
# SUMO Linux: Security utilizing multiple options

By Russ McRee – ISSA member, Puget Sound (Seattle), USA Chapter

## Prerequisites

Bootable DVD reader for 1.0 (2.0 will include CDR &USB releases)

## Similar Projects

SystemResueCD[1]
Ultimate Boot CD[2]

My RSS reader fed me a bit of *toolsmith* nirvana a few of months ago, and I've been looking forward to sharing it with you ever since.

SUMO Linux[3] is the brain child of Marcus Carey of Sun Tzu Data in Washington, D.C area. As part of his DojoSec events and training program, Marcus found himself, and his students, frustrated with needing various tools from different Live CD distributions. Powering down, loading a new disc, and waiting until the new one comes up; annoying and troublesome to say the least.

SUMO Linux 1.0 is the genesis of that teaching experience – one DVD to rule them all. First released in November 2008, this young project represents a multi-boot DVD inclusive of five (that's right, I said five) popular security-related Linux distributions. Bonus!

During my interview with Marcus he revealed that while SUMO Linux is his vision, the lead developer is Jonathon Bennett. As I write this SUMO Linux 2.0 is on the immediate horizon. Plans for the 2.0 release include creating a community to support each tool (a veritable plethora of said tools) to accompany the learning process. There's currently a web-based wiki,[4] and 2.0 will include much of that content in wiki form as well. Marcus informed that he was a bit taken aback by how much pentesters love SUMO (yes, we do) and considers its immediate widespread use a genuine success. SUMO Linux 2.0 will be Debian-based in order to avoid some licensing pitfalls, won't multi-boot (all inclusive instead) and will include additional release media (CD, USB) to aid those with systems that don't boot to DVD. As you read this the beta offering of SUMO Linux 2.0 should soon be available on the SUMO website.

You might enjoy giving a listen to the February 27, 2009 SecuraBit Episdode 23 podcast[5] where they interview Marcus about the pending 2.0 release.

## Using SUMO Linux

### A brief overview of each distribution

Hopefully you're familiar with at least one or two of the distributions included with SUMO Linux:

- The venerable Backtrack 3[6] is the top-rated live distribution dedicated to penetration testing
- Darik's Boot and Nuke (dban)[7] is an extremely useful distribution that securely wipes the hard disks of most computers
- DVL[8] (Damn Vulnerable Linux) is described as the most vulnerable and exploitable operating system ever!
- Helix 2.0 (or 2008), a distribution dedicated to computer forensics, is sadly no longer freely available, another great reason to make use of SUMO Linux.
- Samurai Linux[9] is pre-configured to function as a web pen-testing environment and is offered up by the auspicious team[10] at InGuardians.

## Installation

What installation? Stick SUMO in a machine capable of booting to DVD, power up, and choose your favorite distribution from the menu.


Figure 1 – SUMO Linux menu

I've found that one of the best uses of SUMO is to download the ISO to a computer running VMWare and create at least two virtual machines that boot directly from the single ISO file. You save hard disk space and can boot to any of the five options across multiple

1 http://www.sysresccd.org/Main_Page.
2 http://www.ultimatebootcd.com.
3 http://sumolinux.suntzudata.com.
4 http://sumolinux.com/wiki/Main_Page.
5 http://securabit.com/2009/02/27/491.
6 http://www.remote-exploit.org/backtrack.html.
7 http://www.dban.org.
8 http://www.damnvulnerablelinux.org.
9 http://samurai.inguardians.com.
10 http://inguardians.com/info.

instances. This is ideal when testing Backtrack or Samurai functionality against the intentionally weak DVL (Damn Vulnerable Linux) in order to hone your skills.

## dban

A quick look at dban is important for no other reason than the prevention of data loss. The one way to guarantee you don't leave behind PII or worse when you dispose of old hardware is to either completely destroy the hard drive (I've worked for organizations that opted for this approach) or ensure that is completely wiped.

You may find it useful to boot SUMO Linux on a hardware chassis with external drive connectivity to be used as a wiping station. Choose dban from the menu and opt to ENTER for interactive mode.

Many a security practitioner will argue for at least a DoD 5220.22-M short wipe (3 passes), which will surely prevent data remanence, but there is recent support for the prospect that even a dban Quick Erase (1 pass) will suffice. See Craig Wright's "Overwriting Hard Drive Data"[11] for more details.

