



-: Windows Commands with Examples :-

1. ping (test network connection)

- The ping command tests network connectivity between two devices by sending **ICMP echo requests**.

For example,

In addition, use it for the following:

- Test for packet loss
- Test latency
- Test DNS queries

Ping Examples

To test the connectivity to another device by IP use the command below.

`ping 192.168.100.1`

```
Administrator: Command Prompt

C:\>ping 192.168.100.1

Pinging 192.168.100.1 with 32 bytes of data:
Reply from 192.168.100.1: bytes=32 time<1ms TTL=128
Reply from 192.168.100.1: bytes=32 time<1ms TTL=128
Reply from 192.168.100.1: bytes=32 time<1ms TTL=128
Reply from 192.168.100.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.100.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping by hostname.

`ping dc1.ad.activedirectorypro.com`

2. ipconfig (get network adapter details)

- The ipconfig command is used to display a **computers TCP/IP configuration**. You can display the IP info for a **single or all network cards installed on a computer**.
- This command can also display the **DNS cache on the local machine**, flush DNS, release and renew the DHCP address on all network cards.

Examples:

To view the IP configuration for all network cards on a computer type the command below and press enter.

`ipconfig /all`

```
Administrator: Command Prompt

C:\Users\administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : PC1
Primary Dns Suffix . . . . . : ad.activedirectorypro.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ad.activedirectorypro.com

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . : 
Description . . . . . : Microsoft Hyper-V Network Adapter
Physical Address. . . . . : 00-15-5D-D9-4F-05
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::690f:fd02:6802:7e07%14(Preferred)
IPv4 Address. . . . . : 192.168.100.101(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.1
DHCPv6 IAID . . . . . : 100668765
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-C5-C4-87-00-15-5D-D9-4F-05
DNS Servers . . . . . : 192.168.100.10
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\administrator>
```



To display IP info for all network cards.

```
ipconfig /all
```

Switch to clear the local DNS resolver cache.

```
ipconfig /flushdns
```

Trigger dynamic registration of the DNS names and IP addresses that are configured on the computer.

```
ipconfig /registerdns
```

Release DHCP addresses. This will release DHCP address on the network cards that are configured for DHCP.

```
ipconfig /release
```

Switch will renew DHCP address for all network cards.

```
ipconfig /renew
```

3. nslookup (find dns records)

- The [nslookup](#) command is used to check DNS records and troubleshoot DNS. This is a must-have command for any sysadmin or network engineer.
- You can do all kinds of tests to verify DNS is working correctly, you can check PTR, A, MX, SOA, and many other types of DNS records.

```
Administrator: Command Prompt - nslookup
C:\Users\administrator>nslookup
Default Server:  dc1.ad.activedirectorypro.com
Address:  192.168.100.10

> google.com
Server:  dc1.ad.activedirectorypro.com
Address:  192.168.100.10

Non-authoritative answer:
Name:    google.com
Addresses:  2607:f8b0:4002:c0c::71
           2607:f8b0:4002:c0c::66
           2607:f8b0:4002:c0c::8b
           2607:f8b0:4002:c0c::8a
           74.125.138.138
           74.125.138.100
           74.125.138.102
           74.125.138.139
           74.125.138.113
           74.125.138.101
```

Examples:

To test that the A record of a hostname follow these two steps

Step 1: Type nslookup and press enter

Step 2: type in a domain name and press enter

```
Step 1: Type nslookup  C:\Users\administrator>nslookup
                        Default Server:  dc1.ad.activedirectorypro.com
                        Address:  192.168.100.10

Step 2: Type Domain    > google.com
                        Server:  dc1.ad.activedirectorypro.com
                        Address:  192.168.100.10

