Managing Operating System (OS) Lock Down

SANS ANALYST PROGRAM

Sponsored by Trusted Computer Solutions (TCS)

Managing Operating System (OS) Lock Down: Trusted Computer Solutions' Security Blanket Review

A SANS Whitepaper – March 2010

Written by Dave Shackleford

Overview and Setup

Installation, Clients, and Groups

Security Profiles and Modules

Management, Scheduling, and Reporting

Introduction

Any IT/Security Manager worth his salt knows that configuration management is a mainstay of secure network operations. This year (2010), "Secure configurations for hardware and software on laptops, workstations, and servers " was again on SANS list of top 20 critical security controls.

Nowhere is this more critical than at the operating system (OS) level, where default passwords and vulnerable services and ports are known to be huge exposures. Although organizations are generally good at locking down critical server operating systems initially, these "gold builds" fall out of configuration over time, particularly in distributed organizations where local resources are scarce. For example, when a system is used to test a new application that is never uninstalled, it exposes all the data and vulnerabilities associated with that new application to attackers. In other cases, certain system updates and patches are forgotten or deliberately not applied; new users are added or deleted without updating; or systems are moved and are no longer listed on the active system inventory list.

In the case of OS lock down, organizations need policies to follow throughout the life of their critical server systems that are able to meet differing requirements for specific business uses, including provisions to unlock a system when required. For example, certain configuration changes may lead to application instability or impact performance; having a process to simply rollback these changes would be beneficial. Adding and removing configuration changes comprises the overall configuration management lifecycle.

Configuration management (CM) tools aid in performing assessments and making recommendations for remediation across all systems and applications they are programmed to, including noting whether they find vulnerabilities in operating systems. However, this is not the same as actually locking down the OS to policy, consistently monitoring the configuration for unspecified changes, and other specific OS maintenance and management requirements.

In this paper, we look at a tool specific to OS lock down from Trusted Computer Solutions (TCS) called Security Blanket, which automates OS configuration for a wide variety of UNIX and Linux platforms. Security Blanket can automatically lock down these operating systems based on industry standards and ensure lock down remains in effect following patches, updates and application changes. Through its management console, undoing lock down was as easy to achieve as locking down a system. It also provides auditing and compliance reporting features and guidelines for both OS and service details.

[1] www.sans.org/critical-security-controls/control.php?id=3

Overview and Setup

This paper is an operational review of Security Blanket, which is deceptively simple to use, yet provides a granular list of controls that can be configured on servers. The product consists of **clients** running on servers, which can then be placed into **groups**. An administrator defines a series of **profiles** (some pre-built profiles come out of the box) that are then configured with a number of individual security configuration **modules** representing individual control elements like password policies, management of specific services, user controls, and so on.

We evaluated Security Blanket Enterprise version 4.0.1-r8726 for this review. The purpose of the review was to determine what security features Security Blanket could provide in Linux and Solaris environments to establish and maintain continuous compliance for these systems over time.

A VMware-based test environment was used to create both the console and client systems as virtual machines for this review. Figure 1 and Table 1 define the testing environment employed.

