed daemon
  - "routed" is a legacy daemon which provides network routing
    - Commonly replaced by "gated"

Bastille Linux’s Miscellaneous Daemons Module

- Disables “gated” daemon
  - A daemon used to route network traffic
- Disable NIS server daemons
  - An NIS (Network Information System) server is used to distribute network naming and administration information to other machines on a network
- Disable NIS client daemons
  - Used to receive network naming and administration information from a server machine on its network.
- Disables SNMPD
  - Used to aid in management of machines over the network

Bastille Linux’s Sendmail Module

- Disables the sendmail daemon
- Configures a periodic run of sendmail to process the mail queue
- Disables SMTP (Simple Mail Transport Protocol) VRFY and EXPN commands for systems running a sendmail daemon.
  - The VRFY command allows connecting systems to “verify” the existence of a system user
  - EXPN allows connecting systems to “expand” user name aliases

Bastille Linux’s DNS Module

- Configures needed BIND (Berkeley Internet Name Domain) services to be more secure
  - Configures a “chroot” jail for the BIND daemon
    - “chroot” jails allow a process to be bound to a subset of the file system
  - Configures the BIND daemon to run as a non-root user
    - A non-root user is created for this purpose
- Disables unneeded BIND services running on a system

Bastille Linux’s Apache Module

- Disables Apache daemon if it is unneeded
- Hardens Apache configuration
  - Binds the Apache daemon to specified network interfaces
  - Prohibits Apache from following symbolic links
  - Disables Apache server-side includes
  - Prohibits Apache from executing CGI scripts
  - Disables Apache indexes, the auto generation of index files when an index file is not present

Bastille Linux's Printing, FTP, and TMP directory Modules

- Printing configuration
  - Disables the printing daemon lpd
  - Removes suid and gid bits from the lp and lprm commands
- FTP daemon configuration
  - Disables user privileges on the FTP daemon
  - Disables anonymous download
- TMP directory configuration
  - Configures TMPDIR and TMP environment variables for systems users

Bastille Linux’s Firewall Module

- Configures an IP Chains or IP Tables Firewall
  - Zones network interfaces into three separate trust domains
    - Public Interfaces are completely untrusted
    - Internal Interfaces are untrusted but can have a configuration all together separate from the Public interfaces
    - Trusted Interfaces are completely trusted, e.g. the loopback interface
  - By protocol, service auditing
  - IP address source verification
  - IP Masquerading / NAT (Network Address Translation)
  - Boot time firewall start up scripts

Bastille Linux's PSAD Module

- PSAD (Port Scan Attack Detection) Integration
  - Tunable port scan detection interval
  - Tunable port range scan threshold
  - Scanning tool signature reporting
  - Danger levels reports based on tunable packet thresholds
  - Configurable e-mail notification system
  - Automatic blocking of scanning IP addresses via host based firewall configuration
  - Boot time start up scripts

HP-UX Bastille’s Modules

- Looking at HP-UX functionality
  - HP-UX modules list
    - Patches
    - File Permissions
    - Account Security
    - Secure Inetd
    - Miscellaneous Daemons

HP-UX Bastille’s Modules

- More HP-UX functionality
  - HP-UX modules list continued
    - Sendmail
    - DNS
    - Apache
    - FTP
    - HP-UX
    - IPFilter

HP-UX Bastille’s Patches and File Permissions Modules

- Security Patch Check configuration
  - Provides download and install instructions for SPC (Security Patch Check)
  - Automates a nightly run of SPC
    - SPC run time is tunable
    - Configurable web proxy for security patch catalog download
- File Permissions configuration
  - World-Writeable directory scan
    - Automated script generation to tighten permission allows for custom configurations
    - SD file volatility checks to avoid swverify errors

HP-UX Bastille’s Account Security Module

- Default system “umask”
  - Default configurations for bash, csh, ksh, and zsh
  - “/etc/default/security” system umask
    - Available in HP-UX 11.22 and beyond
- Shadow encrypted passwords on this system
- Password protect single user mode
- System security auditing

HP-UX Bastille’s Account Security Module

- User password policies
  - Configurable password history depth
  - Configurable maximum days between user password change
  - Configurable minimum days between user password change
  - Configurable warning period before password expiration

HP-UX Bastille's Account Security Module

- Configuration of login policies
  - Abort login if a users home directory is non-existent
  - Enable "/etc/nologin" functionality
  - Configurable maximum simultaneous logins per user
  - Configurable default PATH for "su" operations
  - Restrict root user login on network tty's

HP-UX Bastille's Secure Inetd Module

- Inetd service audit
  - Disables telnet service
    - A clear text remote login daemon
  - Disables ftp service
    - A clear text remote file transfer daemon
  - Disables login, shell, and exec services
    - These services implement rlogind, remshd, and rexecd respectively
  - Disables TFTP service
    - Trivial File Transfer Protocol (TFTP) is a UDP-based file transfer program

HP-UX Bastille's Secure Inetd Module

- Inetd service audit (continued)
  - Disables bootp service
    - A Dynamic Host Configuration Protocol (DHCP) server
    - An Internet Boot Protocol (BOOTP) server
    - A DHCP/BOOTP relay agent
  - Disables finger service
    - The server for the RFC 742 Name/Finger protocol
  - Disables uucp service
    - UUCP (Unix to Unix copy) copies files named by the source_files argument to the destination identified by the destination_file argument
  - Disables ntalk service
    - Communication program that predates instant messaging applications

