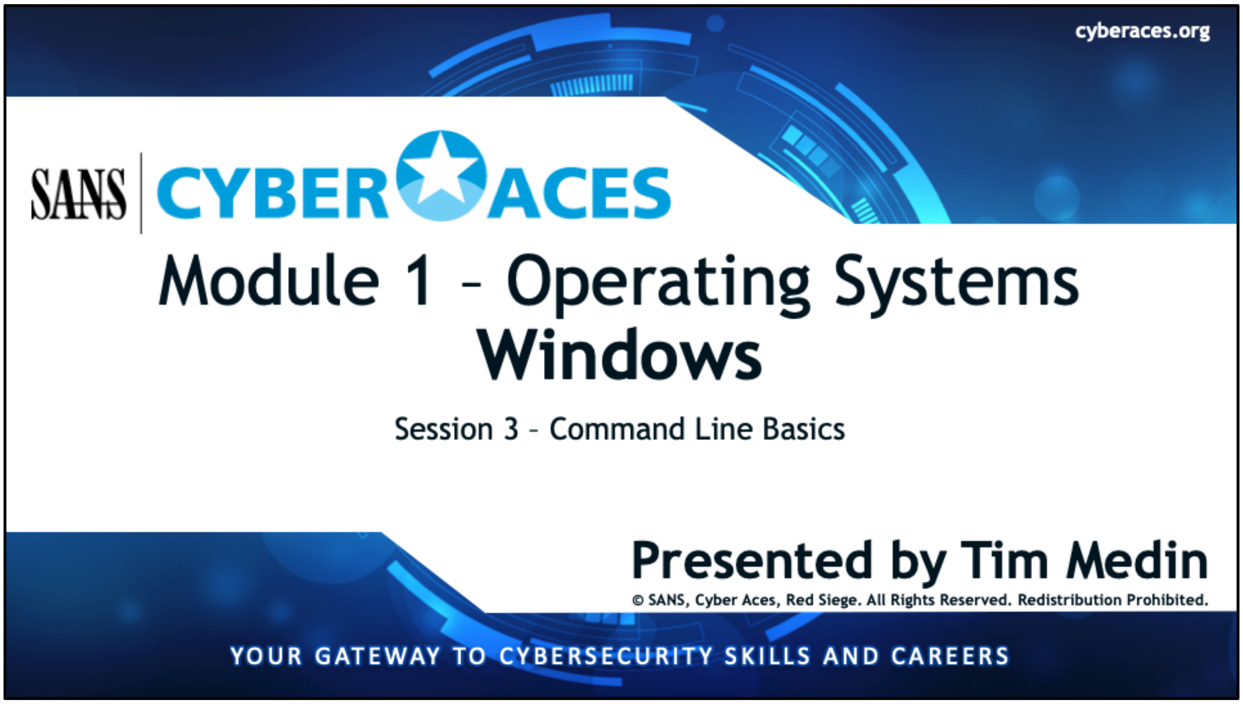


cyberaces.org

SANS | CYBER ACES

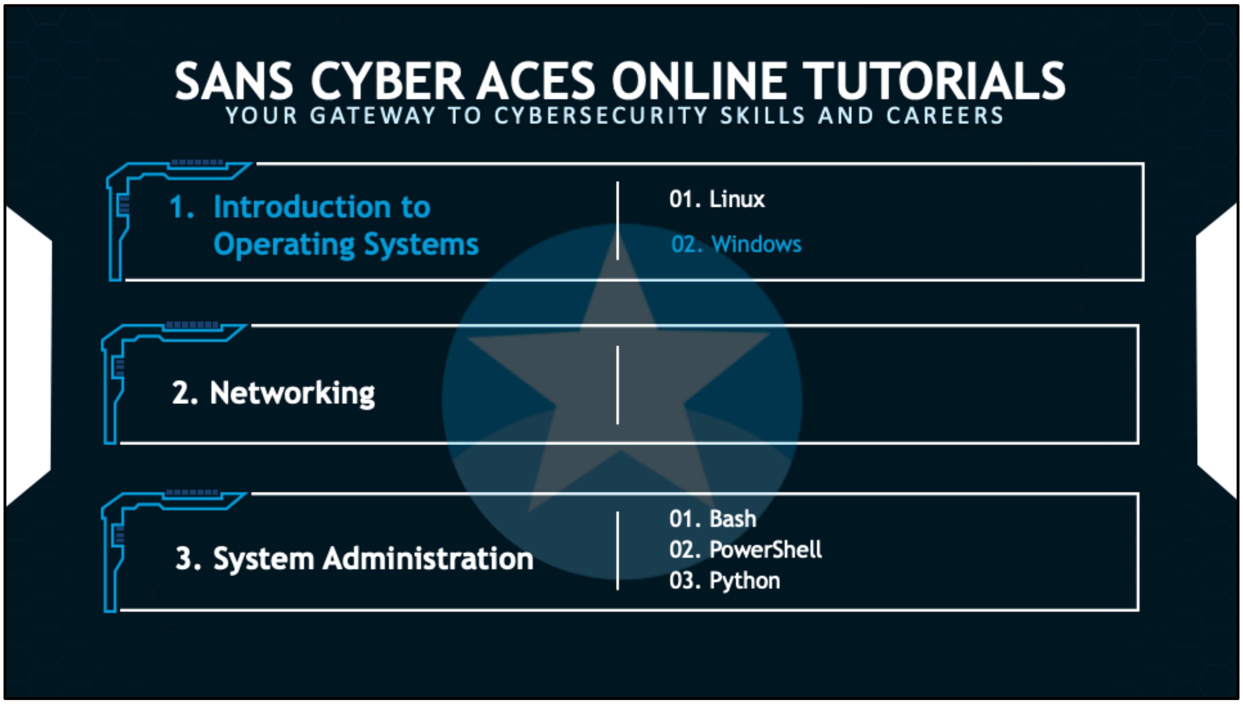
Module 1 – Operating Systems
Windows

Session 3 – Command Line Basics

Presented by Tim Medin

YOUR GATEWAY TO CYBERSECURITY SKILLS AND CAREERS

Welcome to Cyber Aces Online, Module 1! A firm understanding of operating systems is essential to being able to secure or attack one. This module dives in to the basics of the Windows command line using CMD.EXE.



SANS CYBER ACES ONLINE TUTORIALS

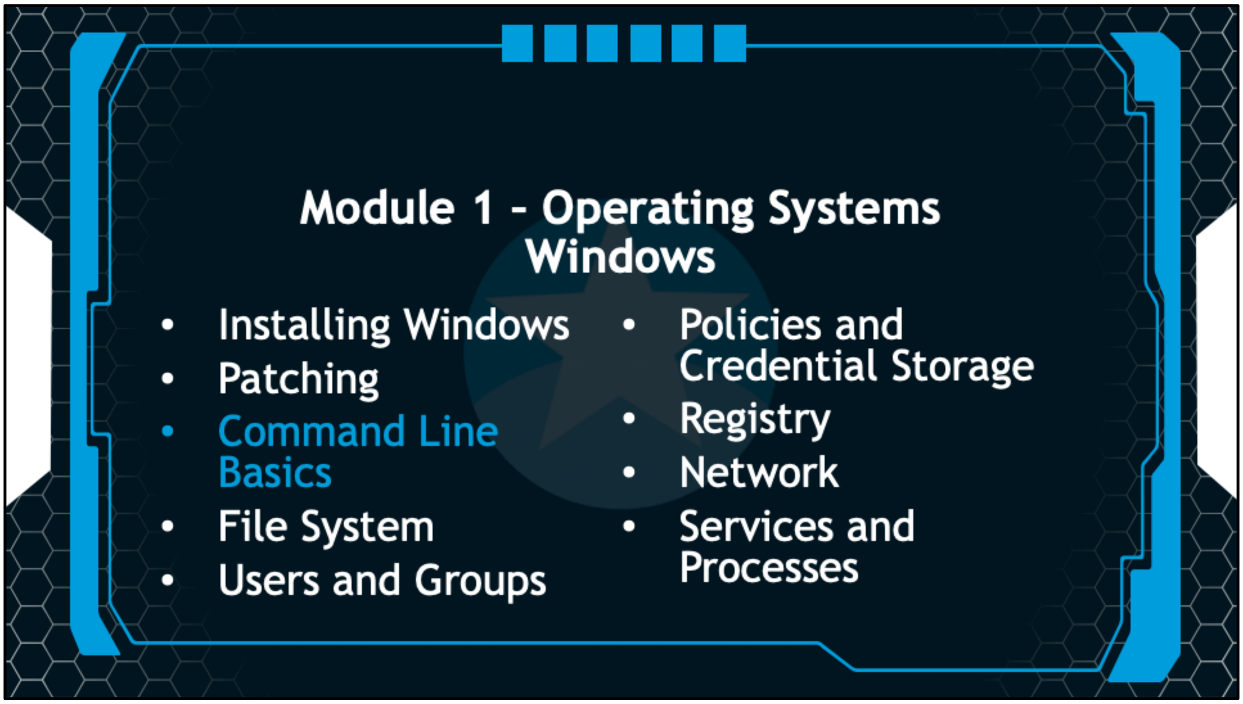
YOUR GATEWAY TO CYBERSECURITY SKILLS AND CAREERS

1. Introduction to Operating Systems
   - 01. Linux
   - 02. Windows
2. Networking
3. System Administration
   - 01. Bash
   - 02. PowerShell
   - 03. Python

This training material was originally developed to help students, teachers, and mentors prepare for the Cyber Aces Online Competition. This module focuses on the basics of what an operating systems is as well as the two predominant OS's, Windows and Linux. This session is part of Module 1, Introduction to Operating Systems. This module is split into two sections, Linux and Windows. In this session, we will continue our examination of Windows.

The three modules of Cyber Aces Online are Operating Systems, Networking, and System Administration.

