**CRTP Cheatsheet**

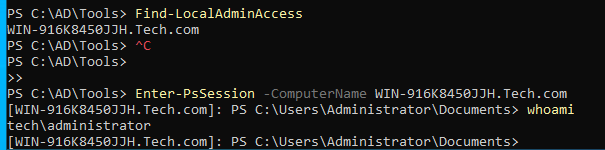
**Lateral Movement**

use derivtive local admin privilages to go to adminsrv

after we ran admin recon or recon from there find out that there are some privilages somewhere where domain admin privilages are available then we escalate our privilages

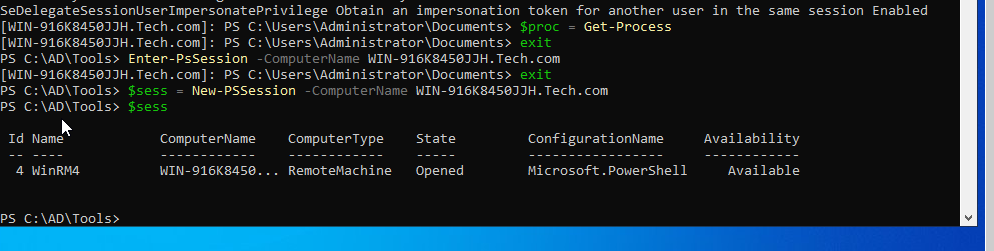
Lateral Movement

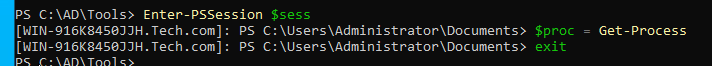
We have admin access to WIN-916K8450JJH.tech.com machine i used enetr ps session now we have interactively logged on to that particular machine



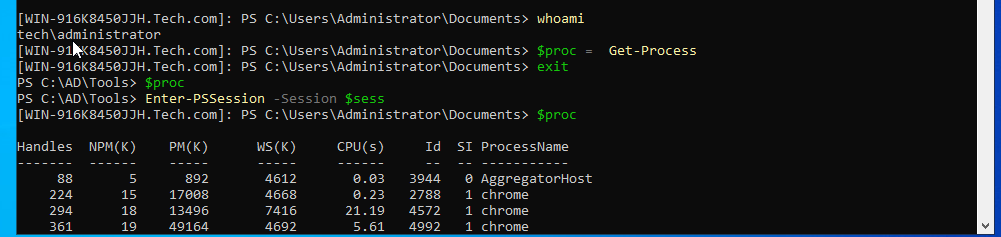
This is one to one remoting

Now $sess variable holds the credentials



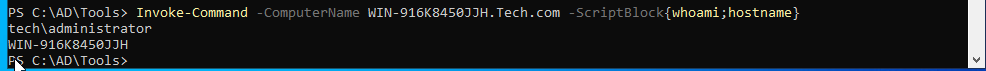


This is what one to one removing is userfull for administration and for lateral movement



When you have 1000 or 10000 or even more machines in such cases one to many remoting

In invoke command we simply provide list of computer it checks for us parrallely

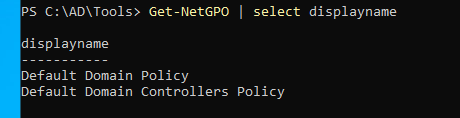


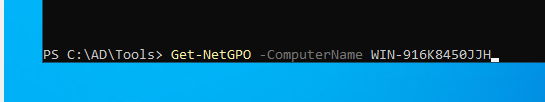
**Mimikatz**

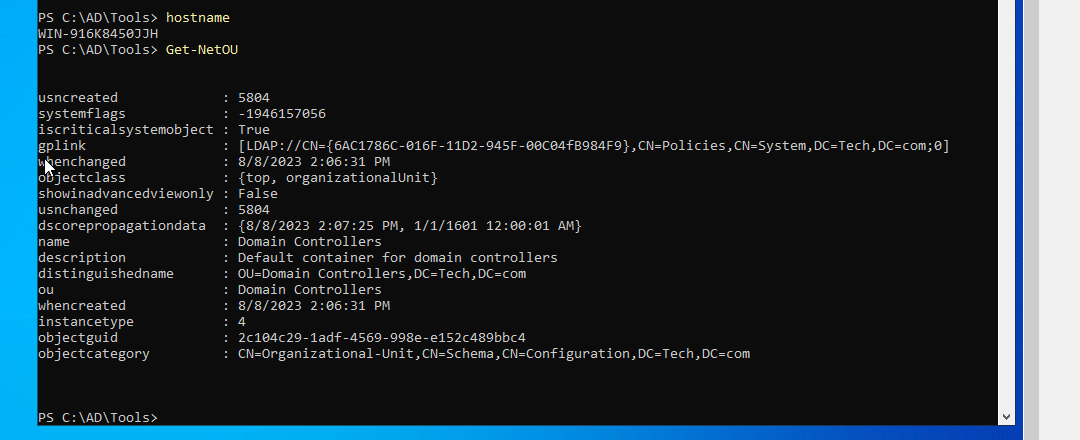
If we have ntlm hash of domain administrator we can run exec tables which hold

