# CYBR-10025 – Lab 3: Deplorable Arts

# Objective(s):

Retrieve the encrypted hash of the root password from a Linux system.

# Introduction:

Deplorable Arts is a community run, community supported website for sharing art. Virtually any image can be uploaded. The website is very simple and the users like it that way, there are no accounts and no administrators except for the Linux system admins who run the application from servers in their own houses.

# Apparatus

* VirtualBox https://www.virtualbox.org/wiki/Downloads
* DeplorableArts.ova from Canvas.

# Procedure

1. Import the deplorablearts.ova
2. ***Start the DeplorableArts VM***
3. ***Note the IP address on the boot screen (likely 192.168.99.101)***
4. ***Point your web browser at:*** [***http://192.168.99.101/deplorable\_arts***](http://192.168.99.101/deplorable_arts)

# What To Hand In

* A MS Word file containing:
  + A written step-by-step log of the different things you investigated, information you gathered and what techniques you tried. Doing well on this assignment depends on writing clear instructions on how to gain high level access. If the person marking can’t repeat your steps and get the same effect this will cost you marks.
  + The encrypted hash of the root account.

# Rules

1. You may not use an automated tool like Nessus.
2. You may not use a local attack: That is an attack that would require you to be in the same room as the Linux machine if the web application was running on a physical machine instead of a VM. All attacks must be executable using remote tools (browser, ssh, netcat, etc…)
3. ***You may do just about anything else.***

# Hints:

1. Explore the web site and make note of form fields, cookies and how they are sent.
2. Examine the HTML look for other directories you might have access to and whether you are able to read from them or write to them.
3. It may be helpful (but not necessary), to try to get the PHP code from the website. This is probably a two-step process, moving it to a place where you have access. Then downloading it.
4. Examine the PHP file for weaknesses.
5. Getting the root password may involve setting up a remote shell. Consult the slide decks where we attempted to create a forward shell. If you’re interested in doing a reverse shell check out this: <https://www.hackingtutorials.org/networking/hacking-netcat-part-2-bind-reverse-shells/>
6. Once you have access to the system, google to see where Linux keeps encrypted passwords.
7. You may need to perform a privilege escalation, consult the appropriate slide decks to help you find files that are exploitable.
8. If you need help in attempting to exploit a particular command check out this guide: <https://gtfobins.github.io/> It has many simple examples for taking advantage of exploitable commands.
9. Keep in mind if you are using local only networking. The IP address of your webbrowser is (usually) 192.168.99.1