HACKTHEBOX

ACTIVE DIRECTORY LDAP
CHEAT SHEET

Command	Description
`xfreerdp /v:<target IP address> /u:htb-student /p:<password>`	RDP to lab target
`Get-ADGroup -Identity "<GROUP NAME" -Properties *`	Get information about an AD group
`whoami /priv`	View a user's current rights
`Get-WindowsCapability -Name RSAT* -Online | Select-Object -Property Name, State`	Check if RSAT tools are installed
`Get-WindowsCapability -Name RSAT* -Online | Add-WindowsCapability –Online`	Install all RSAT tools
`runas /netonly /user:htb.local\jackie.may powershell`	Run a utility as another user
`Get-ADObject -LDAPFilter '(objectClass=group)' | select cn`	LDAP query to return all AD groups
`Get-ADUser -LDAPFilter '(userAccountControl:1.2.840.113556.1.4.803:=2)' | select name`	List disabled users
`(Get-ADUser -SearchBase "OU=Employees,DC=INLANEFREIGHT,DC=LOCAL" -Filter *).count`	Count all users in an OU
`get-ciminstance win32_product | fl`	Query for installed software
`Get-ADComputer -Filter "DNSHostName -like 'SQL*'"`	Get hostnames with the word "SQL" in their hostname

Command	Description
`Get-ADGroup -Filter "adminCount -eq 1" | select Name`	Get all administrative groups
`Get-ADUser -Filter {adminCount -eq '1' -and DoesNotRequirePreAuth -eq 'True'}`	Find admin users that don't require Kerberos Pre-Auth
`Get-ADUser -Filter {adminCount -gt 0} -Properties admincount,useraccountcontrol`	Enumerate UAC values for admin users
`Get-WmiObject -Class win32_group -Filter "Domain='INLANEFREIGHT'"`	Get AD groups using WMI
`([adsisearcher]"(&(objectClass=Computer))").FindAll()`	Use ADSI to search for all computers

HTB ACADEMY CHEATSHEET