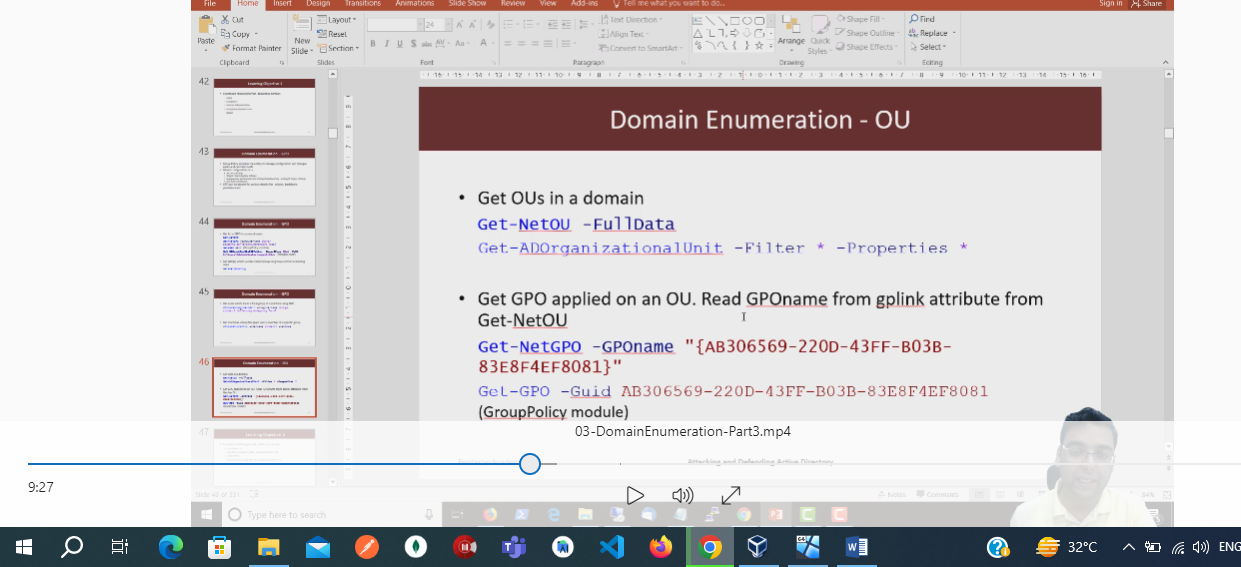
Ticket for domain administrator

**Group Policy**

