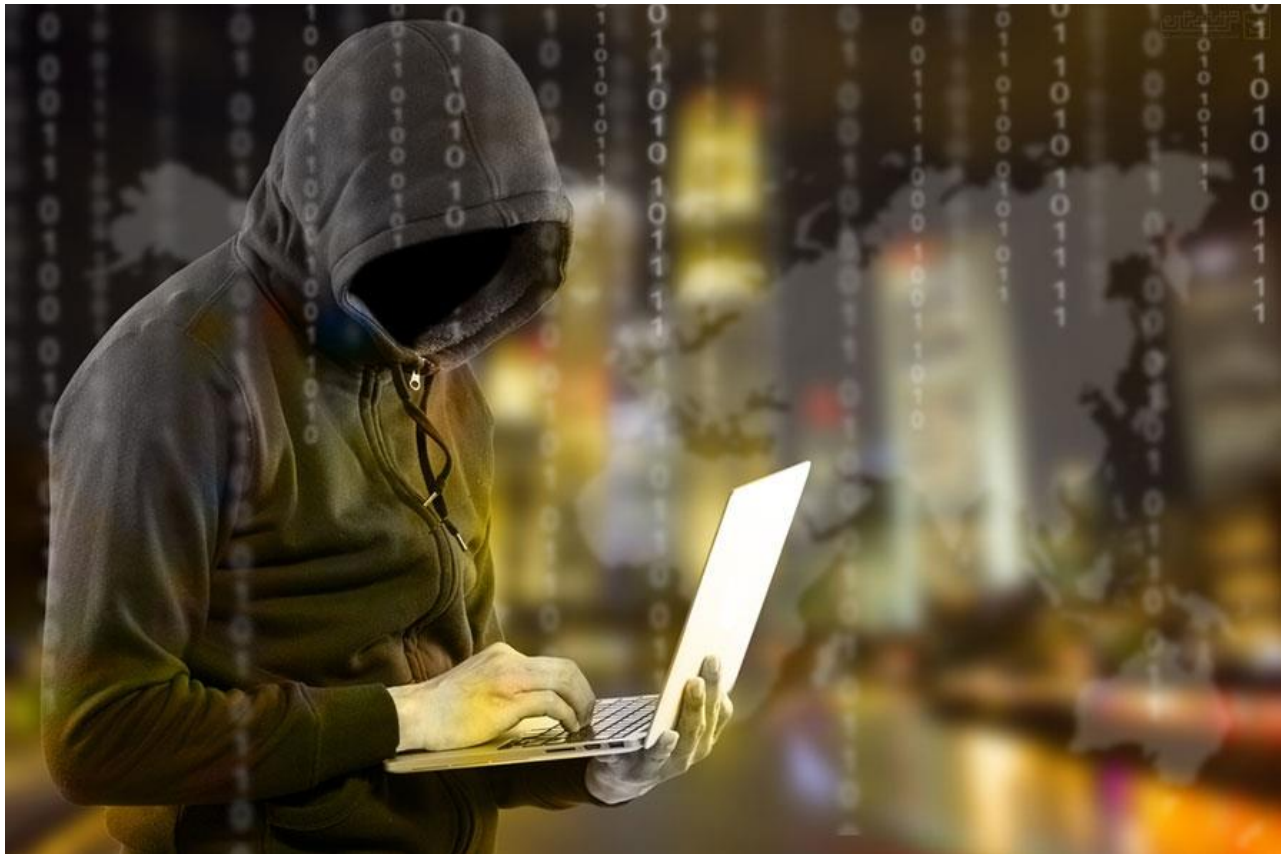
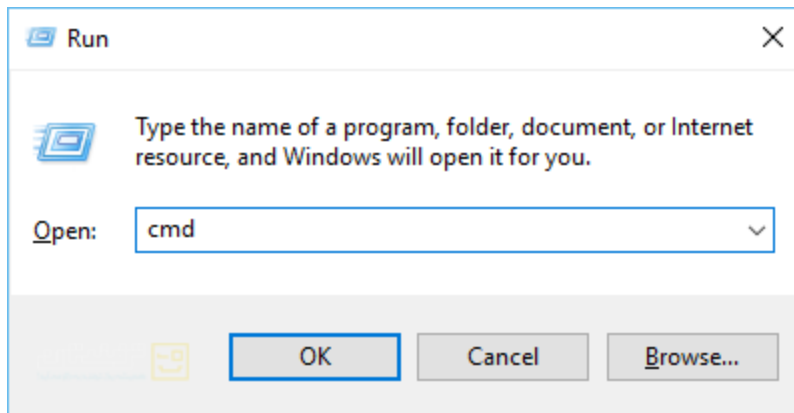


## مفیدترین دستورات CMD برای هکرها



خط فرمان یا Command Prompt یکی از ابزارهای کاربردی هکرها محسوب می‌شود. در این ترفند به معرفی دستوراتی خواهیم پرداخت که توسط هکرها بیشترین استفاده را دارند.