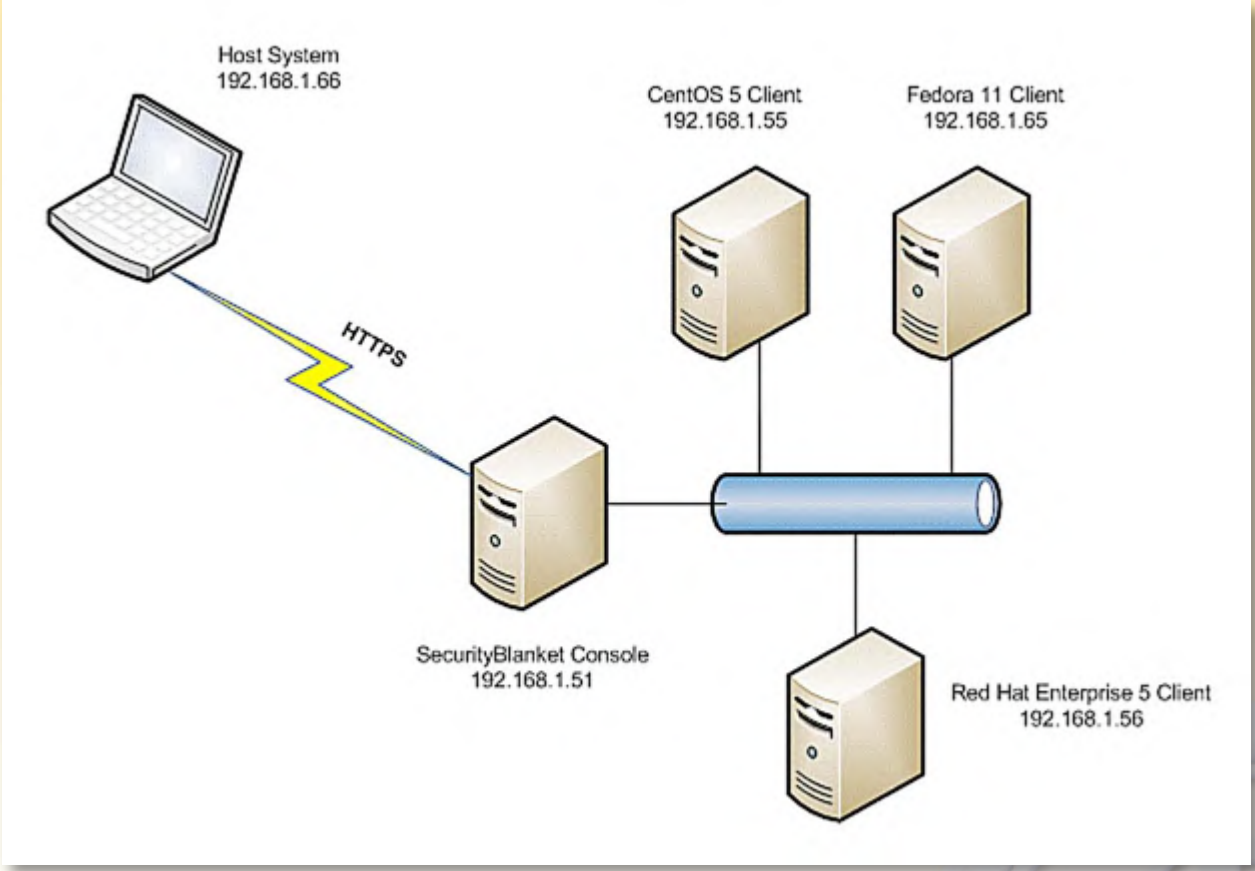


Figure 1: Security Blanket Review Environment

Security Blanket's current release supports Red Hat Enterprise Linux 4 and 5 (32- and 64-bit), CentOS 4 and 5 (32- and 64-bit and Desktop), Oracle Enterprise Linux versions 4 and 5, Solaris 10, Fedora 10 and 11, Novell 11 and OpenSUSE 11. For this review, we tested the client versions listed in Table 1.

Operating System	OS/Kernel Version	Client Version
CentOS 5 (console VM)	Linux2.6.18-53.el5	Security Blanket 4.0.1 -r8710
CentOS 5 (client VM)	Linux2.6.18-53.el5	Security Blanket 4.0.1 -r8710
RHEL 5	Linux2.6.18-164.el5	Security Blanket 4.0.1 -r8710
Fedora 11	Linux2.6.29.4-167.fc11.i686.PAE	Security Blanket 4.0.1 -r8710

Table 1: Security Blanket Clients and OS Versions

Note that Security Blanket is also available in a standalone version, which seems to have the same configuration management features and web-based console as the Enterprise version, but is intended for use on a single system. This version, however, was not assessed during this review.

Installation, Clients, and Groups

Installation of the product was generally straightforward. The same executable is used for both client and console (management server) installation, making it simple to manage. The license was based on the console system's MAC address, and the license received from TCS was easy to integrate. The setup process consisted of running an executable that assesses the system for compatibility and then prompts the user to move through a very fast installation process. Several minor questions came up surrounding dependencies and the setup of certificates (required for console–client communications). Issues were quickly resolved with help from TCS' responsive support team. Overall, the setup was painless, and the documentation was very good.

All communications between the administrator's browser and the console, as well as the console and client systems, is encrypted for security. Figure 2 demonstrates the default configuration, which is the configuration SANS reviewed.

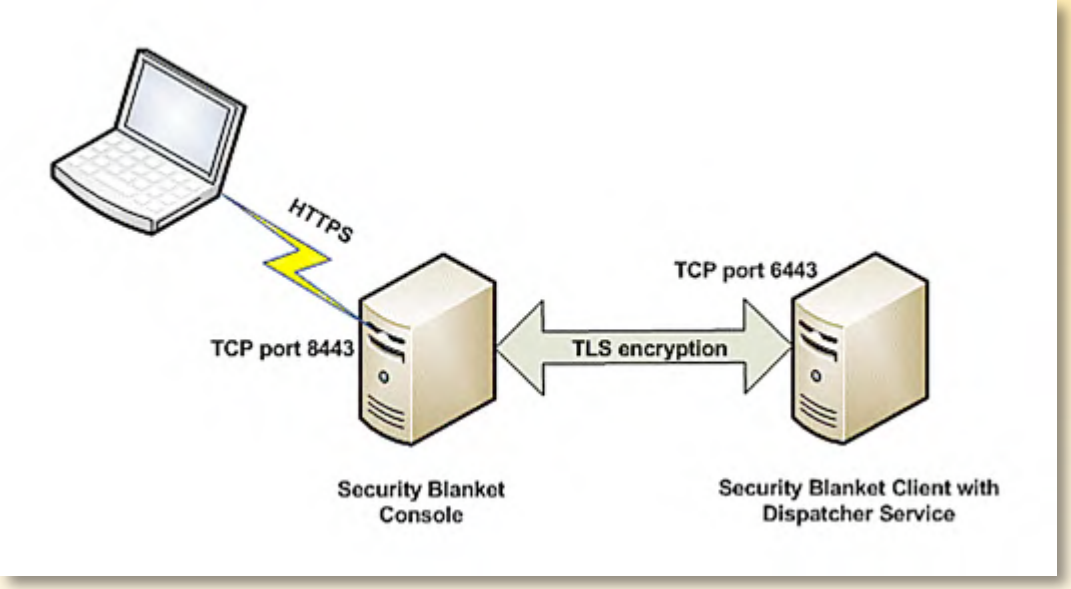


Figure 2: Encrypted Communications and Components

The license file is only applied to the console system, which is also the system that generates certificates for console–client communications. The setup process on each client was even easier, because it wasn't necessary to configure any web services, and the certificates from the console were simply imported. Setting up the console and three (3) separate clients took a total of one hour after resolving dependencies and several other questions.

Upon logging into the console for the first time, we noted that all of the major product functions were neatly laid out within the browser window. There are tabs along the top for each product function: client and group creation, profile definition, viewing of notifications and reports, and task scheduling, as shown in Figure 3.

