1. Once you find that machine supports RCE, you need to get remote access to that machine. To remotely access a machine you can follow below approach
2. If machine has nc installed, then use nc to get remote access. For this use nc commands mentioned [here](http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet).
   1. Most probably this shell will be a ‘DUMB SHELL’. It will have lot of constraints. So, convert this to interactive tty using python’s PTY module. Refer [this](https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/) for more details. To prevent echo’ing of command you typed, use *sty raw -echo*. This should be done before starting nc listener.
3. If nc is not installed, then use msfvenom to create non-staged payload(its format is *shell\_...* and not *shell/….*). In this case, you won’t get interactive-tty. So this approach should not be preferred.
4. Use meterpreter to create appropriate payload. Handle this meterpreter using Metasploit.
5. After getting remote access, start enumerating the system.
   1. If you have access to source code of web-app, look into it for login creds. Just skim over these files. At times, you can get hard-coded username and password. At-times, db. creds are hard-coded in these files.
   2. Follow below steps manually. (See pdf in your directory for more details)
      1. Look for files with SUID/SGID as set and are not generally present in a box.

*find / \( -perm -4000 -o -perm -2000 \) 2>/dev/null;*

*netstat -anop | grep*

* + 1. Look into cron jobs for any tasks that are not present normally in a machine
    2. Look into all listening ports. This will help you in understanding what services are running on this machine.

*netstat -anop | grep -i LIST*

* + 1. For various users present
       1. If you know password for a user, run *sudo -l* to list what commands user can run as sudo.
       2. Look into .ssh folder
       3. Look into *.bash\_history, .bashrc*
  1. Trying running below three scripts for Linux Enumeration.
     1. [LinEnum.sh](https://github.com/rebootuser/LinEnum)
     2. [Linuxprivchecker.py](https://github.com/TheRealHetfield/linuxprivchecker) [Try this file at last]
     3. Unixprivsec.sh [searching for GitHub link]

1. Now, you need to escalate privilege. DirtyCow is pretty common mode for this. Hence, look for kernel-version. If after going through above steps, you aren’t able to find any exploit, use script [Linux-Exploit-Suggestor-2](https://github.com/jondonas/linux-exploit-suggester-2). But remember, scripts such as these has very high false positive rate. They have checks which can easily be by-passed. Hence, script should be your last resort.