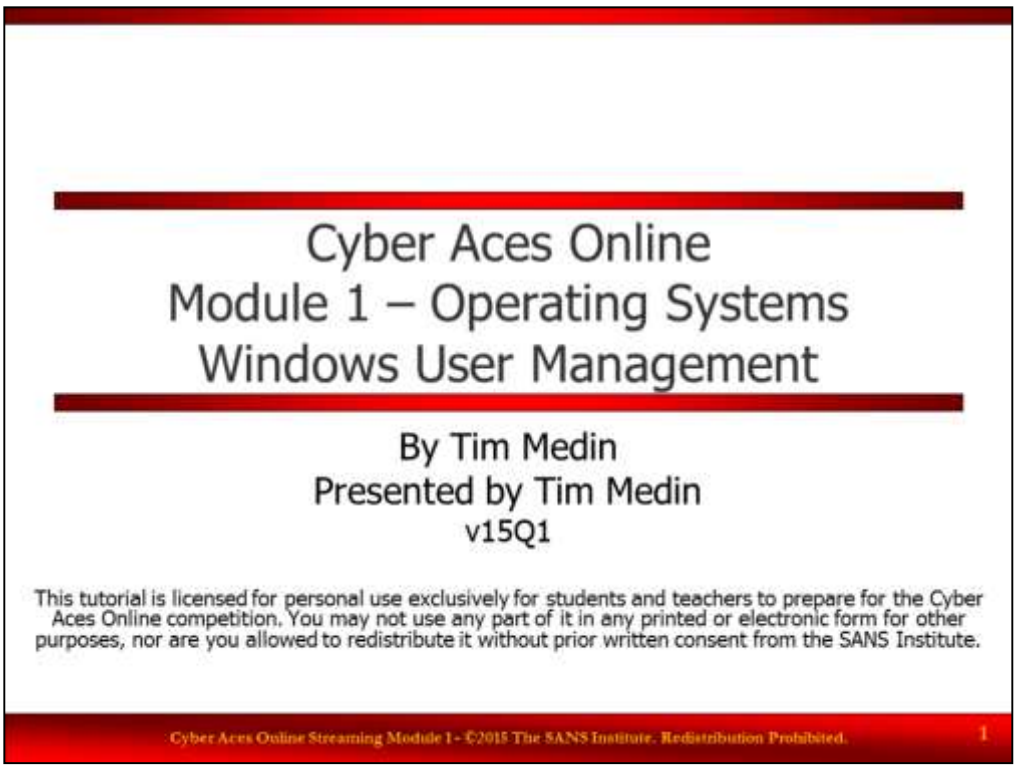
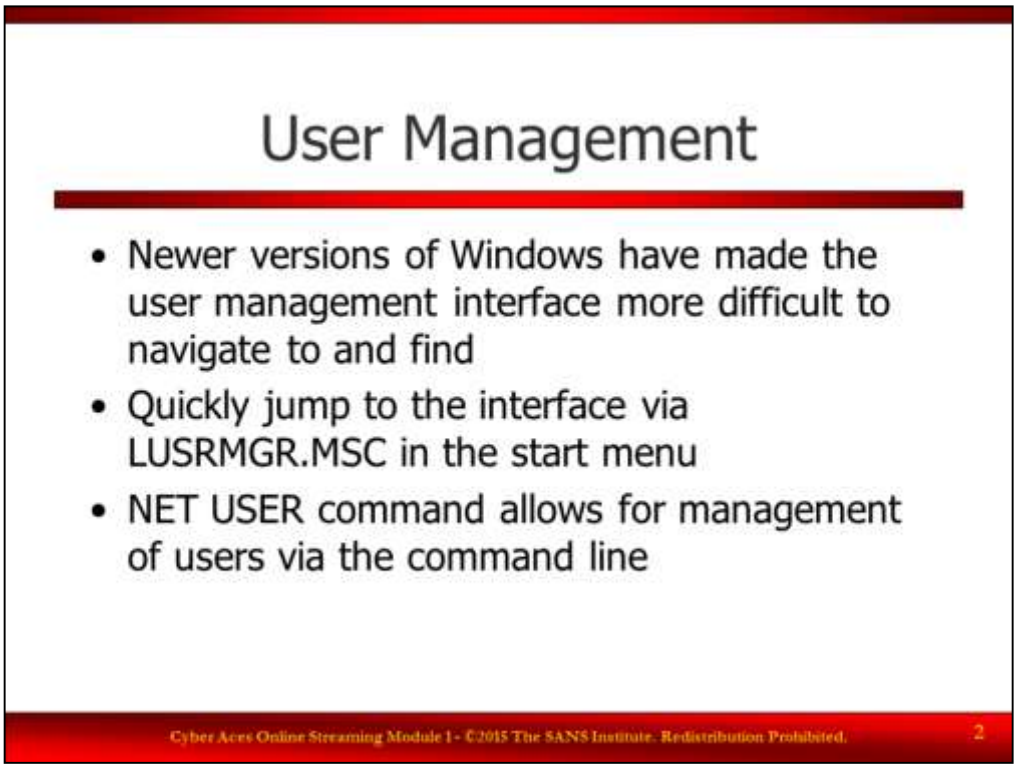


Welcome to Cyber Aces Online, Module 1! A firm understanding of operating systems is essential to being able to secure or attack one. This module dives in to Microsoft Windows Operating System.

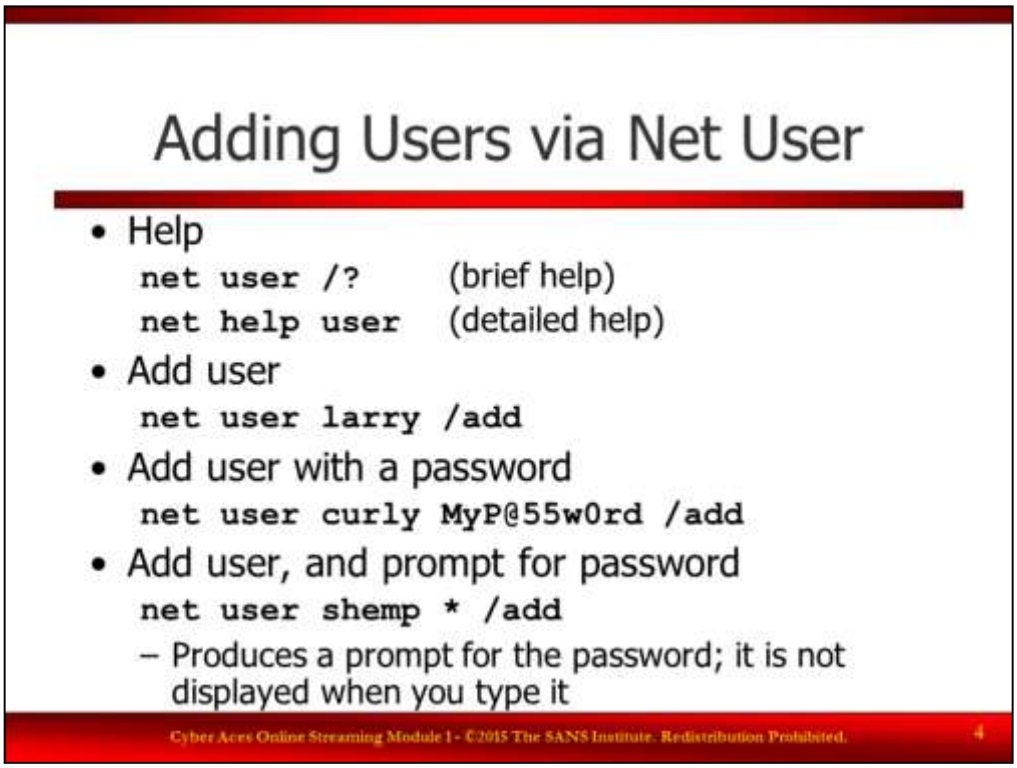


User Management

Under Windows, user accounts are typically managed from the Control Panel, where they may be created, edited, or deleted. Accounts may also be granted or revoked certain privileges. In addition to the "LUSRMGR.MSC" GUI tool, you can also manage users from the command line using the NET command.

Permissions & User Account Control (UAC)

Before you can modify any accounts on your system, you need to use an elevated command prompt. We will discuss User Account Control (UAC) in a while, but for now follow the steps outlined above to get an elevated prompt so we can create and modify accounts.



Adding Users via Net User

The command can be used to add a user without specifying a password. The command can also be run with a specified password or prompt the user to enter the password. The last option provides additional security as the password is not stored in the command history or displayed on the screen.

Net User command reference http://support.microsoft.com/kb/251394

To get detailed help type: **`net help user`**

Changing Passwords with Net User

On the previous page, we created Larry's account but did not set a password. The command we used was:

```
C:\> net user larry /add
```

If the /add option is omitted and a password is supplied then the user's password will be set or changed.

```
C:\> net user larry MyNewP@55w0rd
```

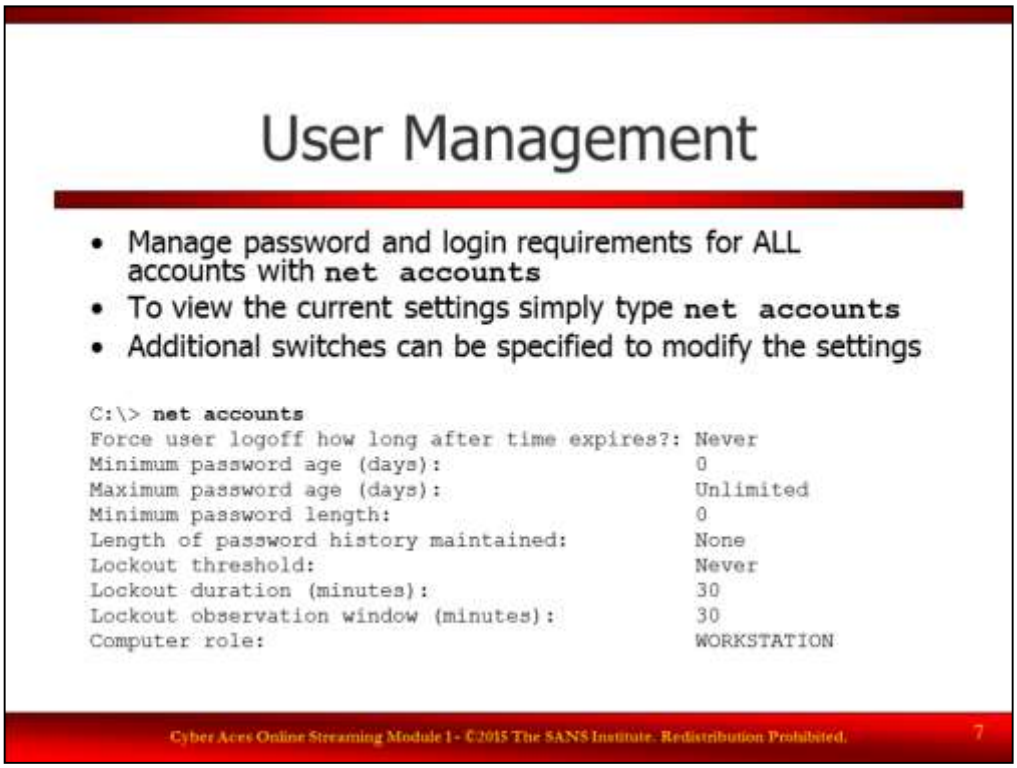
The above command (obviously) displays the password on the screen. If we don't want the password to be echoed on the screen we type an asterisk (*) instead of the password to be prompted for the password in a more secure manner.

```
C:\> net user larry
Type a password for the user:
Retype the password to confirm:
```

In the above case the password is never displayed on the screen.

Deleting and Disabling Accounts with Net User

A user can be deleted with the /delete option. Similarly, an account can be enabled or disabled using the /active option and specifying yes (to activate the account) or no (to deactivate the account).



User Management

The "net accounts" command "updates the user accounts database and modifies password and logon requirements for all accounts". When used without options, it displays the current settings for password, logon limitations, and domain information.

Some of the common options for this command are:

/FORCELOGOFF:{minutes | NO}

The number of minutes before a user is forced to log off. The default NO prevents forced logoff.

/MINPWLEN:length

The minimum password length where the range is between 0 and 14 characters. The default setting is 6 characters.

/MAXPWAGE:{days | UNLIMITED}

The maximum number of days that a password is valid, where the valid range is 1 through 999. The default value UNLIMITED means there is no expiration of the password. Also, the value used here cannot be less than the MINPWAGE.

/MINPWAGE:days

The minimum number of days that must pass after a password is set before a user can change his/her password, where the valid range is 0 through 999. A value of 0 means there is no minimum time. Also, the value used here can't be more than MAXPWAGE.

/UNIQUEPW:number

Requires the user's new password be different from X previous passwords where X is the number specified here. The maximum value is 24.

User Management Review

- Which of the following options will create a user named "John" from the command line on the Windows operating system?
  - useradd John
  - net user John /add
  - add user John -n C:\Users\John
  - manageaccount John /add-new
- Which of the following options will set the password for the username of "John" to "P@ssw0rd" from the command line on the Windows operating system?
  - User John P@ssw0rd set
  - Password reset is not available from the command line
  - net user John P@ssw0rd
  - net user P@ssw0rd John

Answers

- Which of the following options will create a user named "John" from the command line on the Windows operating system?
  - net user John /add
  - This command will create the user John, but it will not set his password upon creation. A password can also be set but using this command:
    net user John mypassword /add
- Which of the following options will set the password for the username of "John" to "P@ssw0rd" from the command line on the Windows operating system?
  - net user John P@ssw0rd
  - The format is "net user <username> <password>

Windows Groups

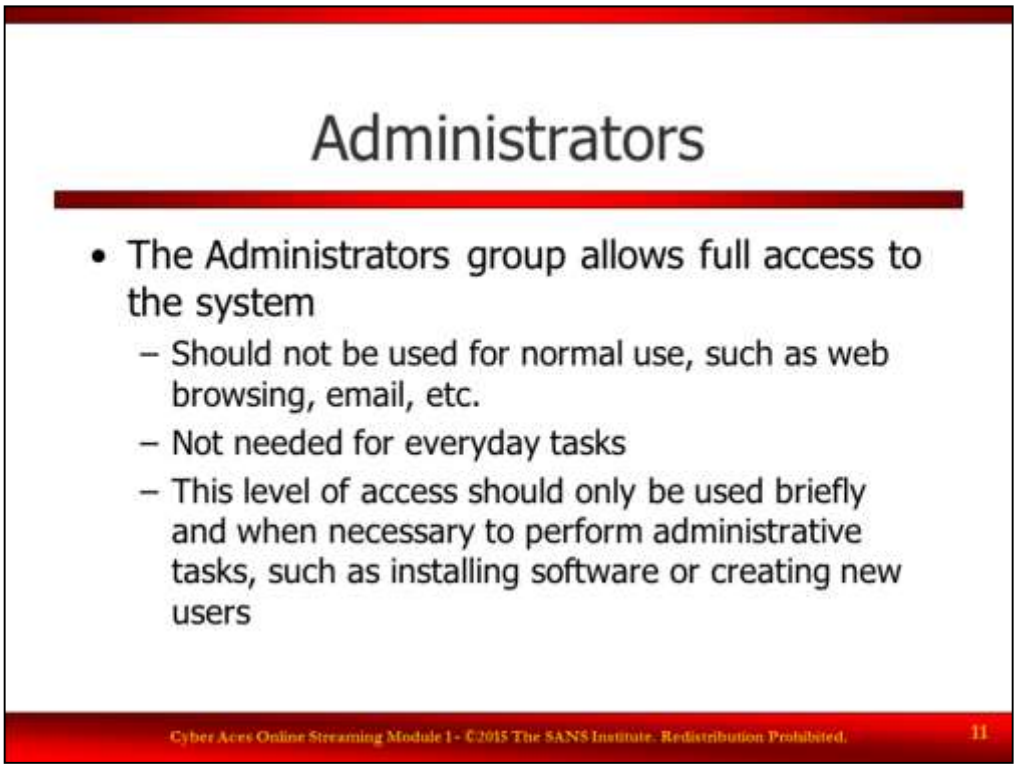
Once users are created, they are placed into "Groups". The groups are assigned NTFS and OS permissions. These groups make administration easier as the group can be given a specific permission and then users can be added and removed from the group as needed without having to make the changes for each individual user.

Windows has several built in groups including the following:

ADMINISTRATORS - Users in the administrators group can perform any action they desire on the computer including modifying the Kernel.

NETWORK CONFIGURATION OPERATORS - Users who have additional permissions enabling them to modify the computer's network settings such as IP address, DNS and Gateway.

USERS - Users is the only built-in group that people need to perform 99% of the activities on your computer. Even people whose job it is to administer their computer should only be in the USERS group and should use a separate account that is in the Administrators group only when performing administrative functions. This can be done using RUNAS.

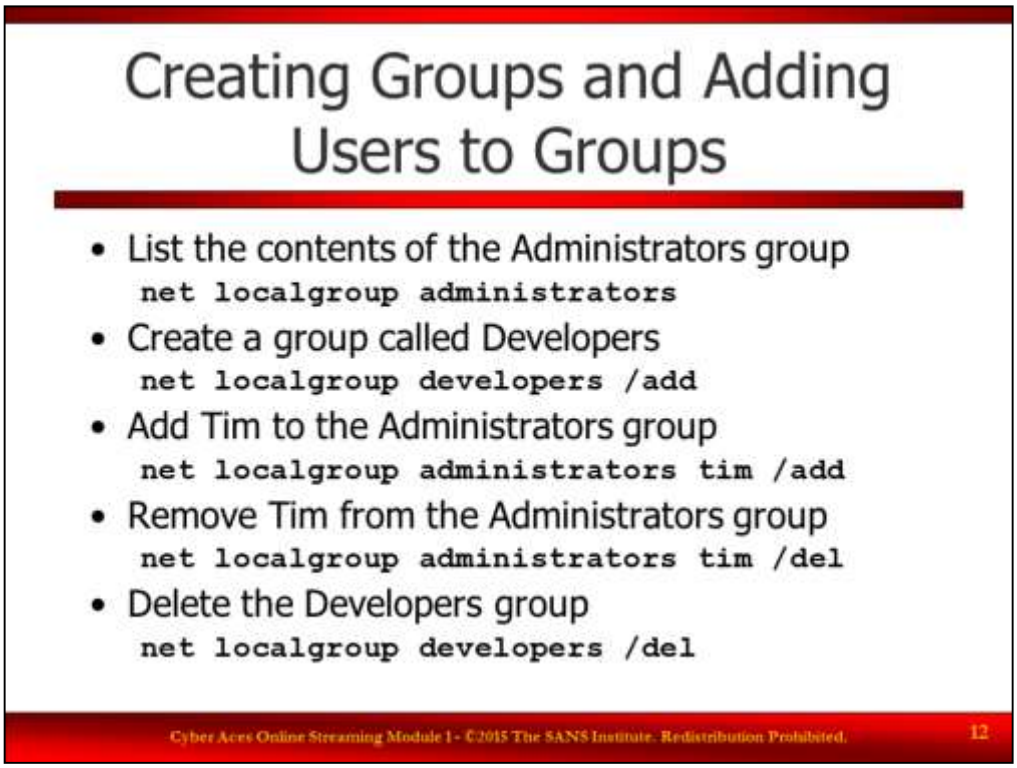


Administrators

Malware executing under administrative privilege can make irrevocable changes to the operating system. It can add itself to registry keys so that it will start automatically. It can modify antivirus software so that it no longer detects the malware or disable the antivirus completely. It can modify the kernel of the operating system, installing a rootkit to hide all kinds of malicious activity. Users should never use administrative privileges during their normal computer use. Administrative privileges should only be used briefly when absolutely necessary and when performing administrative tasks such as installing new software or creating new users.

Read this article on why you should not use administrative privileges for daily activities:

http://blogs.msdn.com/b/aaron_margosis/archive/2004/06/17/157962.aspx



Creating Groups and Adding Users to Groups

The **`net localgroup`** command is used to view and modify groups and group memberships. Below is a list of the common **`net localgroup`** commands used by administrators.

List the contents of the Administrators group

```
C:\> net localgroup administrators
```

Create a group called Developers

```
C:\> net localgroup developers /add
```

Add Tim to the Administrators group

```
C:\> net localgroup administrators tim /add
```

Remove Tim from the Administrators group

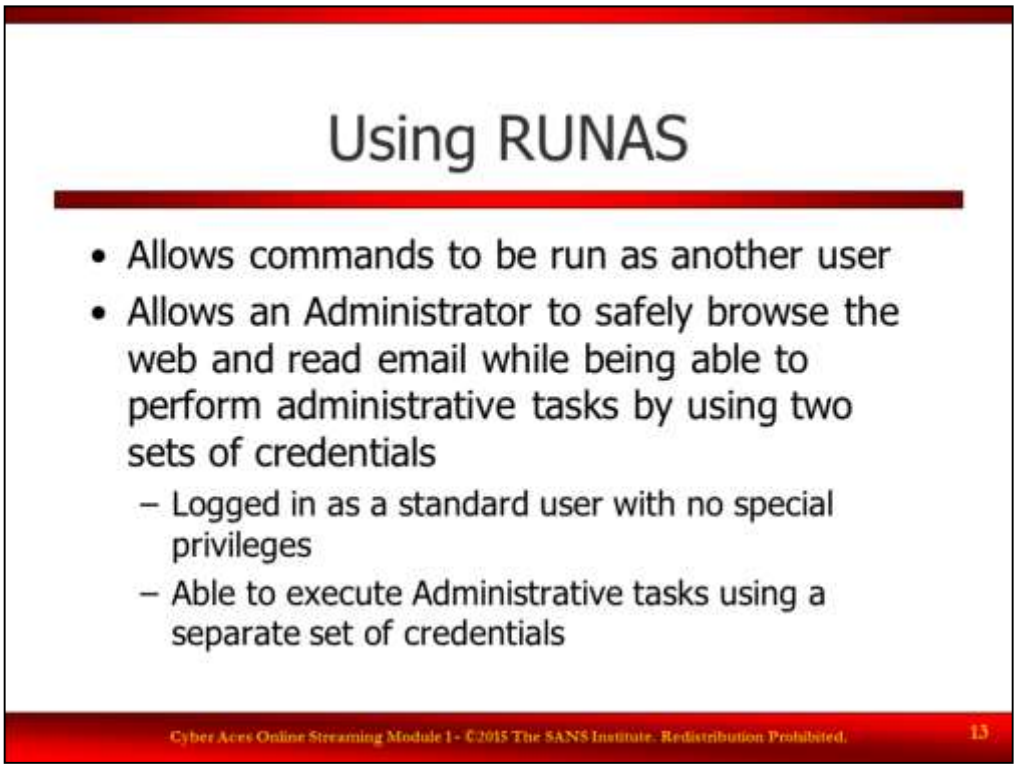
```
C:\> net localgroup administrators tim /del
```

