Using Active Directory in the Enterprise

OBJECTIVE:

CompTIA Security+ Domain:
Domain 5: Access Control and Identity Management

CompTIA Security+ Objective Mapping:
Objective 5.1: Compare and contrast the function and purpose of authentication services.
Objective 5.2: Given a scenario, select the appropriate authentication, authorization, or access control.
Objective 5.3: Install and configure security control when performing account management based on best practices.

OVERVIEW:

Active Directory is a database, which can be used to centrally manage a Microsoft Windows network. In this lab, you will examine the Active Directory Users and Computers interface.

Key Term	Description
organizational unit	An Active Directory container that can hold users, groups, and computers.
dsa.msc	the command to open Active Directory Users and Computers
Active Directory Users and Computers	database which can be used to centrally manage a Windows network
Net user	A Built in Windows command to manage and create users
gpupdate	the command to update group policy

Reading Assignment

Introduction

Active Directory is a database, which can be used to centrally manage a Microsoft Windows network, users, groups, computers, printers, and other objects and resources. In this lab, you will examine the Active Directory objects and group policies at the domain and organizational unit level. Windows System Administrators commonly use Active Directory in their daily work. Figure 1 is the lab topology for this lab which represents a single Windows Server with Active Directory Domain services.

FIGURE 1 – LAB TOPOLOGY

Introduction to Active Directory (AD)

Active Directory (AD) is a database and directory service of an organization's objects and users on a network. AD is a directory service that uses the Lightweight Directory Access Protocol (LDAP). LDAP is an open and cross platform directory services protocol that is used by most directory services. Figure 2 shows the hierarchical nature of Active Directory.

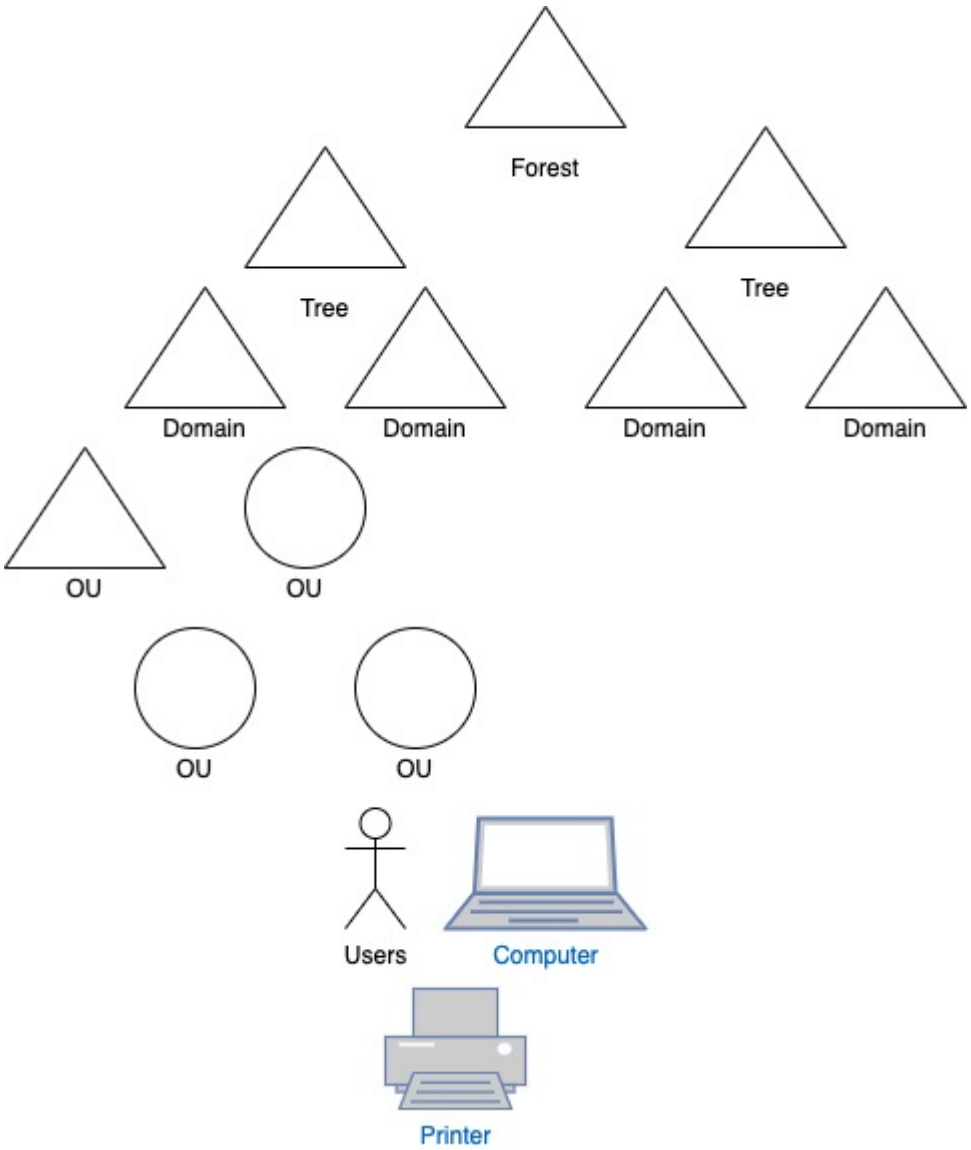


FIGURE 2 – HIERARCHICAL VIEW OF ACTIVE DIRECTORY

Active Directory manages an organization's objects which can be servers, clients, computers, hardware, shared files and folders, and users. An AD object can be a container object such as a folder or a leaf such as a file. An AD domain is organized around a collection of objects. A domain can share policy and use an Active Directory database. A tree is organized around multiple AD domains. Domains in a tree share network configuration. A forest is organized around a group of trees that have the same database. Trees in a forest have different namespace; for example, xbox.com and office.com (both owned by a single organization Microsoft). Figure 3 shows what Active Directory looks like on a Windows server.

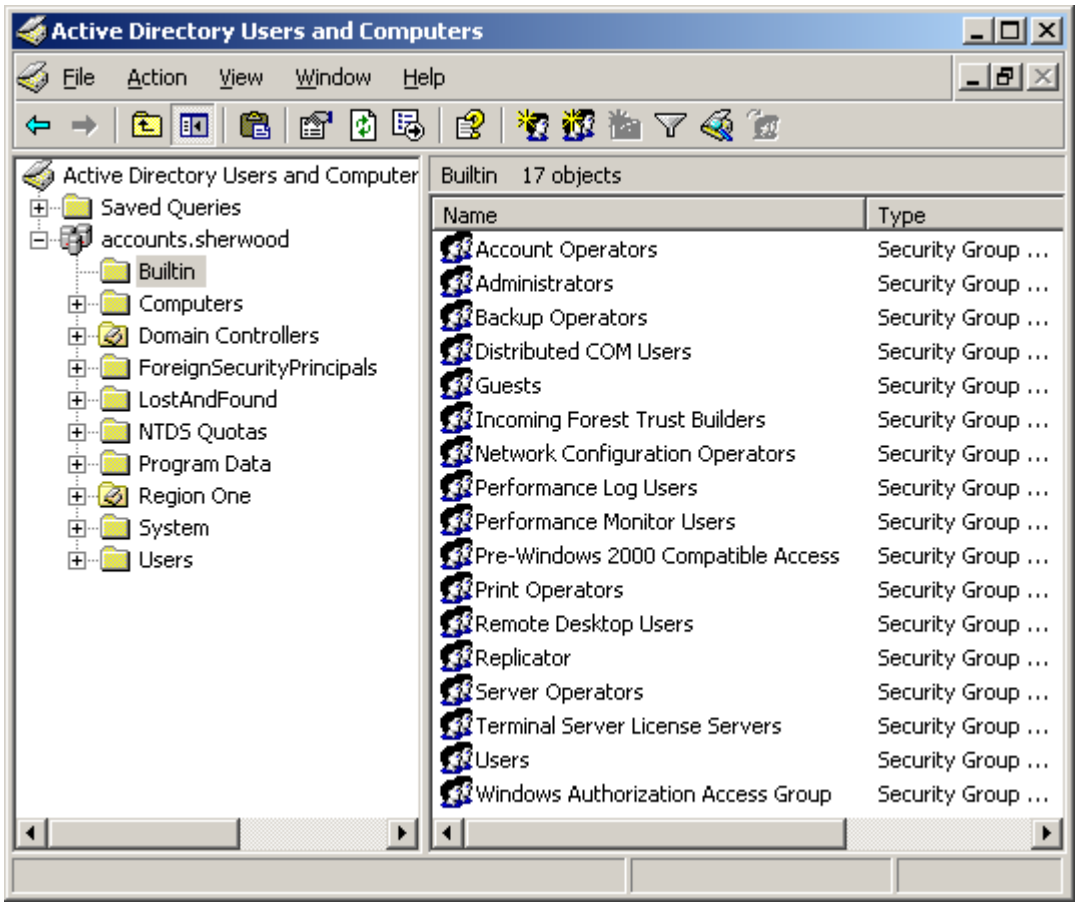


FIGURE 3 – ACTIVE DIRECTORY

Organizational Units (OUs)

Organizational Units (OUs) are AD containers that allow you to place users, printers, groups, computers, and other objects. OUs can be nested inside of each other. You can use OUs to represent an organization's organizational chart. A good reason to use OUs is to be able to assign a group policy to the OU and all users and computers that are members of that OU will get that policy. In this lab, you will create OUs and users in the OU.

Group Policies in Active Directory

Group policies can be set at the site, domain, and organizational level of Active Directory as well as on a local machine. Group policies are applied at the site first, domain second, at the OU level third, and then finally at the local machine. If you set a group policy at the Domain level, everything below the domain will get the Group policy first. Best practice is to not set domain level group policies but set organizational unit level group policies is the better option. Microsoft has setup a hierarchy in active directory when applying group policies. They are applied in this order:

- Local policies
  - Configured on the actual computer itself

- Site policies
    - Configured in Active Directory. You can configure a site which is a representation of a physical location
- Domain policies
    - Configured in Active Directory and applies to all objects in the domain assigned
- OU policies
    - Configured in Active Directory and applies to all objects in the OU

The beauty of group policies is the ability to have greater control over the security of your network as a system administrator.

Here are some ways you can configure group policies in Active Directory:

- Password Policies can be set to establish password length, complexity, and other requirements.
- Systems Management can apply standardized, universal settings across all new users with just a few clicks.
- Health Checking can be used to deploy software updates/patches to ensure your systems are up to date against the latest vulnerabilities.

In this lab, you will set a domain level and organizational unit (OU) group policies.

CONCLUSION:

In this lab, you will learn how to use some basic system administrator's tasks such as creating Active Directory objects, organizational units, and assigning group policies to the domain and organizational unit (OU) level. Active Directory is such a powerful tool to make a system administrator's job easier to manage an organization's resources.

Creating an Organization Unit and Users in Active Directory

1. **Click** on the Windows Server icon in the network topology. After the machine finishes booting, **click** the CTRL-ALT-DELETE button in the upper-right corner.

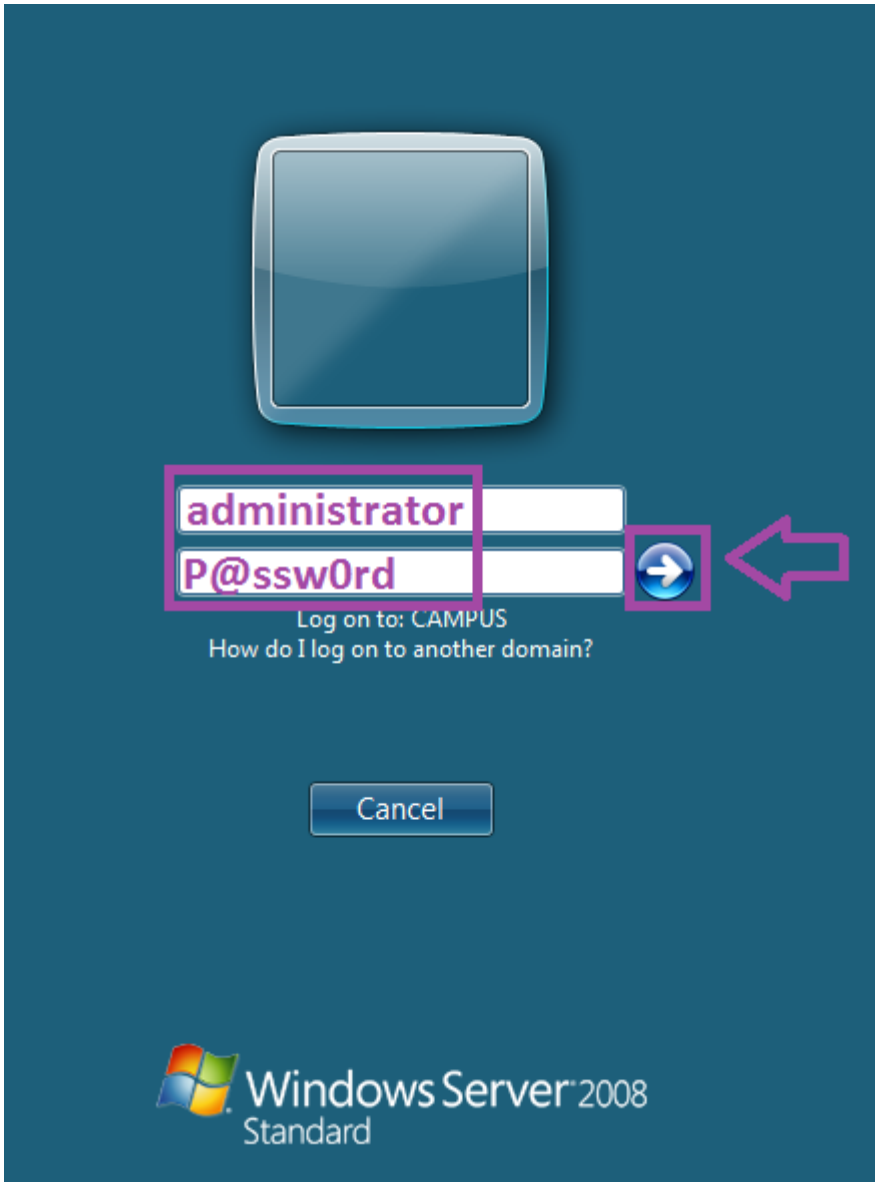
Time remaining: 86:59 STOP

WINDOWS SERVER MACHINE

SERVER IS READY

Note: If the screen remains blank after allowing a minute for sufficient boot-up time, click on the screen.