Non-authoritative answer:
Name:    google.com
Addresses:  2607:f8b0:4002:c0c::71
           2607:f8b0:4002:c0c::66
           2607:f8b0:4002:c0c::8b
           2607:f8b0:4002:c0c::8a
           74.125.138.138
           74.125.138.100
           74.125.138.102
           74.125.138.139
           74.125.138.113
           74.125.138.101
```



4. tracert (network troubleshooting)

- The tracert command is used to **track** the pathway a packet takes **from a source IP to the destination address**. This simply means it's going to display each hop (router) that the packet passes through to reach its destination.

Examples:

The syntax for this command is tracert followed by the hostname or IP.

tracert google.com

```

Select Administrator: Command Prompt

Tracing route to google.com [172.253.124.138]
over a maximum of 30 hops:

  0  <1 ms    <1 ms    <1 ms    192.168.100.1
  1  1 ms     1 ms     1 ms     192.168.5.1
  2  61 ms    36 ms    47 ms    172.26.96.161
  3  61 ms    36 ms    53 ms    107.79.236.228
  4  74 ms    46 ms    59 ms    12.83.186.161
  5  79 ms    46 ms    45 ms    12.83.186.145
  6  57 ms    39 ms    47 ms    gar10.cgscil.ip.att.net [12.122.133.45]
  7  67 ms    43 ms    47 ms    12.255.10.54
  8  77 ms    36 ms    50 ms    108.170.243.174
  9  52 ms    37 ms    57 ms    108.170.243.165
 10  *        *        *        Request timed out.
 11 140 ms    59 ms    56 ms    142.250.208.152
 12 67 ms    79 ms    71 ms    172.253.70.66
 13 60 ms    64 ms    67 ms    209.85.240.202
 14 69 ms    65 ms    69 ms    108.170.236.151
 15 *        *        *        Request timed out.
 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 68 ms    72 ms    60 ms    ys-in-f138.1e100.net [172.253.124.138]

Trace complete.

C:\Users\administrator>

```

5. shutdown command

- The shutdown command does exactly that, it shuts down a computer.
- This command is useful for shutting down or restarting local or remote computers.

```

Administrator: Command Prompt

C:\Users\administrator>shutdown /s

C:\Users\administrator>

```

You're about to be signed out
Windows will shut down in less than a minute.

Close

Examples:

This command will restart computer pc2.

shutdown /r /m \\pc2

This command will shut down the remote computer.

shutdown /s /m \\pc2



Shutdown a remote computer with a custom message.

```
shutdown /m \\pc2 /c "Rebooting computer, have a nice day"
```

Force applications to close without warning.

```
shutdown /s /f
```

6. gpupdate (group policy update)

- The gpupdate command is used to **apply group policies on a computer in a windows domain.**
- Sometimes you can run this command to refresh the GPOs and avoid a reboot.

Examples:

This command will pull down any GPO changes to the computer.

```
gpupdate
```

```

C:\Users\administrator>gpupdate
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\administrator>

```

Use /force to reapply all the GPOs on the computer.

```
gpupdate /force
```

7. netstat (display network connections)

- The netstat command **displays TCP/IP connection information, ethernet stats, and the computer's routing table.**
- We use this command on Windows servers and clients when troubleshooting connection issues.
- We can verify application servers are working correctly by checking that the service is running and listening for connections on the port.

