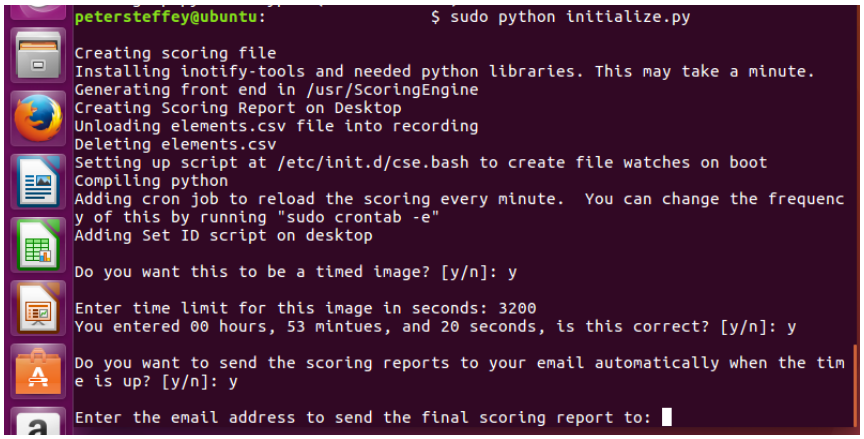
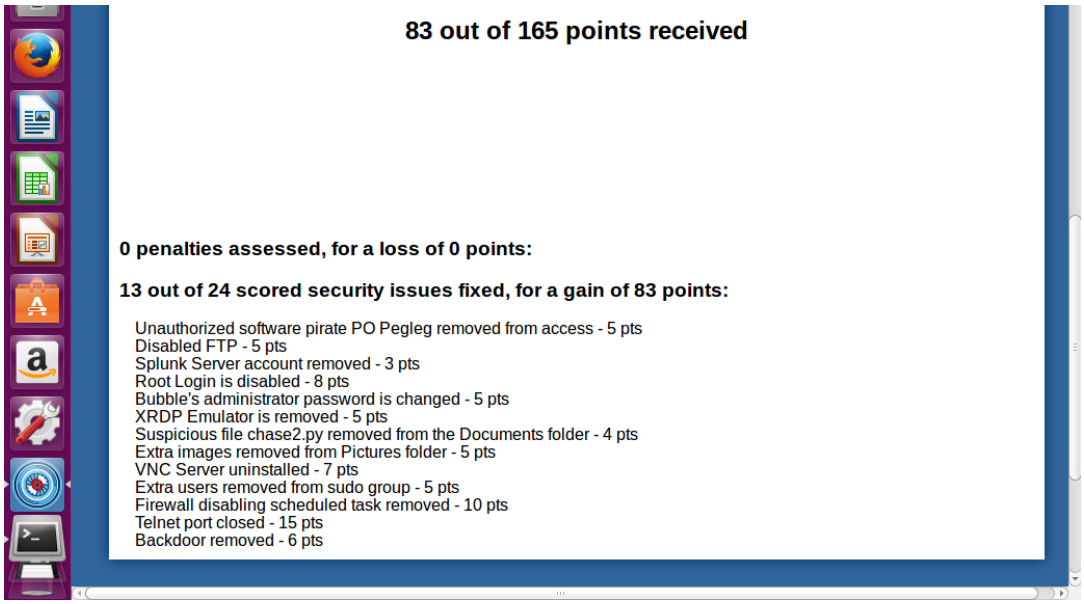
LWASP

Linux Watchful Adaptive Security Profiler

Simple Installation from Excel and Command Line

With easy to follow, interactive instructions for setting up the scoring engine.





Familiar User Interface

Engage users with realistic live scoring.

Flexible and Extensive Framework

Optional ability to modify the code to fit your individual needs.

Scoring Capabilities

What LWASP can check	Examples of what you can score
Contents of a file	• If the guest account is disabled in /etc/lightdm/lightdm.conf • Whether users are added or deleted in the /etc/password file • Password policy in /etc/login.defs and /etc/pam.d/* • Whether automatic updates are enabled in /etc/apt/apt.conf.d/10periodic
If a file or directory exists	• If a backdoor has been removed (such as netcat in /bin/nc) • Whether files are setup for FTP correctly
If a service is running	Critical services such as SSH and Apache
Answers to forensics questions	Answers in files on the desktop in the CyberPatriot format (ANSWER: …)
The version of a program or service	If a certain program or service has been updated
What ports are open	Whether a services are actively broadcasting on a port
Permissions of a file or directory	Whether files such as /etc/passwd and /etc/shadow or directories such as the user's home directory are secure
The output of any shell/bash command	Basically a catchall: • Checking crontab entries • Firewall status • etc.