HACKTHEBOX

INTRODUCTION TO ACTIVE DIRECTORY
CHEAT SHEET

Cheat Sheet IAD

Basic Commands Needed

```
xfreerdp /v:<IP> /u:<User> /p:<Password>
ping <IP>
```

General Commands

Get-Module
Returns a list of loaded PowerShell Modules.

Get-Command -Module ActiveDirectory
Lists commands for the module specified.

Get-Help <cmd-let>
Shows help syntax for the cmd-let specified.

Import-Module ActiveDirectory Imports the Active Directory Module

---

Active Directory PowerShell Commands

AD User Commands

New-ADUser -Name "first last" -Accountpassword (Read-Host -AsSecureString "Super$ecurePassword!") -Enabled $true -OtherAttributes @{'title'="Analyst";'mail'="f.last@domain.com"}
Add a user to AD and set attributes.

```
Remove-ADUser -Identity <name>
```
Removes a user from AD with the identity of 'name'.

```
Unlock-ADAccount -Identity <name>
```
Unlocks a user account with the identity of 'name'.

```
Set-ADAccountPassword -Identity <'name'> -Reset -NewPassword (ConvertTo-
SecureString -AsPlainText "NewP@ssw0rdReset!" -Force)
```
Set the password of an AD user to the password specified.

```
Set-ADUser -Identity amasters -ChangePasswordAtLogon $true
```
Force a user to change their password at next logon attempt.

AD Group Commands

```
New-ADOrganizationalUnit -Name "name" -Path "OU=folder,DC=domain,DC=local"
```
Create a new AD OU container named "name" in the path specified.

```
New-ADGroup -Name "name" -SamAccountName analysts -GroupCategory Security -
GroupScope Global -DisplayName "Security Analysts" -Path
"CN=Users,DC=domain,DC=local" -Description "Members of this group are Security
Analysts under the IT OU"
```
Create a new security group named "name" with the accompanying attributes.

```
Add-ADGroupMember -Identity 'group name' -Members 'ACepheus,OStarchaser,ACallisto'
```
Add an AD user to the group specified.

GPO Commands

```
Copy-GPO -SourceName "GPO to copy" -TargetName "Name"
```
Copy a GPO for use as a new GPO with a target name of "name".

```
New-GPLink -Name "Security Analysts Control" -Target "ou=Security
Analysts,ou=IT,OU=HQ-NYC,OU=Employees,OU=Corp,dc=INLANEFREIGHT,dc=LOCAL" -
LinkEnabled Yes
```
Create a new GPO and link it to a specific OU or security group.

```
Set-GPLink -Name "Security Analysts Control" -Target "ou=Security
Analysts,ou=IT,OU=HQ-NYC,OU=Employees,OU=Corp,dc=INLANEFREIGHT,dc=LOCAL" -
LinkEnabled Yes
```
Link an existing GPO for use to a specific OU or security group.

Computer Commands

```
Add-Computer -DomainName 'INLANEFREIGHT.LOCAL' -Credential 'INLANEFREIGHT\HTB-
student_adm' -Restart
```
Add a new computer to the domain using the credentials specified.

```
Add-Computer -ComputerName 'name' -LocalCredential '.\localuser' -DomainName
'INLANEFREIGHT.LOCAL' -Credential 'INLANEFREIGHT\htb-student_adm' -Restart
```
Remotely add a computer to a domain.

```
Get-ADComputer -Identity "name" -Properties * | select CN,CanonicalName,IPv4Address
```
Check for a computer named "name" and view its properties.

References

Microsoft