```

Administrator: Command Prompt

Active Connections

Proto Local Address          Foreign Address         State
TCP    192.168.100.10:389      192.168.100.11:54590    ESTABLISHED
TCP    192.168.100.10:49667    192.168.100.11:55780    ESTABLISHED
TCP    192.168.100.10:49720    192.168.100.11:50428    ESTABLISHED
TCP    192.168.100.10:64081    192.168.100.11:49668    ESTABLISHED
TCP    [::1]:389              [::1]:49674            ESTABLISHED
TCP    [::1]:389              [::1]:49675            ESTABLISHED
TCP    [::1]:389              [::1]:63945            ESTABLISHED
TCP    [::1]:49667            [::1]:62860            ESTABLISHED
TCP    [::1]:49674            [::1]:389              ESTABLISHED
TCP    [::1]:49675            [::1]:389              ESTABLISHED
TCP    [::1]:62860            [::1]:49667            ESTABLISHED
TCP    [::1]:63945            [::1]:389              ESTABLISHED
TCP    [fe80::712b:ad2c:84c9:d38d%4]:389 [fe80::712b:ad2c:84c9:d38d%4]:63936 ESTABLISHED
TCP    [fe80::712b:ad2c:84c9:d38d%4]:389 [fe80::712b:ad2c:84c9:d38d%4]:63937 ESTABLISHED
TCP    [fe80::712b:ad2c:84c9:d38d%4]:389 [fe80::712b:ad2c:84c9:d38d%4]:63940 ESTABLISHED
TCP    [fe80::712b:ad2c:84c9:d38d%4]:49667 [fe80::712b:ad2c:84c9:d38d%4]:54386 ESTABLISHED
TCP    [fe80::712b:ad2c:84c9:d38d%4]:49667 [fe80::712b:ad2c:84c9:d38d%4]:60449 ESTABLISHED
TCP    [fe80::712b:ad2c:84c9:d38d%4]:54386 [fe80::712b:ad2c:84c9:d38d%4]:49667 ESTABLISHED
TCP    [fe80::712b:ad2c:84c9:d38d%4]:60449 [fe80::712b:ad2c:84c9:d38d%4]:49667 ESTABLISHED
TCP    [fe80::712b:ad2c:84c9:d38d%4]:63119 [fe80::4856:f1a1:7cc:2440%4]:49505 ESTABLISHED
TCP    [fe80::712b:ad2c:84c9:d38d%4]:63936 [fe80::712b:ad2c:84c9:d38d%4]:389 ESTABLISHED
TCP    [fe80::712b:ad2c:84c9:d38d%4]:63937 [fe80::712b:ad2c:84c9:d38d%4]:389 ESTABLISHED
TCP    [fe80::712b:ad2c:84c9:d38d%4]:63940 [fe80::712b:ad2c:84c9:d38d%4]:389 ESTABLISHED
TCP    [fe80::712b:ad2c:84c9:d38d%4]:64170 [fe80::712b:ad2c:84c9:d38d%4]:135 TIME_WAIT
TCP    [fe80::712b:ad2c:84c9:d38d%4]:64171 [fe80::712b:ad2c:84c9:d38d%4]:135 TIME_WAIT

C:\Users\Administrator>

```



Examples:

Display all active and listening ports.

```
netstat -a
```

Display all connections in numerical order.

```
netstat -a -n
```

It shows that my domain controller with IP 192.168.100.10 has established these four connections with IP 192.168.100.11.

```
C:\Users\Administrator>netstat -a -n
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:88	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:464	0.0.0.0:0	LISTENING
TCP	0.0.0.0:593	0.0.0.0:0	LISTENING
TCP	0.0.0.0:636	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3268	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3269	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING
TCP	0.0.0.0:9389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:47001	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49671	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49673	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49676	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49686	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49720	0.0.0.0:0	LISTENING
TCP	127.0.0.1:53	0.0.0.0:0	LISTENING
TCP	192.168.100.10:53	0.0.0.0:0	LISTENING
TCP	192.168.100.10:139	0.0.0.0:0	LISTENING
TCP	192.168.100.10:389	192.168.100.11:54590	ESTABLISHED
TCP	192.168.100.10:49667	192.168.100.11:55965	ESTABLISHED
TCP	192.168.100.10:49720	192.168.100.11:50428	ESTABLISHED
TCP	192.168.100.10:64231	192.168.100.11:49668	ESTABLISHED
TCP	:::88	:::0	LISTENING

More netstat examples

Displays the exe and the process ID (PID) associated with the connection.

```
netstat -ab
```

8. net stop and net start (windows services)

Simple command to start and stop windows services.

```
Administrator: Command Prompt

C:\Users\administrator>net stop spooler
The Print Spooler service is stopping.
The Print Spooler service was stopped successfully.

C:\Users\administrator>net start spooler
The Print Spooler service is starting.
The Print Spooler service was started successfully.

C:\Users\administrator>
```



Examples:

Stop and start the printer spooler service.

```
net stop spooler
```

and now start the spooler service.

```
net start spooler
```

9. systeminfo

The systeminfo command displays configuration details on a computer such as OS name and version, hardware information, boot time, logon server, and more.

