



LWASP Tutorial

1

Prepare a Linux Virtual Machine (VM) with vulnerabilities, such as bad users and backdoors.

2

Download the lwasp folder from the CyberPatriot website (<https://www.uscyberpatriot.org/lwasp>)

3

Generate the elements.csv file using the “LWASP Elements Generator.xlsx” interactive excel file. Follow the instructions in the file, and be sure to enable macros.

I Fill in scoring elements

II Press Button

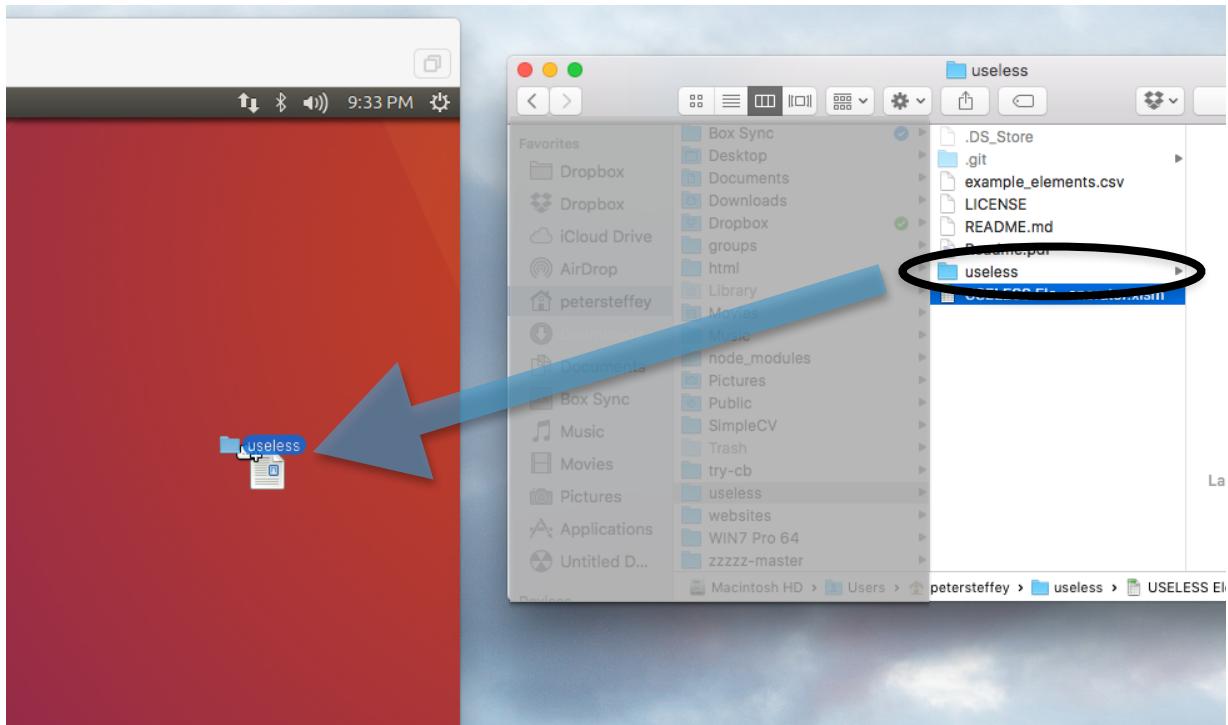
What you need to do:
Using the example above, make your own spreadsheet in the area below of what needs to be scored/penalized based on your image and scenario.
You can use as many or as little of the spaces below as needed. I would not recommend going past 100, as that would be excessive, but there is nothing in the code that is capped at 100.
I'm sure that I have not yet imagined all of the use cases, and because this is open source, and therefore encourage users to push the limits.
When you are done filling out the table, press the export button to the right to generate the csv file. If the command fails, press Abort, then the close window button, then press save, then press save again. Then return to the readme for the rest of the instructions.
If this does not work, simply copy the Title, Mode, Points, Type, and Extras columns, excluding the headers, into a new workbook, and export that as a CSV.