برای دسترسی به CMD کافی است کلیدهای ترکیبی Win+R را فشار دهید تا Run باز شود. سپس عبارت cmd را وارد کرده و Enter بزنید.



## ۱. ping

این دستور به شما اجازه می‌دهد که پی ببرید میزبان مورد نظر شما در حال حاضر در دسترس است یا خیر. بدین معنا که به هنگام اجرای دستور ping، میزبان در صورت متصل بودن چه پاسخی را برای شما ارسال می‌کند.

برای استفاده از این دستور کافی است عبارت ping را به همراه IP یا دامنه‌ی سایت یا کلاینت مورد نظر وارد نمایید. به عنوان مثال:

```
ping ۸.۸.۸.۸
```

```
ping www.google.com
```

پاسخ دریافتی از میزبان بیانگر وضعیت آن است. هر چه زمان درج شده در مقابل time، کم‌تر باشد و پاسخ دریافتی عاری از خطا باشد، به این معناست که سرعت اتصال به آن بیشتر و وضعیت آن نیز پایدارتر است.

```
Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\kasra>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=120ms TTL=39
Reply from 8.8.8.8: bytes=32 time=120ms TTL=39
Reply from 8.8.8.8: bytes=32 time=120ms TTL=39
Reply from 8.8.8.8: bytes=32 time=120ms TTL=39

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 120ms, Maximum = 120ms, Average = 120ms

C:\Users\kasra>
```

## ۲. nslookup

این دستور کاربردهای گوناگونی دارد. یکی از آن‌ها یافتن IP از روی DNS است. فرض کنید آدرس یک سایت را می‌دانید اما از IP آن بی‌خبر هستید. با استفاده از این دستور می‌توانید به IP هر سایتی پی ببرید. به عنوان مثال:

```
nslookup www.google.com
```

یکی دیگر از کاربردهای nslookup در یافتن IP یک میل سرور خاص است. به عنوان مثال برای یافتن IP میل سرورهای یاهو این دستورات بایستی به ترتیب وارد شوند:

```
nslookup
set type=mx
yahoo.com
```

```
C:\Windows\system32\cmd.exe - nslookup
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\kasra>nslookup www.google.com
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
Name: www.google.com
Address: 172.217.19.100

C:\Users\kasra>nslookup
Default Server: UnKnown
Address: 192.168.1.1

> set type=mx
> yahoo.com
Server: UnKnown
Address: 192.168.1.1

Non-authoritative answer:
yahoo.com MX preference = 1, mail exchanger = mta5.am0.yahoodns.net
yahoo.com MX preference = 1, mail exchanger = mta7.am0.yahoodns.net
yahoo.com MX preference = 1, mail exchanger = mta6.am0.yahoodns.net

yahoo.com nameserver = ns2.yahoo.com
yahoo.com nameserver = ns5.yahoo.com
yahoo.com nameserver = ns1.yahoo.com
yahoo.com nameserver = ns3.yahoo.com
```

### ۳. tracert

با استفاده از این دستور می‌توانید از مسیری که یک بسته در شبکه طی می‌کند تا به مقصد برسد اطلاعات خوبی کسب کنید. این دستور (ترفندستان) برای مسیریابی بسته‌ی ارسالی تا مقصد بسیار مفید است.  
مثال:

tracert ۸.۸.۸.۸

tracert www.google.com

### ۴. arp

این دستور جدول arp را برای شما نمایش می‌دهد. در این جدول، IPها و آدرس معادل MAC آنها نگهداری می‌شوند. اگر فعالیت غیرقانونی در شبکه‌ی شما رخ داده است و به عنوان مثال کارت شبکه‌ای بدون اجازه‌ی شما تعویض شده است، از طریق این جدول می‌توانید به سادگی به این موضوع پی ببرید:

arp -a

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\kasra>arp -a

Interface: 192.168.142.1 --- 0x7
Internet Address      Physical Address      Type
192.168.142.254      00-50-56-fb-76-5c    dynamic
192.168.142.255      ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static

Interface: 192.168.1.106 --- 0xf
Internet Address      Physical Address      Type
192.168.1.1          e8-de-27-51-90-64    dynamic
192.168.1.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static