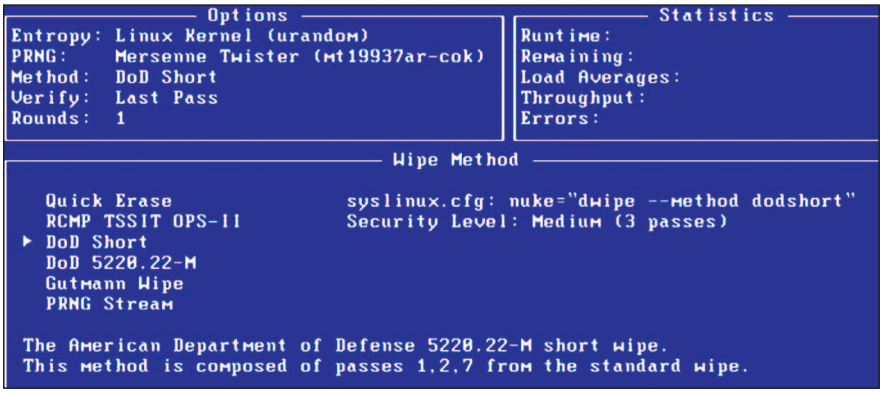


**Figure 2 – Pick your pass pleasure**

Regardless of which option you choose, count this effort in the "you've done the right thing" column. Believe me, simply reformatting a hard drive will provide exactly zero protection against unintended information disclosure.

## The other SUMO distributions

A great deal has been written and discussed with regard to Helix; there's likely little I can offer here that hasn't already been said. It's extremely useful and worthy of the accolades, but I'm not going to mention if further.

I've also spent a great deal of time discussing a variety of Web-application security issues in *toolsmith* and on my blog and website, and I feel like I owe it to you, dear reader, to mix things up a bit.

I will, therefore, say only that you should explore the Samurai Linux distribution at length. I live it and love it; I count it on my "can't live without it" list. Consider firing up Samurai on one VM and DVL on another and "exploring" the DVL Web Exploitation Packages under the *Training Material* menu with the Samurai web testing framework.

That said, DVL also suffers from numerous other gaps, through which we can drive a Mack truck with the likes of Backtrack 3. Using the above mentioned methodology, I powered on two virtual machines, one running Backtrack, the other DVL.

## DVL and Backtrack

I thought I'd explore something I've not been exposed to before, so I opted to use SAINT 6.7.11, included in the menu under Backtrack, then *Vulnerability Detection*. You'll need to get yourself a key and provide the target IP of your DVL instance. Open one of the available text editors, kedit will do, paste the key, save it as `saint.key`, and save it to /opt/saint-6.7.11. In the SAINT gui, select *Configure SAINTexpress Plug-in*, when complete, kill the SAINT shell and restart it, thus updating SAINT to 6.10.3.

I started every service available on the DVL services menu (httpd, ssh, tftpd, etc.) then set up a SAINT scan of the DVL instance from the Backtrack VM. With *Vulnerability Scanning* selected in the SAINT gui, choose *Scan Set-Up*. Add the IP address of your DVL VM, choose the *Scan the target host(s) only* radio button, choose the *Vulnerability Scan* radio button, and check *Exhaustive, Extreme,* and *Full Port Scan*. I bypassed the *Firewall Support* and *Authentication* options as they weren't relevant. Click *Scan Now* and wait for the results; it will take a while (figure 3).

The results correctly indicated *Critical Problems*, but of the seven noted, four were false positives, and three were susceptible to exploit. Of the three valid findings, all were Web server or application related.

SAINT very capably identified all of the intentional vulnerabilities offered in DVL's Web exploitation packages, lending