2. **Log on** as `administrator` with the password of `P@ssw0rd`, then **click** the arrow.



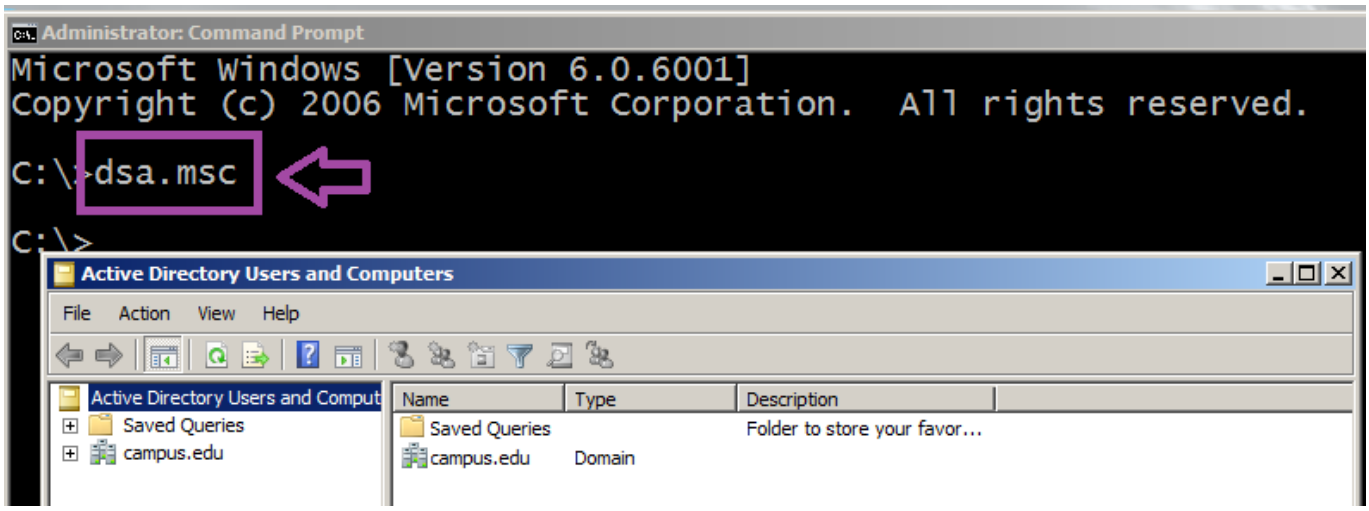
LOG ON TO WINDOWS SERVER

3. **Double-click** on the Command Prompt shortcut on the Windows Server 2008 desktop.

SHORTCUT TO COMMAND PROMPT

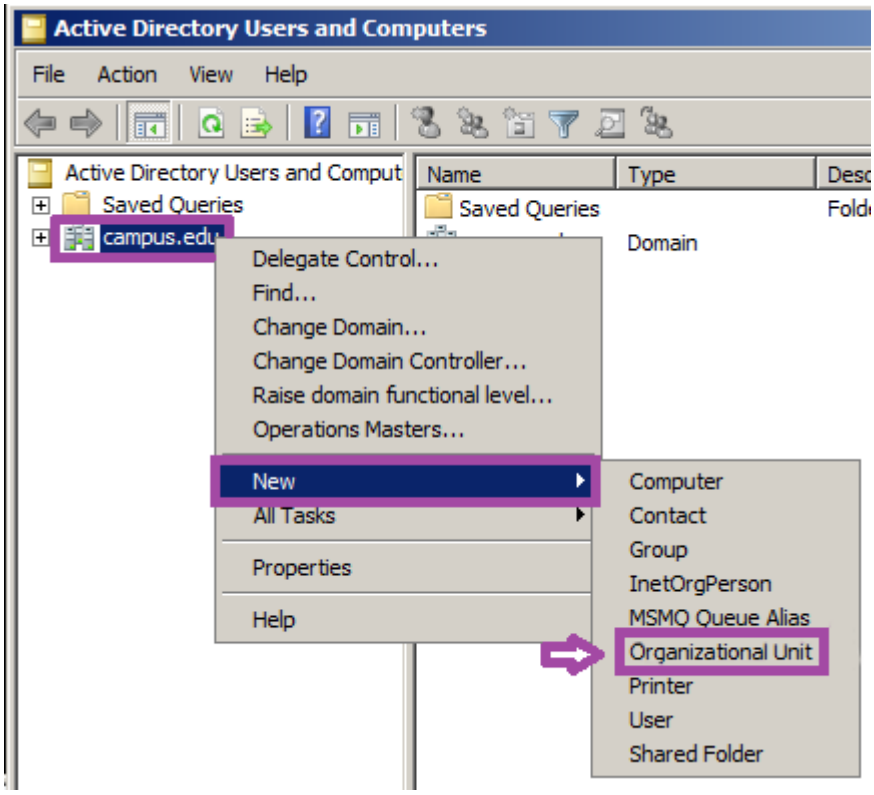
4. **Type** the following command to open the Active Directory Users and Computers interface, then **press** Enter.

C:\>`dsa.msc`



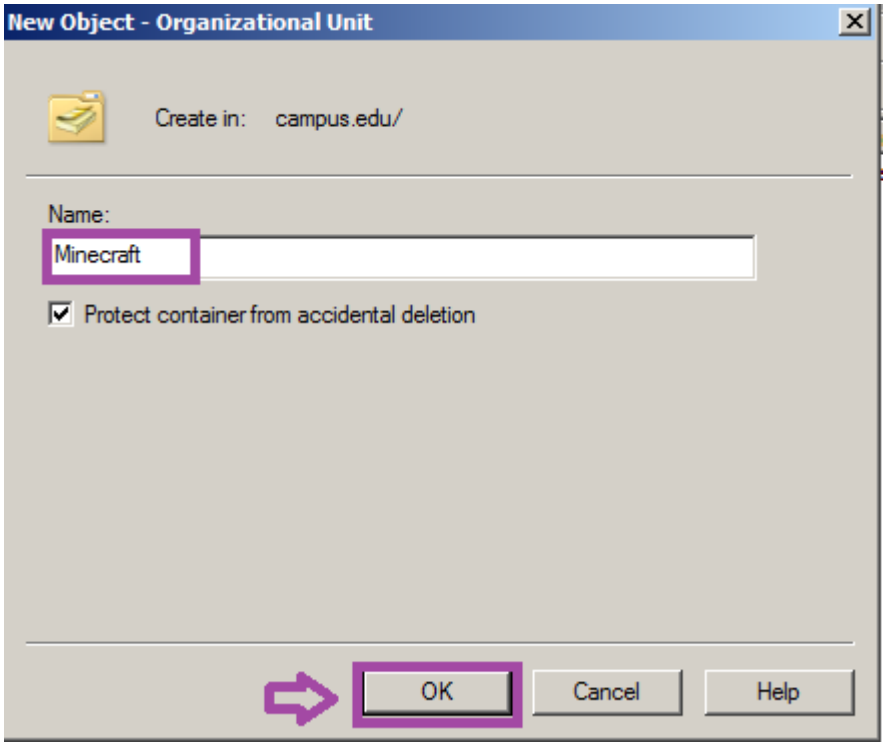
ACTIVE DIRECTORY USERS AND COMPUTERS

5. **Right-click** on the campus.edu domain and **select** New, then **select** Organizational Unit.



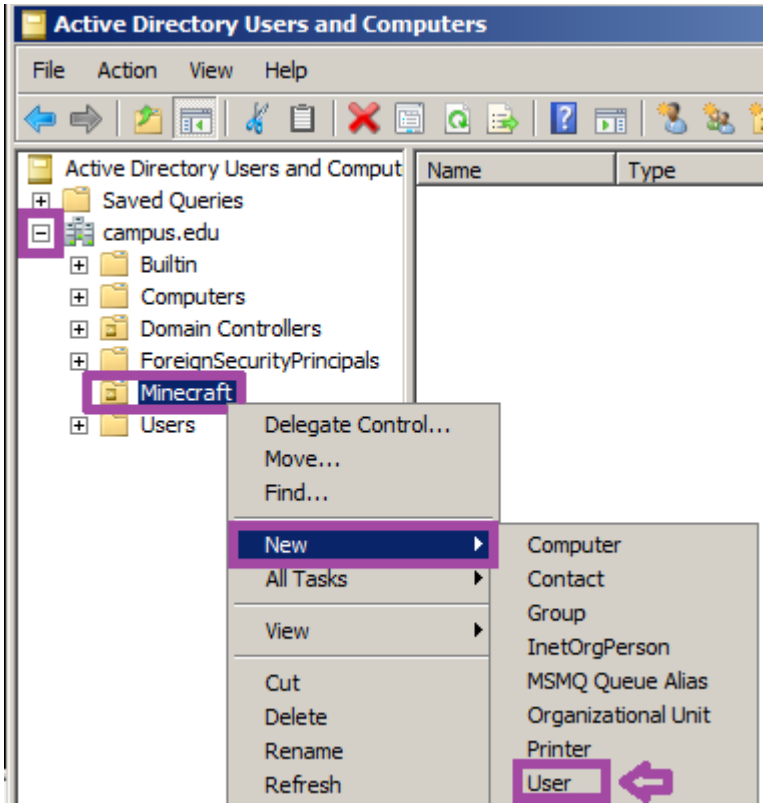
NEW ORGANIZATIONAL UNIT

6. **Type** `Minecraft` for the Name of the organizational unit and **click** OK.



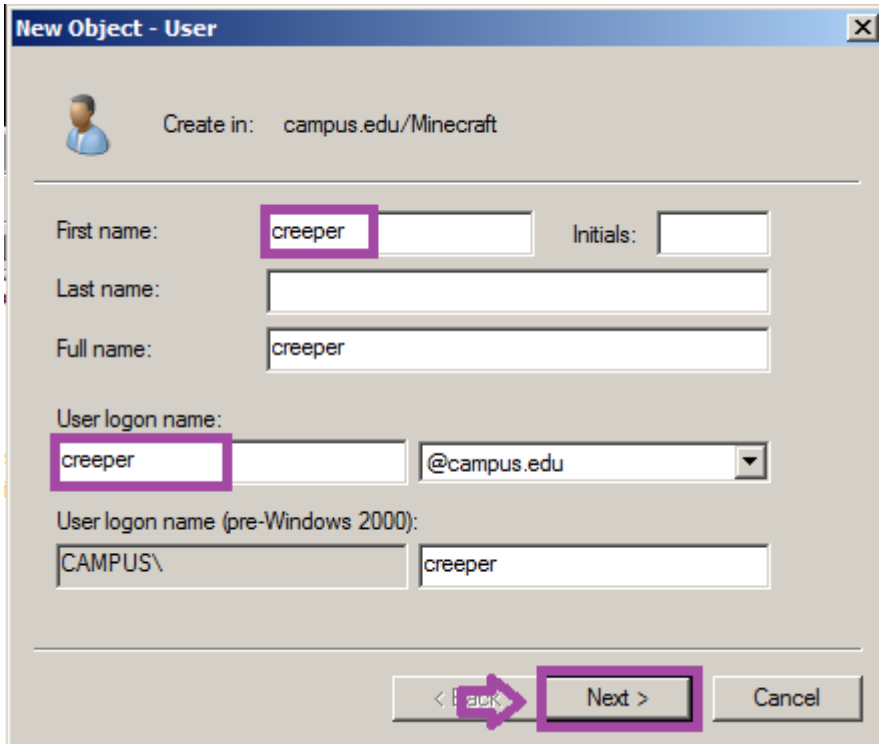
CREATING AN OU

7. **Expand** the campus.edu domain by clicking the + sign beside the icon. **Right-click** on the Minecraft organizational unit and **select** New and then **select** User (bottom option).