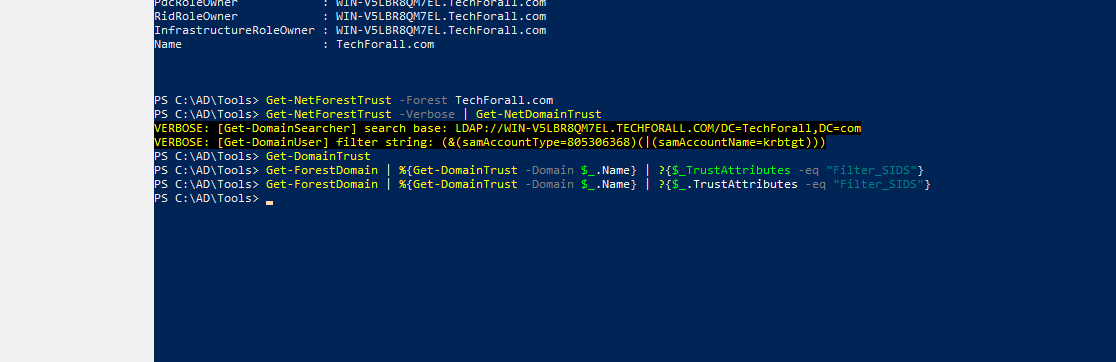


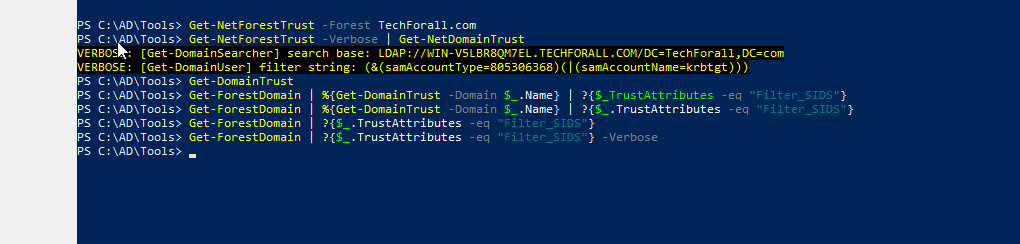


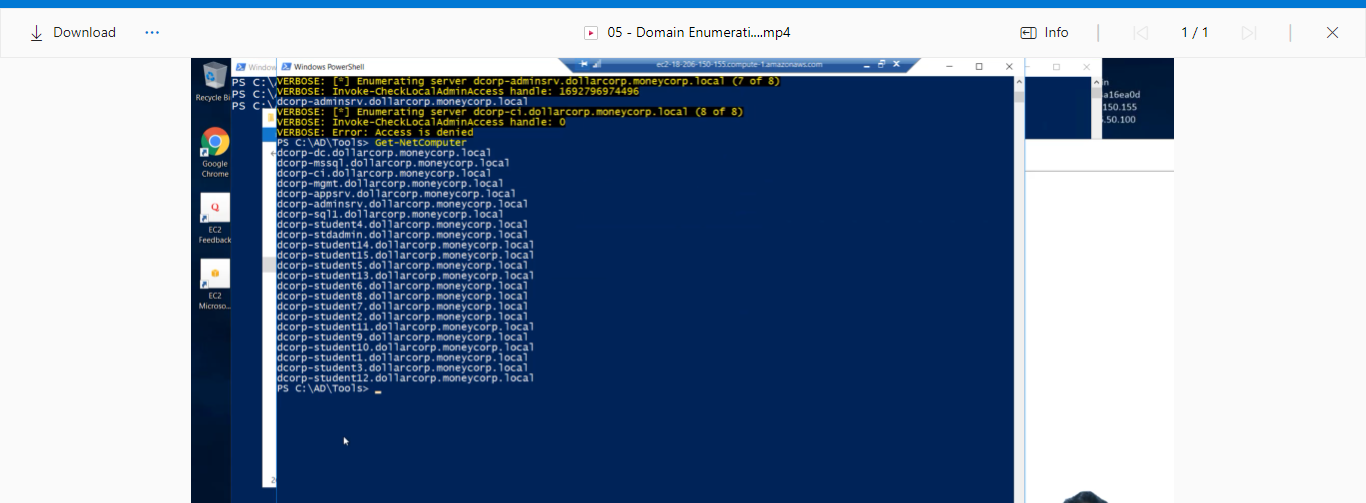