HP-UX Bastille's Secure Inetd Module

- Inetd service audit (continued)
  - Disables ident service
    - Implements the TCP/IP proposed standard IDENT user identification protocol
  - Disables daytime, discard, chargen, and echo services
    - daytime: Sends the current date and time as a human readable character string (RFC 867)
    - discard: Throws away anything that is sent to it, similar to /dev/null.(RFC 863)
    - chargen: Character Generator sends you a stream of some undefined data, preferably data in some recognizable pattern (RFC 862)
    - echo: Simply returns the packets sent to it. (RFC 862)

HP-UX Bastille's Secure Inetd Module

- Inetd service audit (continued)
  - Disables time service
    - The time service that is built into inetd produces machine-readable time, in seconds since midnight on 1 January 1900
  - Disables klogin and kshell services
    - These services implement Kerberos authentication
  - Disables dtspcd, cmsd, and ttdbserver
    - dtspcd: Desktop Sub process Control service is used to invoke a processes on other systems.
    - cmsd: This is used to run Sun's Calendar Manager software database over the network
    - ttdbserver: Sun's ToolTalk Database Server allows OpenWindows programs to intercommunicate.

HP-UX Bastille’s Secure Inetd Module

- Inetd service audit (continued)
  - Disables recserv service
    - HP SharedX Receiver Service is used to receive shared windows from another machine in X without explicitly performing any xhost command
  - Disables swat service
    - Samba configuration utility
  - Disables printer service
    - A line printer daemon that accepts remote spool requests.
- Enables Inetd logging
- Authorized Use Only" messages
  - Login time banner serves as an unwelcome mat
    - Possibly helpful in the prosecution of system crackers.

HP-UX Bastille’s Miscellaneous Daemons Module

- Disables NFS server daemon
  - Network File System (NFS) service allows it's host machine to export file systems onto other designated machines on a network
- Disables NFS client daemons
  - “automount”/”autofs” allow non-root users to mount NFS file systems
  - block I/O daemons, are used on an NFS client to handle read-ahead and write-behind buffer caching
- Disable NIS server daemon
  - An NIS (Network Information System) server is used to distribute network naming and administration information to other machines on a network

HP-UX Bastille’s Miscellaneous Daemons Module

- Disables NIS client daemons
  - Used to receive network naming and administration information from a server machine on its network
- Disables SNMPD
  - SNMP (Simple Network Management Protocol) is used to aid in management of machines over the network
- Disables both the ptydaemon and vtdaemon
  - ptydaemon is used by the shell layers (shl) software which is a historical alternative to job control
  - “vtdaemon” uses “ptydaemon” to provide a remote login method

HP-UX Bastille’s Miscellaneous Daemons Module

- Disables “pwgrd”
  - The Password and Group Hashing and Caching daemon (pwgrd) provides accelerated lookup of password and group information for libc routines
- Disables “rbootd”
  - Used for a protocol called RMP, which is a predecessor to the "bootp" protocol
- Disallows remote X logins
  - XDMCP is an unencrypted protocol which allows remote connections to an X server

HP-UX Bastille’s Sendmail Module

- Disables the sendmail daemon
- Configures a periodic run of sendmail to process the mail queue
- Disables SMTP (Simple Mail Transport Protocol) VRFY and EXPN commands for systems running a sendmail daemon.
  - The VRFY command allows connecting systems to “verify” the existence of a system user
  - EXPN allows connecting systems to “expand” user name aliases

HP-UX Bastille’s DNS Module

- Configures needed BIND (Berkeley Internet Name Domain) services to be more secure
  - Configures a “chroot” jail for the BIND daemon
    - “chroot” jails allow a process to be bound to a subset of the file system
  - Configures the BIND daemon to run as a non-root user
    - A non-root user is created for this purpose

HP-UX Bastille’s Apache and FTP Modules

- Apache hardening
  - Disables Apache daemon if it is unneeded
  - Creates a “chroot” jail from which Apache can run
- FTP configuration
  - Disallows FTP access to system accounts (root, daemon, bin, sys, adm, uucp, lp, nuucp, hpdb, and guest)

HP-UX Bastille’s HP-UX Module

- Enables kernel-based stack execute protection
  - Requires kernel rebuild and reboot
- Restricts remote access to swlist
- Hardens “ndd” tunable parameters for network devices
  - ip_forward_directed_broadcasts disabled
  - ip_forward_src_routed disabled
  - ip_forwarding disabled
  - ip_ire_gw_probe disabled
  - ip_send_redirects disabled
  - ip_send_source_quench disabled
  - tcp_conn_request_max increased to mitigate DOS attacks
  - tcp_syn_rcvd_max increased to mitigate DOS attacks

HP-UX Bastille's IPFilter Module

- Enables a basic stateful host-based firewall
  - Blocks incoming traffic by default requiring the explicit enablement of remote services on a per service basis
  - Allows all outbound traffic by default for ease of use
  - Configures incoming traffic for common services
    - Secure Shell remote terminal service
    - WBEM's multi-system management
    - HIDS (Host Intrusion Detection System) reporting and management
    - Common https web administration
    - DNS query connections and zone transfers
  - The custom-rules mechanism allows for easy server specific customizations

Hands On

We're about to end the lecture portion of this seminar.

Let's answer any questions you have first.

Now, let's demonstrate how you'd use Bastille to lock down a live system.

HP WORLD 2003

Solutions and Technology Conference & Expo

Interex, Encompass and HP bring you a powerful new HP World.

interex
shared knowledge • shared power

encompass
AN HP USER GROUP

hp
invent