**Hacking For Beginners**

* *Linux Console Short Cut*

Copy from Console → Ctrl + K

Paste to Console → Ctrl + Y

Clear Console Text → Ctrl + L

* Access Root User

su Or su -

sudo su

* less

less command is print the file value on the console. The Difference of the ‘cat’ is that command is can move use Pg up and Pg Down or Up Arrow and Down Arrow. Also find some word use slashes. If you want quit less status, press the q.

* traceroute Options

In Linux, Traceroute command defaultly use the UDP Datagram. But Set the I(Upper case I), use the ICMP Echo instead of UDP Datagram.

When I test the difference between Non I Options and I Options, I could see something and it’s curious for me. First Section is result of try traceroute the google.com without I options.

*raceroute to google.com (172.217.24.206), 30 hops max, 60 byte packets*

*1 router.asus.com (192.168.219.1) 0.275 ms 0.286 ms 0.357 ms*

*2 123.212.199.1 (123.212.199.1) 3.660 ms 14.769 ms 14.952 ms*

*3 100.85.73.41 (100.85.73.41) 6.748 ms 6.607 ms 6.856 ms*

*4 10.72.253.14 (10.72.253.14) 6.742 ms 2.610 ms 6.679 ms*

*5 10.222.25.88 (10.222.25.88) 7.103 ms 10.222.25.96 (10.222.25.96) 7.669 ms 10.222.25.88 (10.222.25.88) 7.044 ms*

*6 10.222.25.249 (10.222.25.249) 7.440 ms 10.222.23.201 (10.222.23.201) 6.511 ms 10.222.22.109 (10.222.22.109) 6.749 ms*

*7 142.250.162.182 (142.250.162.182) 37.381 ms 35.739 ms 142.250.162.140 (142.250.162.140) 35.912 ms*

*8 \* \* \**

*9 108.170.233.190 (108.170.233.190) 37.432 ms 209.85.253.56 (209.85.253.56) 33.943 ms 108.170.242.129 (108.170.242.129) 39.100 ms*

*10 108.170.242.177 (108.170.242.177) 38.306 ms 108.170.242.144 (108.170.242.144) 38.645 ms 108.170.242.209 (108.170.242.209) 38.705 ms*

*11 209.85.244.37 (209.85.244.37) 38.405 ms 209.85.244.2 (209.85.244.2) 38.198 ms 216.239.43.157 (216.239.43.157) 39.946 ms*

*12 216.239.63.162 (216.239.63.162) 40.670 ms 64.233.175.104 (64.233.175.104) 38.754 ms \**

*13 \* 72.14.235.147 (72.14.235.147) 68.277 ms 68.228 ms*

*14 \* \* 209.85.142.173 (209.85.142.173) 67.638 ms*

*15 172.253.64.173 (172.253.64.173) 65.002 ms 209.85.142.27 (209.85.142.27) 64.688 ms 64.405 ms*

*16 108.170.241.97 (108.170.241.97) 65.216 ms 65.171 ms 108.170.241.65 (108.170.241.65) 64.476 ms*

*17 209.85.143.123 (209.85.143.123) 63.968 ms 209.85.143.119 (209.85.143.119) 66.760 ms 64.172 ms*

*18 hkg12s13-in-f14.1e100.net (172.217.24.206) 66.187 ms 66.227 ms 60.741 ms*

And Second is output of traceroute after add I options.

*traceroute to google.com (172.217.175.78), 30 hops max, 60 byte packets*

*1 \_gateway (192.168.219.1) 0.249 ms 0.333 ms 0.407 ms*

*2 123.212.199.1 (123.212.199.1) 17.341 ms 17.353 ms 17.378 ms*

*3 100.85.73.41 (100.85.73.41) 6.318 ms 6.512 ms 6.713 ms*

*4 10.72.253.124 (10.72.253.124) 6.638 ms 6.670 ms 6.697 ms*

*5 10.222.25.94 (10.222.25.94) 7.822 ms 7.874 ms 7.899 ms*

*6 10.222.23.201 (10.222.23.201) 9.255 ms 8.714 ms 4.592 ms*

*7 142.250.162.182 (142.250.162.182) 39.604 ms 39.641 ms 39.699 ms*

*8 209.85.245.139 (209.85.245.139) 39.496 ms 39.647 ms 39.676 ms*

*9 172.253.70.183 (172.253.70.183) 40.259 ms 40.306 ms 40.335 ms*

*10 nrt20s20-in-f14.1e100.net (172.217.175.78) 39.309 ms 39.337 ms 39.362 ms*

If you see that, you guess why Second is short more than first? But that is not my curious point. When I try to traceroute, I did same address at google.com. But as look as the destination address is not same between first and second.

* nc(netcat)

The tool of network debugging or hack. The basic syntax is “nc [options] [target IP] [target Port]”

* hping3

ping is work use ICMP however hping3 is work on tcp. Usage is hping3 -s [source port] -p [destination port] [destination address] -[TCP Flag]

* Wireshark Capture filter vs display filter

Wireshark is capturing all packet on specified interface and show that. Display filter is match the rule from capture result and show them. But Capture filter is just capturing the packet that depending on rule.

* Port Scanning

-SYN Scan

Send TCP SYN Packet if port is opened, server is return the SYN/ACK Packet. Otherwise, port is closed, reply packet is set the RST Flag.

* Vulnerabilty and Exploit

Vulnerability is weakness of the system like easy password or simple authentication etc. And Exploit is the taken advantage use the vulnerability. Vulnerability can using as hacking point but not at all.

* CVE & CVSS

-CVE(Common Vulnerabilities and Exposures)

A unique identified for a vulnerabilities. Start with year followed by a number like 2020-2523

-CVSS(Common Vulnerability Scoring System)

Ranges from 0 to 10. The higher the score, the more critical the vulnerability.

* NSE(NMAP Script Engine)

Script file located on /*usr/share/nmap/scripts/ .*

* Openvas

Tool for scan a target. It works on Web Page and easily to use.

* RCE(Remote Code Execution)

Execute code or commands remotely on the target server. It could lead to shell access.

* Metasploit

Metasploit is Open-Source software developed for Ethical Hacking. It is one of the software framework.

- Core commands

→ ?, sessions, set, unset

- Module commands

→ search, info, use, options, back

For start the metasploit on Kali, enter the “msfconsole” in terminal. Msfconsole is need root privileges so if you run that command as non-root user, must set the sudo before command.