Interface: 192.168.66.1 --- 0x11
Internet Address      Physical Address      Type
192.168.66.254       00-50-56-ff-f5-24    dynamic
192.168.66.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
```

۵. route

این دستور اطلاعات کامل مربوط به لیست کارت‌های شبکه، جدول مسیریابی و درگاه‌های هر یک را برای شما بازگو می‌کند:

route print

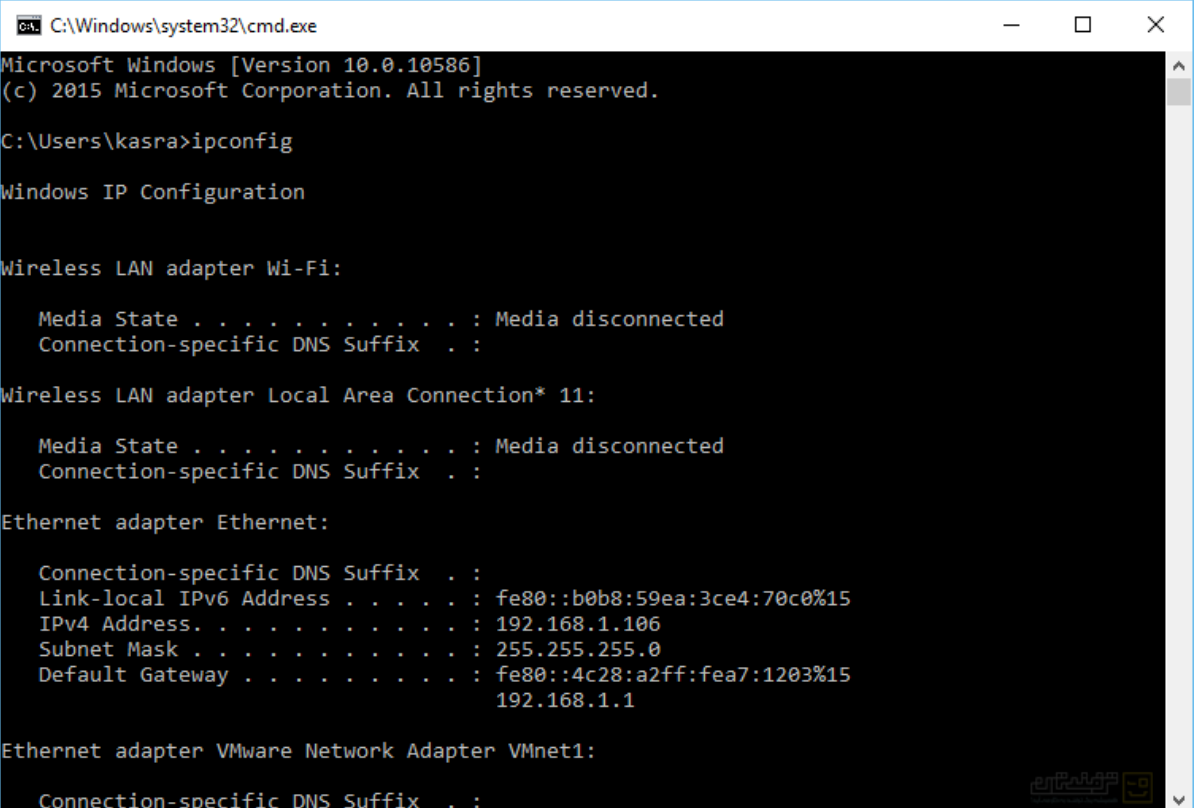
۶. ipconfig

این دستور اطلاعات مفیدی در خصوص IP و Gateway شما، DNS در حال استفاده و نظایر آن را برای شما نمایش می‌دهد:

ipconfig

یا

ipconfig /all



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\kasra>ipconfig

Windows IP Configuration

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::b0b8:59ea:3ce4:70c0%15
    IPv4 Address. . . . . : 192.168.1.106
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::4c28:a2ff:fea7:1203%15
                                192.168.1.1

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix . :
```

همچنین اگر از IP دینامیک استفاده می‌کنید و مایلید IP خود را تغییر دهید با این دستورات می‌توانید این کار را انجام دهید:

```
ipconfig /release
```

```
ipconfig /renew
```

```
v. netstat
```

این دستور وضعیت اتصالات شما را نمایش می‌دهد:

```
netstat
```

نمایش تمامی پورت‌هایی که در وضعیت شنود قرار دارند و اتصال با نام: DNS

```
netstat -a
```

نمایش تمامی اتصالات باز و IP آن‌ها:

```
netstat -n
```

ترکیب دو حالت بالا:

```
netstat -an
```

دستور زیر نیز تمامی پوشه‌های به اشتراک گذاشته شده در رایانه‌ی مقصد را نمایش می‌دهد:

```
net view x.x.x.x
```

net view computername

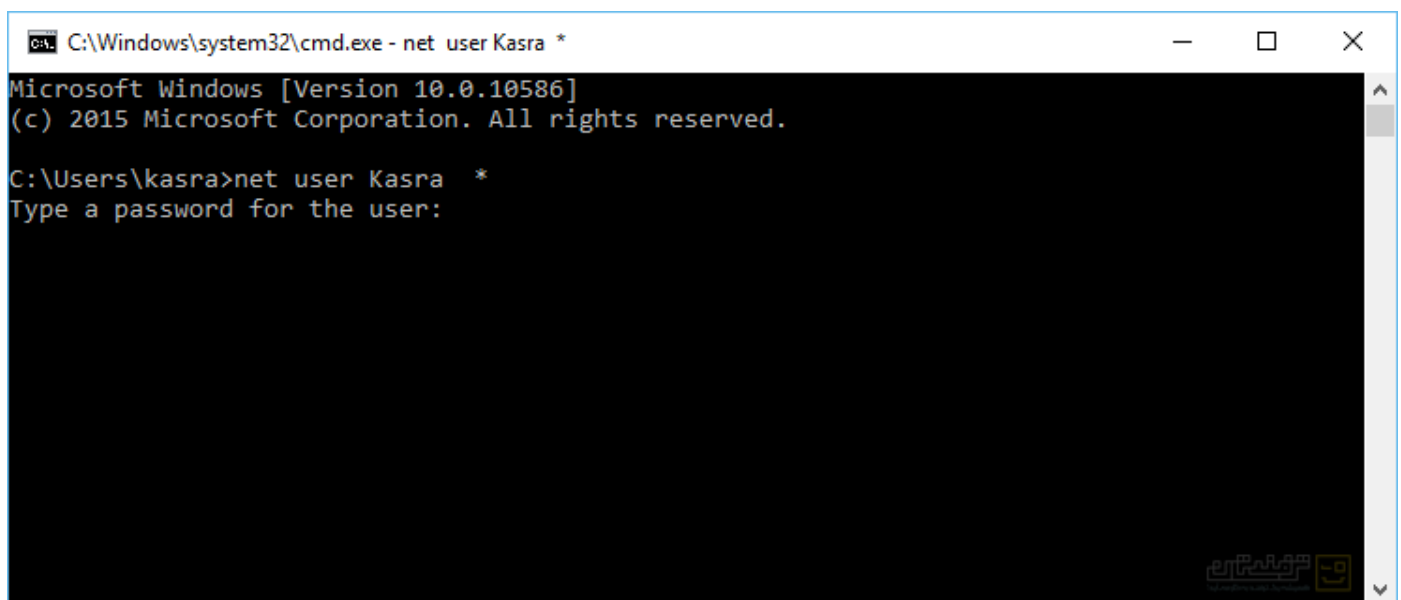
به جای x.x.x.x و computername بایستی آدرس IP یا نام رایانه را وارد نمایید.

۸. netuser

این دستور رمز عبور حساب کاربری ویندوز را بدون دانستن رمز قبلی تغییر می‌دهد:

net user Tarfandestan \*

به جای Tarfandestan نام کاربری ویندوز را بنویسید و پس از فشردن Enter ، رمز جدید را وارد کنید.



```
C:\Windows\system32\cmd.exe - net user Kasra *
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\kasra>net user Kasra *
Type a password for the user:
```

۹. سایر دستورات

دستورات دیگری نیز هستند که می‌توانند به شما کمک کنند.



اتصال به دستگاه مقصد با دسترسی: Administrator

```
net use \ipaddressipc$ "" /user:administrator
```

به جای ipaddress ، آدرس IP را وارد نمایید.

پس از اتصال به مقصد اگر مایل به مرور کل درایو C بودید از این دستور استفاده کنید:

```
net use K: \computernameC$
```

به جای computername نام رایانه را وارد کنید. این دستور موجب ایجاد یک درایو مجازی می‌شود. دقت کنید این دستور زمانی کار می‌کند که رایانه‌ی مقصد رمز عبور Administrator تعیین نکرده باشد.

و در نهایت دستور Help برای دریافت راهنمایی:

```
command /help
```

یا

```
command /?
```

به جای command دستور مورد نظر را بایستی وارد نمایید. با این دستور می‌توانید پی ببرید هر دستور، چه کارایی و چه جزئیاتی دارد.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\kasra>ipconfig /help

Error: unrecognized or incomplete command line.

USAGE:
  ipconfig [/allcompartments] [/? | /all |
          /renew [adapter] | /release [adapter] |
          /renew6 [adapter] | /release6 [adapter] |
          /flushdns | /displaydns | /registerdns |
          /showclassid adapter |
          /setclassid adapter [classid] |
          /showclassid6 adapter |
          /setclassid6 adapter [classid] ]

where
  adapter          Connection name
                   (wildcard characters * and ? allowed, see examples)

Options:
  /?              Display this help message
  /all           Display full configuration information
```