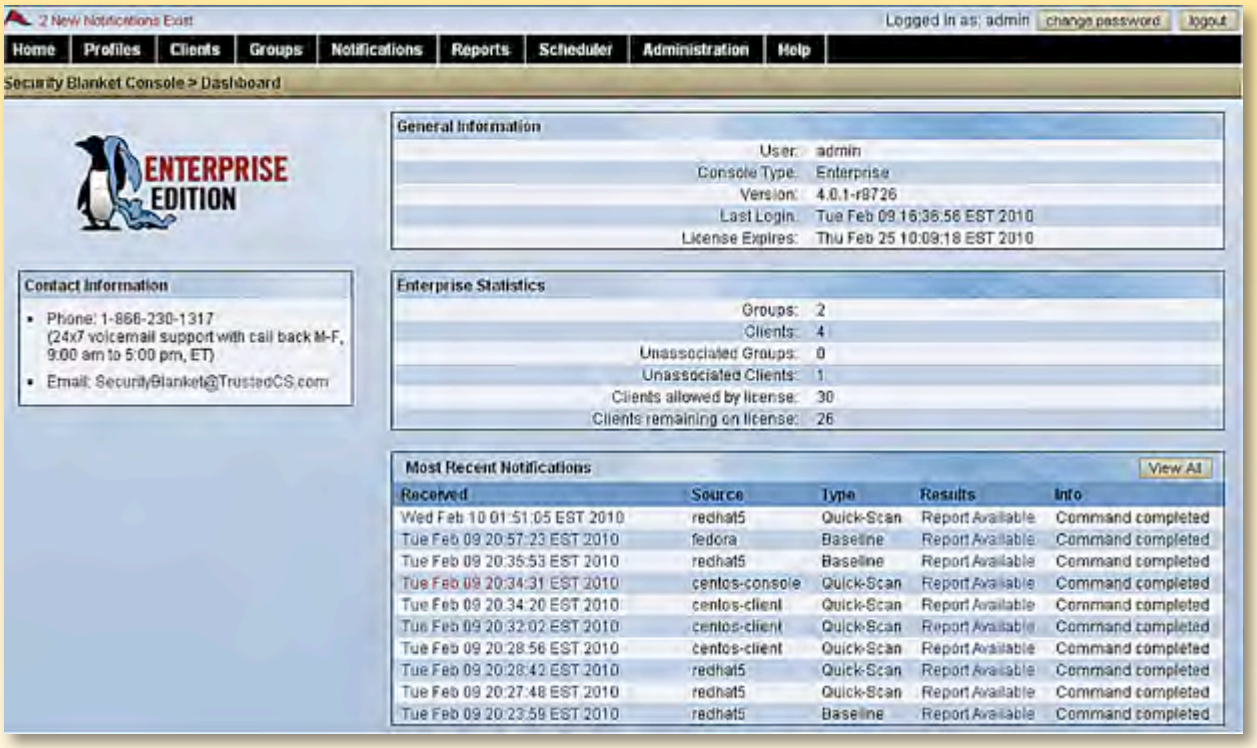


Figure 3: The Main Security Blanket Console

Our first task was to define clients, which we accomplished by clicking the Clients tab. Selecting New gets you to a screen with five (5) possible fields, as shown in Figure 4.

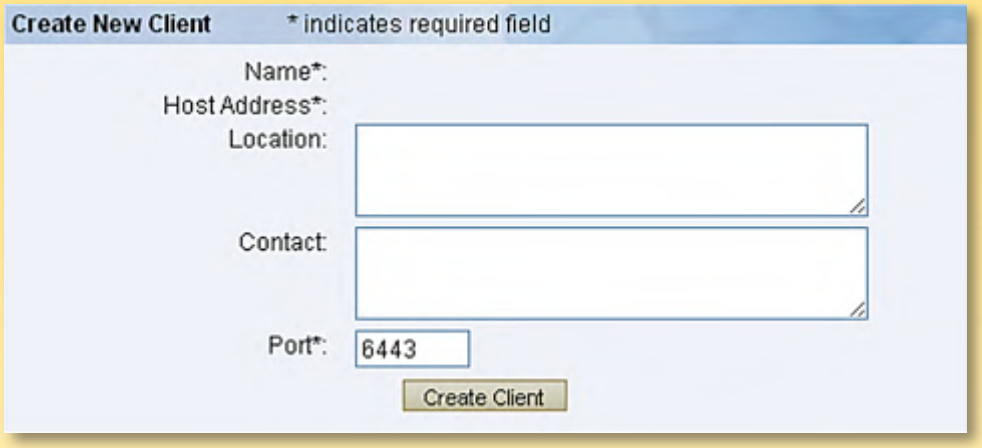


Figure 4: Client Definition Page

After defining all the clients to be assessed, it was time to create test groups for them. Two identical CentOS 5 images were included, one of which was running the Security Blanket Console. These were placed into a specific group called CentOS, and the Red Hat and Fedora systems were placed into a group called Test. When these groups are defined, a profile can be assigned to them. To start the assessment, built-in groups were chosen: The Test group was assigned the CIS benchmarks profile, while the CentOS group was assigned the DISA UNIX STIG profile as shown in Figure 5. These configuration settings weren't actually tested or applied until later in the review; however, at this point in the process they were associated with the particular group and clients.

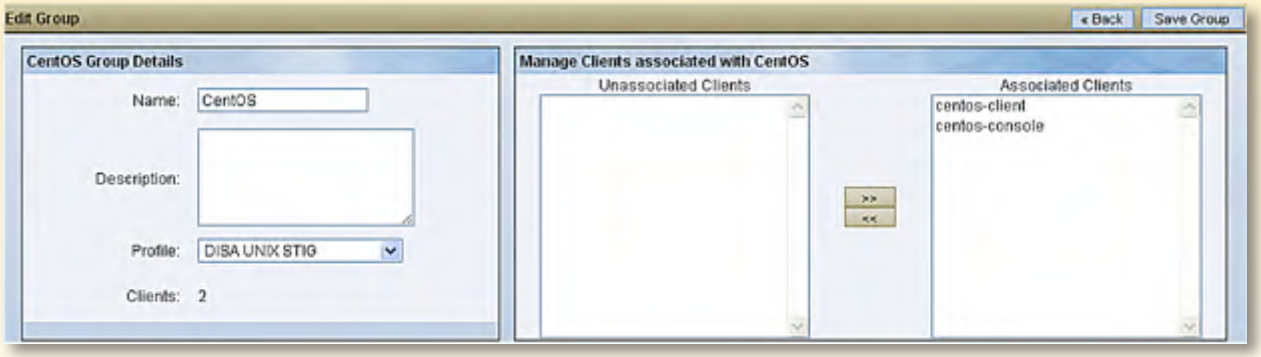


Figure 5: Assigning Clients and Profiles to Groups

Security Profiles and Modules

The most fundamental element of Security Blanket's configuration capabilities is the profile. The default profiles available with the product are a "Who's Who" of well-known configuration hardening guidance, including the following:

- **CIS Benchmarks:** Configuration guides for a wide number of platforms from the Center for Internet Security.
- **DISA UNIX STIGs:** The Defense Information Systems Agency's Security Technical Implementation Guides, often considered the most detailed configuration guides available.
- **Web Services Protection:** A hybrid guide from CIS, DISA, and SANS that addresses configuration guidance for Linux and Solaris systems running Apache, MySQL and PHP for web services.

In addition to these, several compliance- and accreditation-specific profiles are available including DCID 6/3 (certification and accreditation for U.S. federal intelligence agencies), Federal Energy Regulatory Commission (FERC) Critical Infrastructure Protection (CIP) guidance, Payment Card Industry Data Security Standard (PCI DSS), and others. Each of these comes prepopulated with a number of security modules, which are groups of OS and application security settings configured to match the hardening guidance or compliance mandate setting requirements. For example, if an organization wants to use warning banners at employee login for legal reasons, there's a security module for creating a login warning banner as shown in Figure 6. We applied this setting as part of the review. It was present after the change took effect.

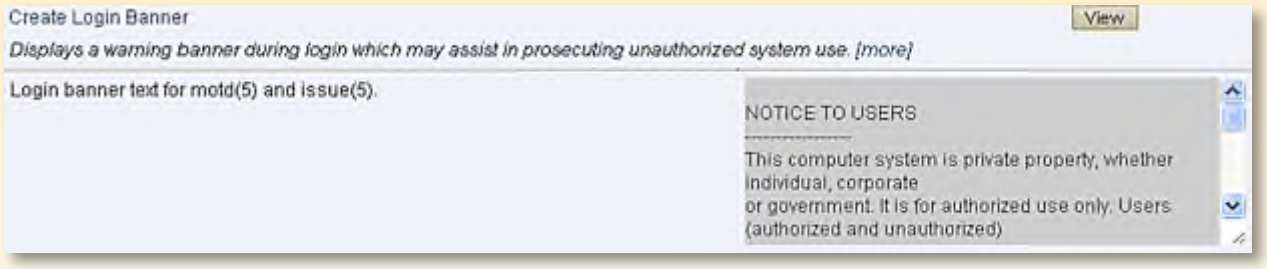


Figure 6: Login Warning Banner Security Module

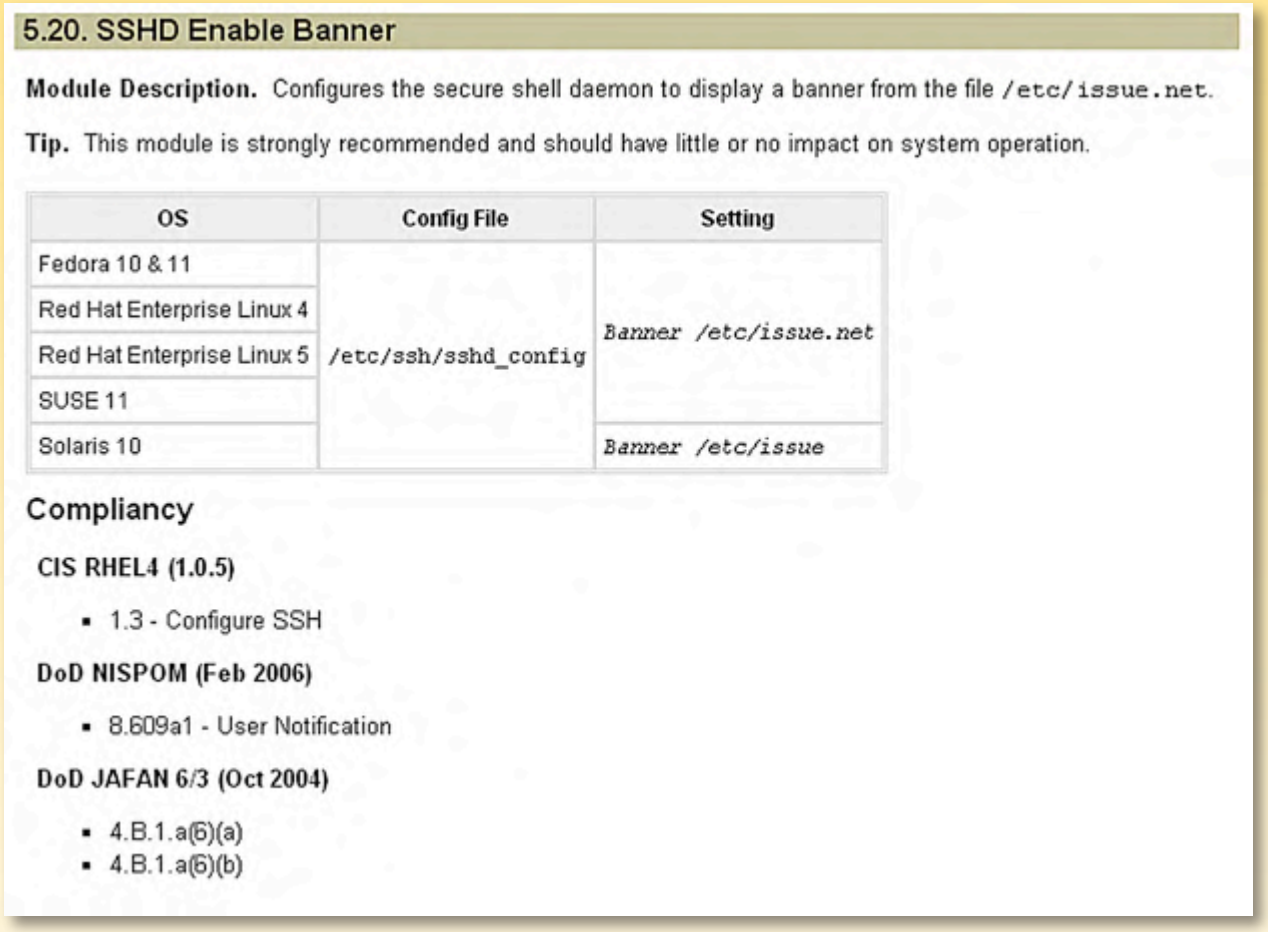
The variety of predefined modules include long and complex lock down profiles, as well as streamlined standards and guides. For example, the DISA UNIX STIG and CIS Benchmarks profiles are very comprehensive, with extensive lists of configured modules available. The profile for the National Industrial Security Program Operating Manual (NISPOM) is not nearly as long, but meets that particular standard. The level of detail provided for each profile and security module is impressive — each control is explained when it's selected, and controls with specific settings or additional details have a View button next to them for the administrator to see how the control is configured.