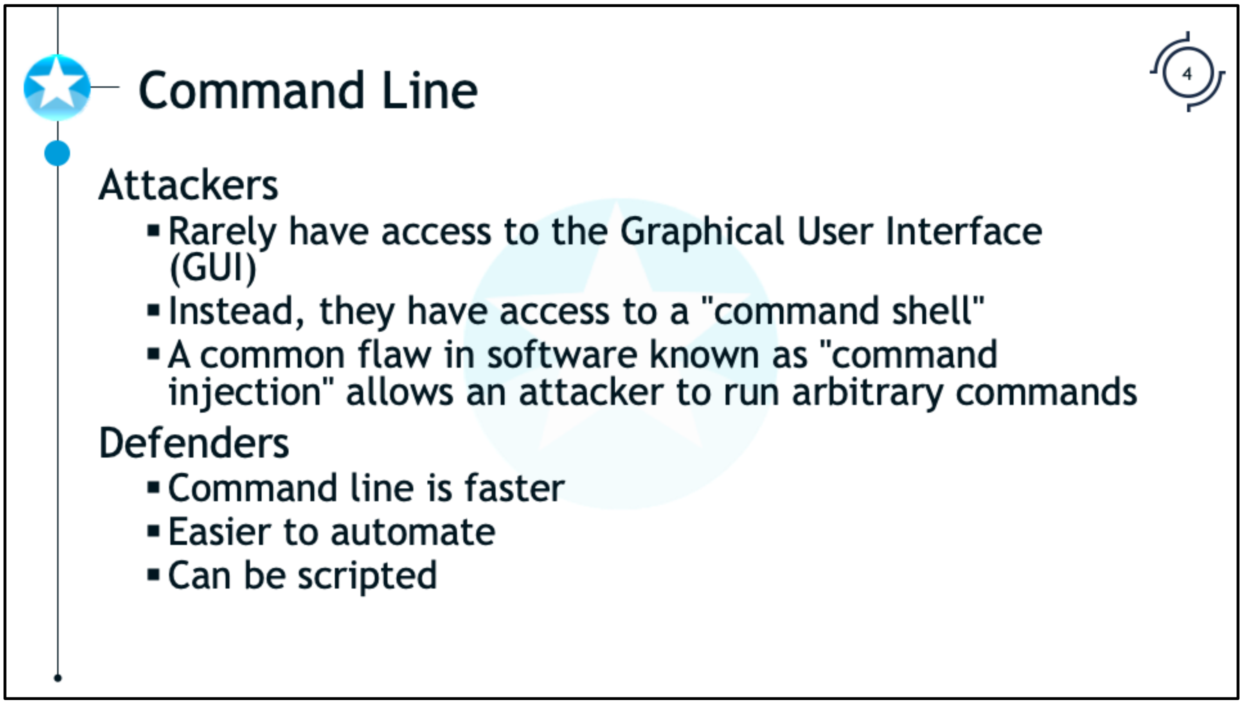
For more information about the Cyber Aces program, please visit the Cyber Aces website at https://CyberAces.org/.



Module 1 - Operating Systems Windows

- Installing Windows
- Patching
- Command Line Basics
- File System
- Users and Groups
- Policies and Credential Storage
- Registry
- Network
- Services and Processes

In this session we will learn some of the Windows command line using CMD.EXE.



Command Line

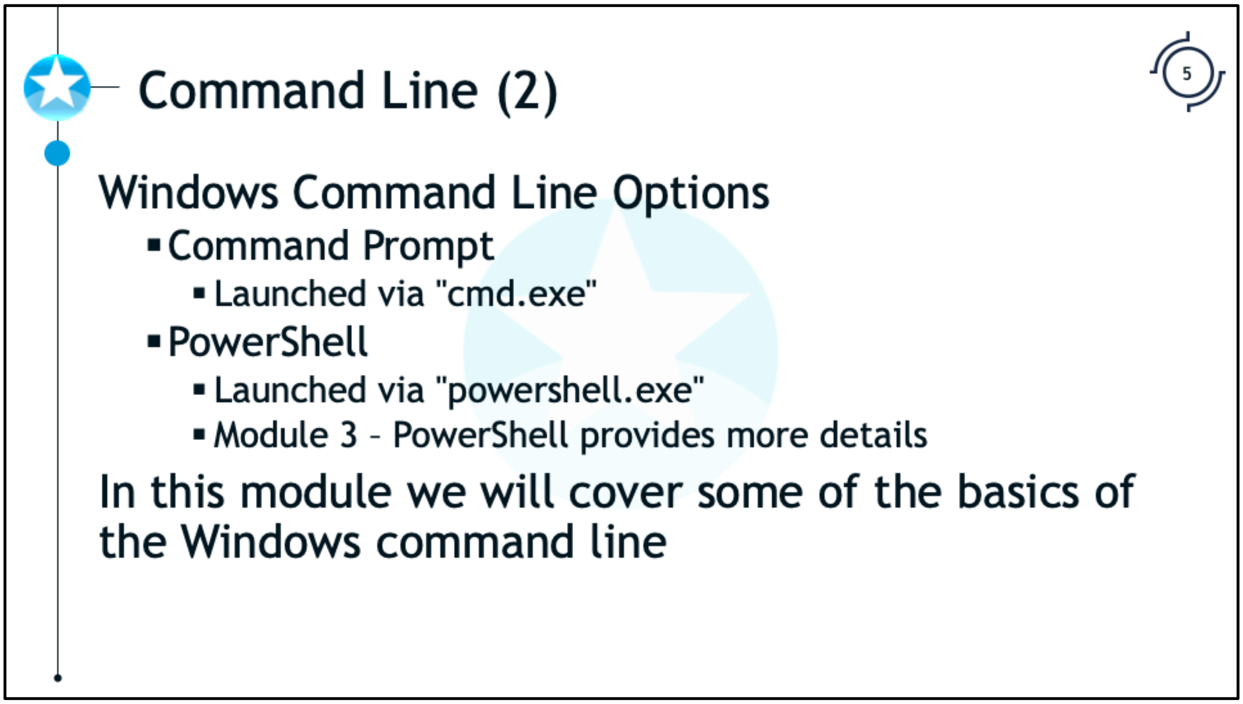
Attackers

- Rarely have access to the Graphical User Interface (GUI)
- Instead, they have access to a "command shell"
- A common flaw in software known as "command injection" allows an attacker to run arbitrary commands

Defenders

- Command line is faster
- Easier to automate
- Can be scripted

Computer attackers often do not have full control of a target system's Graphical User Interface or GUI for short. Instead, they usually get a "command shell" (i.e., Command Line Access, Command Line Interface or CLI) that they could use to gain control of the GUI if they choose. Likewise, defenders often have to rely on the command line to defend their system. Defenders need to automate their defenses using scripts that run at the command line or quickly make a series of changes to the system that would be very SLOW to make if you made those changes through the GUI. Therefore, you should be familiar with the use of the command line. Many of the examples and exercises in this course will make use of the command line, so let's start with a basic introduction to navigating the command line on Windows.



Command Line (2)

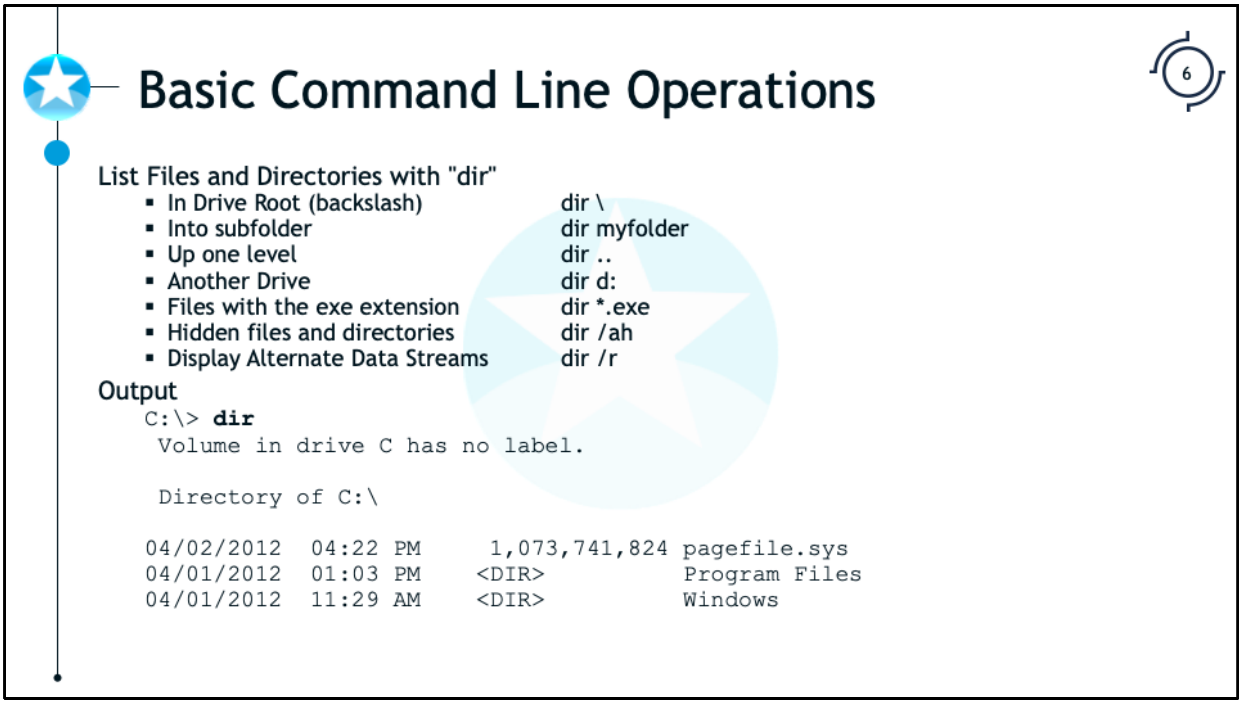
Windows Command Line Options

- Command Prompt
  - Launched via "cmd.exe"
- PowerShell
  - Launched via "powershell.exe"
  - Module 3 – PowerShell provides more details

In this module we will cover some of the basics of the Windows command line

In the Windows operating system, the main command-line interpreter is known as Command Prompt. Other interpreters, also known as command shells, are available for Windows but are not as widely-used. For instance, the Windows PowerShell, which provides an avenue for users to perform more advanced administrative tasks within a script-friendly environment, was first introduced in Windows Server 2008R2 and Windows 7, but installations are available for many earlier version of Windows. Windows 10 includes PowerShell version 5.1.

The Command Prompt may be launched by pressing the Windows button (or moving the mouse to the corner), typing "cmd.exe" (without quotes), and then pressing Enter. The web site https://redsiege.com/ca/cmd provides a brief introduction to using Command Prompt and familiarizes readers with key administrative commands.