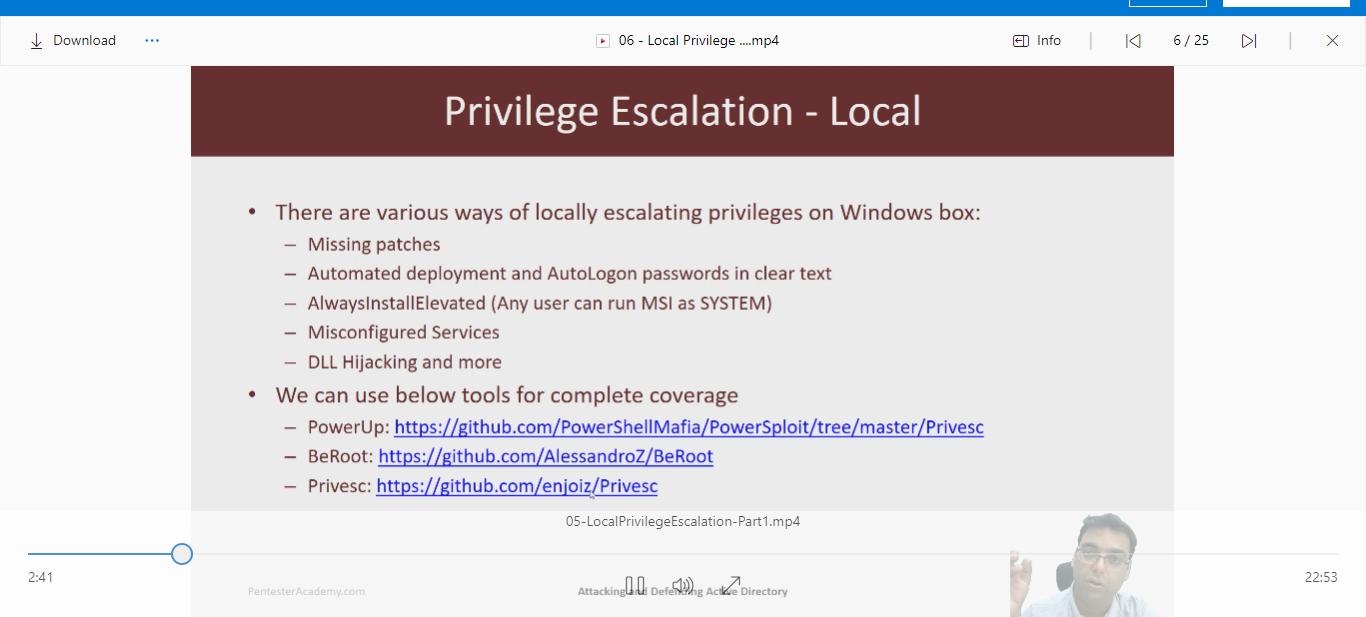


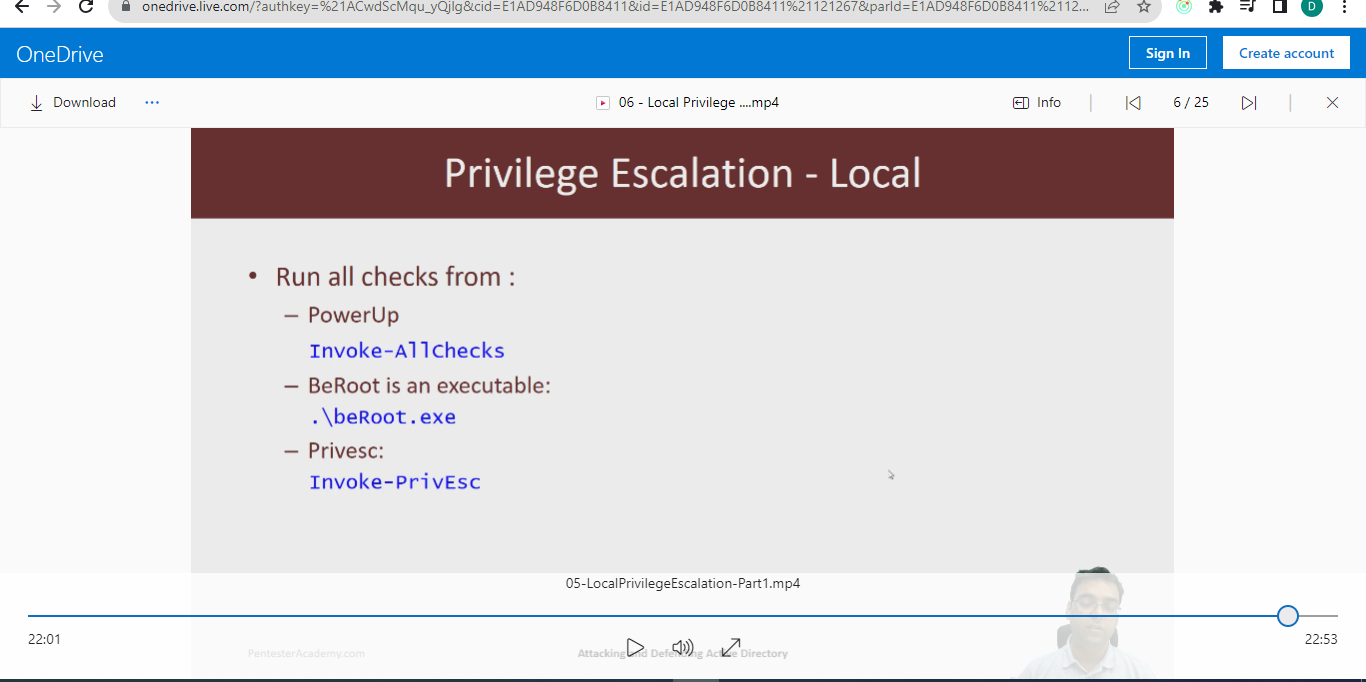
**Learning Objective 