



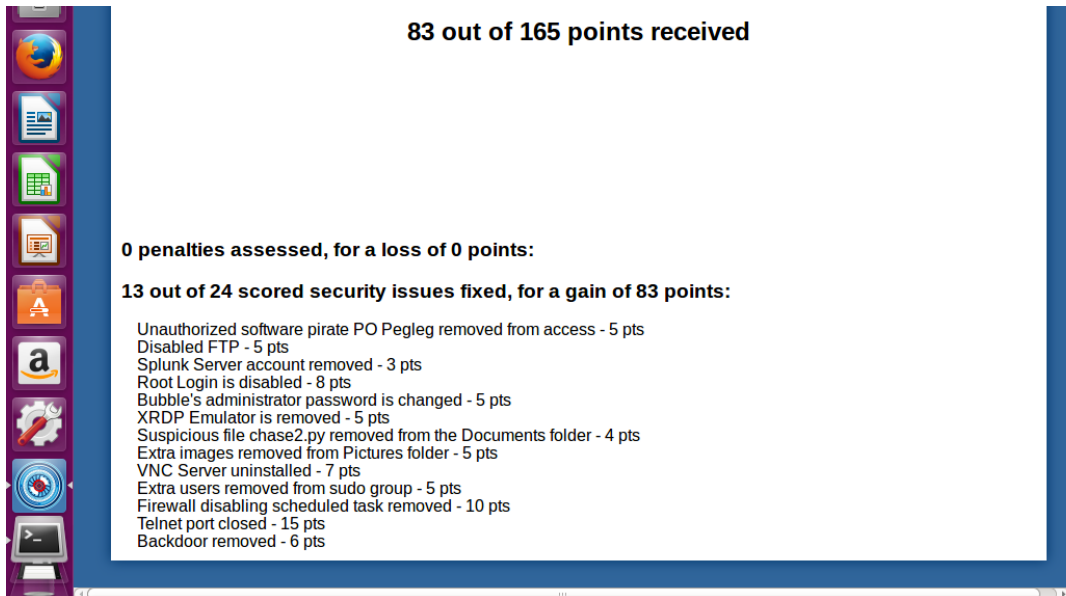
LWASP

Linux Watchful Adaptive Security Profiler

Simple Installation from Excel and Command Line

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

```
petersteffey@ubuntu:~$ sudo python initialize.py
Creating scoring file
Installing inotify-tools and needed python libraries. This may take a minute.
Generating front end in /usr/ScoringEngine
Creating Scoring Report on Desktop
Unloading elements.csv file into recording
Deleting elements.csv
Setting up script at /etc/init.d/cse.bash to create file watches on boot
Compiling python
Adding cron job to reload the scoring every minute. You can change the frequency of this by running "sudo crontab -e"
Adding Set ID script on desktop
Do you want this to be a timed image? [y/n]: y
Enter time limit for this image in seconds: 3200
You entered 00 hours, 53 minutes, and 20 seconds, is this correct? [y/n]: y
Do you want to send the scoring reports to your email automatically when the time is up? [y/n]: y
Enter the email address to send the final scoring report to: [email address]
```

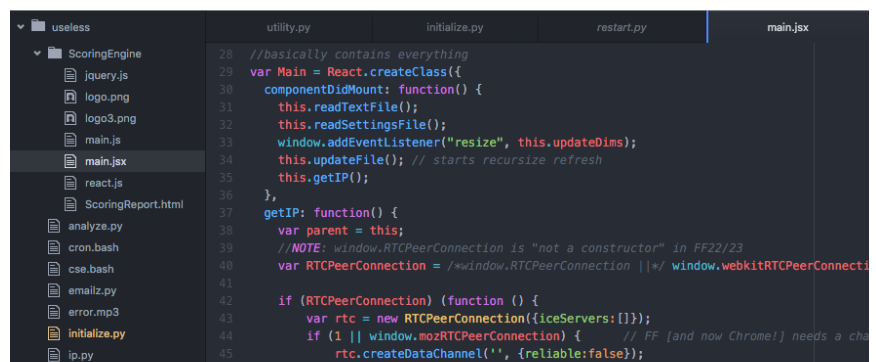


Familiar User Interface

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/passwd` file
- Password policy in `/etc/login.defs` and `/etc/pam.d/*`
- Whether automatic updates are enabled in `/etc/apt/apt.conf.d/10periodic`



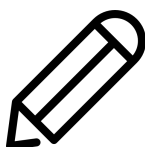
If a file or directory exists

- 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: ...)



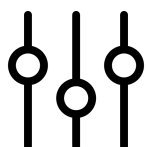
The version of a program or service

If a certain program or service has been updated



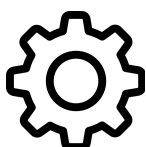
What ports are open

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.