The real power of this tool comes from the ability to define custom profiles and add specific sets of security modules. Any of the predefined profiles can be cloned as a starting point by using the Copy command under the Profiles tab. Once cloned, the profile can be modified as needed. This can be very helpful for organizations that want to modify the best practice standards to better suit their organization's evolving policies. For example, the DISA STIGs are known to be comprehensive and somewhat rigid in locking down UNIX systems. Commercial financial institutions may want to start with the original STIG, but then modify or change some of the modules to be less restrictive. Custom profiles can be created from scratch, too. The administrator simply adds modules as needed. In this review, several profiles were cloned, modified and then applied. For example, the CIS UNIX benchmark was cloned, and in the new profile, multiple settings were changed from the defaults for OS lock down. For testing, specific warning banners were written, permissions on the `/etc/shadow` file were changed from 400 to 777, and so on. All of these settings were correctly applied in the new profile.

The range of modules is broad and provides great coverage of UNIX and Linux security controls. The following is a sample of some of the types of configuration actions users can implement:

- Disabling vulnerable services such as Remote Shell (rsh), NIS, NFS, SNMP, and others
- Setting home directory contents, ownership and permissions
- Setting account controls, such as setting the shell to `/bin/nologin`, disabling accounts with empty password fields, locking nonroot accounts with UID 0, and removing generic system accounts
- Setting a variety of password policies, such as password complexity and re-use, setting single-user mode and GRUB bootloader passwords, and setting permissions on password files like `/etc/passwd` and `/etc/shadow`
- Setting a number of SSHD parameters, such as root login, protocol selection, X11 forwarding, and warning banners

After applying the configuration settings noted above (among many others), we performed a manual examination at the command line to ensure they were all properly set. In every case, the OS lock down setting was accurately applied, which was later reflected in scan reports, as well. An example of the detailed help available for a security module is shown in Figure 7. Note the inclusion of compliance and best practice standards sections to which this control maps.



5.20. SSHD Enable Banner

Module Description. Configures the secure shell daemon to display a banner from the file `/etc/issue.net`.

Tip. This module is strongly recommended and should have little or no impact on system operation.

OS	Config File	Setting
Fedora 10 & 11	`/etc/ssh/sshd_config`	*Banner /etc/issue.net*
Red Hat Enterprise Linux 4		
Red Hat Enterprise Linux 5		
SUSE 11		
Solaris 10		*Banner /etc/issue*

Compliancy

CIS RHEL4 (1.0.5)

- 1.3 - Configure SSH

DoD NISPOM (Feb 2006)

- 8.609a1 - User Notification

DoD JAFAN 6/3 (Oct 2004)

- 4.B.1.a(6)(a)
- 4.B.1.a(6)(b)