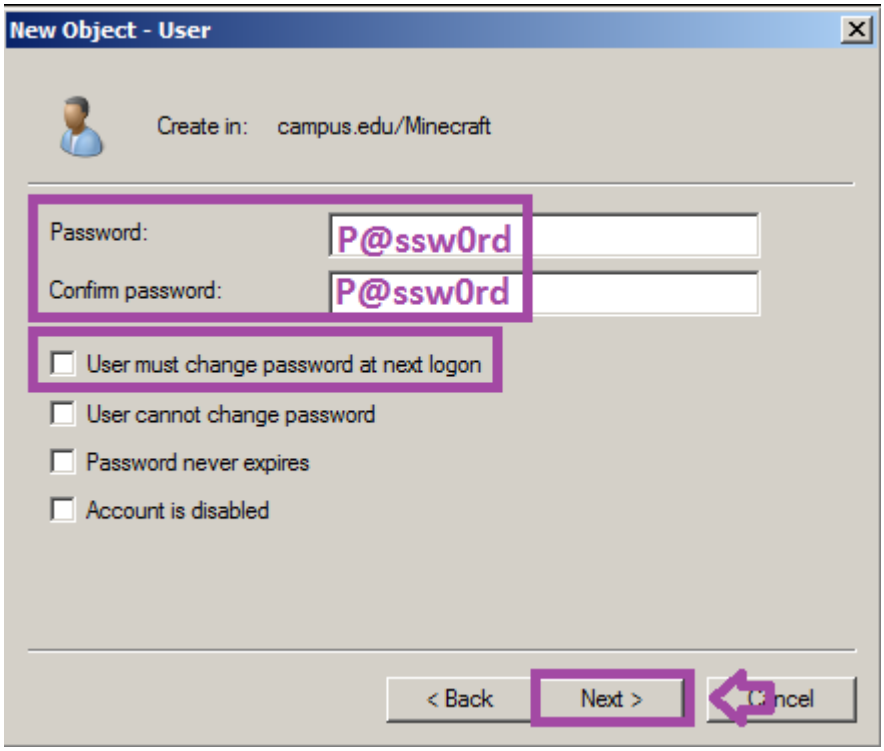
CREATING A NEW USER

8. For the First name, **type** `creeper`, and for the User logon name, **type** `creeper`. **Click** Next.



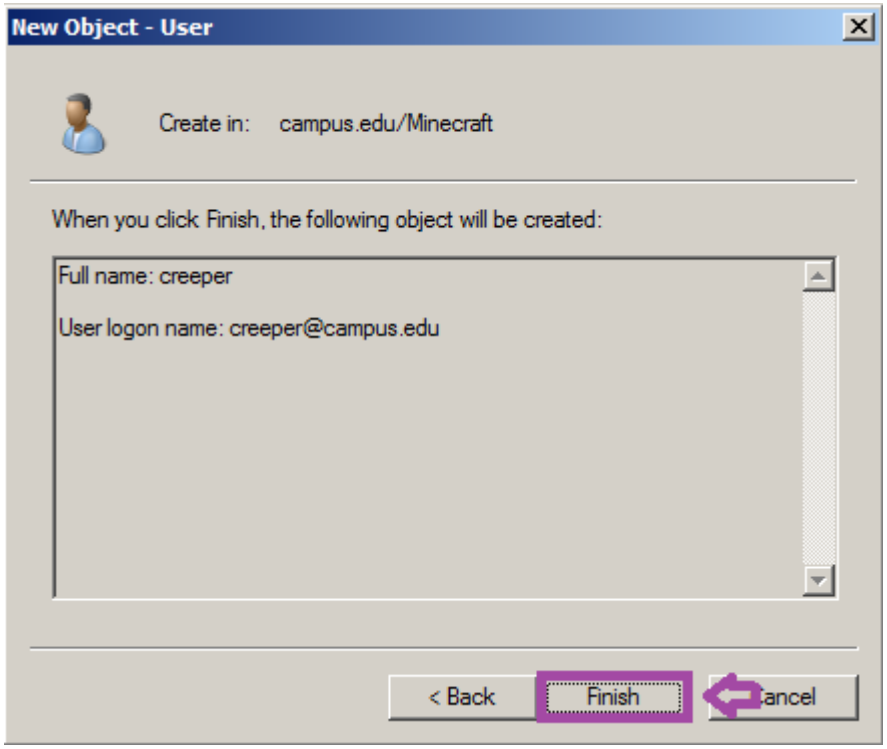
CREATING A NEW USER

9. **Uncheck** the box that states "User must change password at next logon." For the Password, **type** `P@ssw0rd` and **type** `P@ssw0rd` for the Confirm password. **Click** Next.



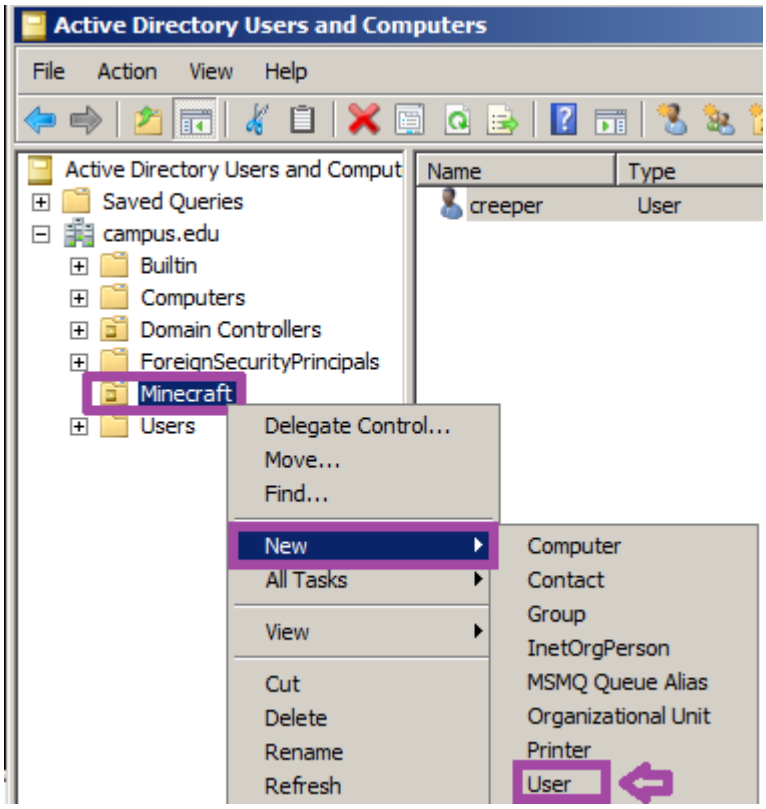
USER'S PASSWORD

10. **Click** the Finish button to create the user creeper in the Minecraft organizational unit.



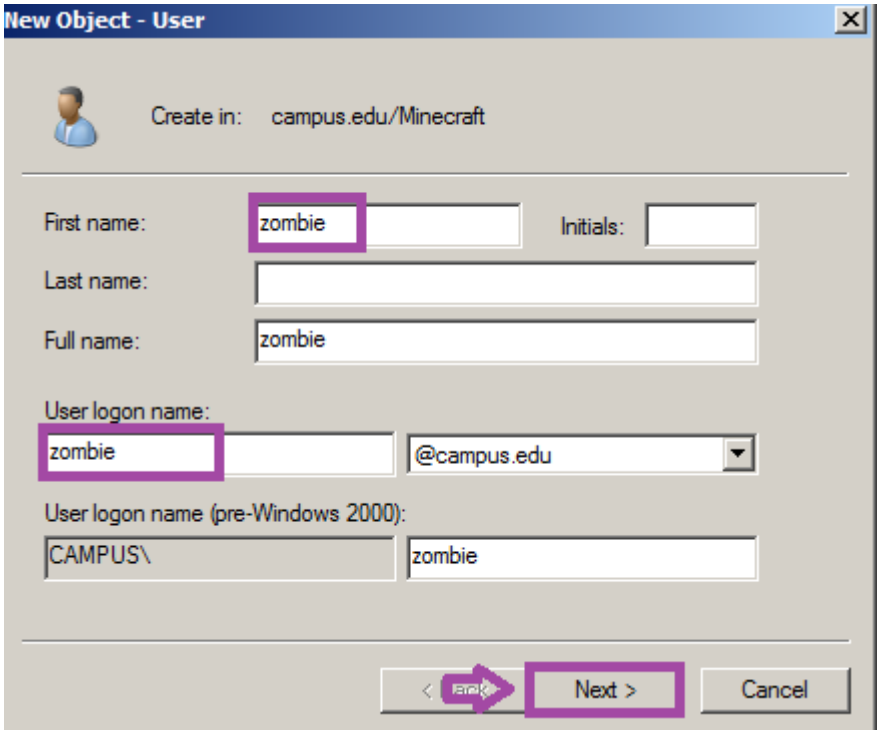
CLICK FINISH

11. **Right-click** on the Minecraft organizational unit and **select** New and then **select** User.



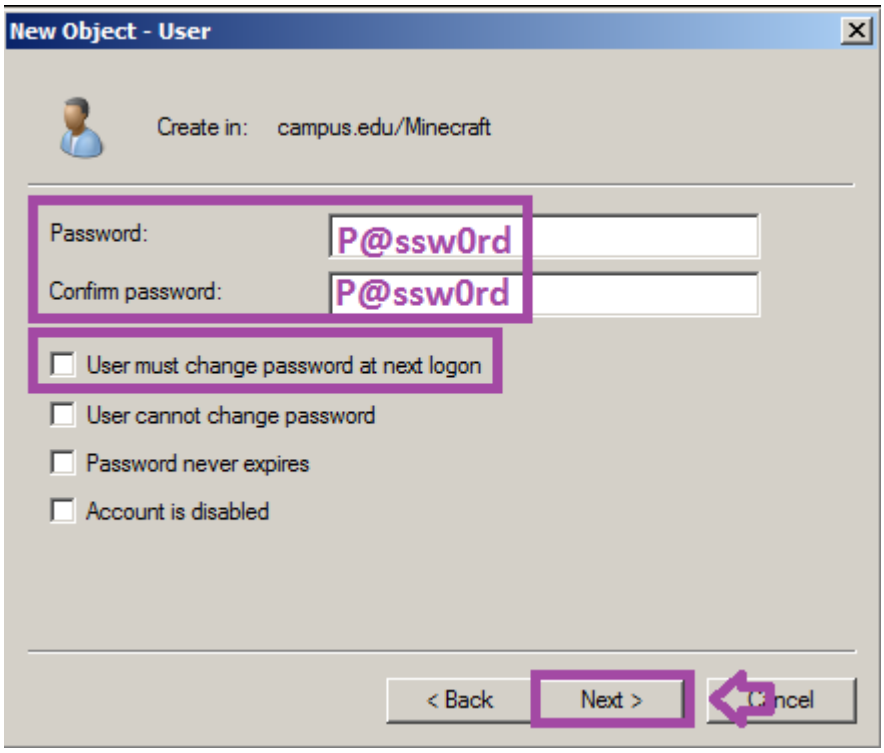
CREATING A NEW USER

12. For the First name, **type** `zombie`, and for the User logon name, **type** `zombie`. **Click** Next.



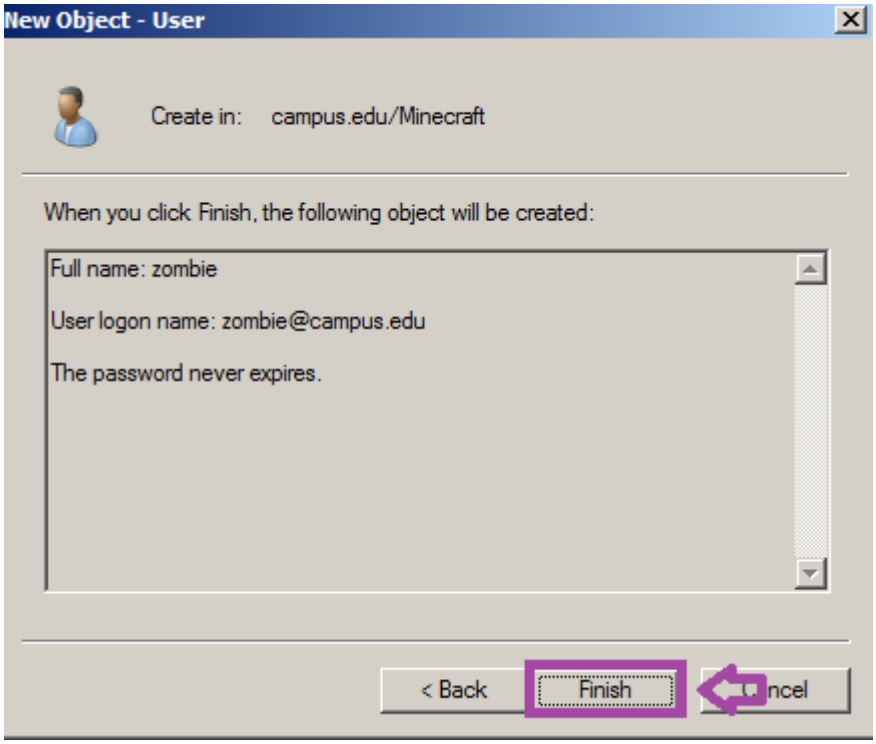
CREATING A NEW USER

13. **Uncheck** the box that states "User must change password at next logon." For the Password, **type** `P@ssw0rd` and **type** `P@ssw0rd` for the Confirm password. **Click** Next.