Basic Command Line Operations

List Files and Directories with "dir"

In Drive Root (backslash)	dir \
Into subfolder	dir myfolder
Up one level	dir ..
Another Drive	dir d:
Files with the exe extension	dir *.exe
Hidden files and directories	dir /ah
Display Alternate Data Streams	dir /r

Output

```
C:\> dir
 Volume in drive C has no label.

 Directory of C:\

04/02/2012  04:22 PM     1,073,741,824 pagefile.sys
04/01/2012  01:03 PM    <DIR>          Program Files
04/01/2012  11:29 AM    <DIR>          Windows
```

The "dir" command is used to list the files and subdirectories in a directory. By default, it looks for files and directories without the hidden attribute set. It displays the last write time, the size of the file or if the item is a directory, and the name.

To view the contents of a specific directory use these commands:

• Current directory:	**`dir`**
• Current drive:	**`dir \`**
• Subdirectory:	**`dir subdir1`**
• Another drive:	**`dir d:`** or **`dir d:\`**
• List files with exe extension:	**`dir *.exe`**
• Parent directory:	**`dir ..`**

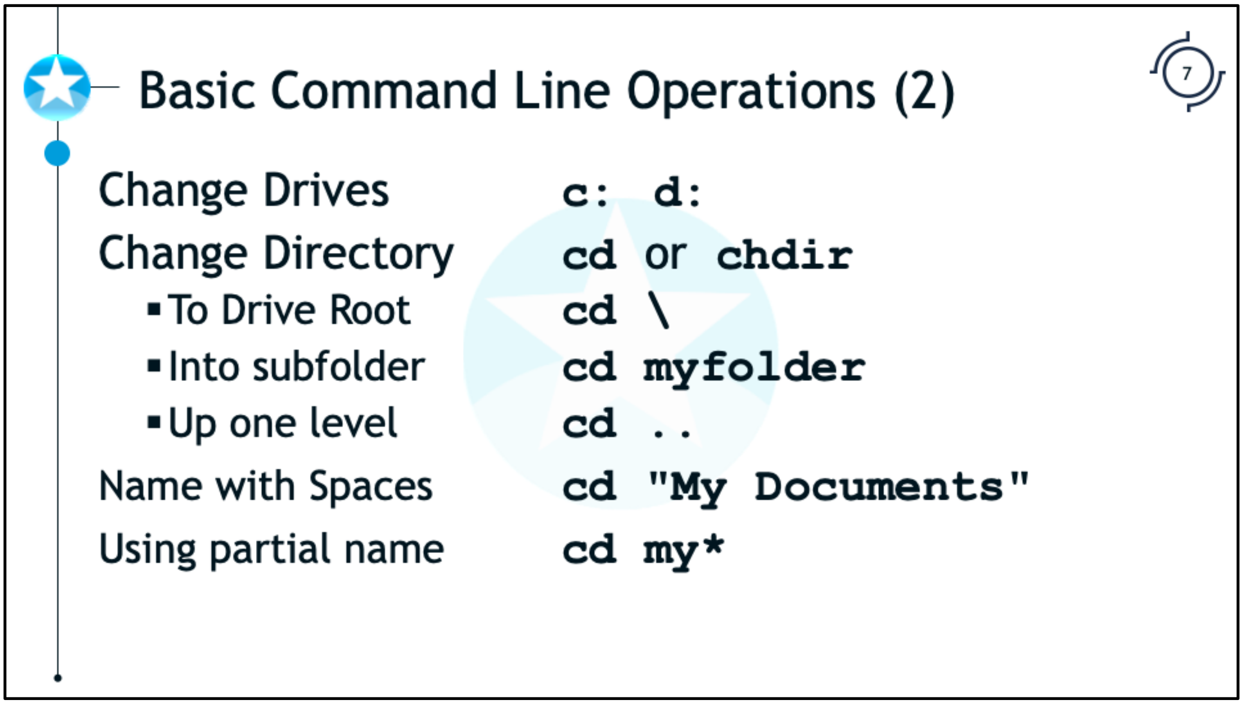
The options can be combined to view the contents of other specific directories:

• Sibling directory:	**`dir ..\otherdir`**
• Grandchild directory:	**`dir subdir1\subdir2`**
• Directory on another drive:	**`dir d:\myfldr\otherdir`**
• Sibling folder:	**`dir ..\otherdir`**

Items with the hidden attribute: **`dir /ah`**

items containing alternate data streams (covered later in this module) use: **`dir /r`**

A full list of options for the "dir" command can be seen by typing: **`dir /?`**



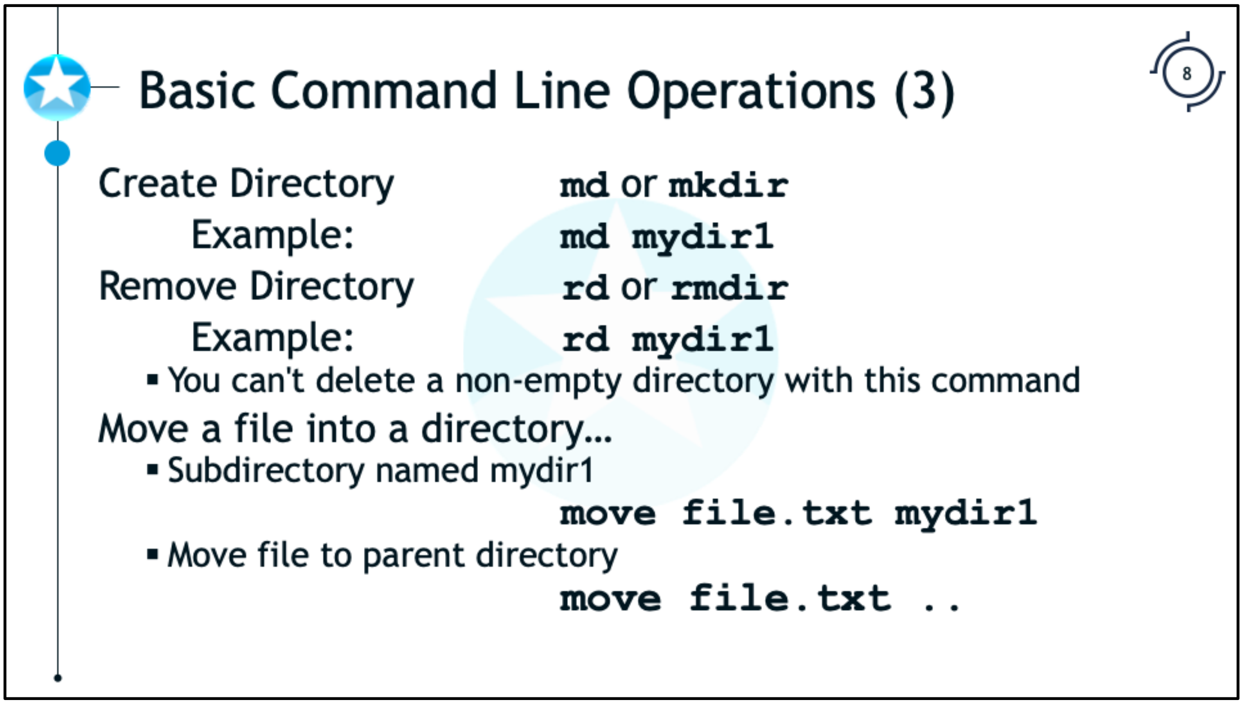
Basic Command Line Operations (2)

Change Drives	**`c:  d:`**
Change Directory	**`cd`** or **`chdir`**
▪ To Drive Root	**`cd \`**
▪ Into subfolder	**`cd myfolder`**
▪ Up one level	**`cd ..`**
Name with Spaces	**`cd "My Documents"`**
Using partial name	**`cd my*`**

To change drives, type the drive letter followed by a colon. For example, to change to the D drive (typically a CD drive) type **`d:`**

The "cd" and "chdir" commands are used to change the current directory, and is short for "change directory". Running the command without any options will display the current working directory, but the command is most often used to change directories. These commands can be used to change to specific directories:

- The root of the current drive: **`cd \`**
- A subdirectory in the current working directory: **`cd myfolder`**
- Move to the parent directory: **`cd ..`**
- Move to the directory whose name contains spaces: **`cd "My Documents"`**
- Move to the directory without typing the full name: **`cd my*`**



Basic Command Line Operations (3)

Create Directory **`md`** or **`mkdir`**

Example: **`md mydir1`**

Remove Directory **`rd`** or **`rmdir`**

Example: **`rd mydir1`**

- You can't delete a non-empty directory with this command

Move a file into a directory...

- Subdirectory named mydir1

```
move file.txt mydir1
```

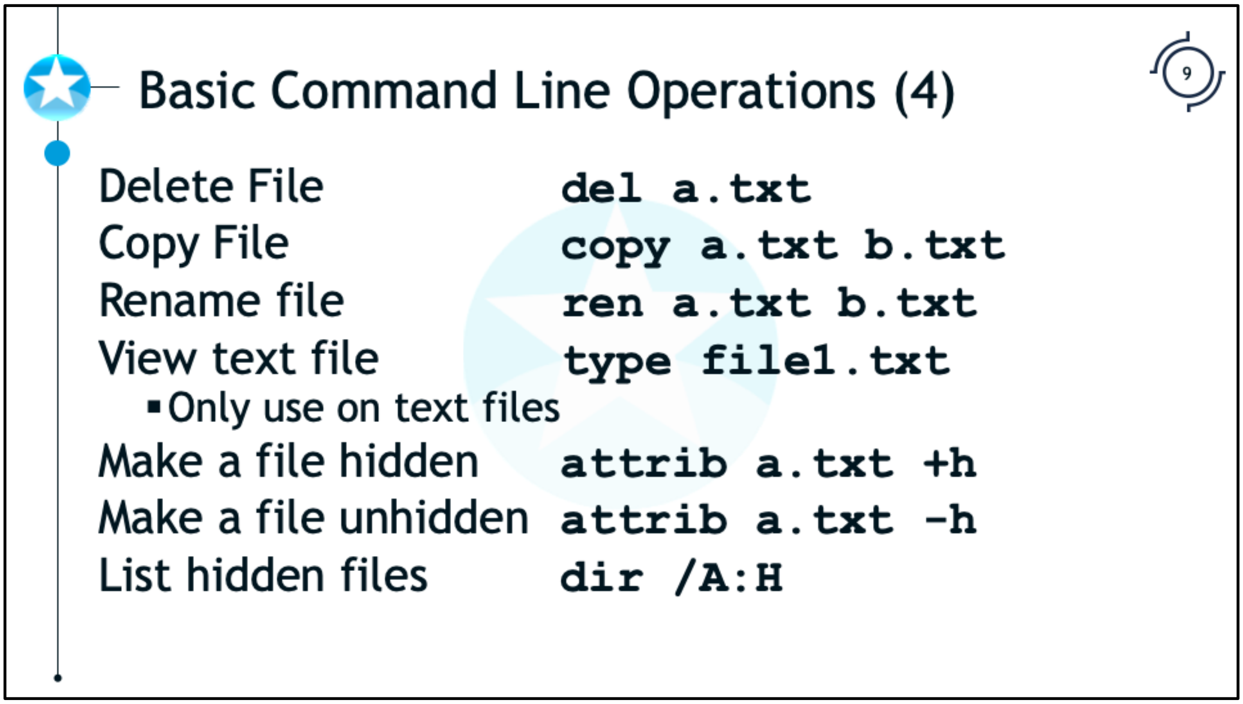
- Move file to parent directory

```
move file.txt ..
```

To make a directory, you can use the command "md" or "mkdir". Similarly, to remove a directory, you can use the command "rd" or "rmdir". Typically the shorter "md" and "rd" commands are used as they are easier to type.