Delete the Developers group

```
C:\> net localgroup developers /del
```

A similar syntax is used with the net group command to modify groups on the domain. Simply replace "localgroup" with "group" and add "/domain". For example, this will add Tim to the Domain Admins group (assuming the current user has the permissions to do so):

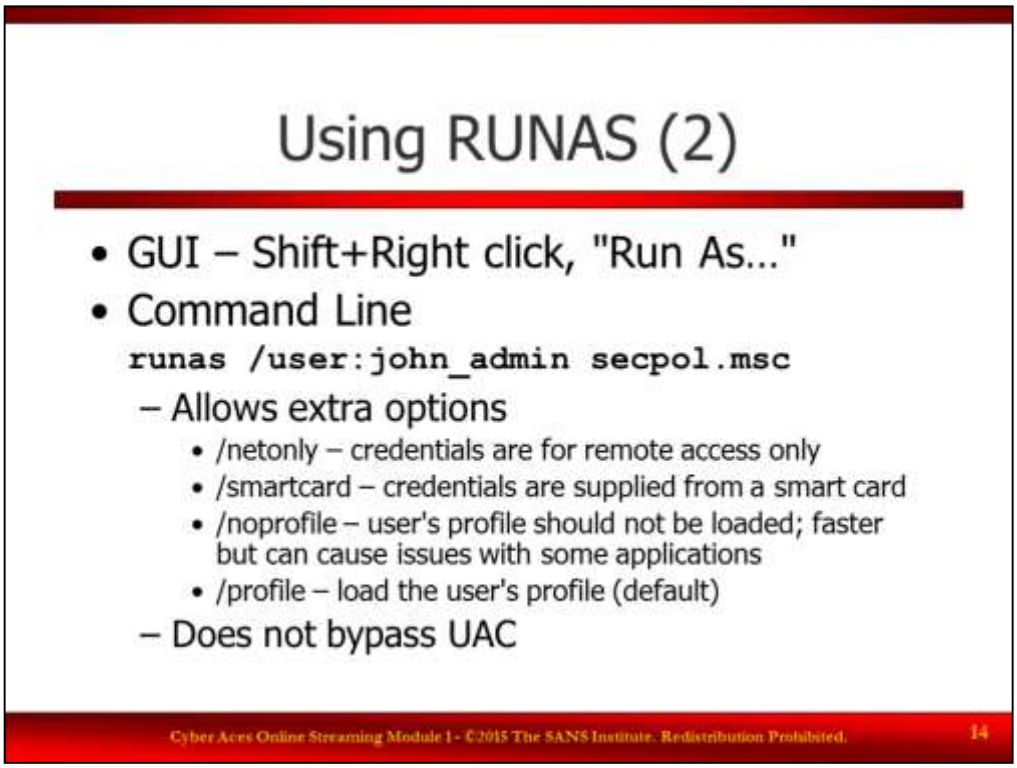
```
C:\> net group "domain admins" tim /add /domain
```



Using RUNAS

The Principle of Least Required Access is a longstanding principle that should be used to govern many of our decisions regarding user access. Windows Explorer and "RUNAS.EXE" from the command line both allow you to specify a different user account to use when executing a program. Browsing the web and reading email are the two most dangerous activities on today's computers. Using administrative permissions to do either of those things is a very dangerous game. Using RUNAS, Domain Administrators and other administrators can execute administrative tasks with one set of credentials and still be logged in as a normal user with no special privileges.

Reference: https://en.wikipedia.org/wiki/Principle_of_least_privilege



Using RUNAS (2)

The items in the control panel can be run via this method as well.