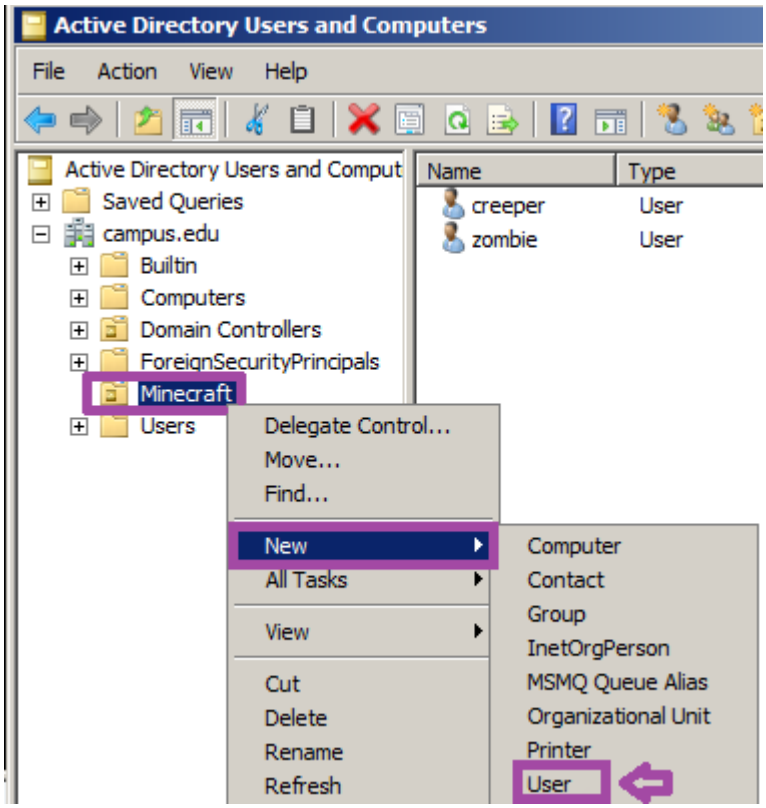
USER'S PASSWORD

14. **Click** the Finish button to create the user zombie in the Minecraft organizational unit.



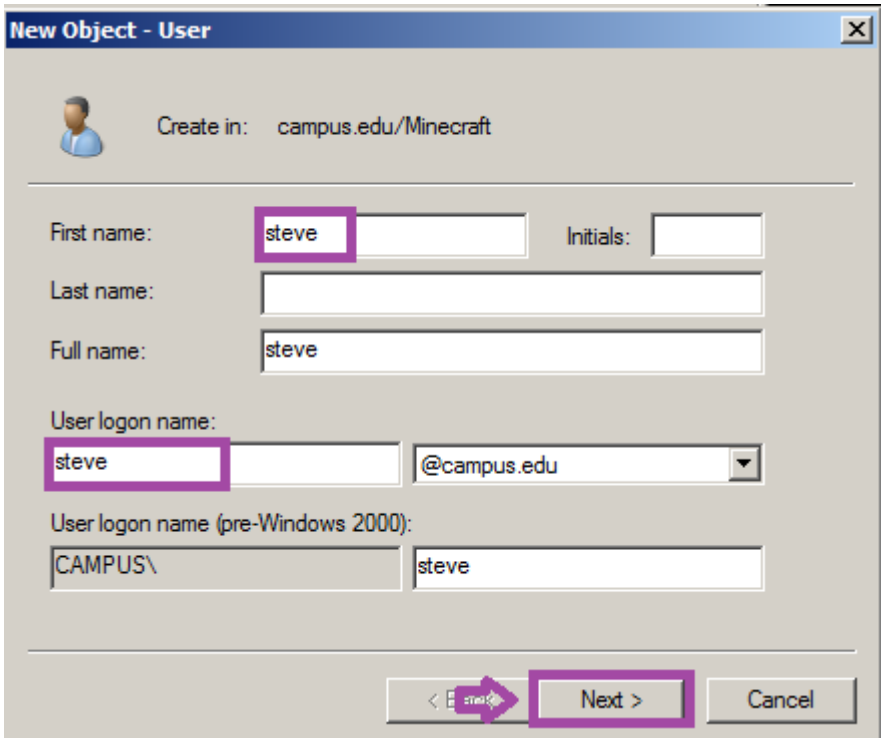
CLICK FINISH

15. **Right-click** on the Minecraft organizational unit and **select** New and then **select** User.



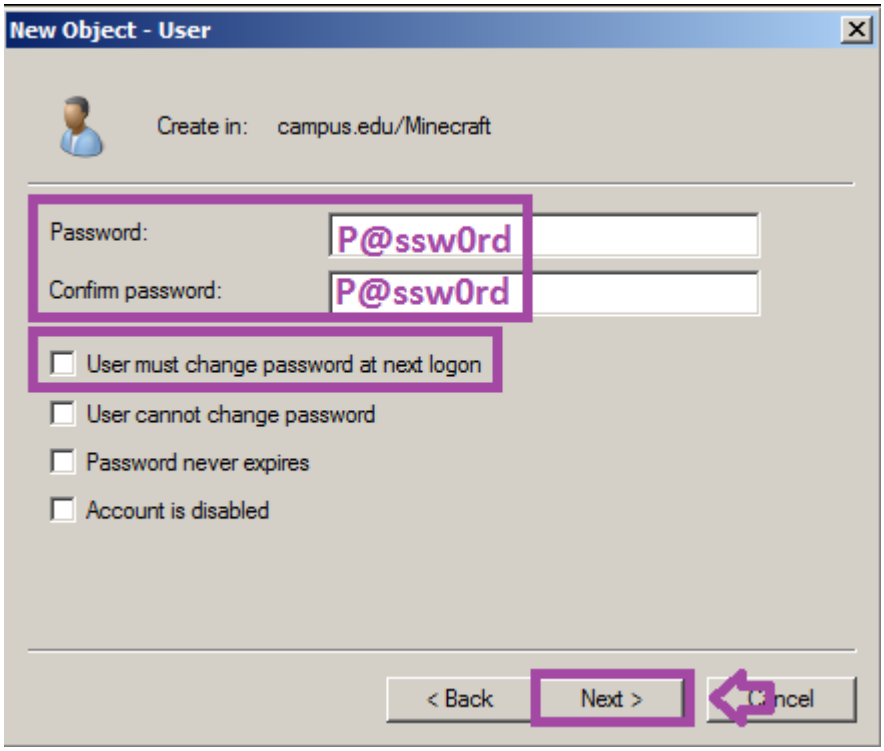
CREATING A NEW USER

16. For the First name, **type** steve, and for the User logon name, **type** steve. **Click** Next.



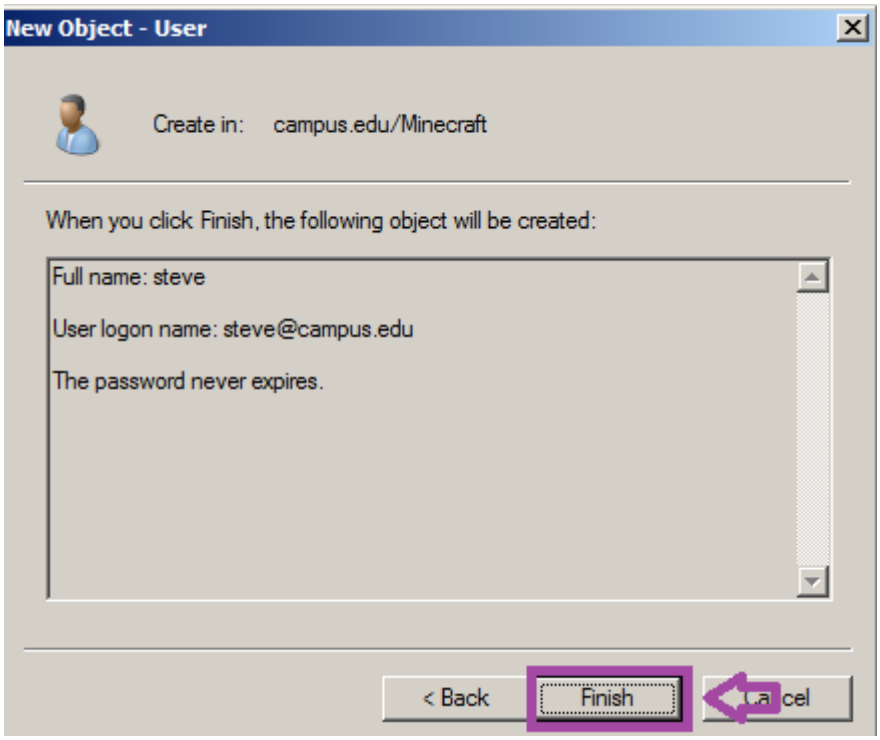
CREATING A NEW USER

17. **Uncheck** the box that states "User must change password at next logon." For the Password, **type** `P@ssw0rd` and **type** `P@ssw0rd` for the Confirm password. **Click** Next.



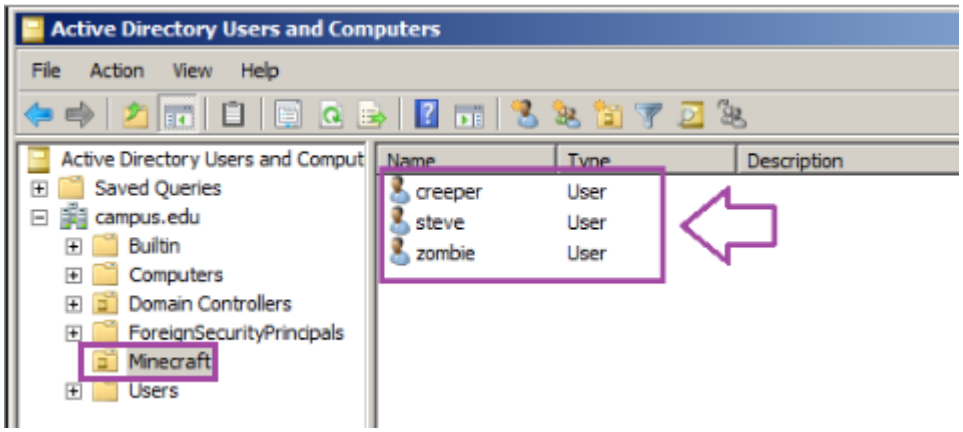
USER'S PASSWORD

18. **Click** the Finish button to create the user steve in the Minecraft organizational unit.



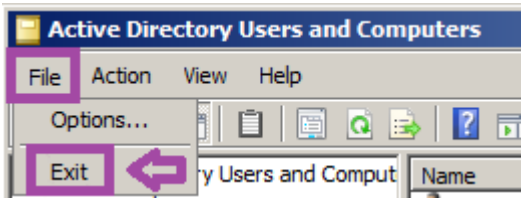
CLICK FINISH

19. **Click** the Minecraft directory, and all three of the users you created in the Minecraft organizational unit will be displayed.



ALL USERS ARE DISPLAYED

20. **Select** File from the Active Directory Users and Computers menu and **select** Exit.



EXIT ACTIVE DIRECTORY

Setting a Domain Level Policy in Active Directory

1. **Type** the following command and **press** Enter to add the user terrance with the password of `P@ssw0rd`,

C:\>`net user terrance P@ssw0rd /add`

```
C:\>net user terrance P@ssw0rd /add
The command completed successfully.
```

THE NET USER COMMAND

2. **Type** the following command and **press** Enter to get information about the user terrance you just created.

