Network Tools

Network Tools

Ping

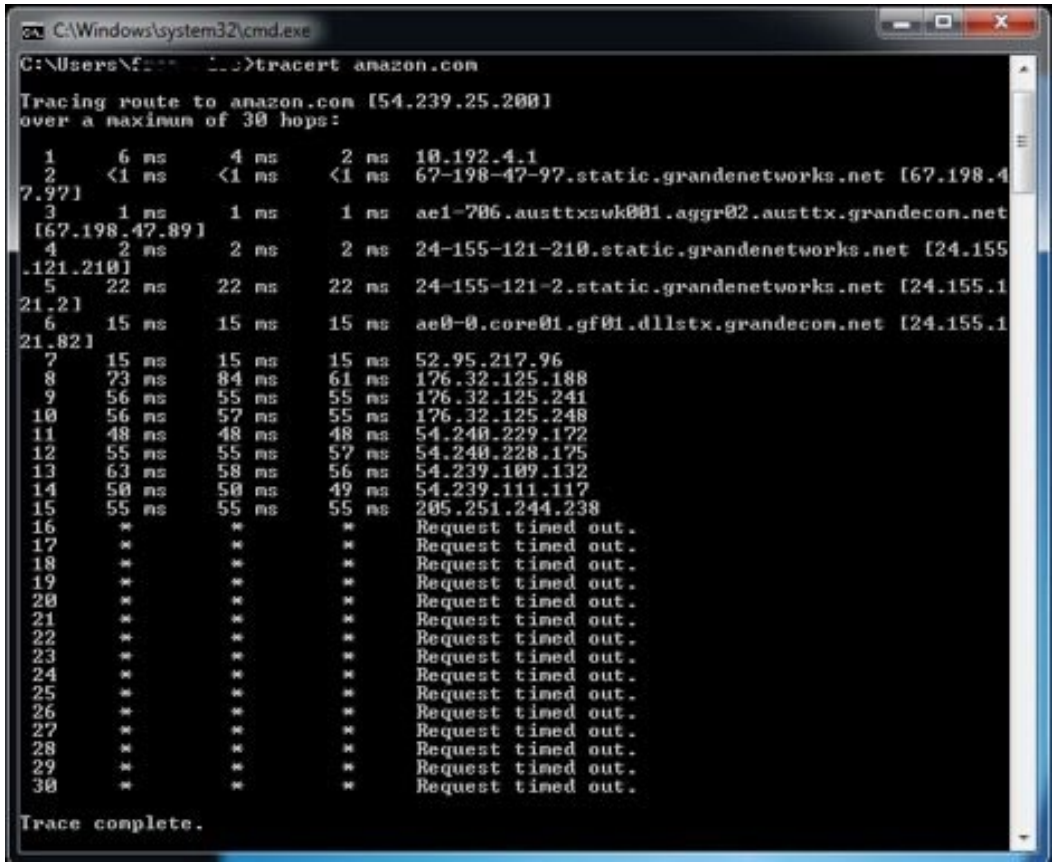
- A network diagnostic utility for testing network connections.
- Sends an ICMP "echo request" packet to an IP address and waits for an ICMP "echo response" packet and reports the time delay in milliseconds.
- If a domain name is used, ping will initiate and use the results of a DNS query.
- Ping (and other ICMP requests) may be blocked at firewalls to prevent network reconnaissance.

```
File  Edit  View  Search  Terminal  Help
$ ping -i 2 -c 10 www.geeksforgeeks.org
PING d13vvqr7dxay1j.cloudfront.net (52.222.128.37) 56(84) bytes of data.
64 bytes from server-52-222-128-37.bom51.r.cloudfront.net (52.222.128.37): icmp_seq=1 ttl=244 time=320 ms
64 bytes from server-52-222-128-37.bom51.r.cloudfront.net (52.222.128.37): icmp_seq=2 ttl=244 time=100 ms
64 bytes from server-52-222-128-37.bom51.r.cloudfront.net (52.222.128.37): icmp_seq=3 ttl=244 time=2133 ms
64 bytes from server-52-222-128-37.bom51.r.cloudfront.net (52.222.128.37): icmp_seq=4 ttl=244 time=844 ms
64 bytes from server-52-222-128-37.bom51.r.cloudfront.net (52.222.128.37): icmp_seq=5 ttl=244 time=926 ms
64 bytes from server-52-222-128-37.bom51.r.cloudfront.net (52.222.128.37): icmp_seq=6 ttl=244 time=1704 ms
64 bytes from server-52-222-128-37.bom51.r.cloudfront.net (52.222.128.37): icmp_seq=7 ttl=244 time=1496 ms

--- d13vvqr7dxay1j.cloudfront.net ping statistics ---
10 packets transmitted, 7 received, 30% packet loss, time 20434ms
rtt min/avg/max/mdev = 100.846/1075.329/2133.966/685.503 ms, pipe 2
$
```