Figure 7: Detailed Information on a Security Module

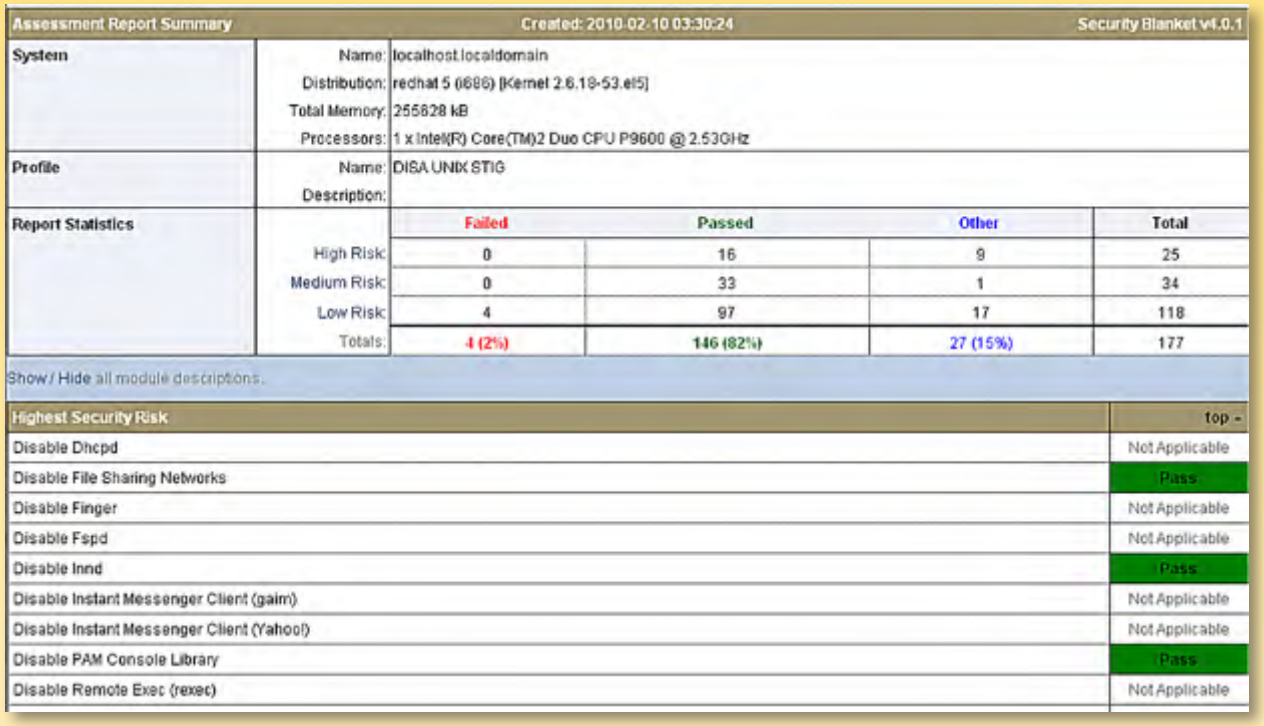
Management, Scheduling, and Reporting

Now that we've taken a look at what kinds of profiles and security settings can be controlled with Security Blanket, how does it work? Security Blanket enables a number of different actions that can be taken for each client or group:

- **Quick Scan Assessment:** The client or group is scanned and assessed against its selected profile, but any system-intensive security modules are skipped.
- **Scan:** The entire range of security modules applied to the profile is analyzed.
- **Apply:** The client or group's selected profile is actually applied to the system. In essence, this automates the application of numerous configuration settings at one time.
- **Undo:** This action reverses a previous Apply action, allowing an administrator to reverse any overly stringent security settings that may have resulted from configuring a system.
- **Baseline:** This action allows an administrator to take a snapshot of a system's current state, capturing numerous details about its configuration for comparison to previous baselines and other systems' baselines.

In this review, we tested the following actions:

- **Scan, Apply, and Undo:** Multiple clients had the DISA UNIX STIG and CIS Benchmarks applied and removed (via the Undo action). After these actions, the clients were evaluated at the console command line to determine whether security settings had been applied and then removed. In both cases, Security Blanket performed the specific actions as requested. See an example of a full scan against the DISA UNIX STIG profile in Figure 8.
- **Compare Baselines:** The CentOS group members each had baselines run at various times. Comparisons between the two systems' baselines were run, as was a baseline comparison for one of the systems before and after the DISA UNIX STIG was applied.
- **Customize Profiles:** A custom profile was created with several test security modules added and configured. The profile was applied to a CentOS system as well as to the Test group, and the changes were validated at the command line on each system.



Assessment Report Summary		Created: 2010-02-10 03:30:24			Security Blanket v4.0.1
System	Name:	localhost.localdomain			
	Distribution:	redhat 5 (i686) [Kernel 2.6.18-53.el5]			
	Total Memory:	255628 kB			
	Processors:	1 x Intel(R) Core(TM)2 Duo CPU P9600 @ 2.53GHz			
Profile	Name:	DISA UNIX STIG			
	Description:				
Report Statistics		Failed	Passed	Other	Total
	High Risk:	0	16	9	25
	Medium Risk:	0	33	1	34
	Low Risk:	4	97	17	118
	Totals:	4 (2%)	146 (82%)	27 (15%)	177

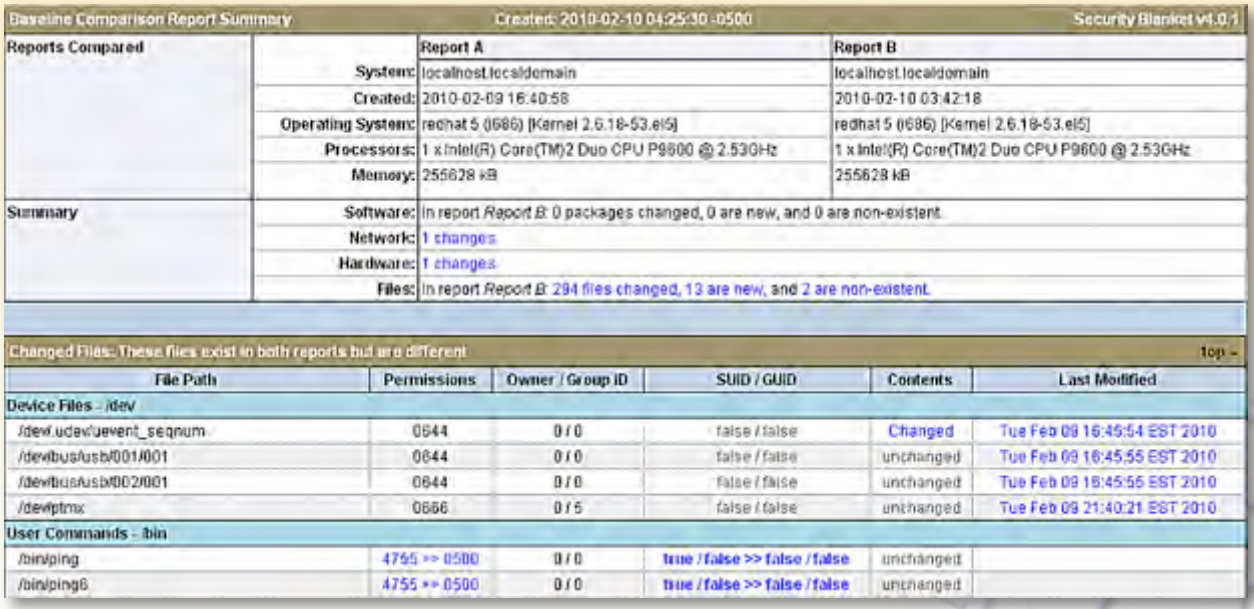
Show / Hide all module descriptions.