Export to elements.csv

Number	Title	Mode	Points	Type	Extras
1	Guest account is disabled	V	10	FileContents	/etc/lightdm/lightdm.conf TRUE allow-guest=false
2	Unauthorized users RedTeam and Backdoor are removed	V	15	FileContents	/etc/shadow FALSE redteam backdoor
3	Maximum password age is set for 30 days	V	12	FileContents	/etc/login.defs TRUE PASS_MAX_DAYS 30
4	Backdoor file at /home/user/.backdoor is removed	V	20	FileExistence	/home/user/.backdoor FALSE
5	Firewall is Active	V	8	Command	sudo ufw status FALSE inactive
6	Disabled FTP	V	10	Service	vsftpd FALSE
7	Forensics Question is correct	V	13	Forensics	(/home/user/Desktop/ForensicsQuestion.txt some answer FALSE
8	Apache (Web) Server is down	P	50	Service	apache2 FALSE
9	Critical user Admin has been disabled	P	10	FileContents	/etc/shadow FALSE admin:\$

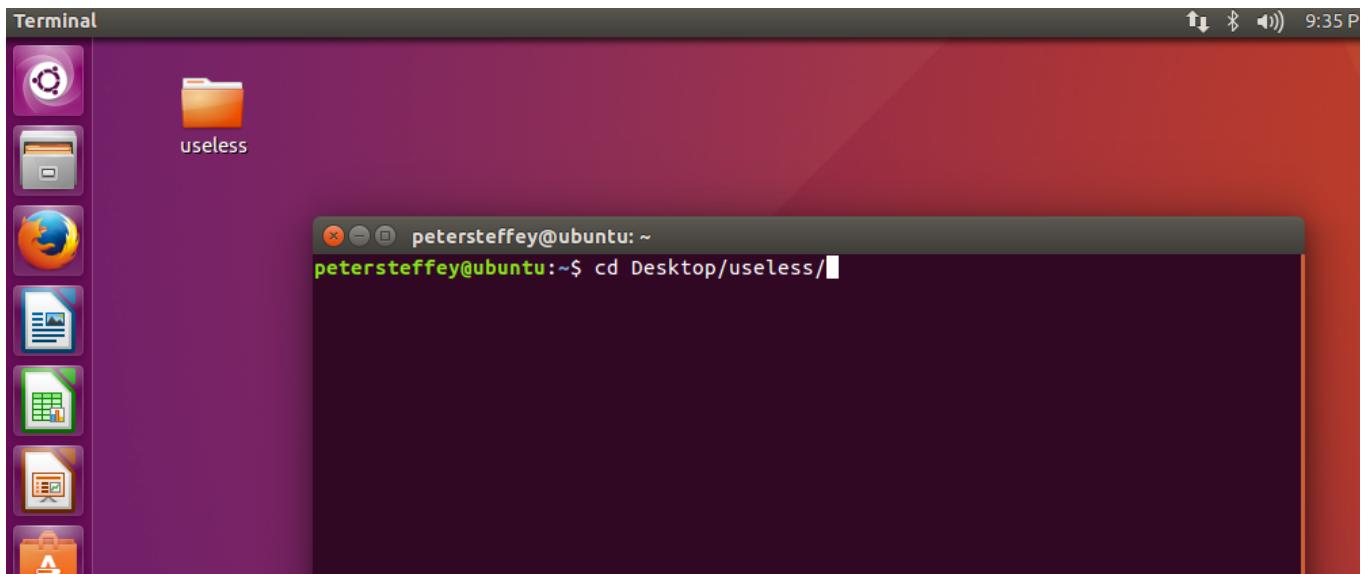
4

Move the internal Iwasp folder into the virtual machine.
It doesn't matter where you put it on the VM.