5**

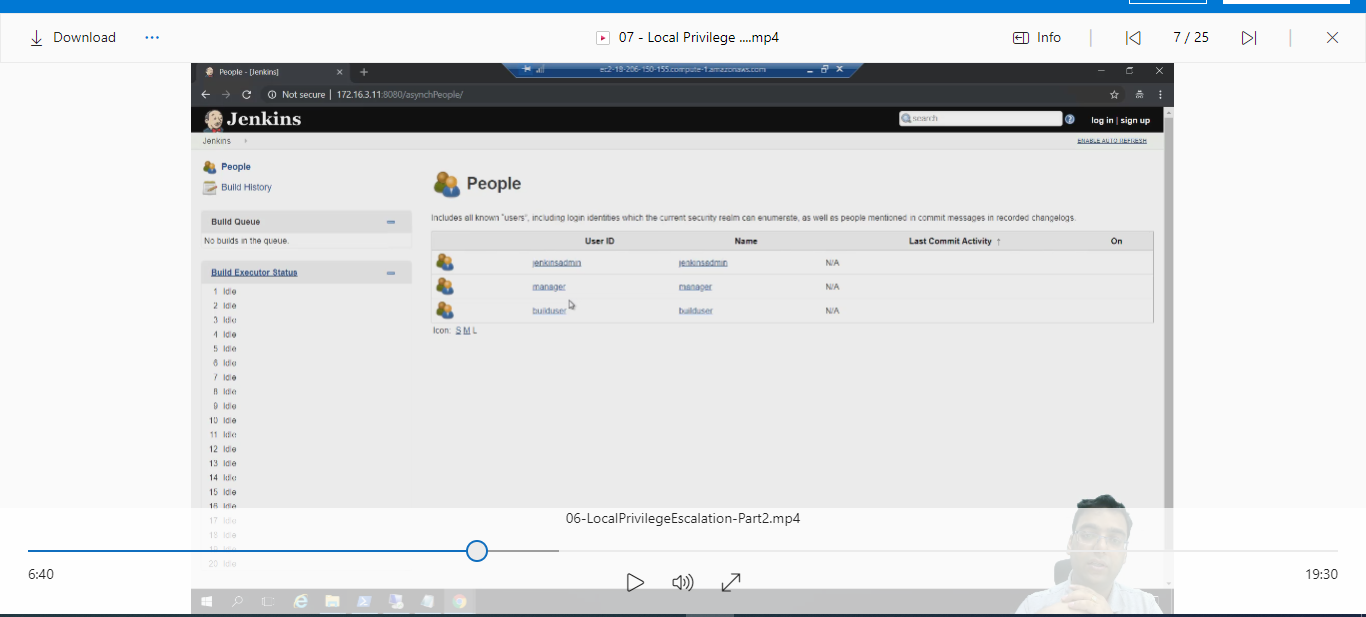




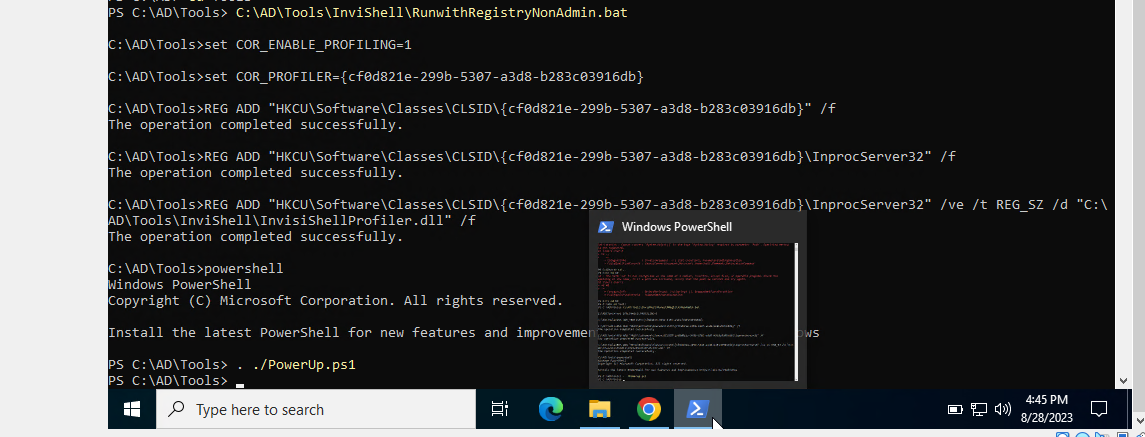


