TechTarget Data Center Media

SearchDataCenter.com SearchServerVirtualization.com SearchVMware.com
SearchEnterpriseLinux.com Search400.com Data Center Decisions

SearchEnterpriseLinux.com Pocket E-Guide

Expert Tips for Eliminating Linux Security Risks

Linux security vulnerabilities often arise as a result of the inefficiencies and oversights of today's Linux administrators. In this expert Pocket E-Guide, brought to you by SearchEnterpriseLinux.com and Trusted Computer Solutions, you will discover the five most common Linux security challenges that are currently overlooked in many of today's businesses. Discover the pivotal role default installations, maintenance and system testing play in overcoming Linux security weaknesses. Learn why it is important to test Linux-based systems for vulnerabilities on a periodic and consistent basis.

Sponsored By:

SECURITY BLANKET BY TCS ™

TechTarget®
The Technology Media ROI Experts

SearchEnterpriseLinux.com Pocket E-Guide

Expert Tips for Eliminating Linux Security Risks

Table of Contents:

Five common Linux security vulnerabilities you may be overlooking

Kevin Beaver

I am frequently asked about the typical vulnerabilities in Linux that I find when performing security assessments. Interestingly – and contrary to popular belief – the Linux systems I come across tend to be just as vulnerable as their Windows counterparts. The weaknesses I'm finding are not necessarily the fault of the operating systems (OS), but are due to oversights by Linux administrators. Specifically, they're oversights related to default installations, lack of maintenance, and not testing systems rigorously enough with the right tools to discover weaknesses.

In no particular order, here are the most common Linux vulnerabilities I see – the very things that may be contributing to your organization's business risks:

1. **General lack of patch management for the OS:** Every organization seems to have a patching system and methodology for Windows, but Linux tends to get overlooked. For example, I just came across a Red Hat system missing the Red Hat 2003:138-08 patch for Samba. This patch fixes a remote code execution vulnerability that can be exploited by the free Metasploit tool. The outcome is a remote command prompt with full access to the system – something a malicious user can exploit without anyone ever knowing about it. The IT administrators were proud of their patch management tools and procedures. They just forgot to include Linux in on things.

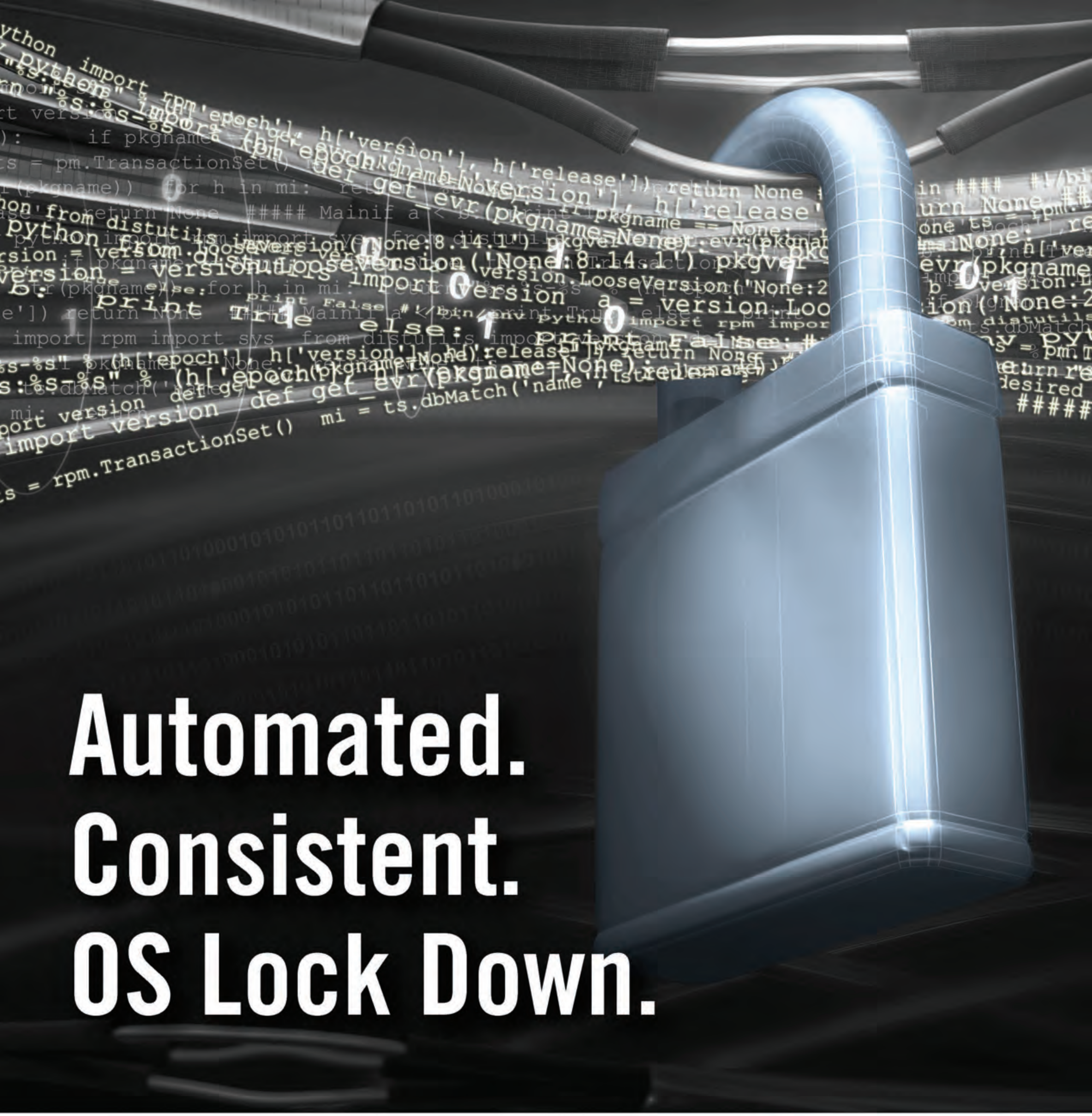
2. **Outdated third-party applications:** Another area for Linux exploitation is facilitated by systems running outdated software such as Apache, PHP, MySQL, OpenSSL, and VNC. As with missing OS patches, outdated applications create a large footprint where malicious intent can lead to exploitation and unauthorized system access (e.g., systems running SSH version 1 with weak encryption ciphers). A malicious internal user or outside third-party can gain unauthorized entry, especially when accessed over an unsecured communications channel such as a wireless network.