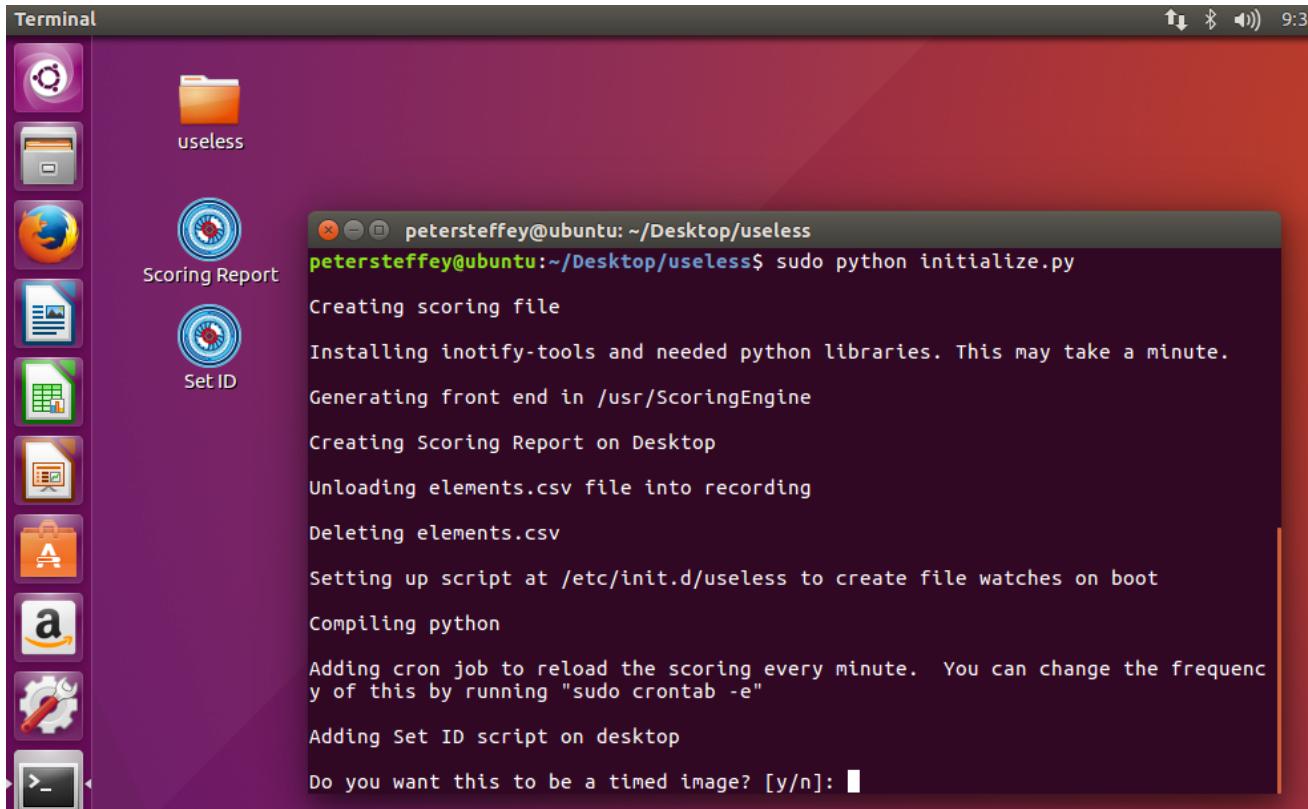
5

Open a terminal on the VM, and cd (change directory) into the folder.