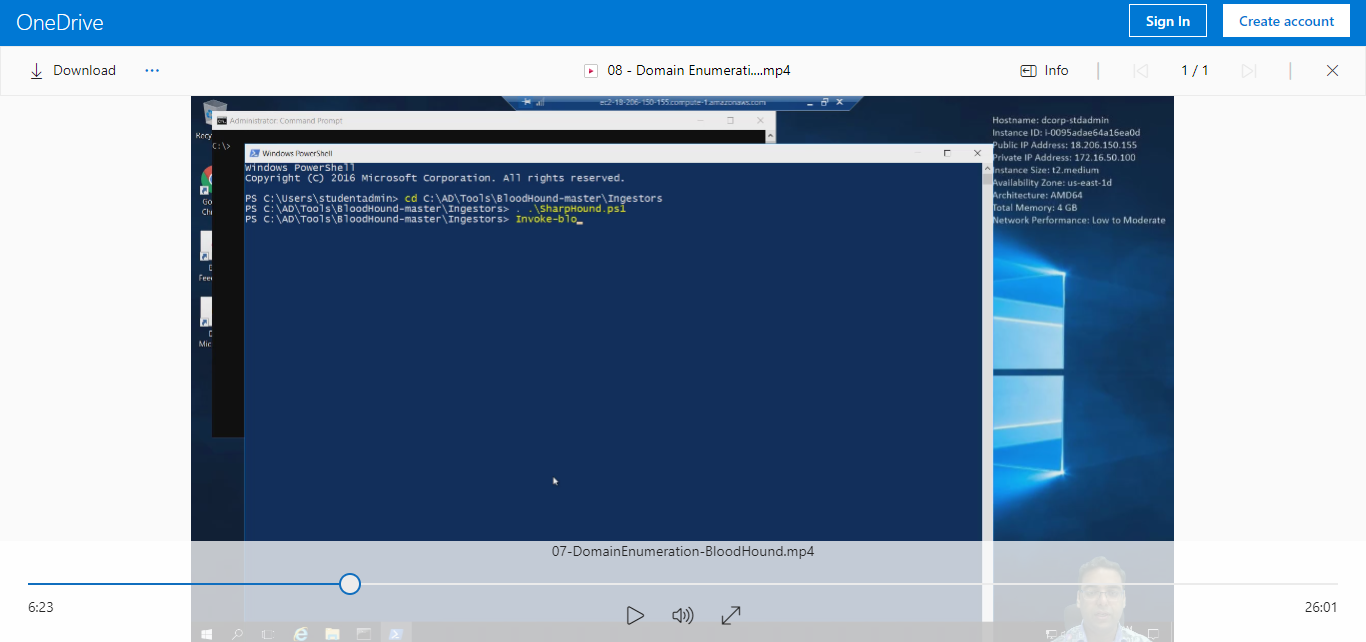


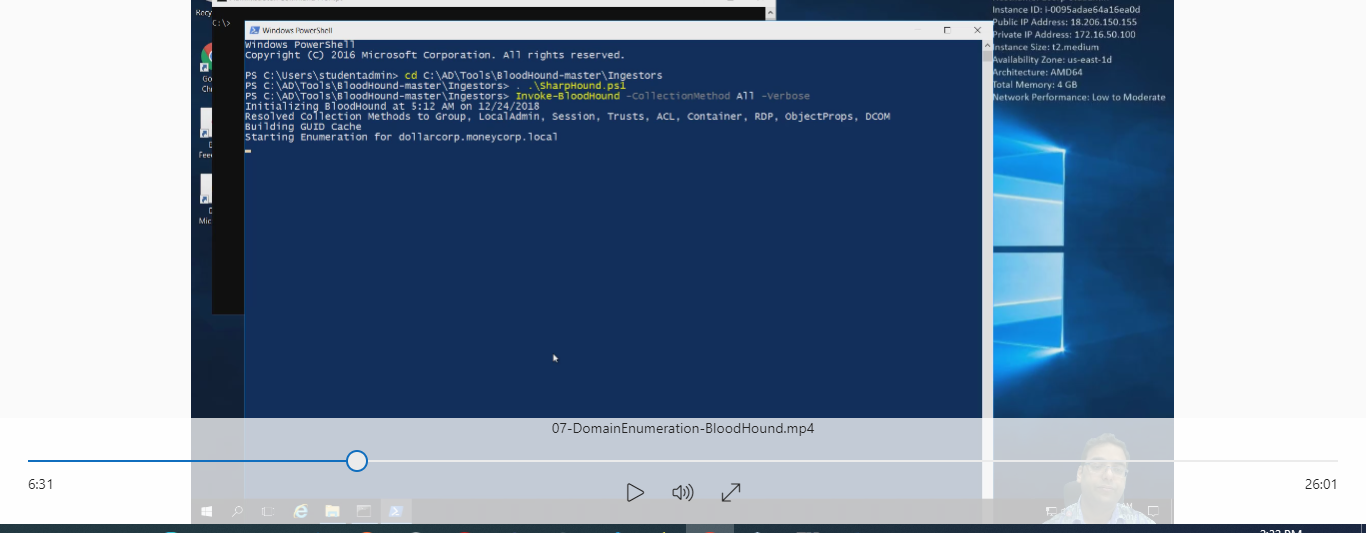


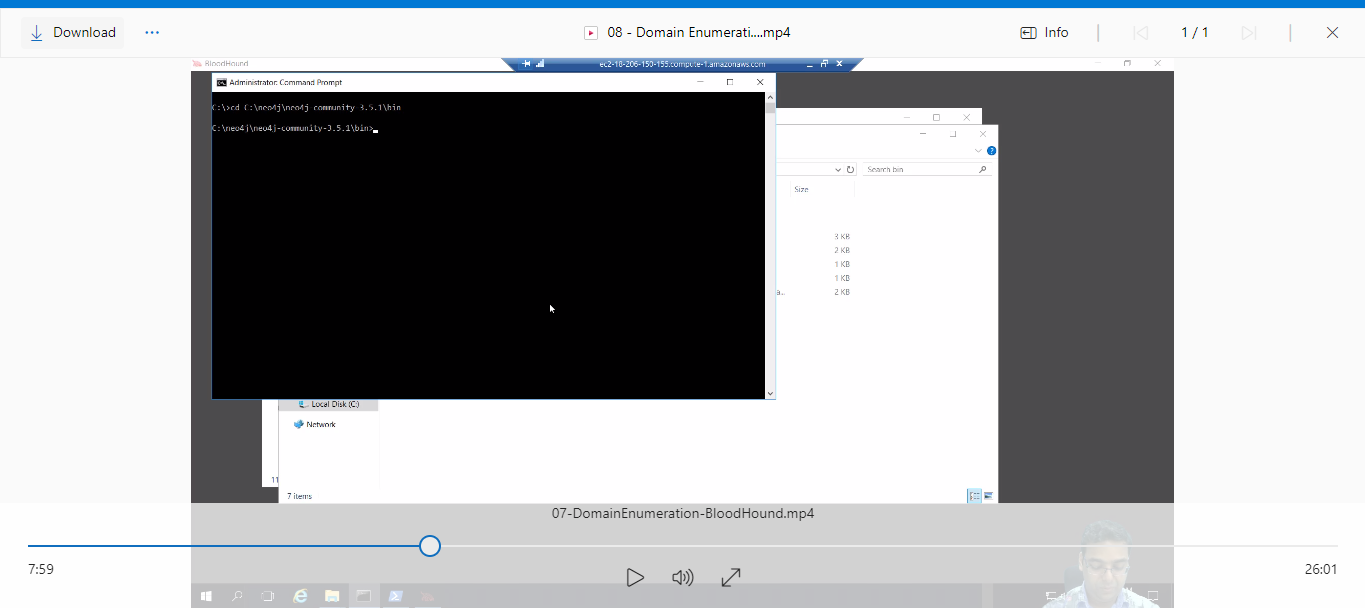