SWINBURNE UNIVERSITY OF TECHNOLOGY

Traceroute/Tracert

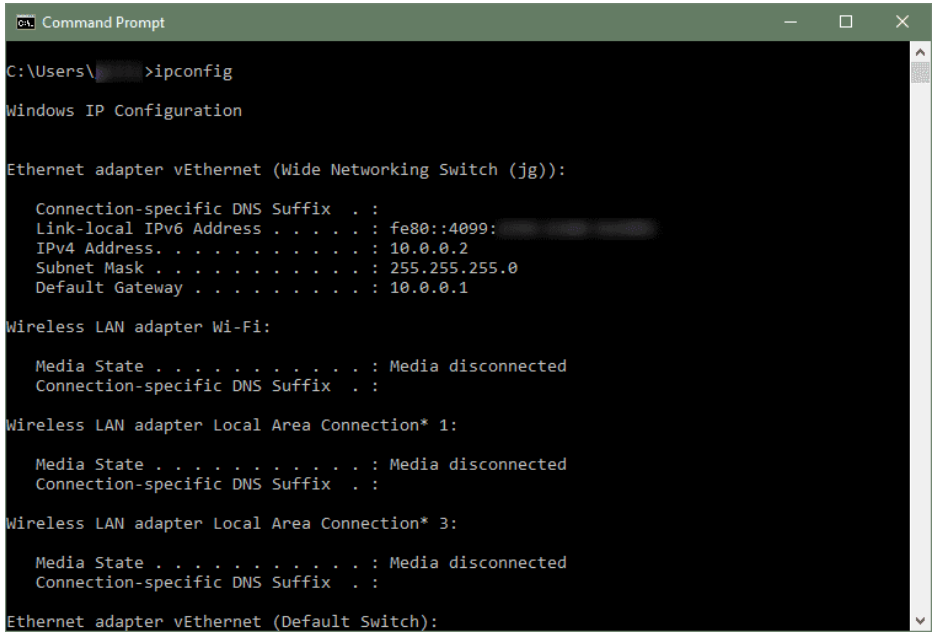
- A network tool for tracking the path taken by IP packets.
- Sends a sequence of UDP or TCP packets with incrementally increasing TTL (time to live) values.
- Collects the resulting ICMP "time exceeded" packets.
- Displays the source IP addresses and host names of the ICMP packets in sequence to show the path taken by the original packets.



```
C:\Windows\system32\cmd.exe
C:\Users\f[illegible]>tracert amazon.com

Tracing route to amazon.com [54.239.25.200]
over a maximum of 30 hops:

  1     6 ms     4 ms     2 ms  10.192.4.1
  2    <1 ms    <1 ms    <1 ms  67-198-47-97.static.grandenetworks.net [67.198.4
7.97]
  3     1 ms     1 ms     1 ms  ae1-706.austtxswk001.aggr02.austtx.grandecon.net
 [67.198.47.89]
  4     2 ms     2 ms     2 ms  24-155-121-210.static.grandenetworks.net [24.155
.121.210]
  5    22 ms    22 ms    22 ms  24-155-121-2.static.grandenetworks.net [24.155.1
21.2]
  6    15 ms    15 ms    15 ms  ae0-0.core01.gf01.dllstx.grandecon.net [24.155.1
21.82]
  7    15 ms    15 ms    15 ms  52.95.217.96
  8    73 ms    84 ms    61 ms  176.32.125.188
  9    56 ms    55 ms    55 ms  176.32.125.241
 10    56 ms    57 ms    55 ms  176.32.125.248
 11    48 ms    48 ms    48 ms  54.240.229.172
 12    55 ms    55 ms    57 ms  54.240.228.175
 13    63 ms    58 ms    56 ms  54.239.109.132
 14    50 ms    50 ms    49 ms  54.239.111.117
 15    55 ms    55 ms    55 ms  205.251.244.238
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

Ipconfig

- Displays or configures the local computer's network interfaces (NICs).
- Displays the current IP addresses of each network card.
- Can be used to initiate a DHCP request (for a new IP address), refresh the DNS cache.



Netstat

- Displays all current network connections including TCP and UDP and other protocols.
- Can indicate the presence of trojans and spyware "phoning home".