There are a lot of details this command displays.

```
Administrator: Command Prompt

C:\Users\administrator>systeminfo

Host Name:                PC1
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19041 N/A Build 19041
OS Manufacturer:          Microsoft Corporation
OS Configuration:         Member Workstation
OS Build Type:              Multiprocessor Free
Registered Owner:          jojo
Registered Organization:
Product ID:                 00330-80953-28576-AA507
Original Install Date:      9/4/2021, 5:18:10 PM
System Boot Time:           9/26/2021, 5:55:06 AM
System Manufacturer:        Microsoft Corporation
System Model:               Virtual Machine
System Type:                x64-based PC
Processor(s):               1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2594 Mhz
BIOS Version:               American Megatrends Inc. 090008 , 12/7/2018
Windows Directory:          C:\Windows
System Directory:           C:\Windows\system32
Boot Device:                \Device\HarddiskVolume1
System Locale:               en-us;English (United States)
Input Locale:                en-us;English (United States)
Time Zone:                  (UTC-06:00) Central Time (US & Canada)
Total Physical Memory:       1,620 MB
Available Physical Memory:   489 MB
Virtual Memory: Max Size:    3,540 MB
Virtual Memory: Available:   2,141 MB
```

10. getmac (get mac address)

- This command returns the MAC address from all the network cards on a system. This command is the best way to quickly grab a computer's MAC address.

```
C:\Users\administrator>getmac

Physical Address    Transport Name
=====
00-15-5D-D9-4F-05   \Device\Tcpip_{D84EF120-0918-4A13-934F-2448AB852631}

C:\Users\administrator>
```

To run it on a local computer just type
`getmac`.

To run on a remote computer, use the /s parameter.

```
getmac /s pc1
```

11. whoami command

- This command displays who is currently logged on to the local system.
- It also can display what groups a user belongs to.



Administrator: Command Prompt

```
C:\Users\administrator>whoami
adpro\administrator

C:\Users\administrator>_
```

Get the current logged on user.

whoami

Display the user groups to which the current user belongs.

whoami /groups

```
C:\Users\administrator>whoami /groups

GROUP INFORMATION
-----

```

Group Name	Type	SID
Everyone	Well-known group	S-1-1-0
BUILTIN\Users	Alias	S-1-5-32-545
BUILTIN\Administrators	Alias	S-1-5-32-544
wner		
NT AUTHORITY\REMOTE INTERACTIVE LOGON	Well-known group	S-1-5-14
NT AUTHORITY\INTERACTIVE	Well-known group	S-1-5-4
NT AUTHORITY\Authenticated Users	Well-known group	S-1-5-11
NT AUTHORITY\This Organization	Well-known group	S-1-5-15
LOCAL	Well-known group	S-1-2-0
ADPRO\Domain Admins	Group	S-1-5-21-1314716284-1752886444-3868204627-512
ADPRO\Group Policy Creator Owners	Group	S-1-5-21-1314716284-1752886444-3868204627-520
ADPRO\Schema Admins	Group	S-1-5-21-1314716284-1752886444-3868204627-518
ADPRO\Enterprise Admins	Group	S-1-5-21-1314716284-1752886444-3868204627-519
Authentication authority asserted identity	Well-known group	S-1-18-1
ADPRO\IT_Local	Alias	S-1-5-21-1314716284-1752886444-3868204627-1161
roup		
ADPRO\Denied RODC Password Replication Group	Alias	S-1-5-21-1314716284-1752886444-3868204627-572
roup		
ADPRO\IT_Folders	Alias	S-1-5-21-1314716284-1752886444-3868204627-1160
roup		
Mandatory Label\High Mandatory Level	Label	S-1-16-12288

Displays all information for the current user

whoami /all

12. telnet client

Use the windows telnet client to test if a remote host is allowing connection on a specific port.