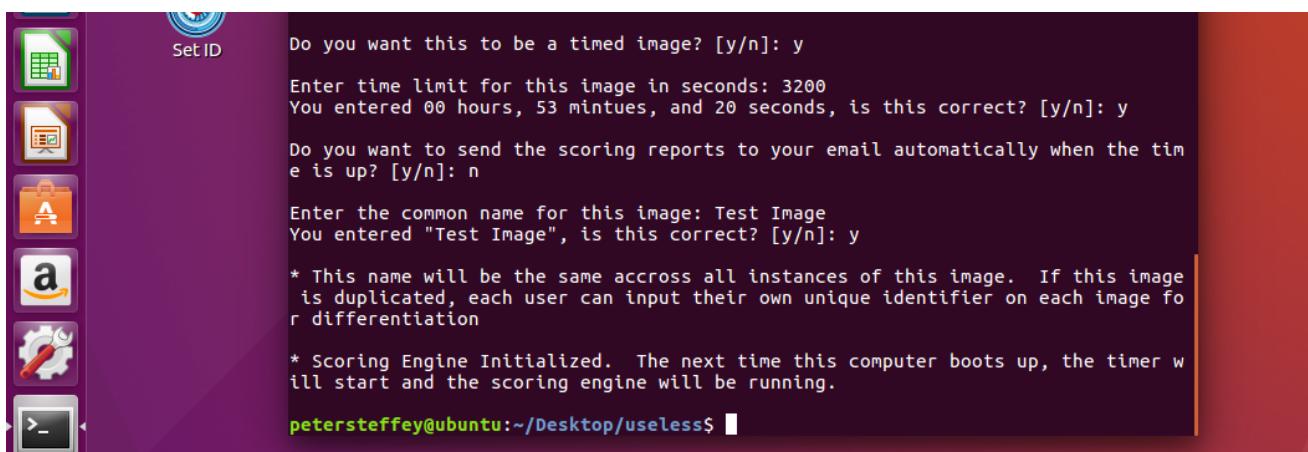
5

Run the command: sudo python initialize



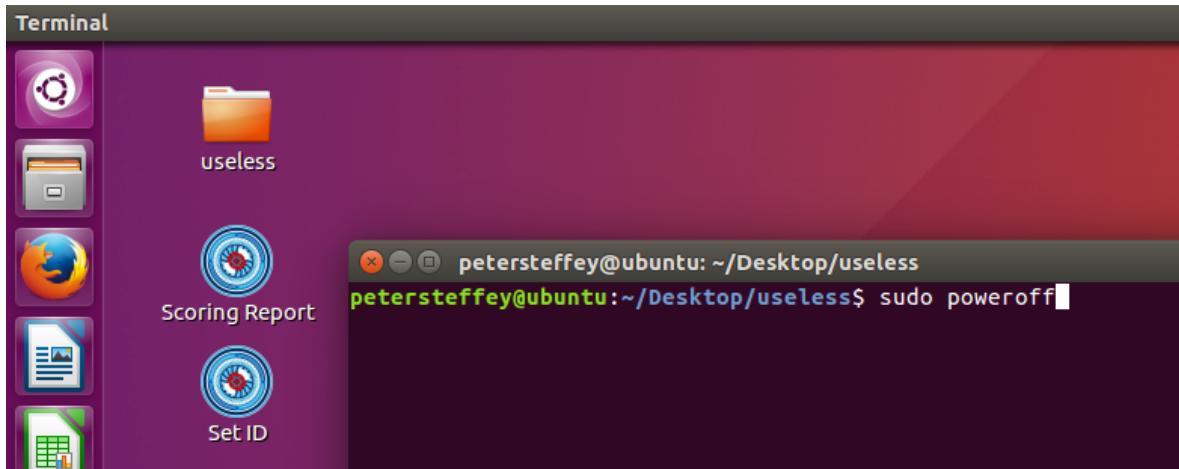
b

Follow the detailed prompts to setup the image.
Make sure not to modify anything in the lwasp folder after this point.



7

Shutdown the image using the command: sudo poweroff



8

Distribute the image to all of the competitors, and then run them using VMWare Player or VSphere Client on Windows, or VMWare Fusion on Mac

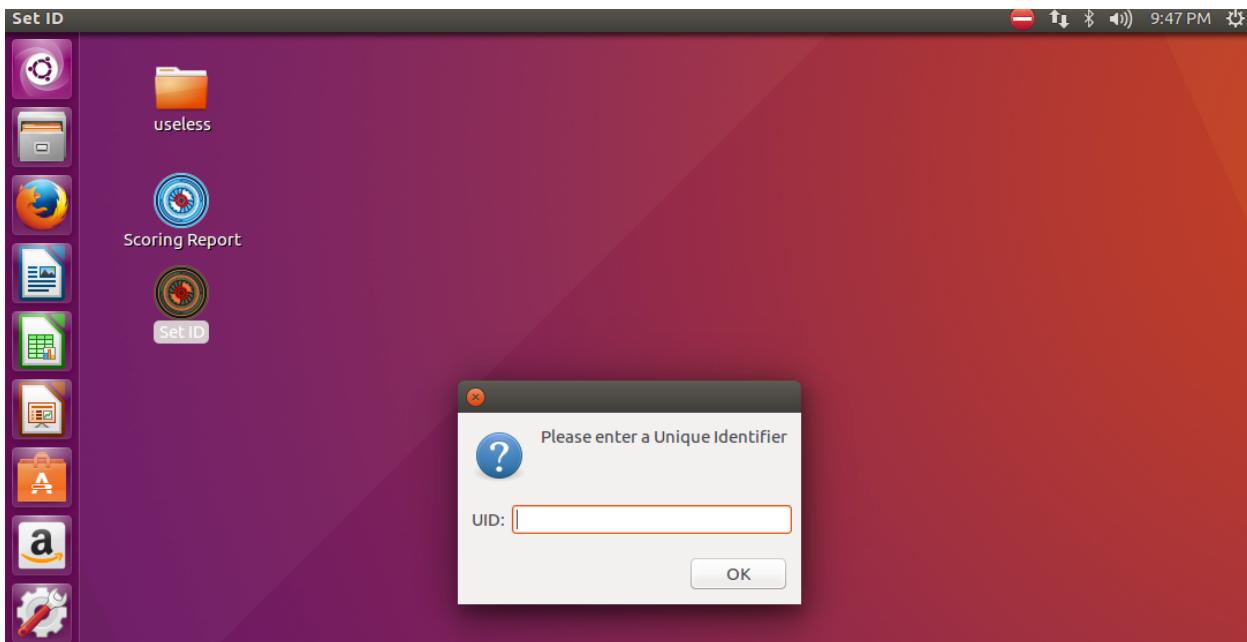
9

Once booted, each competitor should open up the scoring report to make sure it is working.



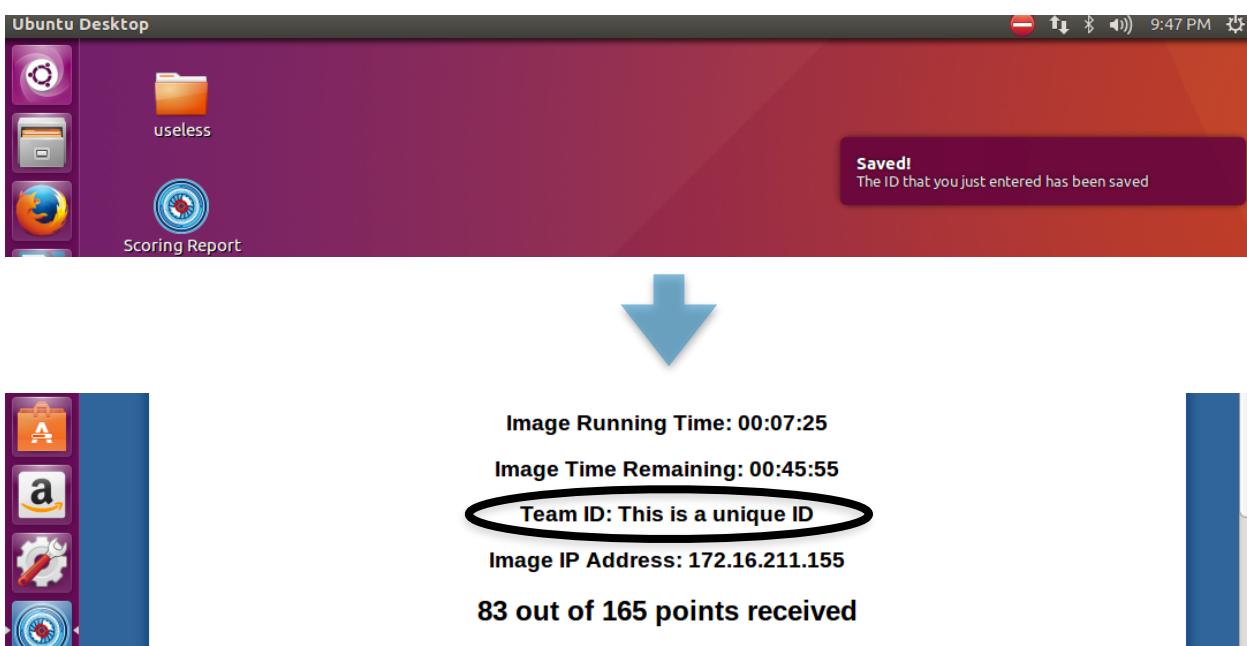
10

As noted on the scoring report, each competitor should run the Set ID program on the desktop, so that you, as the coach or mentor, can differentiate between the scoring reports from various competitors. This will usually be a competitor's name or some other sort of identifier.



11

The notification will indicate that this was save correctly, and this ID will be saved on the scoring report.



12

If you enabled email reporting, the scoring report will be emailed to you either when the time is run out, or, if this is not a timed image, when the competitor runs the Send Scoring Report program on the desktop. If you did not enable email reporting, the competitors can send you pictures or a web archive of their scoring report.

13

Email any feedback or feature requests about the LWASP scoring engine to steffeydev@icloud.com