You can move files via the aptly named "move" command. You can also move files using similar path qualifiers as used with the "cd" command. Examples:

Make a new directory:	`mkdir newdir`
Delete a directory:	`rd newdir`
Move a file to a subdirectory:	`move file.txt mysubdir`
Move a file to the parent directory:	`move file.txt ..`
Move a file to a sibling directory:	`move file.txt ..\otherdir`
Move a file to the root of the current drive:	`move file.txt \`
Move a file to a directory on another drive:	`move file.txt z:\dir1\subdir`



Basic Command Line Operations (4)

Delete File	`del a.txt`
Copy File	`copy a.txt b.txt`
Rename file	`ren a.txt b.txt`
View text file	`type file1.txt`
▪ Only use on text files	
Make a file hidden	`attrib a.txt +h`
Make a file unhidden	`attrib a.txt -h`
List hidden files	`dir /A:H`

Basic Command Line Operations (4)

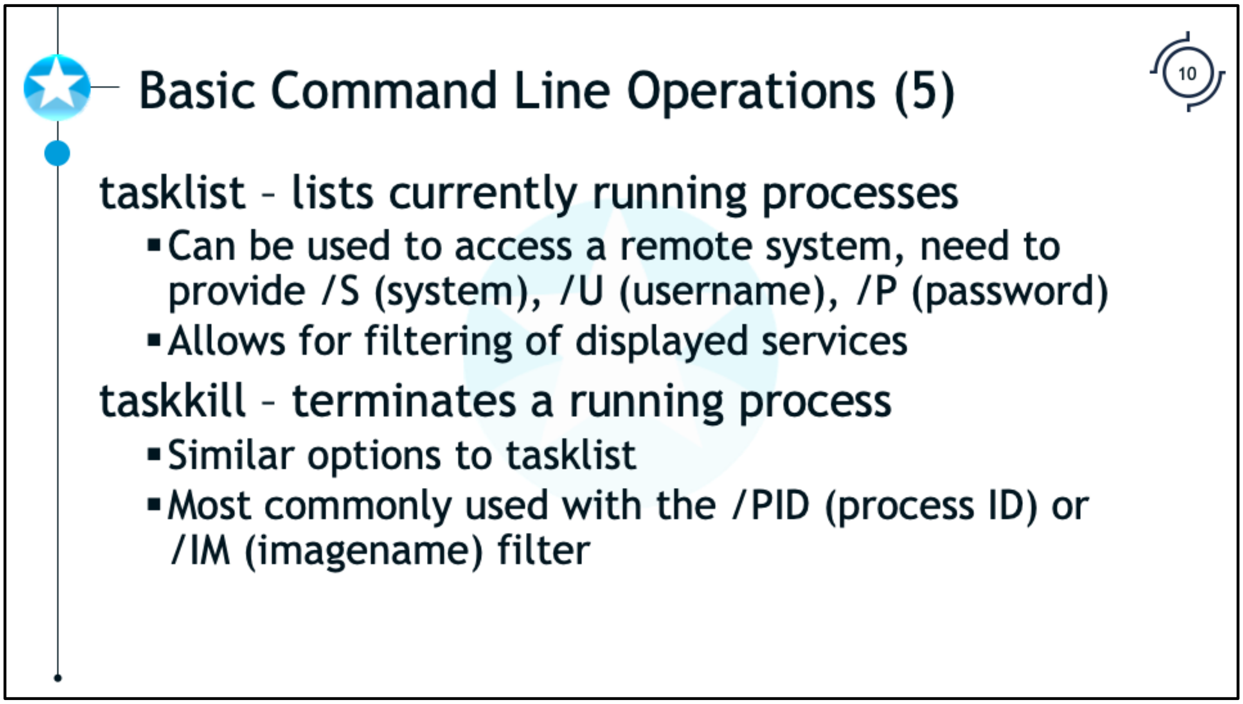
Use the "del" command to delete a file: `del a.txt`

Use the "copy" command to copy a file

- Create a backup copy: `copy a.txt myfilebackup.txt`
- To another drive and directory: `copy a.txt z:\myfiles\`
- These command can also use the path qualifiers previously discussed with the "cd" command

Use the "ren" command to rename a file: `ren a.txt b.txt`

The "attrib" command is used to set attributes on files. Files can be marked as Read-Only (r), Archive (a), System (s), or Hidden (h). The attributes are not exclusive, so more than one attribute can be set. The plus (+) can be used to add an attribute and the minus (-) can be used to remove the attribute. The attrib command can also be used to set the attributes on all files in the directory tree by specifying the directory and using the /S option. (e.g. attrib +h /s mydir). To apply the attribute changes to directories too, use the /D option. The /S and /D options can be used to together to modify the attributes on files and folders.



Basic Command Line Operations (5)

tasklist – lists currently running processes

- Can be used to access a remote system, need to provide /S (system), /U (username), /P (password)
- Allows for filtering of displayed services

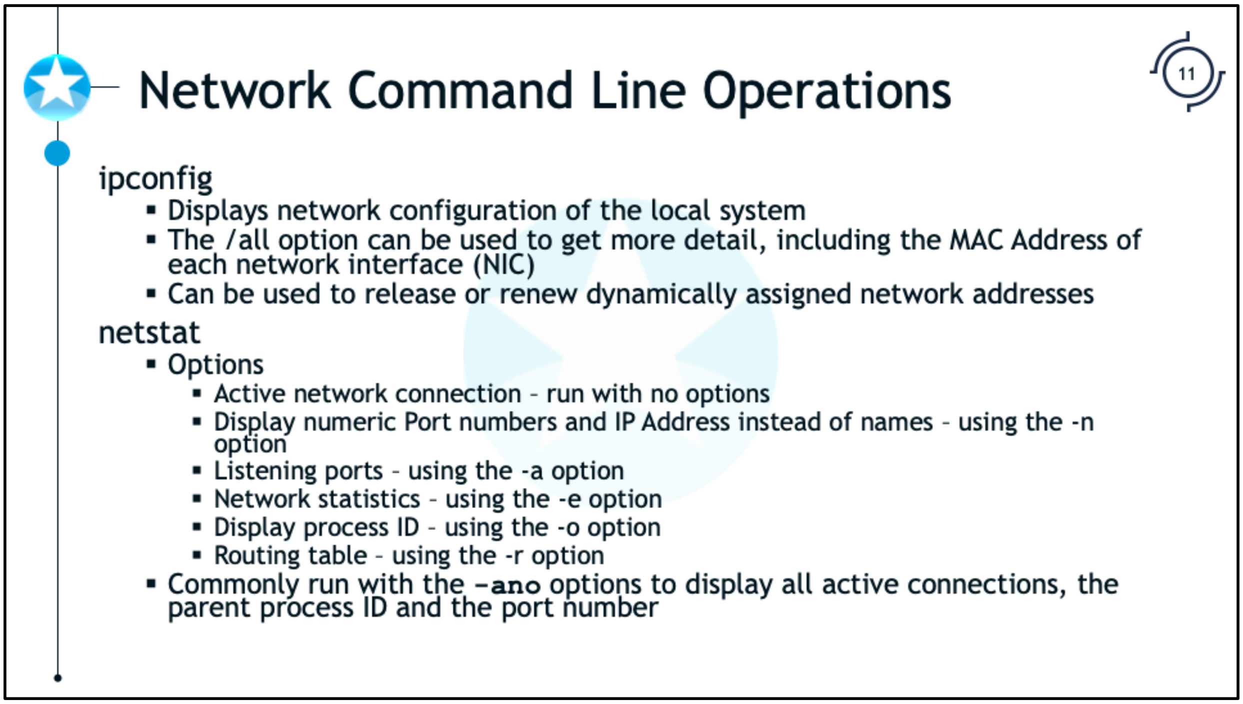
taskkill – terminates a running process

- Similar options to tasklist
- Most commonly used with the /PID (process ID) or /IM (imagename) filter

The "tasklist" command displays the processes that are currently running on the local or a remote system. To specify a remote system the /S (system), /U (user) and /P (password) options must be used. You can filter the list of processes by using the /fi option and using these filter options:

<table>
<tr><th>Filter Name</th><th>Valid Operators</th><th>Valid Value(s)</th></tr>
<tr><td>STATUS</td><td>eq, ne</td><td>RUNNING | NOT RESPONDING | UNKNOWN</td></tr>
<tr><td>IMAGENAME</td><td>eq, ne</td><td>Image name</td></tr>
<tr><td>PID</td><td>eq, ne, gt, lt, ge, le</td><td>PID value</td></tr>
<tr><td>SESSION</td><td>eq, ne, gt, lt, ge, le</td><td>Session number</td></tr>
<tr><td>SESSIONNAME</td><td>eq, ne</td><td>Session name</td></tr>
<tr><td>CPUTIME</td><td>eq, ne, gt, lt, ge, le</td><td>CPU time in the format of hh:mm:ss.
(hh - hours, mm - minutes, ss – seconds)</td></tr>
<tr><td>MEMUSAGE</td><td>eq, ne, gt, lt, ge, le</td><td>Memory usage in KB</td></tr>
<tr><td>USERNAME</td><td>eq, ne</td><td>User name in [domain\]user format</td></tr>
<tr><td>SERVICES</td><td>eq, ne</td><td>Service name</td></tr>
<tr><td>WINDOWTITLE</td><td>eq, ne</td><td>Window title</td></tr>
<tr><td>MODULES</td><td>eq, ne</td><td>DLL name</td></tr>
</table>

The "taskkill" command uses the same filtering options as tasklist.