```
admin@tecmint ~ $ sudo netstat  -ltup
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:http                  *:*                     LISTEN      1423/nginx -g daemo
tcp        0      0 tecmint:domain          *:*                     LISTEN      2992/dnsmasq
tcp        0      0 *:ssh                   *:*                     LISTEN      1409/sshd
tcp        0      0 localhost:ipp           *:*                     LISTEN      2738/cupsd
tcp        0      0 *:https                 *:*                     LISTEN      1423/nginx -g daemo
tcp6       0      0 [::]:http               [::]:*                  LISTEN      1423/nginx -g daemo
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      1409/sshd
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN      2738/cupsd
tcp6       0      0 [::]:https              [::]:*                  LISTEN      1423/nginx -g daemo
udp        0      0 *:ipp                   *:*                                 2740/cups-browsed
udp        0      0 *:mdns                  *:*                                 1022/avahi-daemon:
udp        0      0 *:36390                 *:*                                 2992/dnsmasq
udp        0      0 *:59072                 *:*                                 1022/avahi-daemon:
udp        0      0 tecmint:domain          *:*                                 2992/dnsmasq
udp        0      0 *:bootpc                *:*                                 2982/dhclient
udp        0      0 tecmint:ntp             *:*                                 1465/ntpd
udp        0      0 localhost:ntp           *:*                                 1465/ntpd
udp        0      0 *:ntp                   *:*                                 1465/ntpd
udp6       0      0 [::]:43740              [::]:*                              1022/avahi-daemon:
udp6       0      0 [::]:mdns               [::]:*                              1022/avahi-daemon:
udp6       0      0 fe80::dd8c:3d40:817:ntp [::]:*                              1465/ntpd
udp6       0      0 ip6-localhost:ntp       [::]:*                              1465/ntpd
udp6       0      0 [::]:ntp                [::]:*                              1465/ntpd
admin@tecmint ~ $
```

Packet Sniffing

- Packet sniffers record IP packets on the network. They were originally designed to help diagnose problems in networks.
  - Good for picking up MAC addresses, IP addresses
- Many internet-based services expect to receive user names and passwords in plain text.
  - Telnet, FTP, SNMP
- Computer users get lazy and re-use the same user names and passwords.
  - If you can get their FTP password, you can probably use it on other accounts.
- Popular Sniffers:
  - TCPDump, Snort, W*ireshark*. Windows and Linux versions.
  - reviews: http://sectools.org/sniffers.html

Packet Sniffers

Wireshark

- Text (tethereal) and GUI (wireshark) versions available for Windows and Linux
- Lists packet contents on the screen and logs them to a file for analysis later.
- Summarises types of packets intercepted.

Snort

- Text-based IDS with packet sniffing and logging abilities.
- Separates packets into IP address and port number
- Easy to search packets using *grep* (linux)