HACKTHEBOX

ACTIVE DIRECTORY POWERVIEW

CHEAT SHEET

Command	Description
`xfreerdp /v:<target IP address> /u:htb-student /p:<password>`	RDP to lab target
`Get-DomainPolicy`	View the domain password policy
`.\SharpView.exe ConvertTo-SID -Name sally.jones`	Convert a username to a SID
`.\SharpView.exe Convert-ADName -ObjectName S-1-5-21-2974783224-3764228556-2640795941-1724`	Convert a SID to a username
`Get-DomainUser harry.jones | ConvertFrom-UACValue -showall`	List all UAC values
`.\SharpView.exe Get-Domain`	View information about the current domain
`.\SharpView.exe Get-DomainOU`	List all OUs
`.\SharpView.exe Get-DomainUser -KerberosPreauthNotRequired`	Find ASREPRoastable users
`Get-DomainComputer`	Get a listing of domain computers
`.\SharpView.exe Get-DomainGPO | findstr displayname`	List all GPO names
`Get-DomainGPO -ComputerIdentity WS01`	List GPOs on a specific host
`Test-AdminAccess -ComputerName SQL01`	Test local admin access on a remote host

Command	Description
`.\SharpView.exe Get-NetShare -ComputerName SQL01`	Enumerate open shares on a remote computer
`Find-DomainUserLocation`	Find machines where domain users are logged in
`Get-DomainTrust`	View a list of domain trusts
`(Get-DomainUser).count`	Count all domain users
`.\SharpView.exe Get-DomainUser -Help`	Get help about a SharpView function
`Get-DomainUser -Properties samaccountname,description | Where {$_.description -ne $null}`	Find non-blank user description fields
`.\SharpView.exe Get-DomainUser -SPN`	Find users with SPNs set
`Find-ForeignGroup`	Find foreign domain users
`Get-DomainGroup -Properties Name`	List domain groups
`.\SharpView.exe Get-DomainGroupMember -Identity 'Help Desk'`	Get members of a domain group
`.\SharpView.exe Get-DomainGroup -AdminCount`	List protected groups
`.\SharpView.exe Find-ManagedSecurityGroups`	List managed security groups
`Get-NetLocalGroup -ComputerName WS01`	Get local groups on a host
`.\SharpView.exe Get-NetLocalGroupMember -ComputerName WS01`	Get members of a local group
`.\SharpView.exe Get-DomainComputer -Unconstrained`	Find computers that allow unconstrained delegation
`Get-DomainComputer -TrustedToAuth`	Find computers set with constrained delegation
`Get-DomainObjectAcl -Identity harry.jones`	Enumerate ACLs on a user

Command	Description
`Find-InterestingDomainAcl`	Find objects in the domain with modification rights over non built-in objects
`Get-PathAcl "\\SQL01\DB_backups"`	Find the ACLs set on a directory
`gpresult /r /S WS01`	Get a report of all GPOs applied to a host
`Get-DomainGPO | Get-ObjectAcl`	Find GPO permissions
`Get-DomainTrustMapping`	Enumerate trusts for our domain/reachable domains