Highest Security Risk	top ▲
Disable Dhcpd	Not Applicable
Disable File Sharing Networks	Pass
Disable Finger	Not Applicable
Disable Fspd	Not Applicable
Disable Innd	Pass
Disable Instant Messenger Client (gaim)	Not Applicable
Disable Instant Messenger Client (Yahoo!)	Not Applicable
Disable PAM Console Library	Pass
Disable Remote Exec (rexec)	Not Applicable

Figure 8: Full Scan Using the DISA UNIX STIG Profile

The ability to create baselines and reports, and then compare them at later times, gives Security Blanket the ability to act as a continuous compliance management tool, ensuring each system remains at the desired security level, all while auditing any changes that may have occurred.

Figure 9 demonstrates the results of a baseline comparison between a CentOS system prior to applying the DISA UNIX STIG and after the application. Note the timestamps and notifications on modifications.



Baseline Comparison Report Summary		Created: 2010-02-10 04:25:30 -0500		Security Blanket v4.0.1
Reports Compared		Report A	Report B	
	System:	localhost.localdomain	localhost.localdomain	
	Created:	2010-02-09 16:40:58	2010-02-10 03:42:18	
	Operating System:	redhat 5 (i686) [Kernel 2.6.18-53.el5]	redhat 5 (i686) [Kernel 2.6.18-53.el5]	
	Processors:	1 x Intel(R) Core(TM)2 Duo CPU P9600 @ 2.53GHz	1 x Intel(R) Core(TM)2 Duo CPU P9600 @ 2.53GHz	
	Memory:	255628 kB	255628 kB	
Summary	Software:	In report *Report B*: 0 packages changed, 0 are new, and 0 are non-existent.		
	Network:	1 changes		
	Hardware:	1 changes		
	Files:	In report *Report B*: 294 files changed, 13 are new, and 2 are non-existent.		

Changed Files: These files exist in both reports but are different — top ▲

File Path	Permissions	Owner / Group ID	SUID / GUID	Contents	Last Modified
Device Files - /dev					
/dev/.udev/uevent_seqnum	0644	0 / 0	false / false	Changed	Tue Feb 09 16:45:54 EST 2010
/dev/bus/usb/001/001	0644	0 / 0	false / false	unchanged	Tue Feb 09 16:45:55 EST 2010
/dev/bus/usb/002/001	0644	0 / 0	false / false	unchanged	Tue Feb 09 16:45:55 EST 2010
/dev/ptmx	0666	0 / 5	false / false	unchanged	Tue Feb 09 21:40:21 EST 2010
User Commands - /bin					
/bin/ping	4755 >> 0500	0 / 0	true / false >> false / false	unchanged	
/bin/ping6	4755 >> 0500	0 / 0	true / false >> false / false	unchanged	

Figure 9: Baseline Comparison Before and After DISA UNIX STIG Application

To help accomplish the goal of ongoing compliance, Security Blanket provides an easy-to-use scheduler capability. Administrators can schedule individual daily, weekly or monthly actions (or a series of actions) that can help automate the process of scanning, configuring (applying), or baselining a group of systems, as shown in Figure 10. In our review, several scheduled scans and baseline tasks were initiated, and the resulting reports were available for review afterward. This is a very handy utility that could be used in conjunction with other monitoring solutions to help maintain a steady state of OS lock down in any environment.

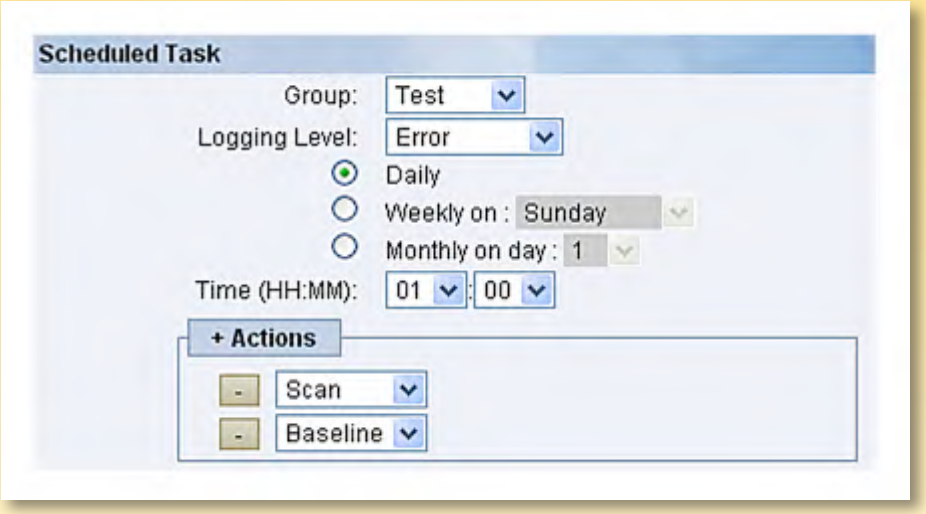


Figure 10: Scheduling Actions for a Group

Security Blanket provides two additional report types as audit trails for the Security Blanket Console system itself and any UNIX/Linux clients. Under the Reports tab are sections for both Console Audit Log and Client Application Logs, which can be leveraged to show that operational tasks have been performed, who performed them, and when they were completed. This can help organizations demonstrate compliance by showing auditors that configuration tasks have been completed in a timely manner (via console activities or on the client itself), meeting policies and compliance requirements. Figure 11 shows the pattern highlighting feature in the Console Audit Log report.