C:\>`net user terrance`

```
C:\>net user terrance
User name                    terrance
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            6/3/2016 11:45:07 PM
Password expires             7/15/2016 11:45:07 PM
Password changeable          6/4/2016 11:45:07 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.
```

THE NET USER COMMAND

3. There is another account on the system called superman. **View** the information about the superman account by typing the following command:

C:\>`net user superman`

```
C:\>net user superman
User name                    superman
Full Name
Comment                      flag:999818
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/25/2018 9:48:13 PM
Password expires             Never
Password changeable          2/26/2018 9:48:13 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.
```

SUPERMAN ACCOUNT INFORMATION

4. **Notice** the flag of 999818. **Click** on the Challenge icon and **type** the flag number into the answer box. This is just to show you how to **capture** Challenge Flags you will see throughout this lab.

Challenge Sample #

3. **Get** the information for below Challenge Flag by using the same techniques from the previous steps.

Challenge #

3. **Get** the information for below Challenge Flag by using the same techniques from the previous steps.

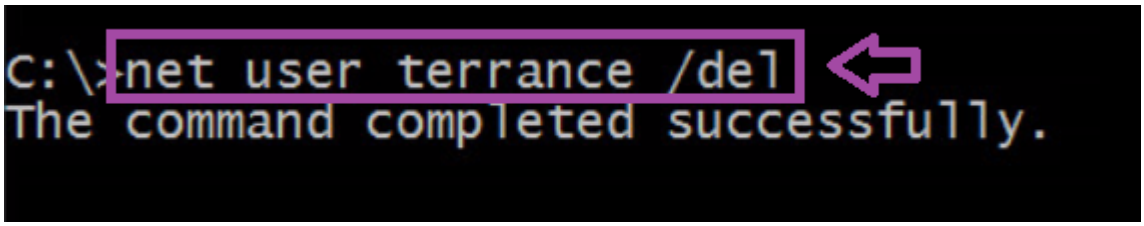
Challenge #

3. **Get** the information for below Challenge Flag by using the same techniques from the previous steps.

Challenge #

3. **Type** the following command and **press** Enter to delete the user terrance.

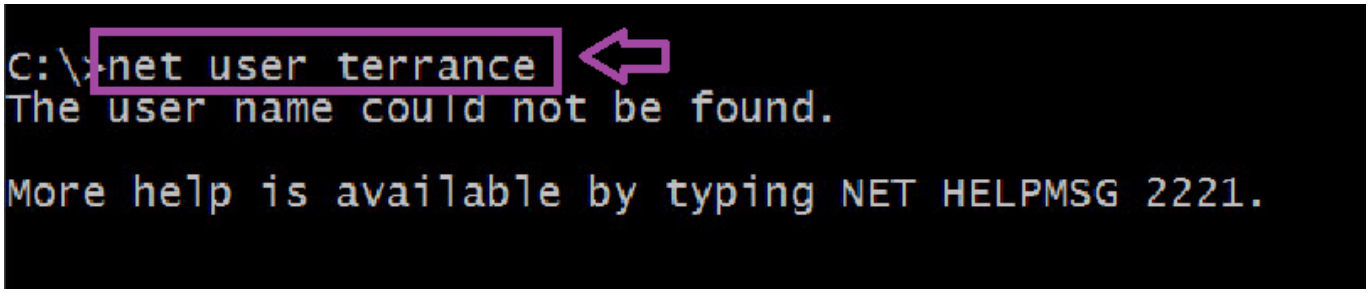
C:\>`net user terrance /del`



THE NET USER COMMAND

4. **Type** the following command and **press** Enter to verify that the user terrance has been deleted.

C:\>`net user terrance`



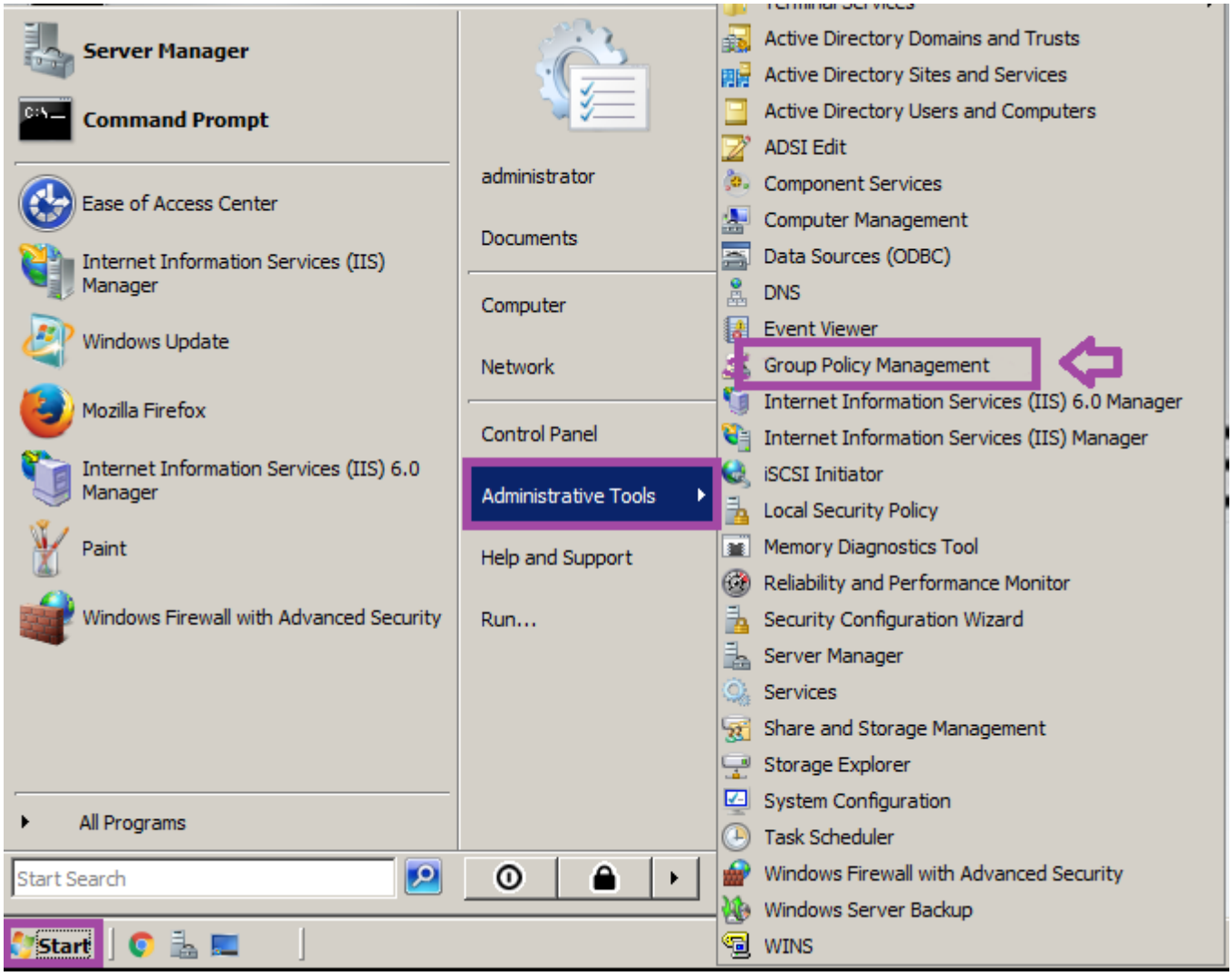
THE NET USER COMMAND

5. **Type** the following command and **press** Enter to exit the command prompt, then **press** Enter.

C:\>`exit`

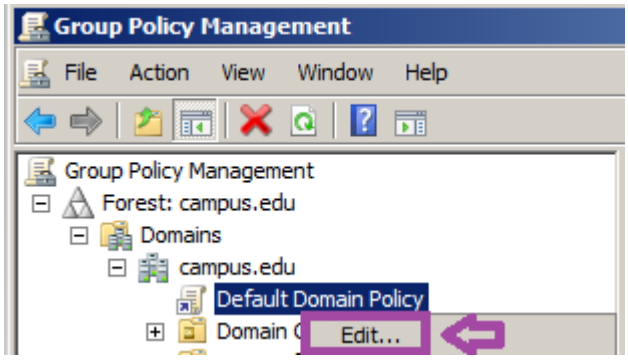
THE EXIT COMMAND

6. **Click** on Start, **select** Administrative Tools and then **select** Group Policy Management.



GROUP POLICY MANAGEMENT

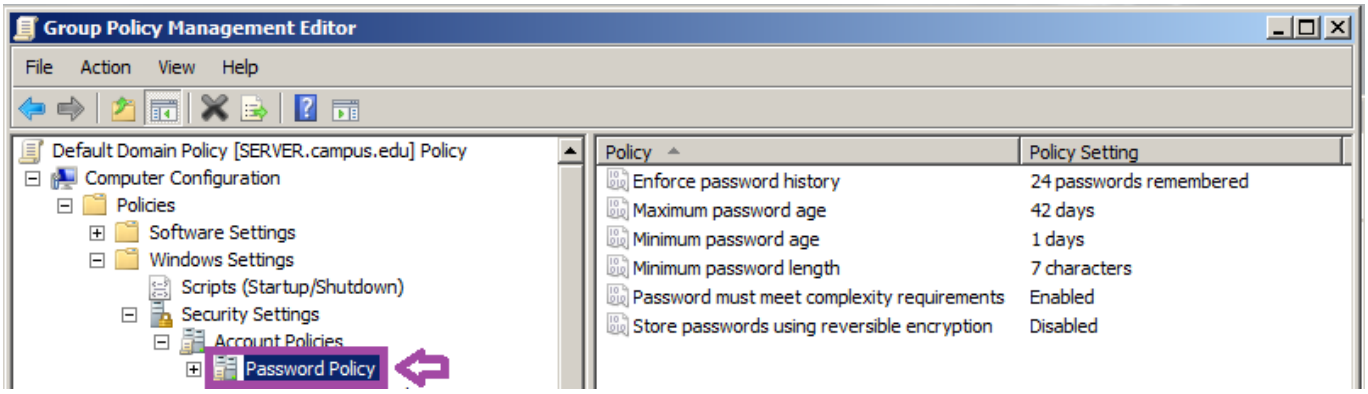
7. **Click** the + button to expand Forest: campus.edu. **Click** the + button to expand Domains and then **click** the + button to expand campus.edu. **Right-click** Default Domain Policy and **select** Edit.



EDIT THE DEFAULT DOMAIN POLICY

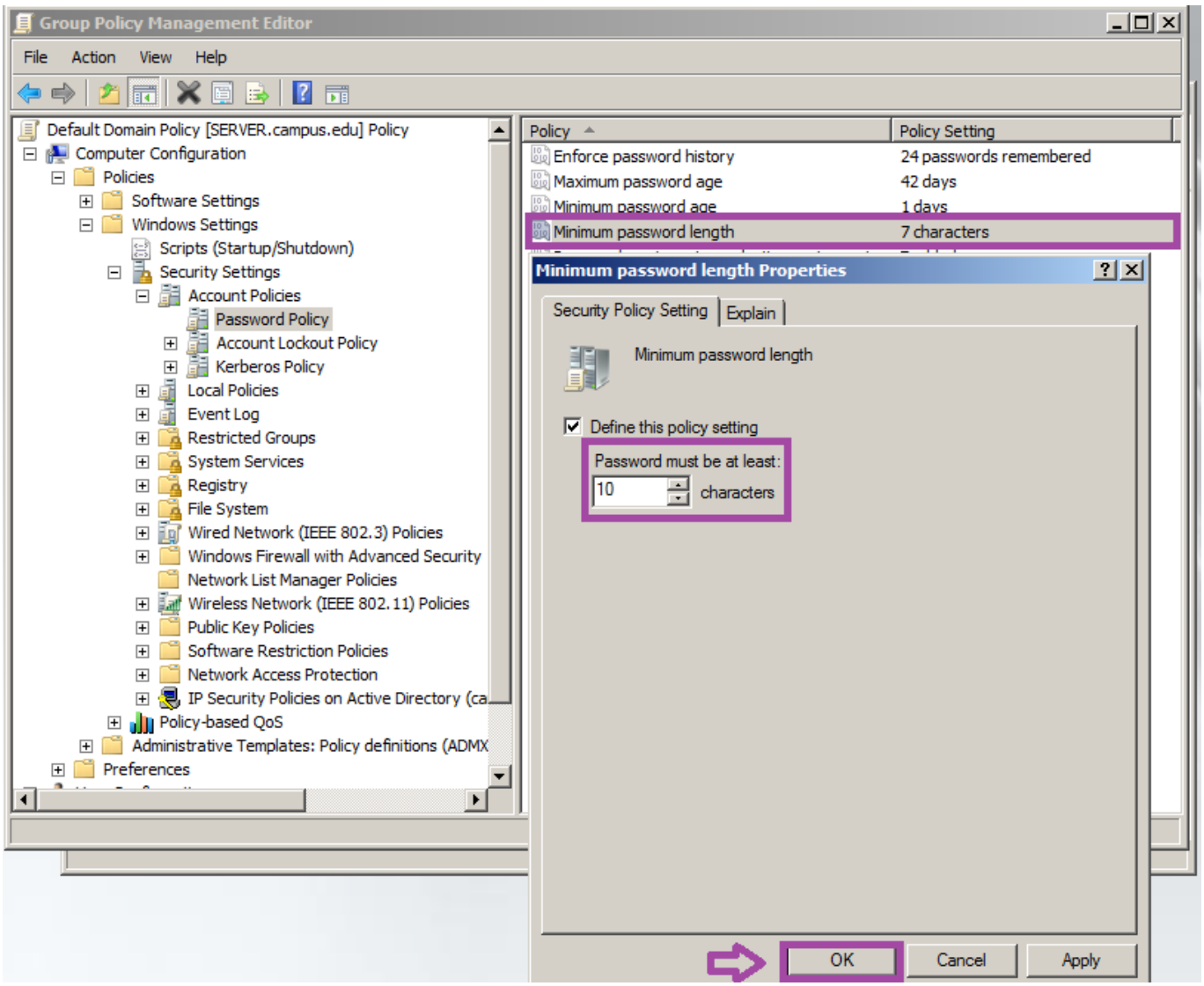
8. **Click** the + button to expand Computer Configuration.

Click the + button to expand Policies.
Click the + button to expand Windows Settings.
Click the + button to expand Security Settings.
Click the + button to expand Account Policies.
Click on Password Policy.



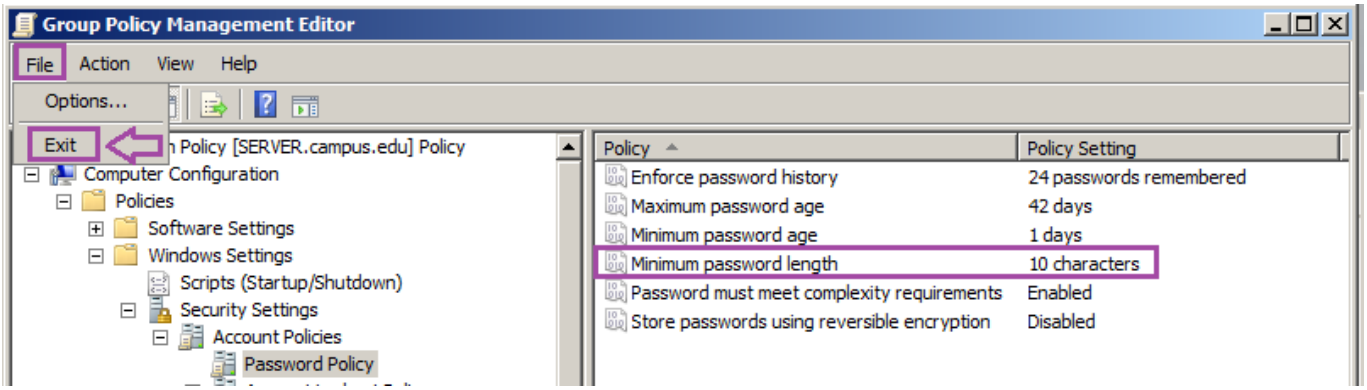
GROUP POLICY MANAGEMENT

9. **Double-click** Minimum password length. **Change** the default value of the policy setting Password must be at least: from 7 characters to 10 characters. **Click** OK to apply this setting to the campus.edu domain.



MINIMUM PASSWORD LENGTH POLICY

10. **Verify** that the minimum password length is now 10 characters. **Select** File and **choose** Exit.



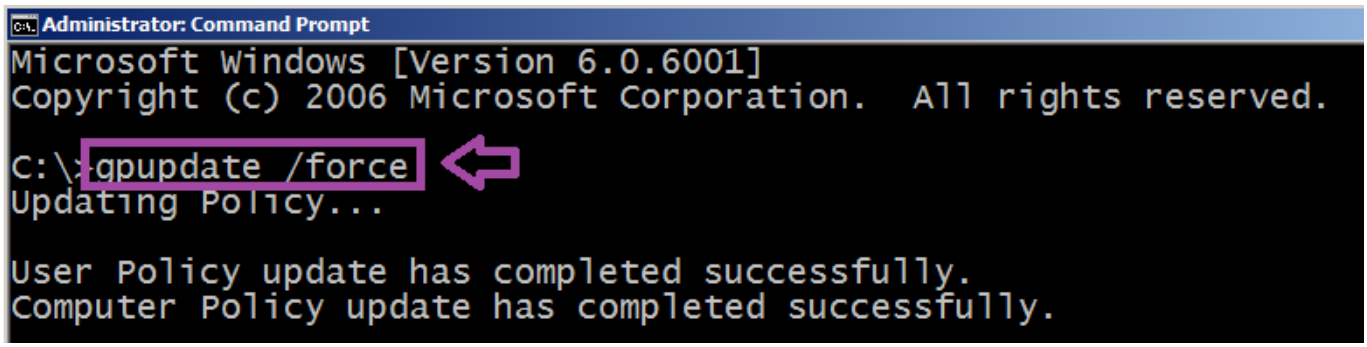
EXITING THE GROUP POLICY MANAGEMENT CONSOLE

11. **Double-click** on the Command Prompt shortcut on the Windows Server 2008 desktop.

SHORTCUT TO COMMAND PROMPT

12. **Type** the following command and **press** Enter to refresh the Group Policy Settings on the machine.

C:\>`gpupdate /force`



THE GPUPDATE COMMAND

13. **Type** the following command and **press** Enter to attempt to add the user peaches with the password of `P@ssw0rd`.

C:\>`net user peaches P@ssw0rd /add`

```
C:\>net user peaches P@ssw0rd /add
The password does not meet the password policy requirements. Check the minimum p
assword length, password complexity and password history requirements.

More help is available by typing NET HELPMSG 2245.
```

THE NET USER COMMAND

Note: This command failed because of the new minimum password length policy of 10 characters.

14. **Type** the following command and **press** Enter to add the user peaches with the password of `P@ssw0rd12`.

C:\>`net user peaches P@ssw0rd12 /add`

```
C:\>net user peaches P@ssw0rd12 /add
The command completed successfully.
```

THE NET USER COMMAND

15. **Type** the following command and **press** Enter to delete the user peaches.

C:\>`net user peaches /del`

```
C:\>net user peaches /del
The command completed successfully.
```

THE NET USER COMMAND

16. **Type** the following command and **press** Enter to attempt to change the password of the creeper account to `P@ssw0rd1`.

C:\>`net user creeper P@ssw0rd1`

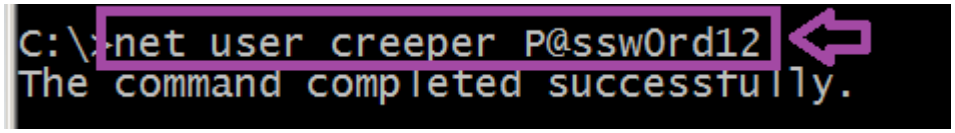
```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\>net user creeper P@ssw0rd1
The password does not meet the password policy requirements. Check the
mum password length, password complexity and password history requirem


More help is available by typing NET HELPMSG 2245.
```

THE NET USER COMMAND

NOTE: The command failed because of the new minimum password length policy of 10 characters.

17. **Type** the following command and **press** Enter to change the password of the creeper account to `P@ssw0rd12`.

C:\>`net user creeper P@ssw0rd12`



THE NET USER COMMAND

NOTE: The command was a success because of meeting the new minimum password length policy of 10 characters.

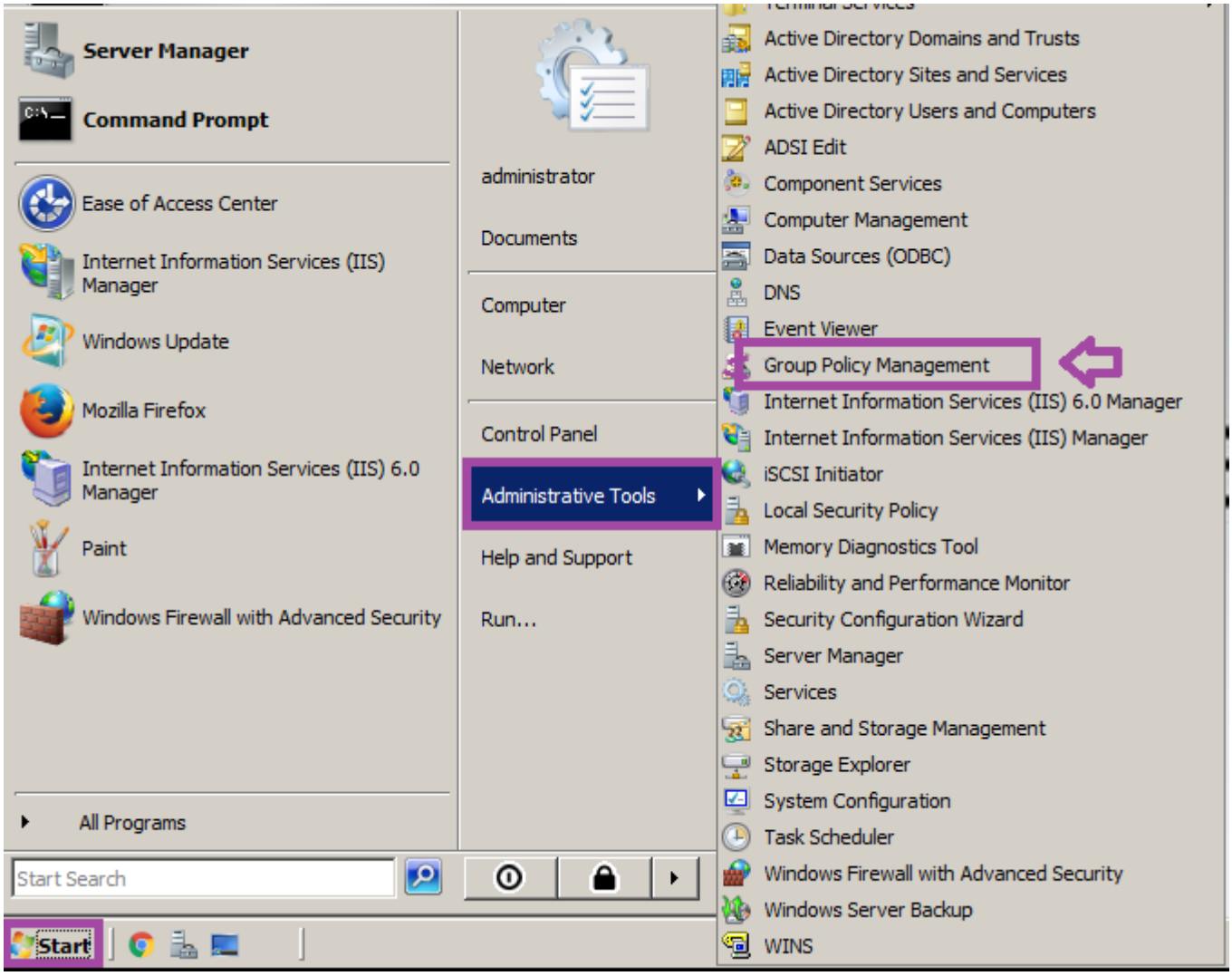
18. **Type** the following command and **press** Enter to exit the command prompt.

C:\>`exit`

THE EXIT COMMAND

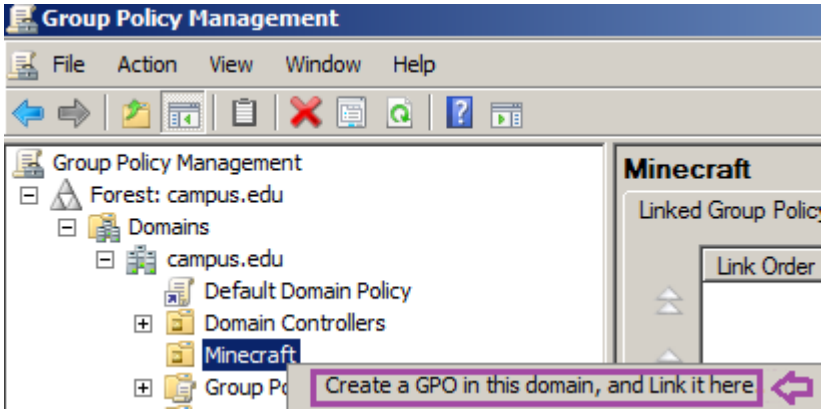
Setting an Organizational Level Policy in Active Directory

1. **Click** on Start, select Administrative Tools, and then **select** Group Policy Management.



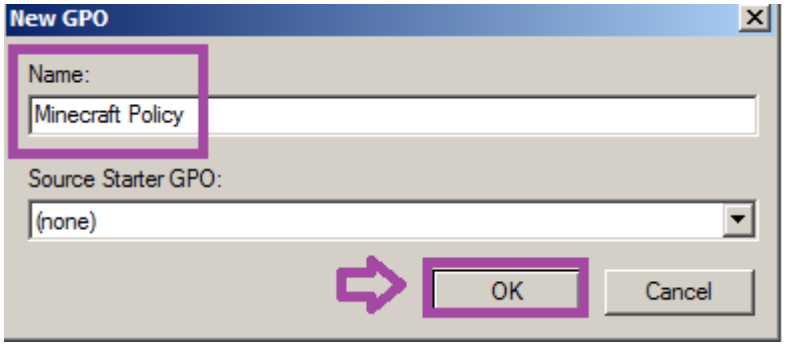
GROUP POLICY MANAGEMENT

2. **Click** the + button to expand Forest:campus.edu. **Click** the + button to expand Domains and then **click** the + button to expand campus.edu. **Right-click** on the Minecraft organizational unit and **select** Create a GPO in this domain, and Link it here...



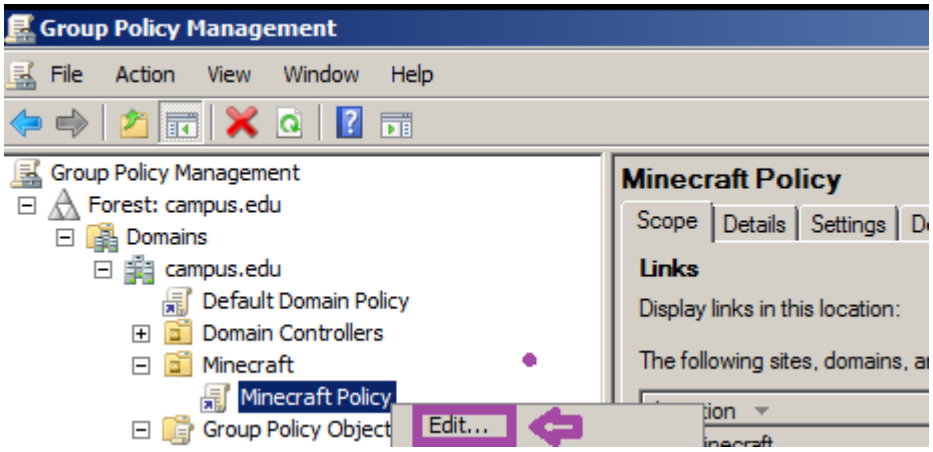
EDIT THE DEFAULT DOMAIN POLICY

3. In the New GPO box, **type** `Minecraft Policy`. **Leave** the Source Starter GPO set to (none) and **click** the OK button to create the new group policy for the Minecraft OU.



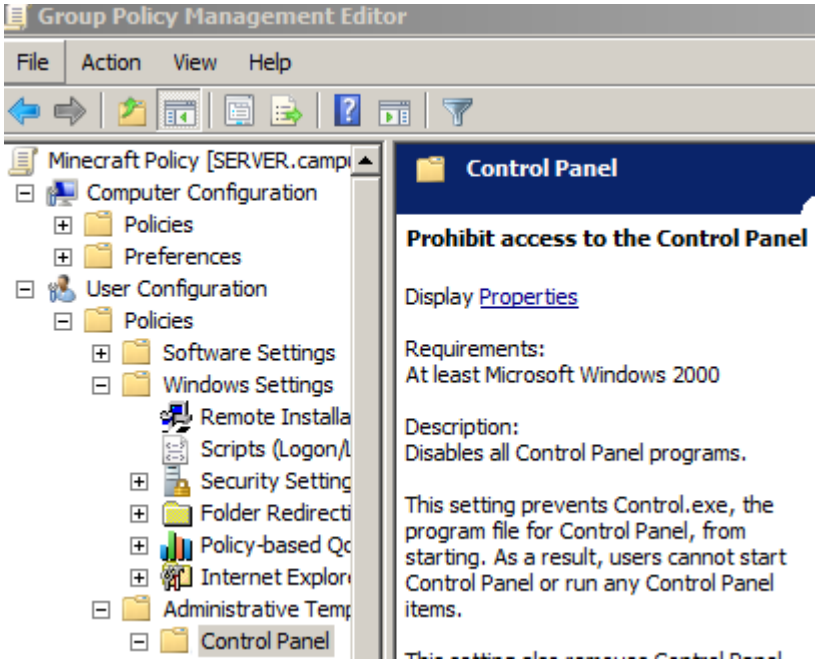
EDIT THE DEFAULT DOMAIN POLICY

4. **Click** the + button to expand Minecraft. **Right-click** on the Minecraft Policy and **choose** Edit.



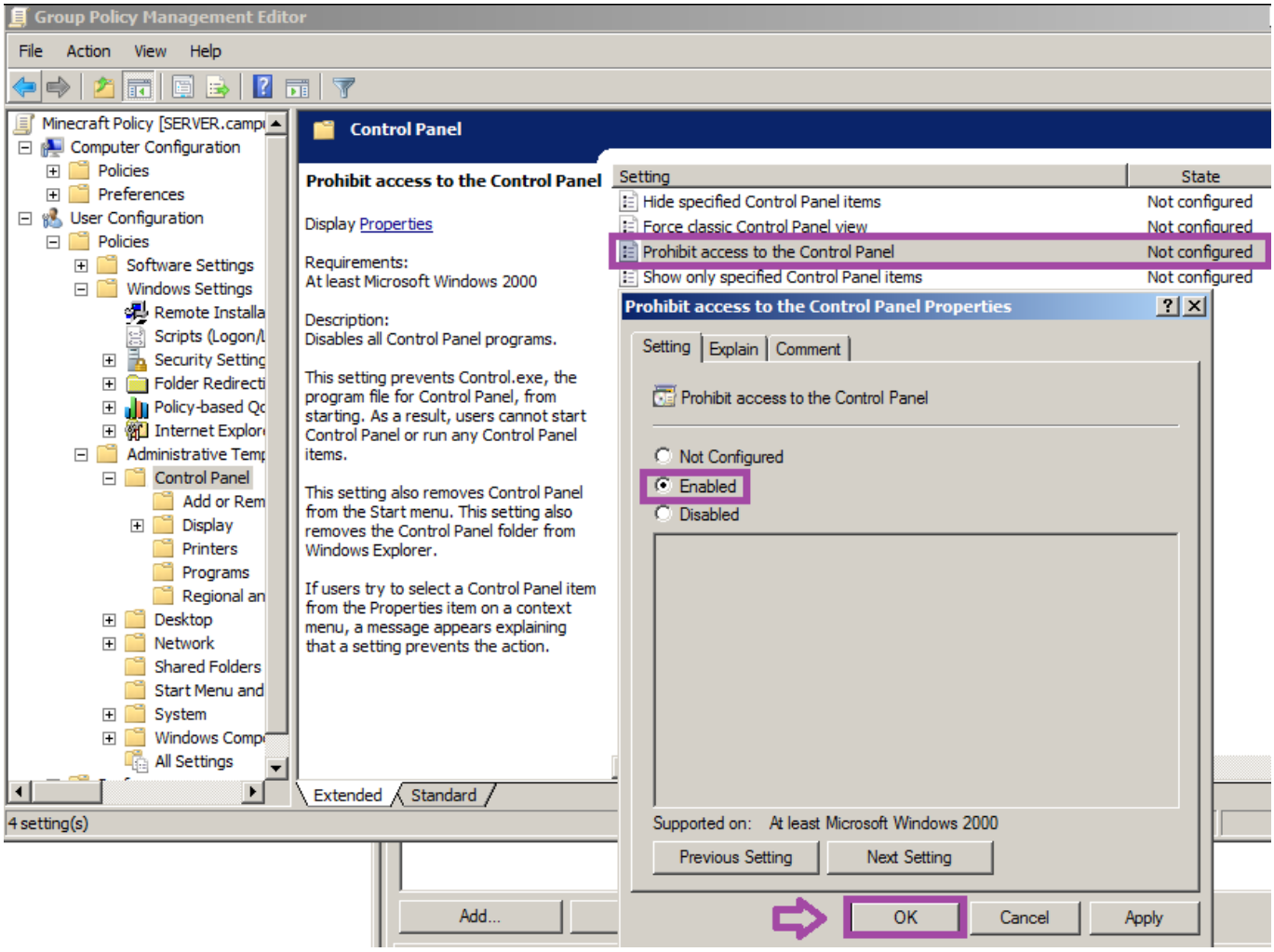
EDIT THE DEFAULT DOMAIN POLICY

5. **Click** the + button to expand User Configuration. **Click** the + button to expand Policies. **Click** the + button to expand Administrative Templates. Then **double-click** on Control Panel.



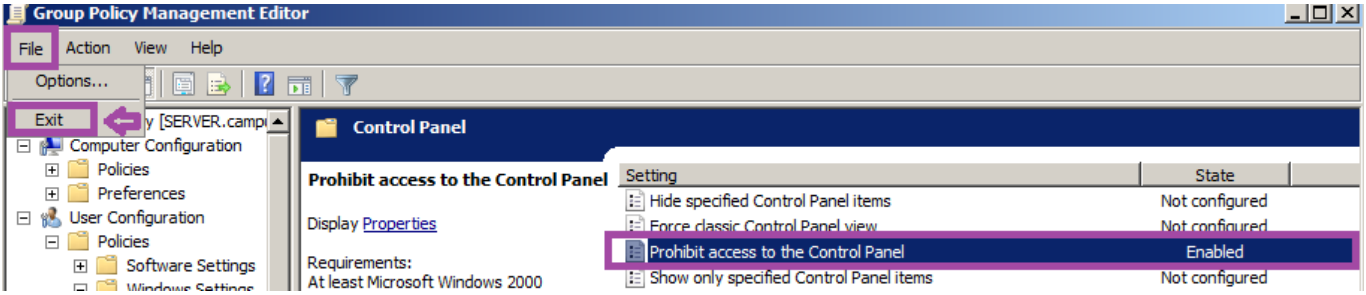
GROUP POLICY MANAGEMENT

6. **Double-click** Prohibit access to the Control Panel. **Click** the Enabled button. **Click** OK.



DENY ACCESS TO THE CONTROL PANEL

7. **Verify** that Prohibit access to the Control Panel is enabled. **Select** File and **choose** Exit.



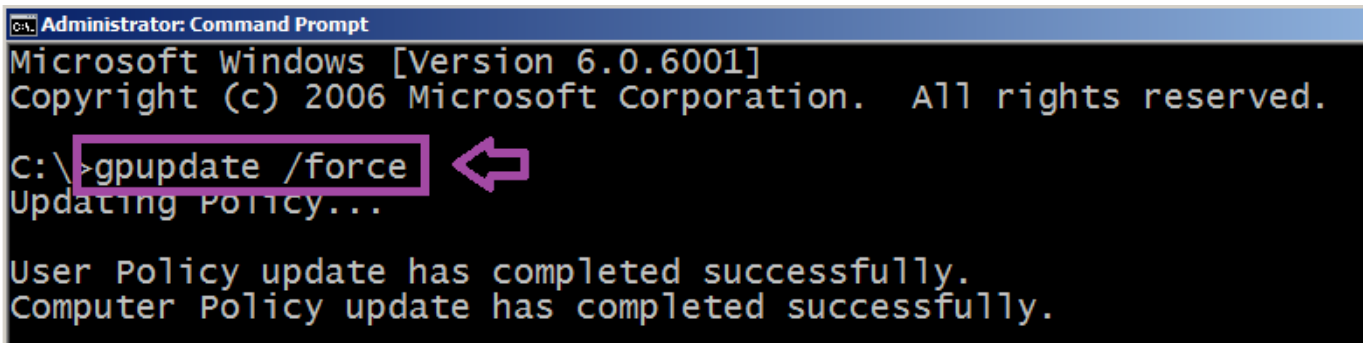
EXITING THE GROUP POLICY MANAGEMENT CONSOLE

8. **Double-click** on the Command Prompt shortcut on the Windows Server 2008 desktop.

SHORTCUT TO COMMAND PROMPT

9. **Type** the following command to refresh the group policy settings on the machine, then **press** Enter.

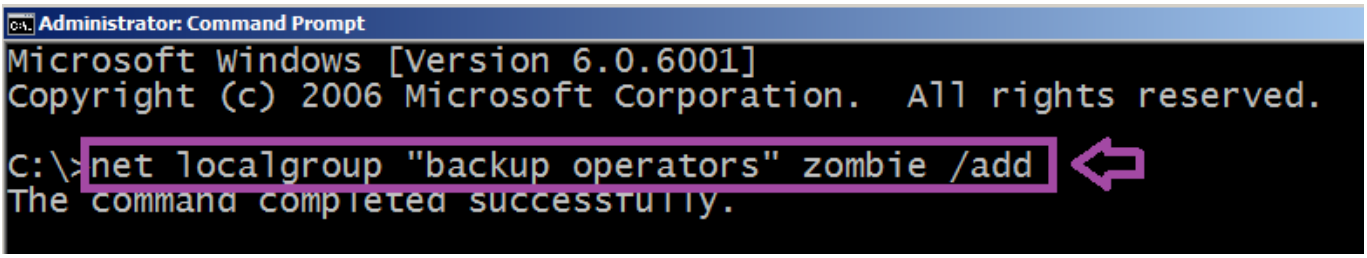
C:\>`gpupdate /force`



THE GPUPDATE COMMAND

10. **Type** the following command to add the user zombie to the backup operators group, then **press** Enter.

C:\>`net localgroup “backup operators” zombie /add`



THE NET LOCALGROUP COMMAND

11. **Type** the following command to **view** the user zombie in the backup operators group, then **press** Enter.

C:\>`net localgroup “backup operators”`

Challenge #

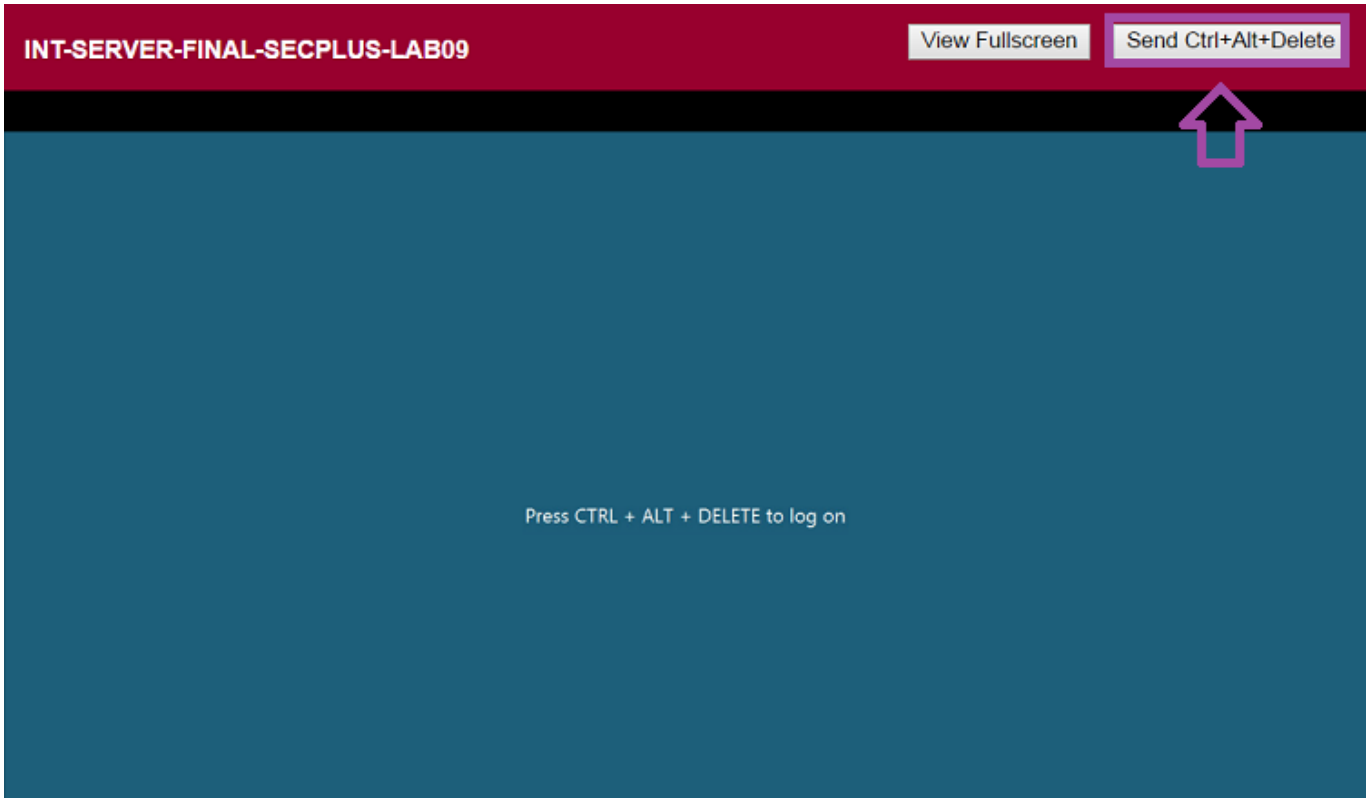
Challenge #

11. **Type** the following command to close the administrator's session on Windows Server, then **press** Enter.

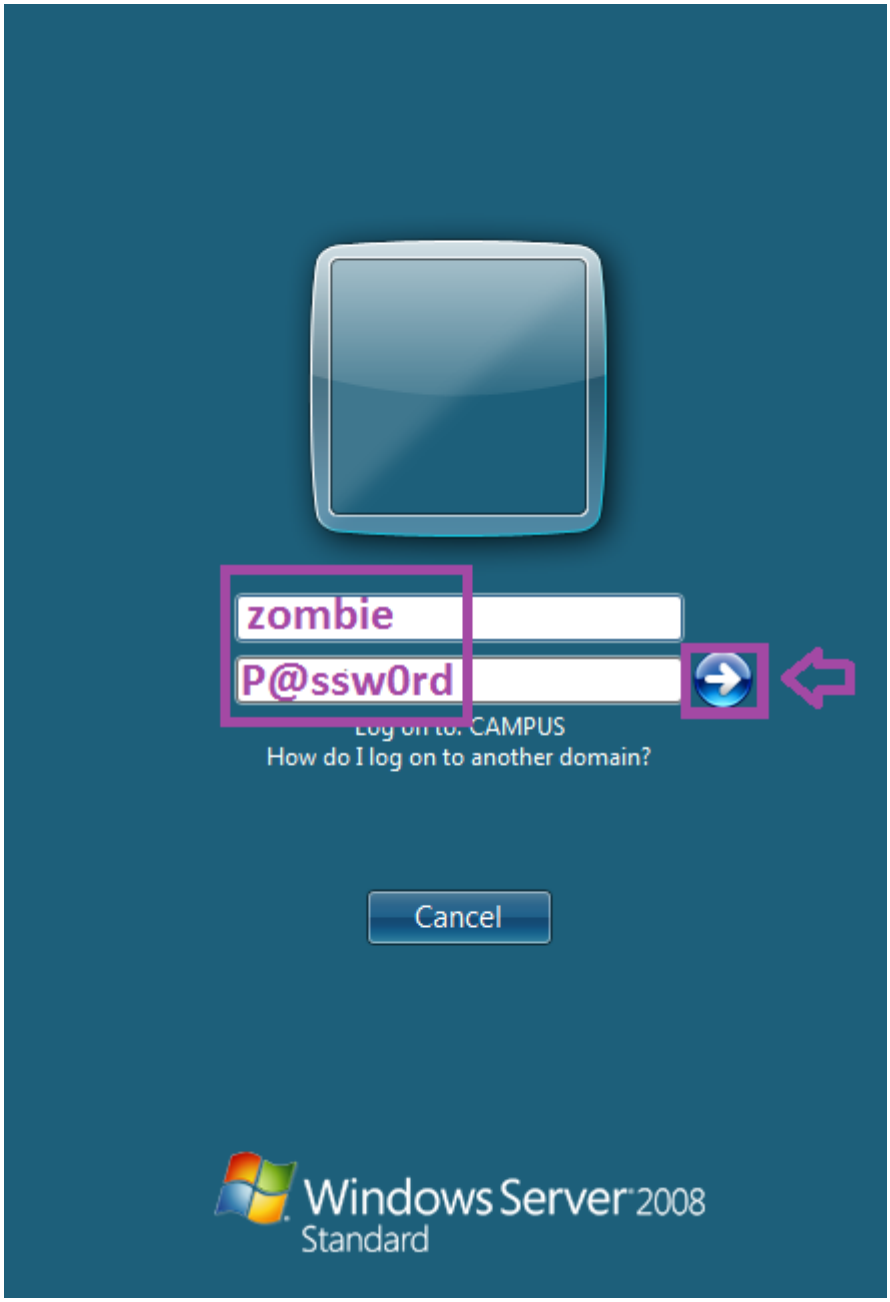
C:\>`logoff`

THE EXIT COMMAND

12. After the machine reboots, click the CTRL-ALT-DELETE button. Then **log in** as `zombie` with the password of `P@ssw0rd`, and **click** the arrow.

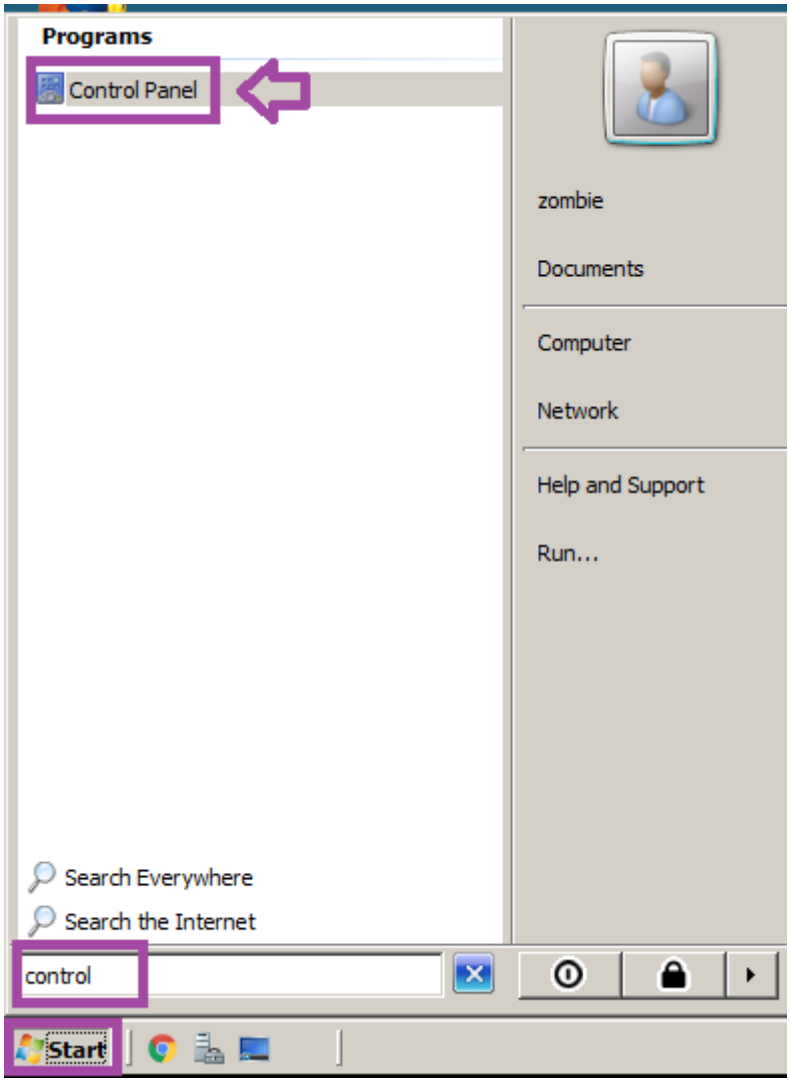


CTRL+ALT+DELETE BUTTON



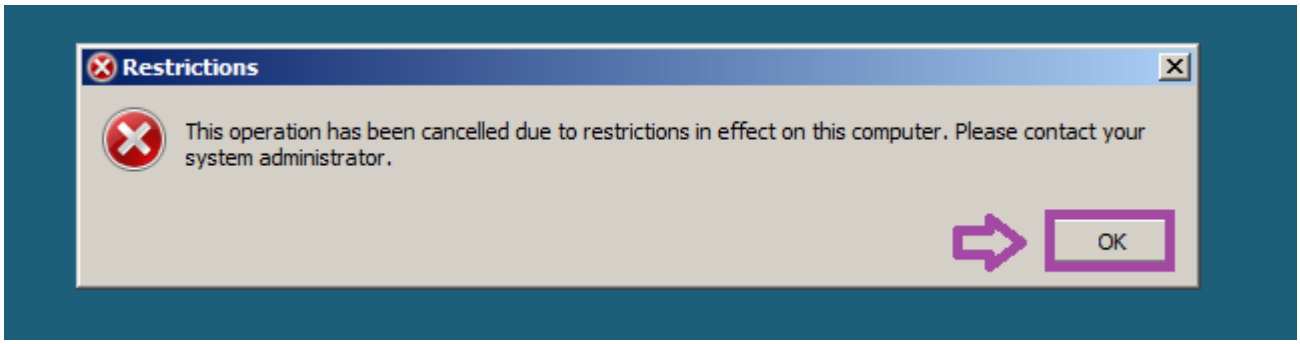
LOG ON TO WINDOWS SERVER

13. **Click** on Start and **type** `control` in the Start search box. **Click** the Control Panel link.



CONTROL COMMAND

14. You will receive a message that "This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator." **Click** the OK button.



MINECRAFT OU USERS ARE RESTRICTED FROM CONTROL PANEL USE

Note: Press the STOP button to complete the lab.