3. **Lack of password enforcement:** As with patches, admins tend to be lax on the Linux side when it comes to enforcing strong passwords. I'm unclear on the reason as the enforcement mechanisms are built in. So user names can be easily-gleaned and, ultimately, passwords are cracked.

4. **General lack of system hardening:** Be it SNMP running with default community strings, anonymous FTP providing everyone access to sensitive files, telnet communications susceptible to interception (especially over under-secured wireless networks), and unprotected Samba shares that allow for user account enumeration, you name the service and it's almost always accessible to anyone and everyone. Thus, people who don't need system configuration information now have it, providing them a leg up on further penetrating the system.

5. Lack of backups: The final predictable security weakness with Linux is related to data backups. They're just not being done. I think part of the problem is that certain Linux-based systems are often thought of as non-critical. Web servers, syslog servers, and FTP servers aren't minor systems if you ask me. I sometimes see admins who have a basic file-copy backup of their Linux systems but not the entire OS installation. Then, in the wake of a disaster or drive failure they encounter a long – if not indefinite – recovery.

In many cases, these vulnerabilities are related to Windows-focused admins that do not know how to manage Linux systems. In other cases, I've seen savvy Linux-focused admins being held back by a general lack of management security buy-in and policy enforcement. Whatever's causing the underlying problem, it needs to be addressed. You need to make it a priority to test your Linux-based systems for vulnerabilities on a periodic and consistent basis. Pay special attention to the weaknesses I've listed here. You never know when they're going to be exploited.



Security Blanket ensures enterprise-wide security policy configuration with fully automated OS lock down.

SECURITY BLANKET BY TCS ™

Security Blanket automatically configures the operating system using the most up-to-date industry standard security guidelines. Whether locking down one server or an entire enterprise, Security Blanket performs fast, consistent, and repeatable OS lock down.

Try it for free at www.trustedcs.com/SecurityBlanket or call us at 1-888-662-2724 for more information.

Resources from Trusted Computer Solutions

SECURITY
BLANKET
BY TCS
™

[Automatically Lock Down Linux and Solaris](#)

[Check Out the Security Blanket Blog Spot](#)

[Get a FREE Trial of Security Blanket](#)

About Trusted Computer Solutions
Founded in 1994, Trusted Computer Solutions (TCS) is an industry leader in providing cross domain and cyber security solutions for both the private and public sectors. The company's portfolio of products include the SecureOffice Suite, a group of cross domain solutions that enable secure access and sharing of sensitive or classified information; Security Blanket, an industry award-winning operating system lock down tool for Linux and Solaris; and CounterStorm, an aomaly detection system for identifying targeted and zero day attacks.