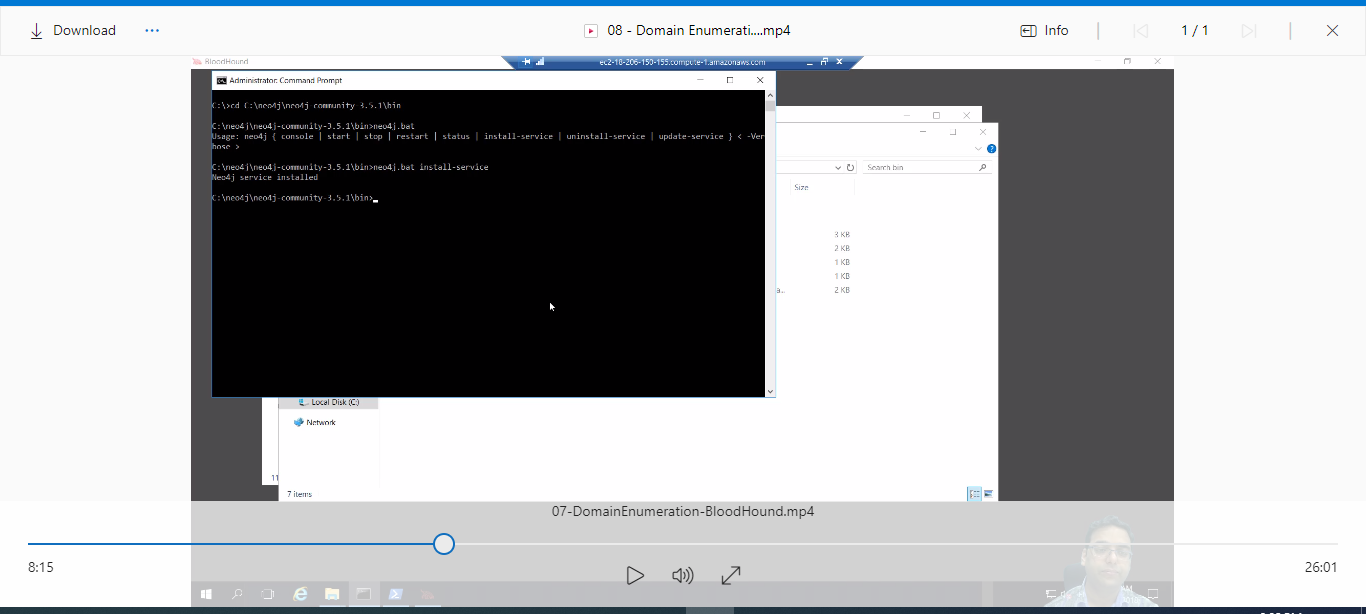
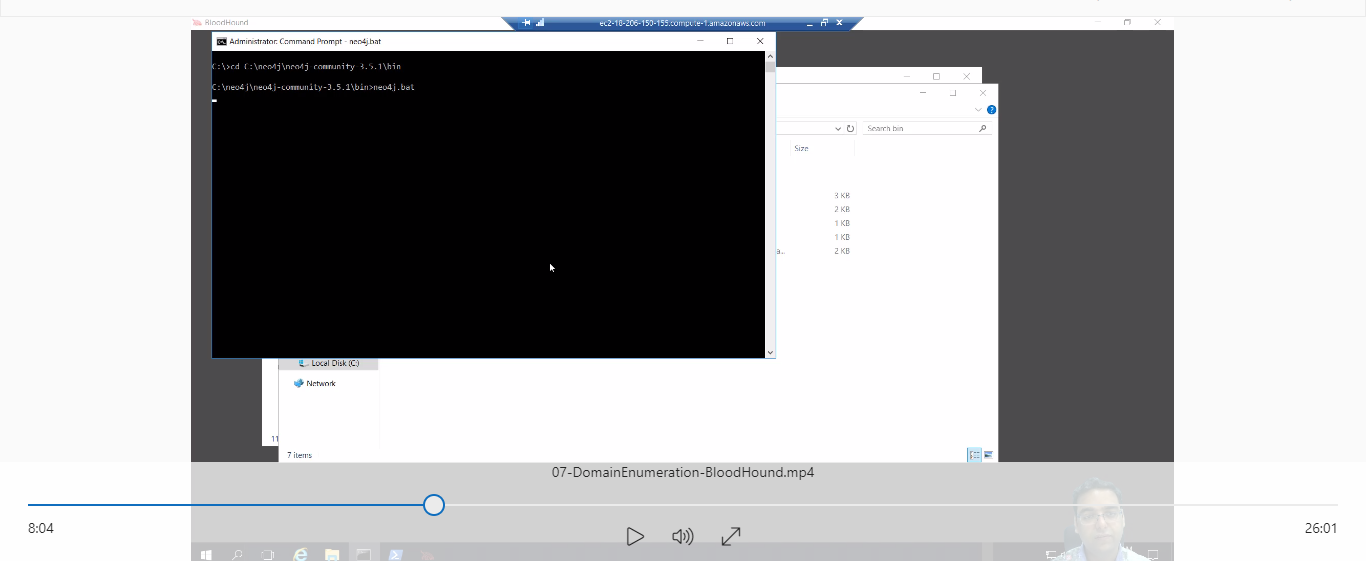
**Learning Objective 5**