Start "Date and Time Properties":

```
C:\> runas /user:john_admin timedate.cpl
```

Start "Add or Remove Programs":

```
C:\> runas /user:john_admin appwiz.cpl
```

Start "System Properties":

```
C:\> runas /user:john_admin sysdm.cpl
```

If you need to run a number of higher privileged commands you can spawn a new administrative command prompt:

```
C:\> runas /user:john_admin cmd.exe
```

You can change the color of this command prompt to something that stands out by running this command in your prompt.

```
C:\> color fc
```

RUNAS Review

- Bob runs the command "runas /user:bob_admin cmd.exe". When prompted for the password, bob enters "bob<3alice" and a Command Prompt is successfully launched. Which of the following statements must be true?
  - Bob_admin must be a valid account on the local system
  - Bob_admin must love Alice
  - Bob uses the same password as Bob_admin
  - Bob is a member of the Administrators group
- Which of the following will launch Windows Explorer as the user "bob"?
  - runas /u:bob /run:explorer.exe
  - runas /user:bob explorer.exe
  - runas-bob-cmd=explorer
  - runas /user:bob /run:explorer.exe

Answers

- Bob runs the command "runas /user:bob_admin cmd.exe". When prompted for the password bob enters "bob<3alice" and a Command Prompt is successfully launched. Which of the following statements must be true?
  - **Bob_admin must be a valid account on the local system**
  - This is a very common method of using two accounts for safety. The regular "bob" account is used for everyday tasks (email, web browsing, etc) and the bob_admin account is used for administrative functions.

- Which of the following will launch Windows Explorer as the user "bob"?
  - **runas /user:bob explorer.exe**
  - This method will allow the user to view and modify files to which Bob has access

User Account Control (UAC)

Unfortunately, due to politics, not understanding the seriousness of the threat, or perhaps laziness on the part of system administrators, users often end up in the Administrators group. This is a very bad situation to be in. To address this threat, Windows Vista introduced a new technology called User Account Control (UAC). When UAC is enabled, permissions are stripped from the Administrators of the machine when their access tokens are created. When a process requires administrative access, it will prompt the user for credentials before granting the request. Read more about UAC at http://www.windowsecurity.com/articles/Understanding-User-Account-Control-Vista.html. Microsoft also provides an in-depth step-by-step article concerning UAC at https://technet.microsoft.com/en-us/library/cc709691(WS.10).aspx.

Exercise

- Use what you have just learned to perform the following tasks using only the command line (you can verify via the GUI if you like)
  - List all the accounts in the Administrators Group
  - Create a new user "Alice"
  - Add Alice to the Administrators group
  - Start a command prompt as Alice using RunAs
  - Try to create a user from Alice's shell
  - Add the user "Bob"
  - Create the group "Developers"
  - Add Bob and Alice to the group Developers
  - List the members of the group Developers
  - Delete the Developers group, Bob, and Alice

Cyber Aces Online Streaming Module 1 - ©2015 The SANS Institute. Redistribution Prohibited.

STOP!

- On the next few pages are the answers
- Feel free to look ahead if you need help completing the task

Answers

- List all the accounts in the Administrator's Group
  ```
  net localgroup administrators
  ```
- Create a new user "Alice"
  ```
  net user alice SomePassword /add
  ```
- Add Alice to the Administrators group
  ```
  net localgroup administrators alice /add
  ```
- Add the user "Bob"
  ```
  net user bob AnotherPassword /add
  ```
- Start a command prompt as Alice using RunAs
  ```
  runas /user:alice cmd.exe
  ```
- Try to create a user from Alice's shell
  - This will fail

Answers

- Create the group "Developers"

```
net localgroup Developers /add
```

- Add Bob and Alice to the group Developers

```
net localgroup developers alice /add
net localgroup developers bob /add
```

- List the members of the group Developers

```
net localgroup developers
```

- Delete the Developers group, Bob, and Alice

```
net user bob /del
net user alice /del
net localgroup developers /del
```

Exercise Complete!

- Congratulations!
- You have completed the tutorial on user management