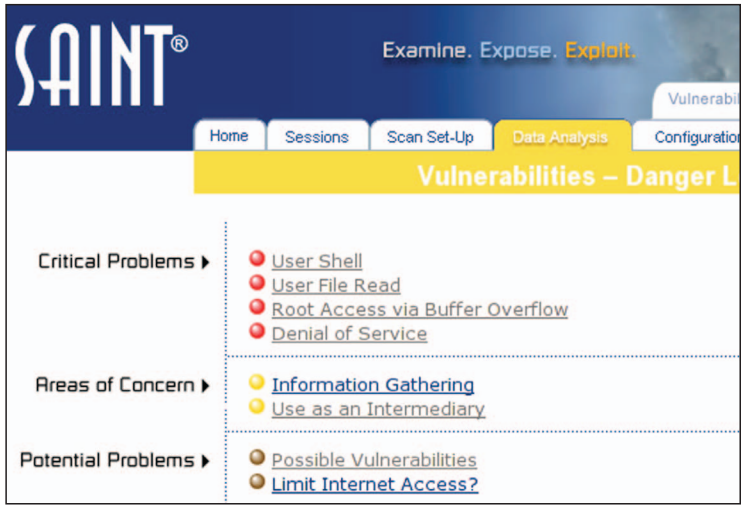


**Figure 3 – SAINT results**

11 http://sansforensics.wordpress.com/2009/01/15/overwriting-hard-drive-data.

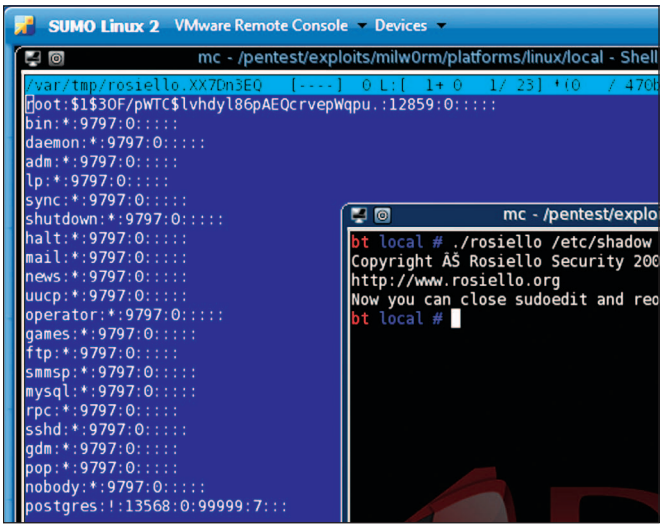


**Figure 4 – I don't think /etc/shadow belongs there.**

strength to my argument that you'll have a blast using Samurai Linux against DVL, given that the vast majority of remote exploit opportunities are Web-related.

I also recommend testing SAINT in Windows-centric enterprise environments (with safe checks on); it offers many Windows, HP, Trend Micro, and Oracle tests and exploits.

DVL also offers some excellent local binary exploitation opportunities, best explored directly on the DVL VM.

In the oldie but goodie category, for this exercise we'll break sudo version 1.6.8, found in the DVL menu under *Damn Vulnerable Linux, Training Material*, and finally *Binary Exploitation*.

Open two instances of the SudoEdit 1.6.8 shell; the exploit requires it.

The flaw in sudo 1.6.8 exists in the sudoedit (`sudo –u`) feature, giving an attacker read rights to an otherwise unreadable file.

In both shells, pass `cd /pentest/exploits/milw0rm/platforms/linux/local`.

In one shell, execute `gcc 470.c –o rosiello`.

This will compile Angelo Rosiello's sudoedit exploit[12] into binary to be read by sudoedit.

In one shell execute `sudoedit rosiello`.

In the other shell, execute `./rosiello /etc/shadow`.

The result should read *Now you can close sudoedit and reopen rosiello!*

Back in the shell running sudoedit, hit F10 to close sudoedit, the rerun `sudoedit rosiello`.

Yep, that's `/etc/shadow` you're looking at (Figure 4). Good times. ;-)

If time allowed for it, you could spend endless hours studying broken software at great length with the DVL distro, either local to it on a VM, or firing away at it from other SUMO Linux distributions.

## In conclusion

From an organizational perspective SUMO Linux can well serve your training cause, offering you the opportunity to create scenarios for class members to work through.

I look forward to the next release of SUMO Linux and believe it will offer great insight for those seeking to enhance and hone security skills, or use the vast toolkit for audit/pentest engagements.

Cheers…until next month.

## Acknowledgments

Marcus Carey for the vision that is SUMO Linux.

## About the author

*Russ McRee, GCIH, GPEN, GCFA, CISSP, is a security analyst on the Security Incident Management team for Microsoft's Online Services. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ@holisticinfosec.org.*

12 http://www.milw0rm.com/exploits/470.