We can typically use this when someone says your firewall is blocking a program from working.

If you know the **port number** the **application runs** on you can use the command below. In this example, we installed filezilla server, so port 21 should be open.

The syntax is **telnet + hostname or IP + port number**

telnet srv01 21

You may or may not get a response back from the remote server. In this case with filezilla. You could also just get a blank screen on a successful connection.



Administrator: Command Prompt

```
C:\Users\administrator>telnet srv01_21
```

Telnet dc1

```
220-FileZilla Server 1.0.1
220 Please visit https://filezilla-project.org/
```

If it doesn't get a connection, you should get a message like the below.

Administrator: Command Prompt

```
C:\Users\administrator>telnet dc1 21
Connecting To dc1...Could not open connection to the host, on port 21: Connect failed
C:\Users\administrator>
```

13. cd (change directory)

- The cd command allows you to **change to another directory on your computer**.

For example, to change to the windows directory use this command.

`cd windows`

Command Prompt

```
c:\>cd windows
```



```
c:\Windows>
```

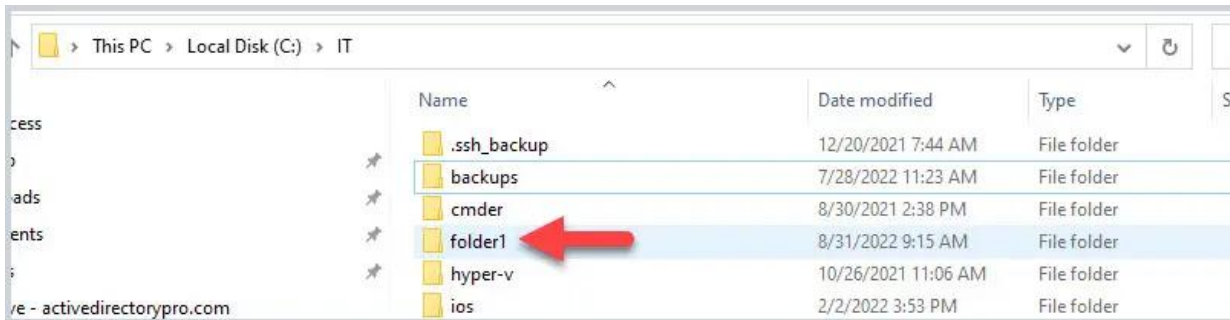
14. mkdir (make directory)

- The mkdir command will **create a directory or subdirectory**. It creates the directory in the current directory.



```
C:\IT>mkdir folder1  
C:\IT>
```

If we look in windows explorer, I'll see the folder1 directory.



15. tasklist (display running processes)

- Tasklist will display the running processes on the local computer.

```
C:\IT>tasklist
```

Image Name	PID	Session Name	Session#	Mem Us
System Idle Process	0	Services	0	
System	4	Services	0	2,85
Secure System	240	Services	0	275,77
Registry	380	Services	0	88,46
smss.exe	948	Services	0	1,30
csrss.exe	1264	Services	0	5,05
wininit.exe	1548	Services	0	5,16
csrss.exe	1556	Console	1	5,57
services.exe	1632	Services	0	10,70
LsaIso.exe	1652	Services	0	2,63

16. taskkill (end process)

Terminate a process by the PID number. In this example, I forcefully end process PID 1808.

`taskkill /pid 1808 /f`

```
C:\IT>taskkill /pid 1808 /f  
SUCCESS: The process with PID 1808 has been terminated.  
C:\IT>
```

17. cls (clear screen)

- The cls command will clear the command prompt console. This is useful when the screen has a lot of information on it and you want a blank screen.

At the windows command prompt type `cls` and press enter to clear the screen.



18. del

- The del command is used to delete files and folders. Deleting files with the del command does not go to the recycle bin.

Delete a single file.

```
del c:\it\pass.txt
```

Delete all exe files.

```
del c:\it\*.exe
```

Delete files and subfolders.

```
del c:\it\*.*
```

19. schtasks (scheduled tasks)

- The schtasks commands lets you **add, remove, change and view scheduled tasks** on the local computer.

View scheduled tasks:

```
Schtasks
```

Delete a scheduled task:

```
SCHTASKS /Delete /TN "\Backup\Backup and Restore"
```

20. net user

- The net user command displays user account information on a local computer or the domain.

On a PC type net user to see the computer's account info.

```

C:\> Command Prompt

Z:\>net user
User accounts for \\PC1

-----
Administrator      DefaultAccount      Guest
jojo                WDAGUtilityAccount
The command completed successfully.

```

To get all the user accounts from the domain controller.

```
net user /domain
```

```

Z:\>net user /domain
The request will be processed at a domain controller for domain ad.activedirectorypro.com.

User accounts for \\DC2.ad.activedirectorypro.com

-----
$Q54000-S88DFRGLOV40  Aaron.Delgado        Aaron.Vincent
Abbie.Peters           Abel.Austin          Abel.Dietrich
Abel.Evans             Abigail.Chavez       Adam.Anderson
Adam.Baldwin           Adam.Fredericks      Adam.Hickey
Adam.Hilton            Adam.Lawhorn         Adam.Mata
Adam.Reed              Adelina.Martin       Administrator
Adrian.Bell            Adrian.Hernandez    Agnes.Dibble
Agnes.Harris           Agnes.Haywood        Agnes.Ouellette
Agnes.Zarate           Agustin.Mejia        Aimee.Delk
Aja.Walls              Al.Cox               Al.Hammer
Alaina.Osborne         Alan.Gilchrist        Alan.Hendrix
Alan.Keys              Alanna.McCoy         Albert.Alt
Albert.Atkins          Albert.Coulter        Albert.Council
Albert.Dull            Albert.Griffin        Albert.King
Albert.Smith           Albert.Wing           Alberta.Meyer
Alberta.Shockley       Alberta.Weber         Alejandro.Gutierrez
Alex.Matias            Alex.Pospisil        Alex.Rambo

```



21. arp

- The arp command **displays** and modifies the Address Resolution Protocol (ARP) **cache on the local computer**.

Display the arp cache for all interfaces:

```
arp -a
```

To clear the arp cache use this command:

```
arp -d
```

22. hostname

- This windows command displays the host name of the computer.

hostname

```
C:\>hostname
DESKTOP-CF208JL
C:\>
```

23. psexec

- PSEXEC allows you to execute commands on remote computers. This is useful when you need to troubleshoot a remote computer without taking full control of it.

In this example, I'll run ipconfig on the remote computer pc1 to get the IP address information.

```
psexec \\pc1 ipconfig
```

```
C:\Users\Administrator>psexec \\pc1 ipconfig

PsExec v2.4 - Execute processes remotely
Copyright (C) 2001-2022 Mark Russinovich
Sysinternals - www.sysinternals.com

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::a1bd:129f:cef5:57
    IPv4 Address. . . . . : 192.168.100.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

ipconfig exited on pc1 with error code 0.

C:\Users\Administrator>
```

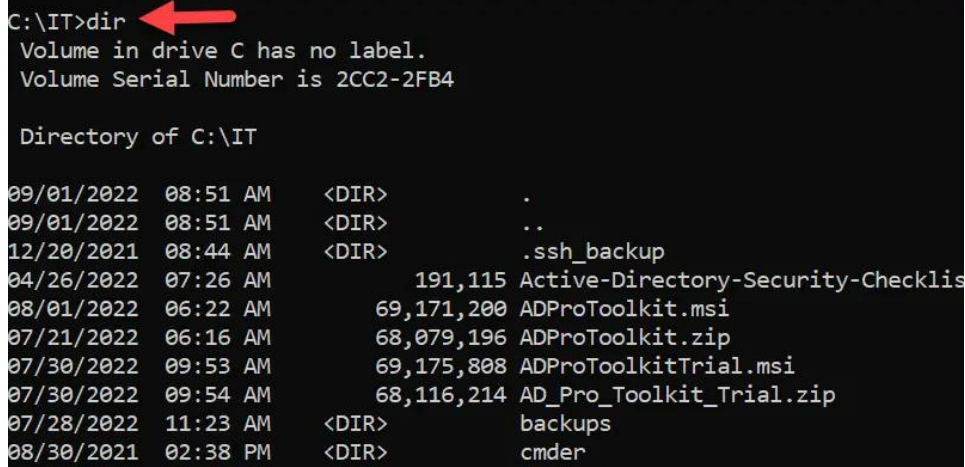


24. dir

- The dir command lists all files and directories in a specific directory.

To list the contents of the current directory use this command:

dir



```
C:\IT>dir
Volume in drive C has no label.
Volume Serial Number is 2CC2-2FB4

Directory of C:\IT

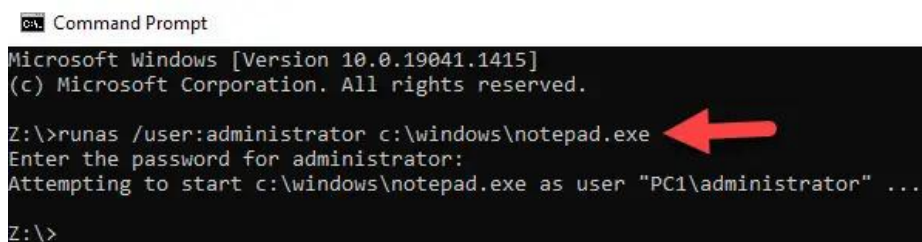
09/01/2022  08:51 AM    <DIR>          .
09/01/2022  08:51 AM    <DIR>          ..
12/20/2021  08:44 AM    <DIR>          .ssh_backup
04/26/2022  07:26 AM             191,115 Active-Directory-Security-Checklis
08/01/2022  06:22 AM             69,171,200 ADProToolkit.msi
07/21/2022  06:16 AM             68,079,196 ADProToolkit.zip
07/30/2022  09:53 AM             69,175,808 ADProToolkitTrial.msi
07/30/2022  09:54 AM             68,116,214 AD_Pro_Toolkit_Trial.zip
07/28/2022  11:23 AM    <DIR>          backups
08/30/2021  02:38 PM    <DIR>          cmdr
```

25. runas

- Runas allows you to **run** a specific tool or program **as a different user**.

For example, you are logged in as a regular user (no administrator rights) and you need to run a program with an account that has local administrator rights.

runas /user:administrator c:\windows\notepad.exe



```
Microsoft Windows [Version 10.0.19041.1415]
(c) Microsoft Corporation. All rights reserved.

Z:\>runas /user:administrator c:\windows\notepad.exe
Enter the password for administrator:
Attempting to start c:\windows\notepad.exe as user "PC1\administrator" ...

Z:\>
```

26. rmdir (remove directories)

- Do you need to remove a directory? The rmdir command will delete a directory.
- The default command will only delete empty directories. If you want to delete a directory and the files in the directory use the /s switch.

For example, delete the c:\it\private and all files in that directory.

rmdir c:\it\private /s

27. ver

- The ver command displays the Windows version.



```
C:\>ver

Microsoft Windows [Version 10.0.19043.1889]

C:\>
```