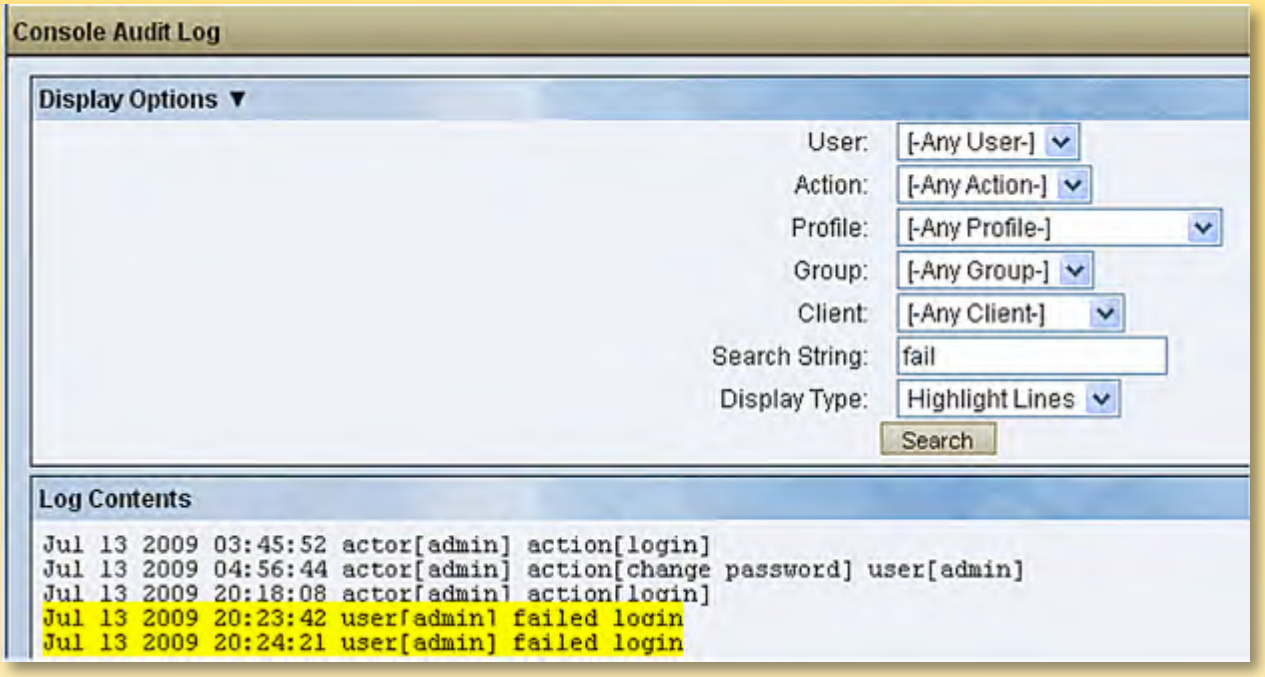


Figure 11: Search String Highlighting in Console Audit Logs

In particular, the Undo feature was very useful. There are many cases in which organizations need to test configuration changes on new and existing systems. In some situations, these changes could have adverse effects on the systems. When they do, the configuration needs to be rolled back to prevent interruption of business services and overall functionality. In this review, we tested the Undo feature multiple times for simple, unique changes as well as entire profile applications. In all cases, the Undo feature successfully removed the changes within a minute or two. For organizations trying to develop new policies and standards for OS security settings, this feature is invaluable.

Security Blanket allows organizations to define configuration policies, apply and remove them, and report on the state of systems at any given time. In addition, the ability to monitor changes to systems is invaluable, helping many administrators keep up with exactly what is happening in their environments.

Security Blanket was simple to use. The review environment was set up and running in a short period of time, and test cases were easy to generate and test. In a number of specific instances, using multiple different compliance and configuration profiles, Security Blanket locked the platforms down to the specifications in the profile, and also undid them on demand. Custom profiles were created and tested, and they were equally as effective. Baseline reports were generated, and comparisons against former baselines and different system's baselines were run with clear, obvious results of what differed between the two. In short, for the features it advertises, Security Blanket worked as it says it does.

Conclusion

It is often said that each UNIX or Linux system is like a snowflake — unique and unlike any other. This is not a flattering description when considering locking down or hardening the many operating systems used in our enterprises today.

Security Blanket makes managing lock down of these systems appear easy. Starting with baseline assessment, the tool also applies and monitors lock down rules for complex systems and keeps systems in continuous compliance. Should systems need to be unlocked for any reason (including adverse effects, changing policies or procedures, or installation of new applications and services), the Undo feature in Security Blanket provides simple and effective capabilities to remove configuration lock down settings easily.

Overall, Security Blanket is a critical layer of defense-in-depth that meets a singular need in enterprises — the protection of critical server operating systems. As such, Security Blanket plays into the larger assessment and configuration management story at the foundational layer — the OS — while at the same time allowing granular control of configuration policies across all critical and sensitive UNIX and Linux systems.

About the Author

Dave Shackleford, Director of Security Assessments and Risk & Compliance at Sword & Shield Enterprise Security, is a SANS Analyst, instructor and GIAC technical director. He has consulted with hundreds of organizations in the areas of regulatory compliance, security, and network architecture and engineering. He's worked as CSO for Configuresoft, CTO for the Center for Internet Security, and as a security architect, analyst, and manager for several Fortune 500 companies.

SANS would like to thank this paper's sponsor:

Last Updated: June 23rd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Paris 2017	OnlineFR	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced