

LEARN PING AND ITS USES

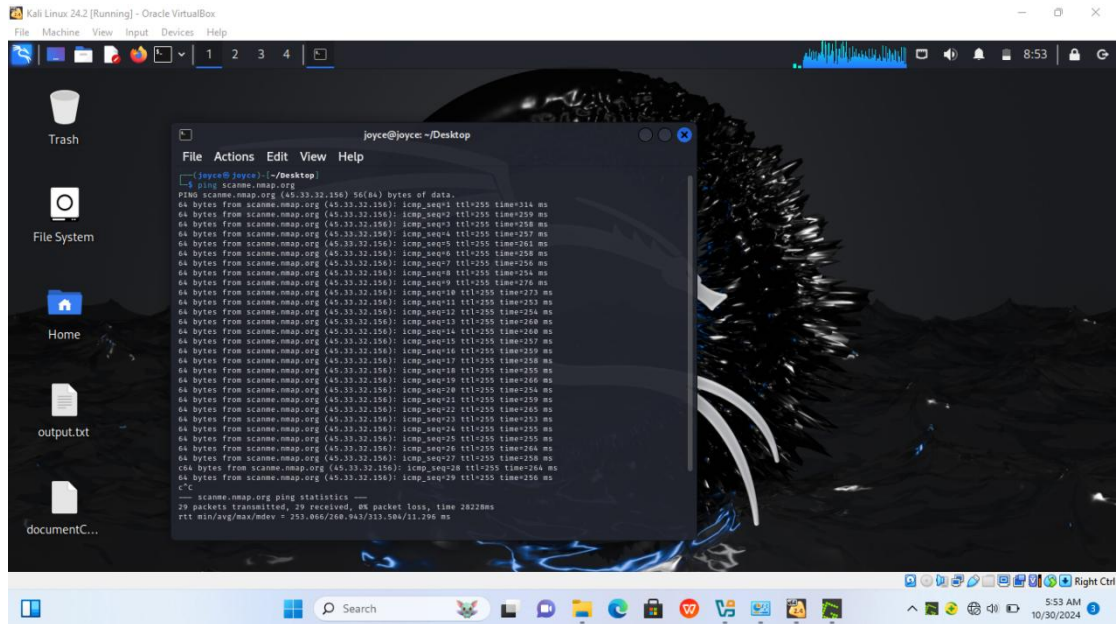
Project Objective: Learn how to use ping and its different parameters.

Ping is a simple and useful network-based utility which can be used to identify if a host is up. It can also be called an “echo” reply.

Project Tool: Kali Linux

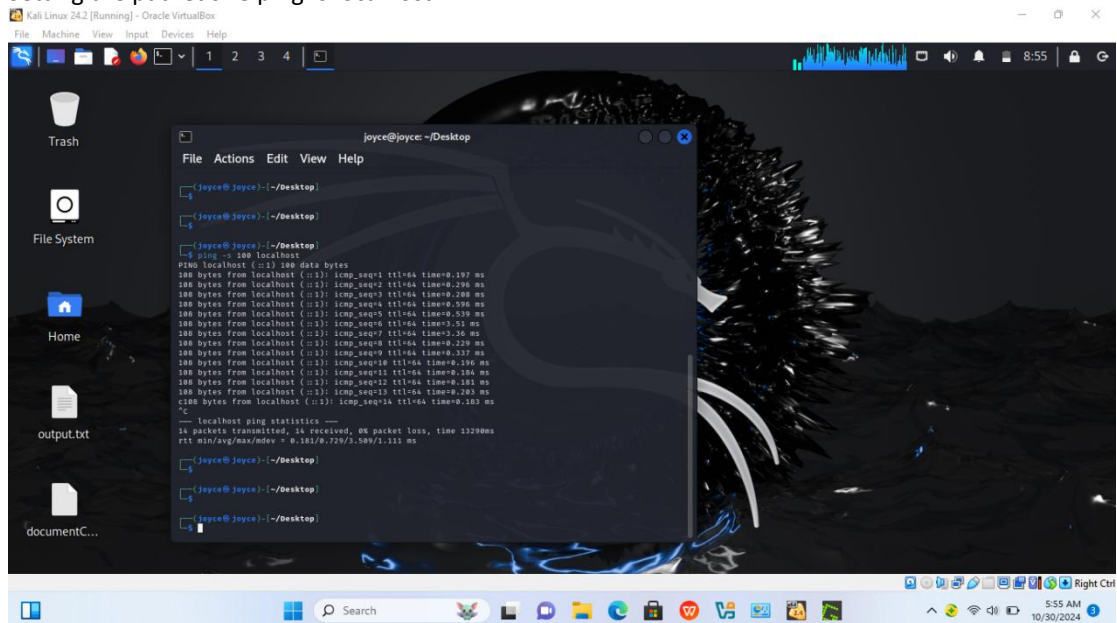
Ping scanme.nmap.org: This command will continue to send ICMP packages to the destined IP address until the Ctrl+C key.

It sent 29 packets, it received 29 packets, indicating that the host is up.

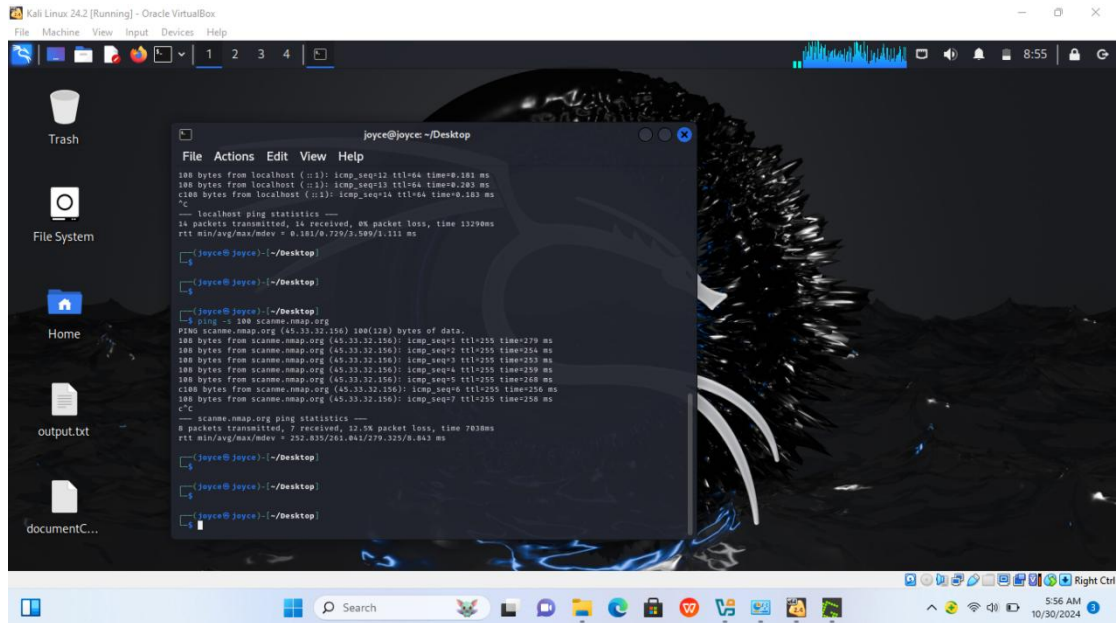


```
joyce@joyce: ~/Desktop
File Actions Edit View Help
joyce@joyce:~/Desktop
$ ping scanme.nmap.org
PING scanme.nmap.org (45.33.32.156) 56(64) bytes of data:
64 bytes from scanme.nmap.org: icmp_seq=1 ttl=255 time=214 ms
64 bytes from scanme.nmap.org: icmp_seq=2 ttl=255 time=259 ms
64 bytes from scanme.nmap.org: icmp_seq=3 ttl=255 time=258 ms
64 bytes from scanme.nmap.org: icmp_seq=4 ttl=255 time=257 ms
64 bytes from scanme.nmap.org: icmp_seq=5 ttl=255 time=261 ms
64 bytes from scanme.nmap.org: icmp_seq=6 ttl=255 time=258 ms
64 bytes from scanme.nmap.org: icmp_seq=7 ttl=255 time=259 ms
64 bytes from scanme.nmap.org: icmp_seq=8 ttl=255 time=254 ms
64 bytes from scanme.nmap.org: icmp_seq=9 ttl=255 time=270 ms
64 bytes from scanme.nmap.org: icmp_seq=10 ttl=255 time=273 ms
64 bytes from scanme.nmap.org: icmp_seq=11 ttl=255 time=253 ms
64 bytes from scanme.nmap.org: icmp_seq=12 ttl=255 time=254 ms
64 bytes from scanme.nmap.org: icmp_seq=13 ttl=255 time=260 ms
64 bytes from scanme.nmap.org: icmp_seq=14 ttl=255 time=249 ms
64 bytes from scanme.nmap.org: icmp_seq=15 ttl=255 time=257 ms
64 bytes from scanme.nmap.org: icmp_seq=16 ttl=255 time=259 ms
64 bytes from scanme.nmap.org: icmp_seq=17 ttl=255 time=258 ms
64 bytes from scanme.nmap.org: icmp_seq=18 ttl=255 time=255 ms
64 bytes from scanme.nmap.org: icmp_seq=19 ttl=255 time=256 ms
64 bytes from scanme.nmap.org: icmp_seq=20 ttl=255 time=254 ms
64 bytes from scanme.nmap.org: icmp_seq=21 ttl=255 time=255 ms
64 bytes from scanme.nmap.org: icmp_seq=22 ttl=255 time=255 ms
64 bytes from scanme.nmap.org: icmp_seq=23 ttl=255 time=253 ms
64 bytes from scanme.nmap.org: icmp_seq=24 ttl=255 time=255 ms
64 bytes from scanme.nmap.org: icmp_seq=25 ttl=255 time=255 ms
64 bytes from scanme.nmap.org: icmp_seq=26 ttl=255 time=264 ms
64 bytes from scanme.nmap.org: icmp_seq=27 ttl=255 time=256 ms
64 bytes from scanme.nmap.org: icmp_seq=28 ttl=255 time=264 ms
64 bytes from scanme.nmap.org: icmp_seq=29 ttl=255 time=256 ms
^C
--- scanme.nmap.org ping statistics ---
29 packets transmitted, 29 received, 0% packet loss, time 2822ms
rtt min/avg/max/mdev = 253.066/268.943/313.504/11.296 ms
```

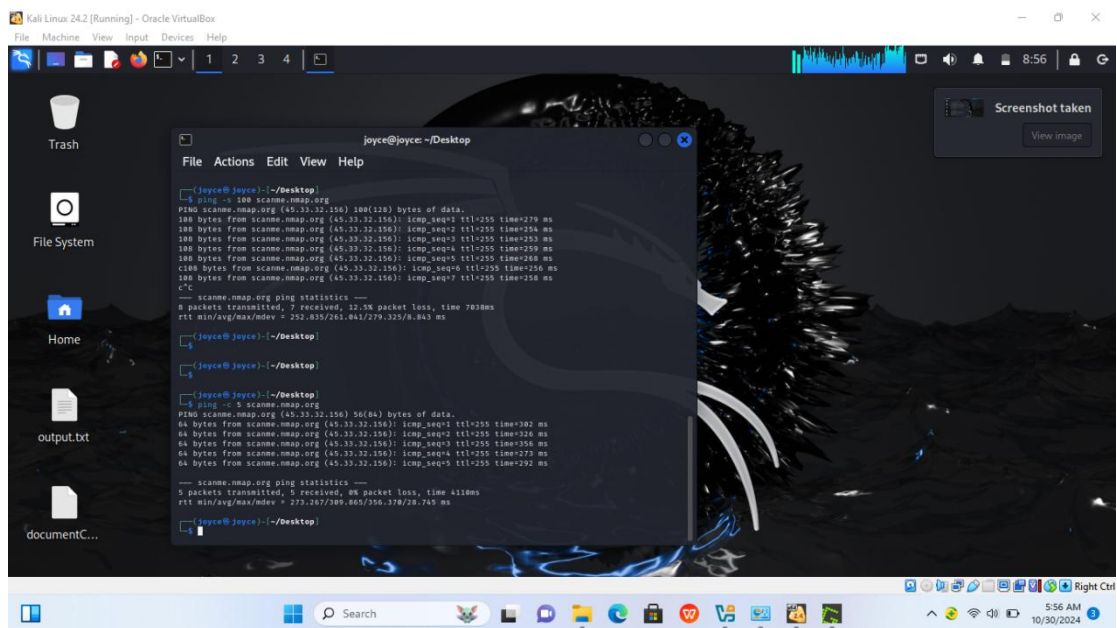
Setting the packet size ping -s localhost

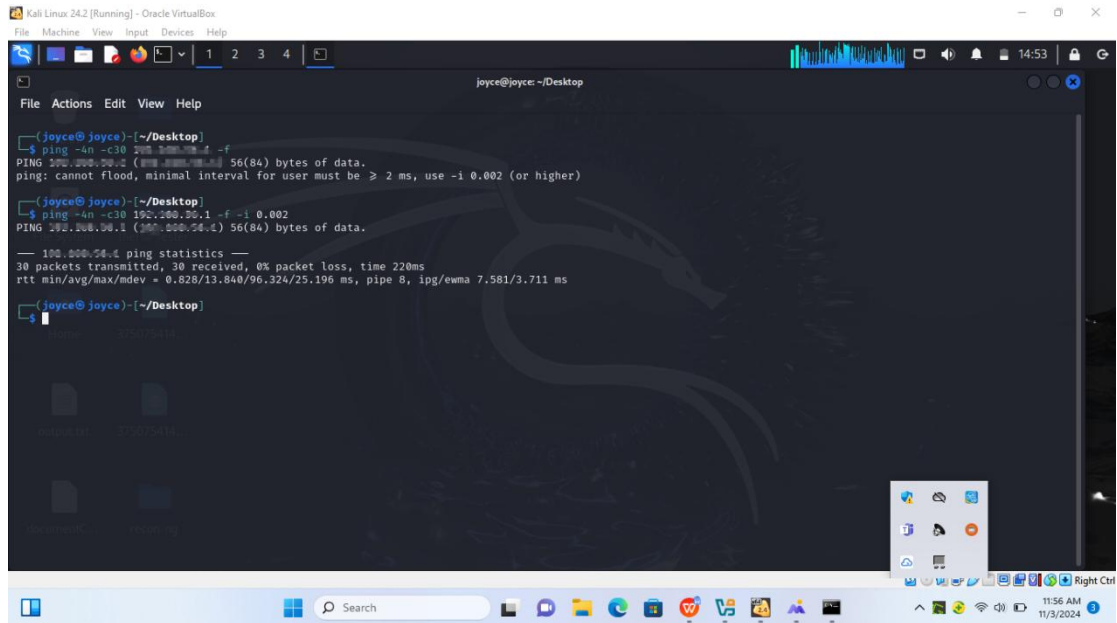


```
joyce@joyce: ~/Desktop
File Actions Edit View Help
joyce@joyce:~/Desktop
$ ping -s 100 localhost
PING localhost (::1) 100 data bytes:
100 bytes from localhost (::1): icmp_seq=1 ttl=64 time=0.197 ms
100 bytes from localhost (::1): icmp_seq=2 ttl=64 time=0.296 ms
100 bytes from localhost (::1): icmp_seq=3 ttl=64 time=0.268 ms
100 bytes from localhost (::1): icmp_seq=4 ttl=64 time=0.596 ms
100 bytes from localhost (::1): icmp_seq=5 ttl=64 time=0.539 ms
100 bytes from localhost (::1): icmp_seq=6 ttl=64 time=0.551 ms
100 bytes from localhost (::1): icmp_seq=7 ttl=64 time=0.36 ms
100 bytes from localhost (::1): icmp_seq=8 ttl=64 time=0.229 ms
100 bytes from localhost (::1): icmp_seq=9 ttl=64 time=0.337 ms
100 bytes from localhost (::1): icmp_seq=10 ttl=64 time=0.186 ms
100 bytes from localhost (::1): icmp_seq=11 ttl=64 time=0.184 ms
100 bytes from localhost (::1): icmp_seq=12 ttl=64 time=0.281 ms
100 bytes from localhost (::1): icmp_seq=13 ttl=64 time=0.283 ms
100 bytes from localhost (::1): icmp_seq=14 ttl=64 time=0.183 ms
^C
--- localhost ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 1029ms
rtt min/avg/max/mdev = 0.181/0.729/3.509/1.111 ms
```



Ping -s localhost. This is useful when testing a system to see how it responds differently to very small or very large packets.





```
joyce@joyce: ~/Desktop
File Actions Edit View Help

[joyce@ joyce] ~/Desktop
$ ping -n -c30 255.255.255.255 -f
PING 255.255.255.255 (255.255.255.255) 56(84) bytes of data.
ping: cannot flood, minimal interval for user must be ≥ 2 ms, use -i 0.002 (or higher)

[joyce@ joyce] ~/Desktop
$ ping -n -c30 192.168.56.1 -f -i 0.002
PING 192.168.56.1 (192.168.56.1) 56(84) bytes of data.
— 100.000.56.4 ping statistics —
30 packets transmitted, 30 received, 0% packet loss, time 220ms
rtt min/avg/max/mdev = 0.828/13.840/96.324/25.196 ms, pipe 8, ipg/ewma 7.581/3.711 ms

[joyce@ joyce] ~/Desktop
$
```

In flood ping; for every ECHO REQUEST sent a period "." is printed, while for every ECHO REPLY received, the last printed period "." is removed. This provides a rapid display of how many packets are being dropped. If interval is not given, it sets interval to zero and outputs packets as fast as they come back or one hundred times per second, whichever is more. Only the super-user may use this option with a zero interval. As a root user, flood target system with sending 30 ping packages. Using local router or Access point.