Network Command Line Operations

ipconfig

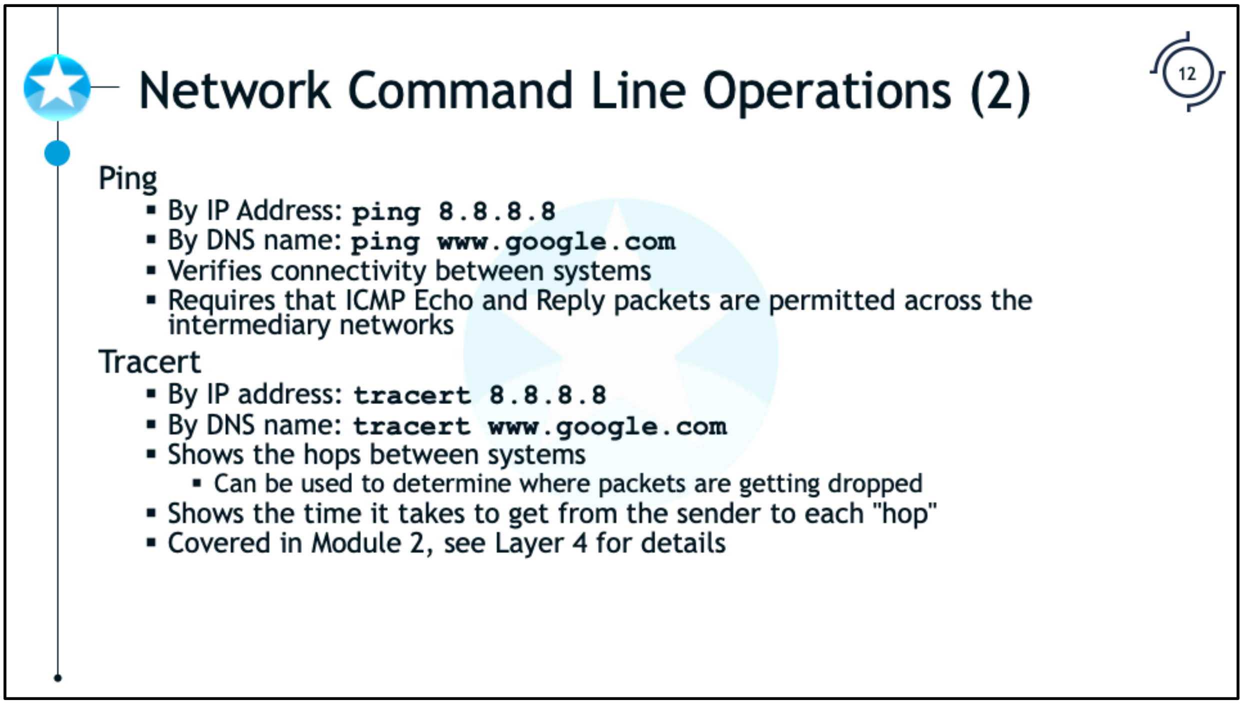
- Displays network configuration of the local system
- The /all option can be used to get more detail, including the MAC Address of each network interface (NIC)
- Can be used to release or renew dynamically assigned network addresses

netstat

- Options
  - Active network connection - run with no options
  - Display numeric Port numbers and IP Address instead of names - using the -n option
  - Listening ports - using the -a option
  - Network statistics - using the -e option
  - Display process ID - using the -o option
  - Routing table - using the -r option
- Commonly run with the `-ano` options to display all active connections, the parent process ID and the port number

The "ipconfig" command is commonly used to display the network configuration of the local system. More detail, including the MAC address, is displayed when the command is run with the /all option. The /renew and /release options can be used to renew or release (respectively) IP Addresses obtained by a DHCP server.

The netstat command is a very useful command to system administrators and incident handlers as provides information regarding currently open connections or open ports. It can also be used to determine the process ID of the process that opened the connection or port. This is useful to determine which processes are communicating with other systems.



Network Command Line Operations (2)

Ping

- By IP Address: `ping 8.8.8.8`
- By DNS name: `ping www.google.com`
- Verifies connectivity between systems
- Requires that ICMP Echo and Reply packets are permitted across the intermediary networks

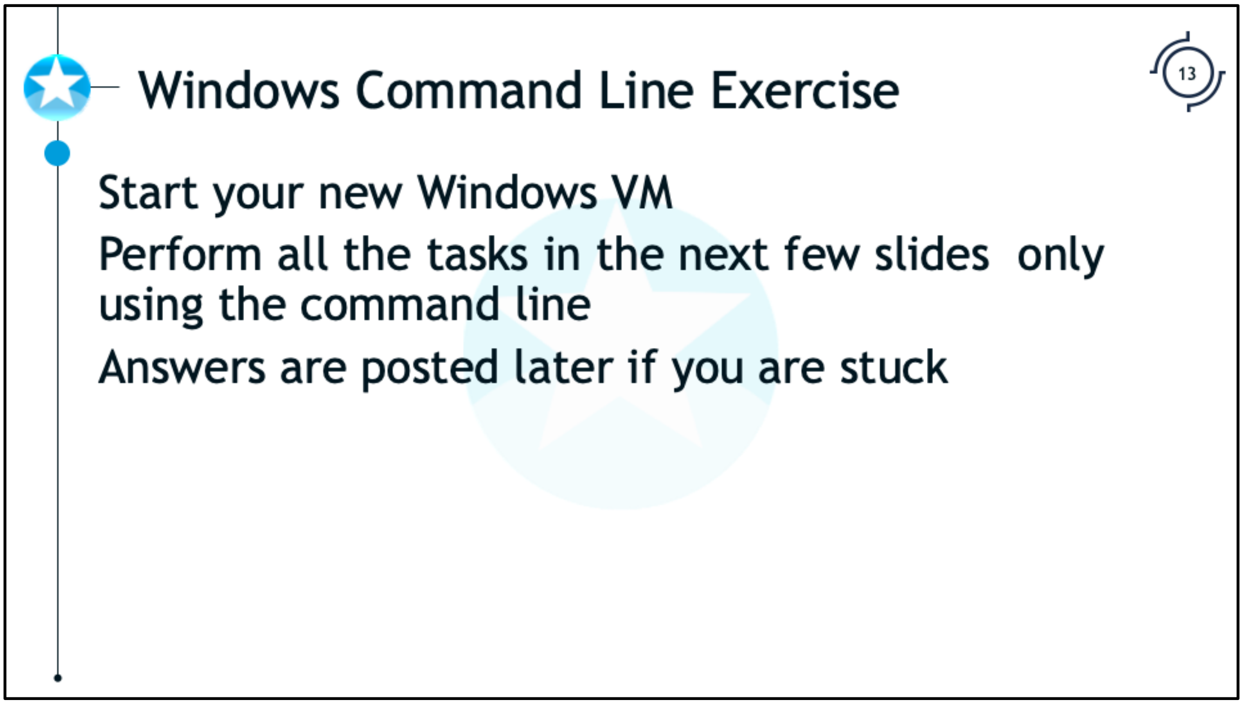
Tracert

- By IP address: `tracert 8.8.8.8`
- By DNS name: `tracert www.google.com`
- Shows the hops between systems
  - Can be used to determine where packets are getting dropped
- Shows the time it takes to get from the sender to each "hop"
- Covered in Module 2, see Layer 4 for details

The "ping" command is used to verify connectivity and check for issues between two systems. The command sends an Echo packet via the ICMP Protocol (Internet Control Message Protocol). The receiving system responds with an ICMP Echo-Reply packet. If there are any network issues in either direction between the two nodes, the system executing the ping will not receive the echo-reply packets. In addition, the sending host times how long it takes between sending the Echo-Request packet and the receipt of the Echo-Reply packet to determine the latency of the links between the hosts.

To work properly, the ping command requires that ICMP Echo-Request and Echo-Reply packets are permitted across the networks and that the remote system is not blocking ping requests. For example, if you ping www.google.com you will get a reply, but www.sans.org does not send reply packets. The rationale for blocking ping is that it is not essential traffic and it is not necessary for continued operation of the provided internet services (web, mail, etc).

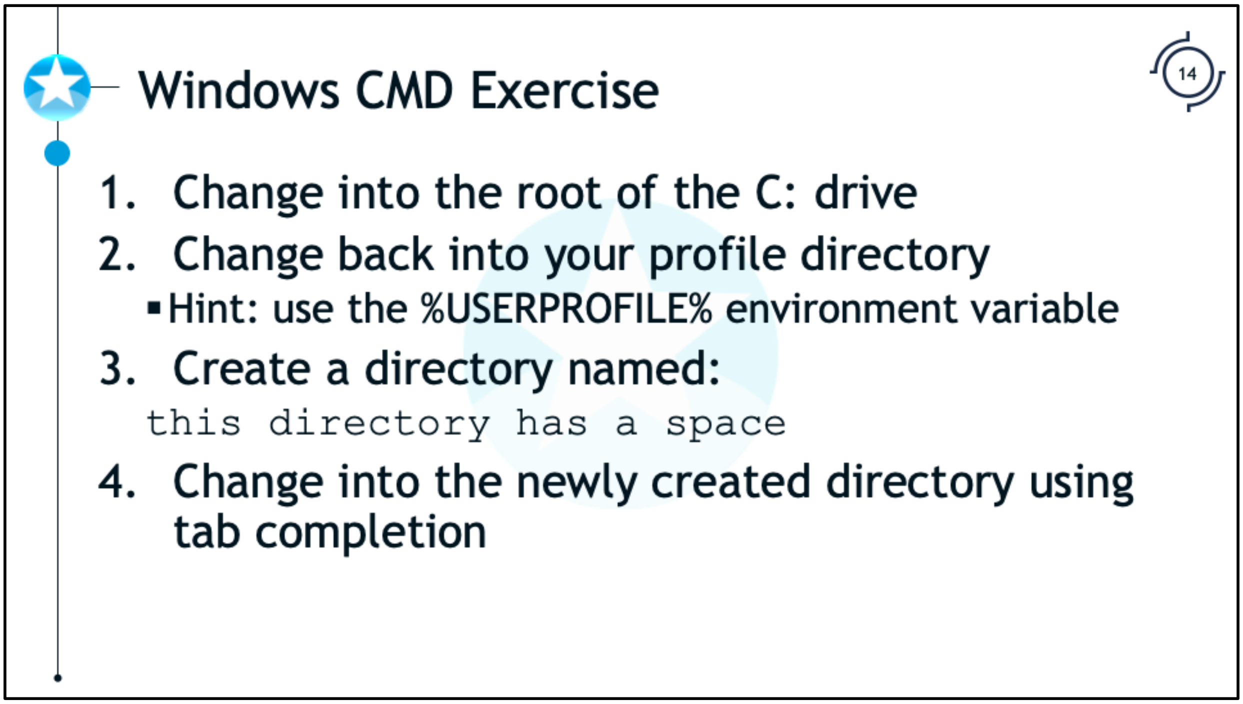
The "tracert" (short for Trace Route) command is useful for displaying the path and measuring the latency of packets as they move across the network. The command is quite useful for troubleshooting as it can reveal slow or down links. It does require that the intermediate systems send ICMP Time Exceeded packets and that your host is able to receive such packets. For an explanation as to how tracert works check out the link on Wikipedia: https://en.wikipedia.org/wiki/Traceroute



Windows Command Line Exercise

- Start your new Windows VM
- Perform all the tasks in the next few slides only using the command line
- Answers are posted later if you are stuck

We will practice some of the commands we just learned using the Windows VM built earlier. You will need to start your VM and then perform the tasks presented on the next few pages. If you get stuck, jump ahead for answers.



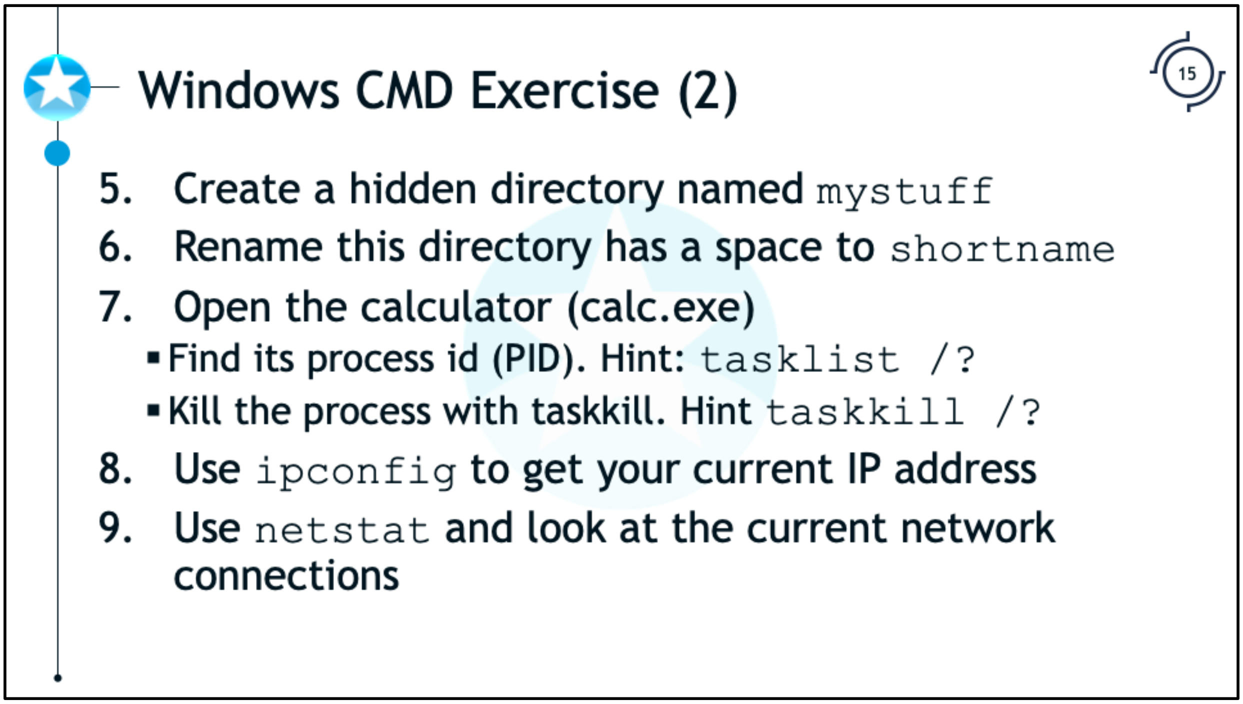
Windows CMD Exercise

1. Change into the root of the C: drive
2. Change back into your profile directory
   - Hint: use the %USERPROFILE% environment variable
3. Create a directory named:
   `this directory has a space`
4. Change into the newly created directory using tab completion

Windows CMD Exercise

Perform these tasks. If you are stuck then skip ahead for the answers.

1. Change into the root of the C: drive
2. Change back to your profile directory
3. Create a directory with the name "this directory has a space"
4. Change into the newly created directory using tab completion



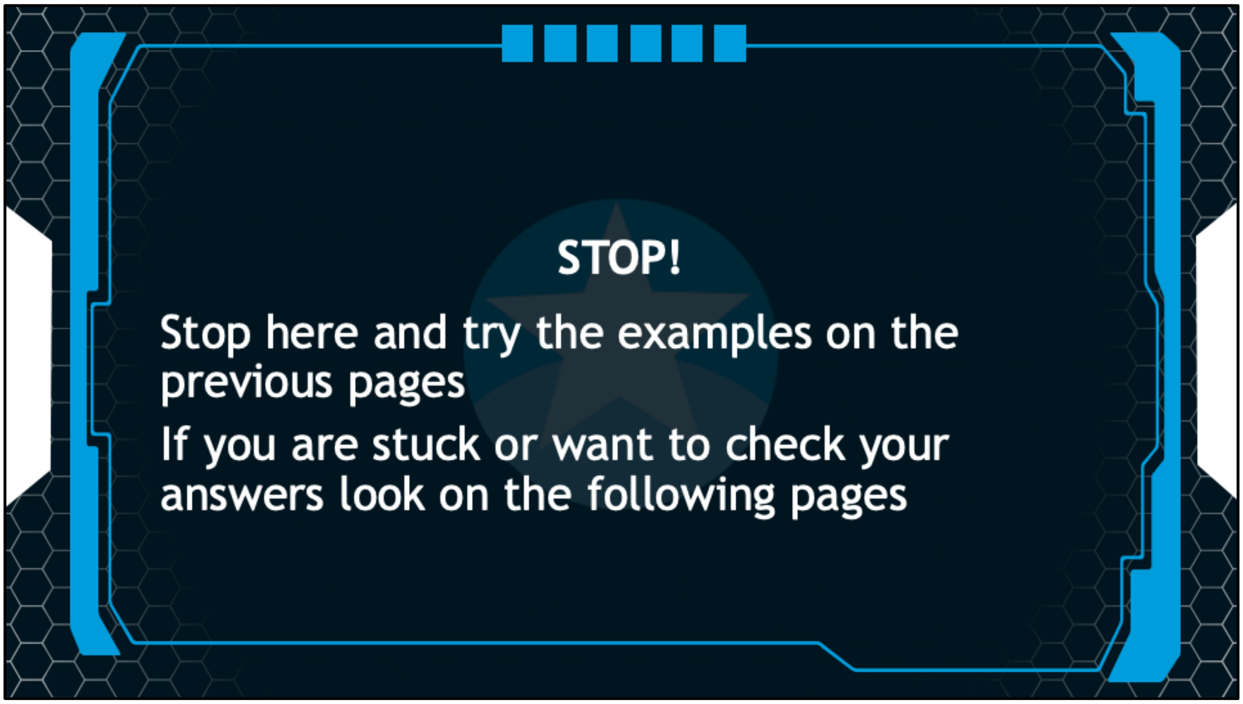
Windows CMD Exercise (2)

5. Create a hidden directory named `mystuff`
6. Rename this directory has a space to `shortname`
7. Open the calculator (calc.exe)
   - Find its process id (PID). Hint: `tasklist /?`
   - Kill the process with taskkill. Hint `taskkill /?`
8. Use `ipconfig` to get your current IP address
9. Use `netstat` and look at the current network connections

Windows CMD Exercise (2)

Continue by attempting to to complete the following tasks:

5. Create a hidden directory named "mystuff"
6. Rename "this directory has a space" to "shortname"
7. Open the calculator from the command line (calc.exe)
   a. Find the process ID
   b. Kill the process
8. Use ipconfig to get your current IP address
9. Use netstat and look at the current network connections



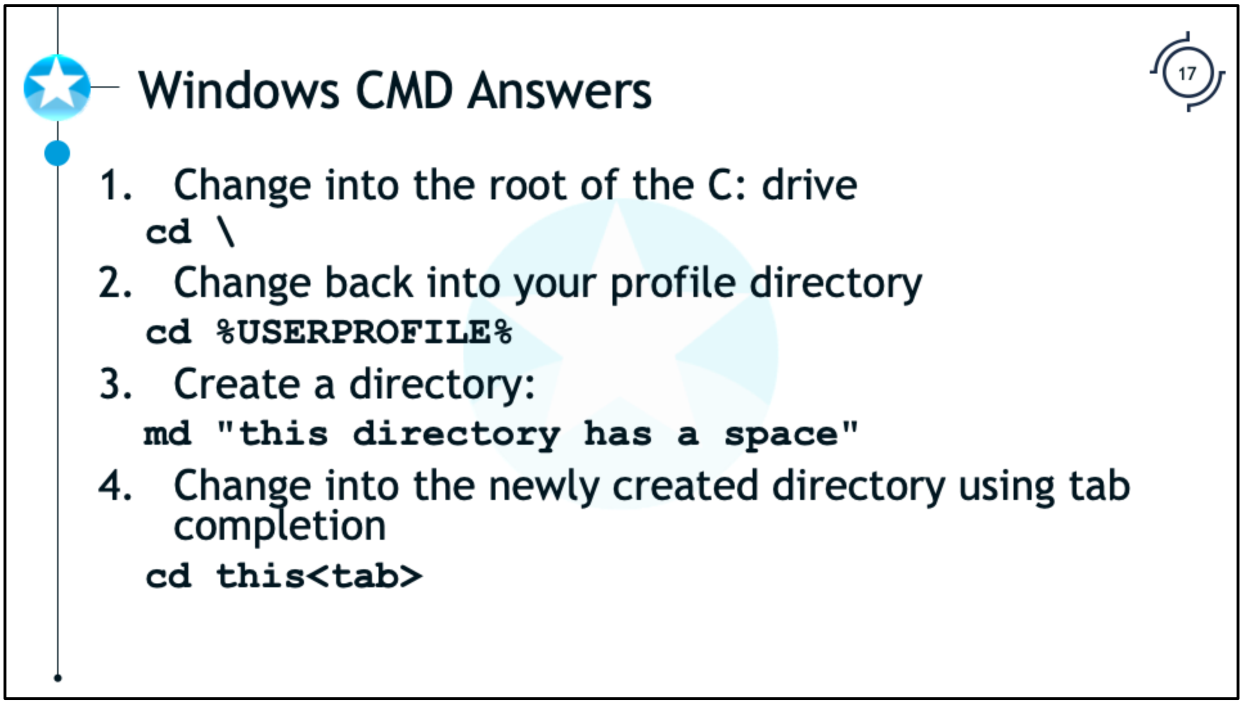
STOP!

Stop here and try the examples on the previous pages

If you are stuck or want to check your answers look on the following pages

STOP!

The answers are on the following pages. Stop here and use your new knowledge to accomplish the tasks on the previous slides.



Windows CMD Answers

1. Change into the root of the C: drive

```
cd \
```

2. Change back into your profile directory

```
cd %USERPROFILE%
```

3. Create a directory:

```
md "this directory has a space"
```

4. Change into the newly created directory using tab completion

```
cd this<tab>
```

Windows CMD Answers

Here are some examples of commands that can be used to accomplished the tasks outlined earlier:

1. Change into the root of the C: drive:

```
cd \
```

2. Change back to your profile directory:

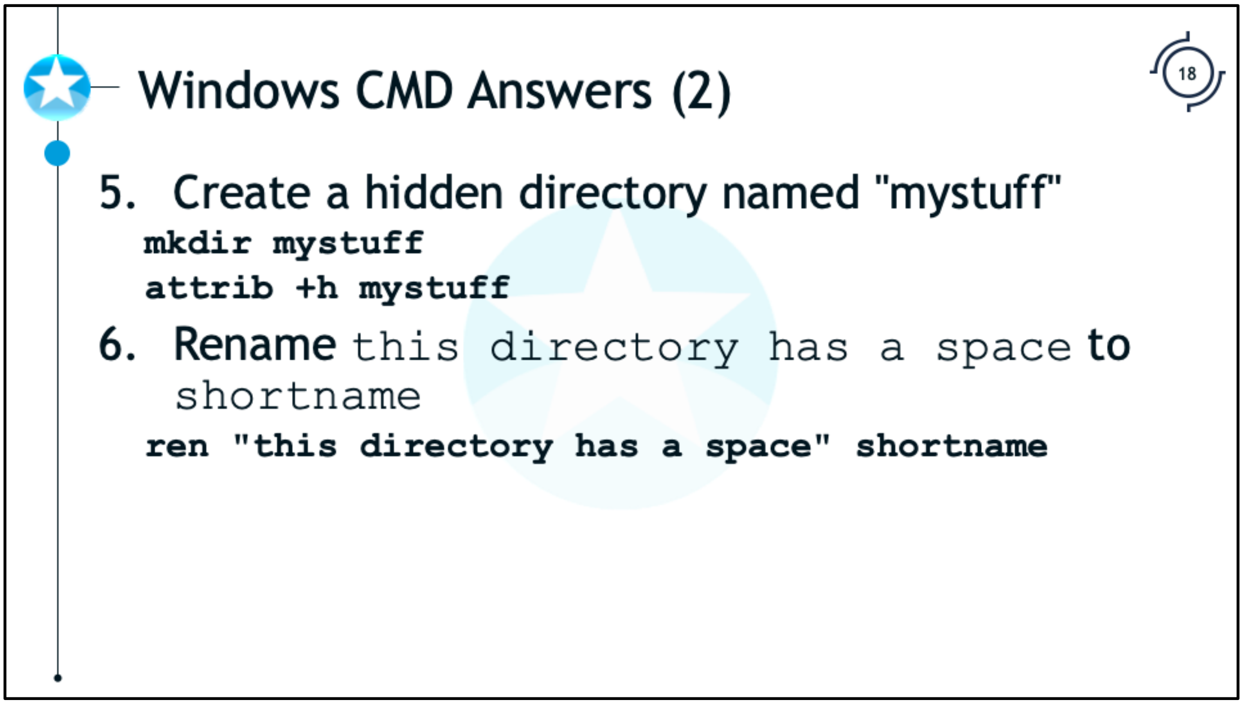
```
cd %USERPROFILE%
```

3. Create a directory with the name "this directory has a space":

```
md "this directory has a space"
```

4. Change into the newly created directory using tab completion:

```
cd this<tab>
```



Windows CMD Answers (2)

5. Create a hidden directory named "mystuff"

```
mkdir mystuff
attrib +h mystuff
```

6. Rename `this directory has a space` to `shortname`

```
ren "this directory has a space" shortname
```

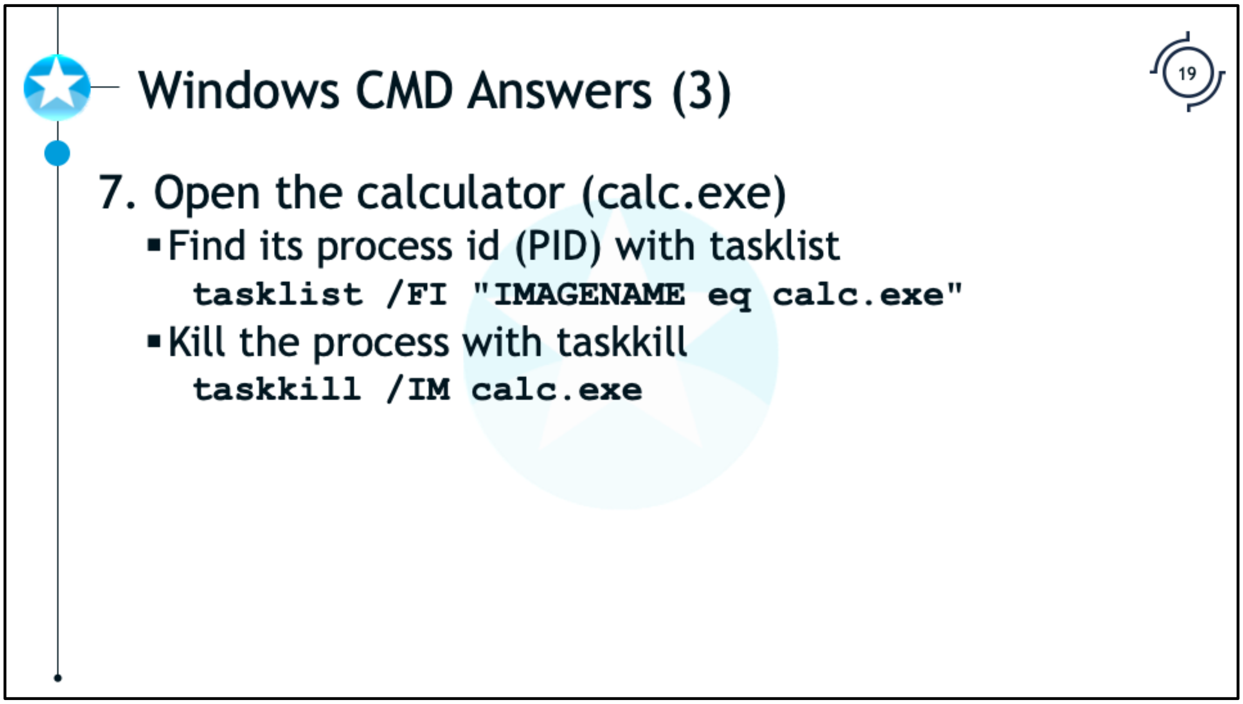
Windows CMD Answers

5. Create a hidden directory named "mystuff"

```
mkdir mystuff
attrib +h mystuff
```

6. Rename "this directory has a space" to "shortname":

```
ren "this directory has a space" shortname
```



Windows CMD Answers (3)

7. Open the calculator (calc.exe)
   - Find its process id (PID) with tasklist

     ```
     tasklist /FI "IMAGENAME eq calc.exe"
     ```

   - Kill the process with taskkill

     ```
     taskkill /IM calc.exe
     ```

Windows CMD Answers (3)

7. Open calc.exe by typing calc.exe in the command line.
   a. Find the process ID using tasklist

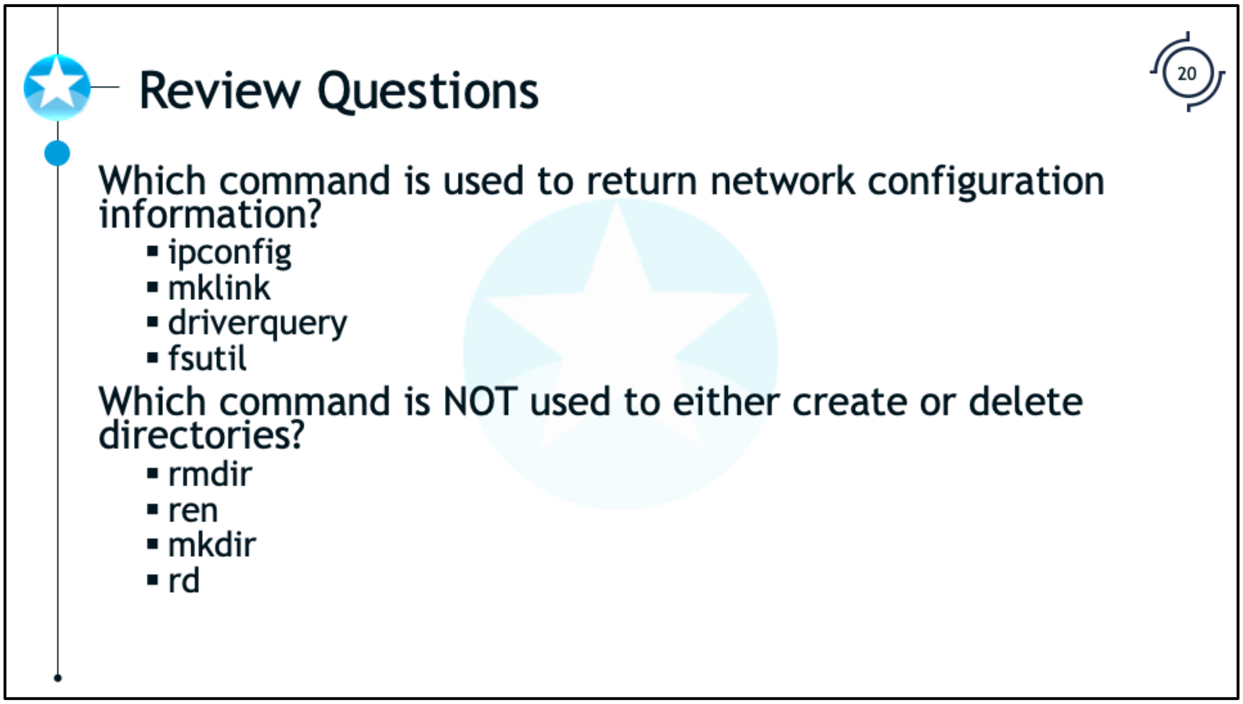
      ```
      tasklist /FI "IMAGENAME eq calc.exe"
      ```

   b. Kill the process with taskkill

      ```
      taskkill /IM calc.exe
      ```

      or

      ```
      taskkill <process ID>
      ```



Review Questions

Which command is used to return network configuration information?

- ipconfig
- mklink
- driverquery
- fsutil

Which command is NOT used to either create or delete directories?

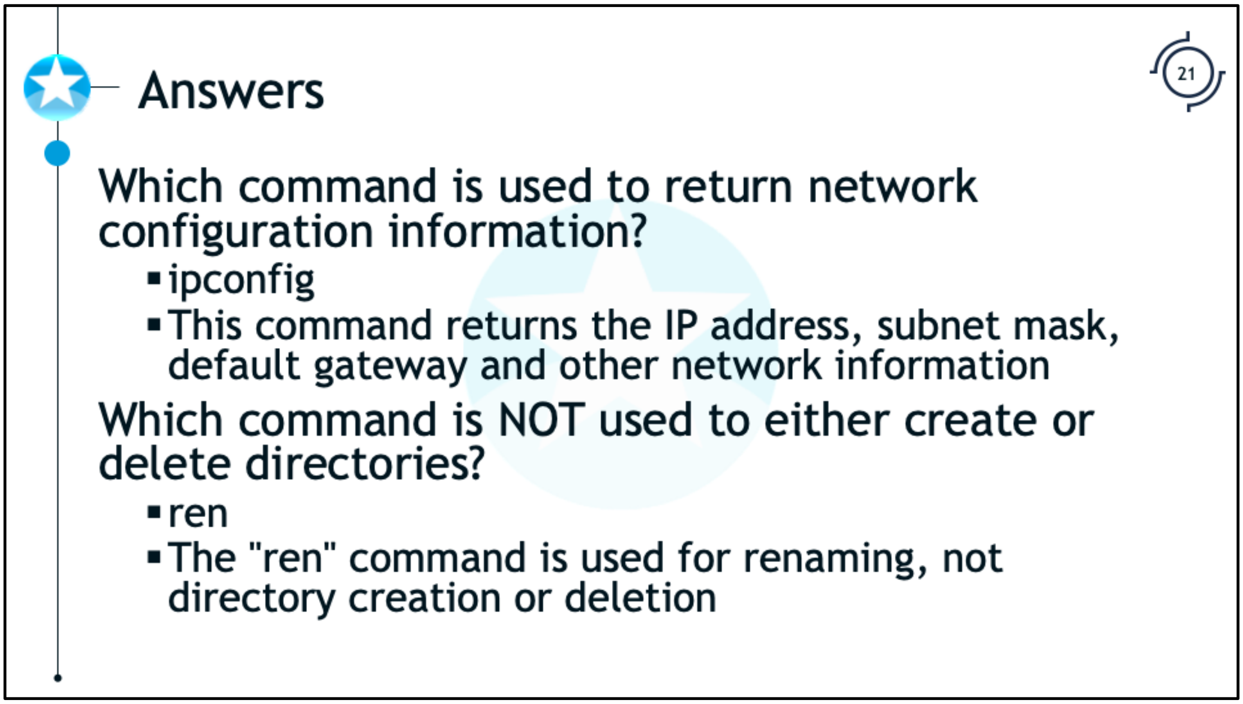
- rmdir
- ren
- mkdir
- rd

Which command is used to return network configuration information?

- ipconfig
- mklink
- driverquery
- Fsutil

Which command is NOT used to either create or delete directories?

- rmdir
- ren
- mkdir
- rd



Answers

Which command is used to return network configuration information?

- ipconfig
- This command returns the IP address, subnet mask, default gateway and other network information

Which command is NOT used to either create or delete directories?

- ren
- The "ren" command is used for renaming, not directory creation or deletion

Which command is used to return network configuration information?

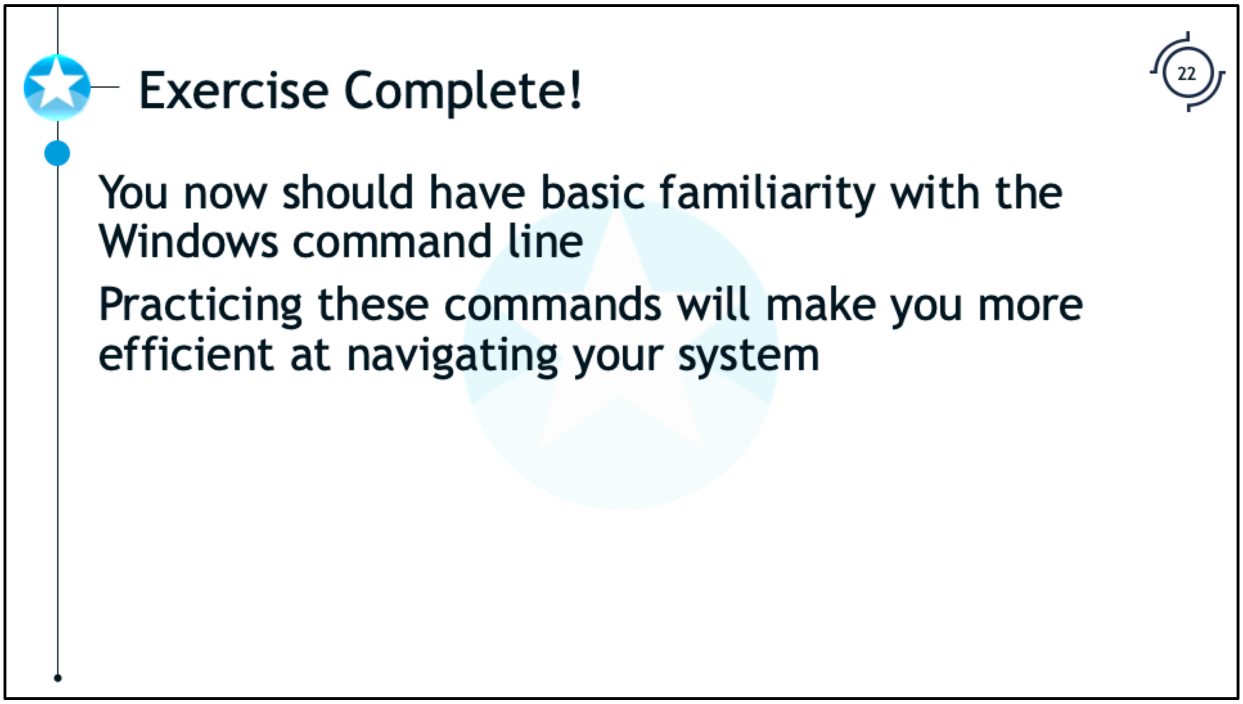
```
ipconfig
```

This command returns the IP address, subnet mask, default gateway and other network information

Which command is NOT used to either create or delete directories?

```
ren
```

The "ren" command is use for renaming, not directory creation or deletion

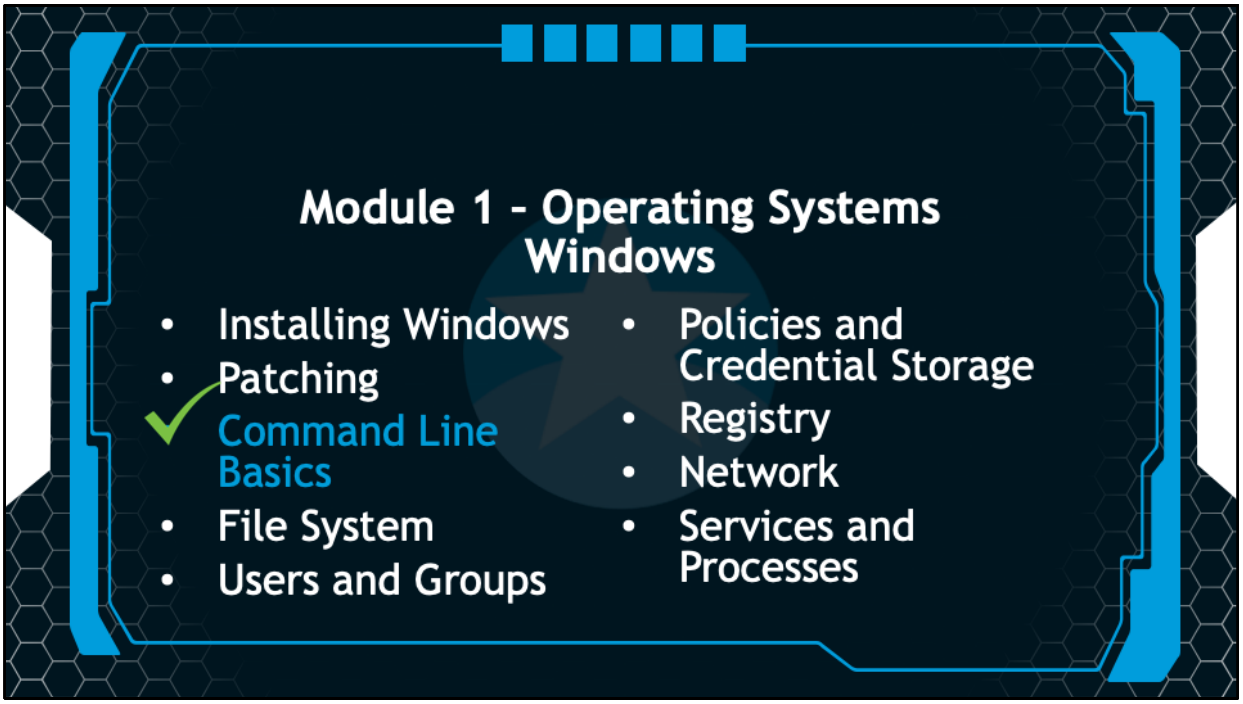


Exercise Complete!

You now should have basic familiarity with the Windows command line

Practicing these commands will make you more efficient at navigating your system

Congratulations, you are done with this exercise!



Module 1 - Operating Systems Windows

- Installing Windows
- Patching
- ✓ Command Line Basics
- File System
- Users and Groups
- Policies and Credential Storage
- Registry
- Network
- Services and Processes

In the next session we will examine the Windows file system.