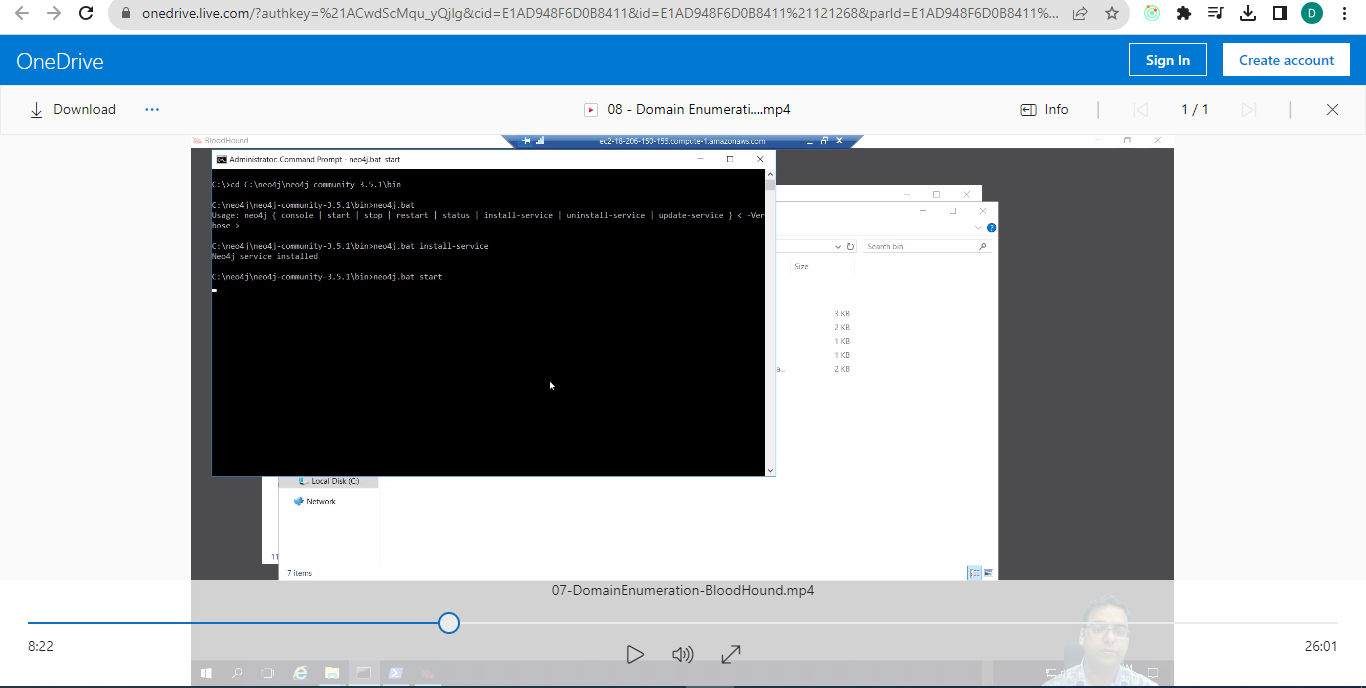


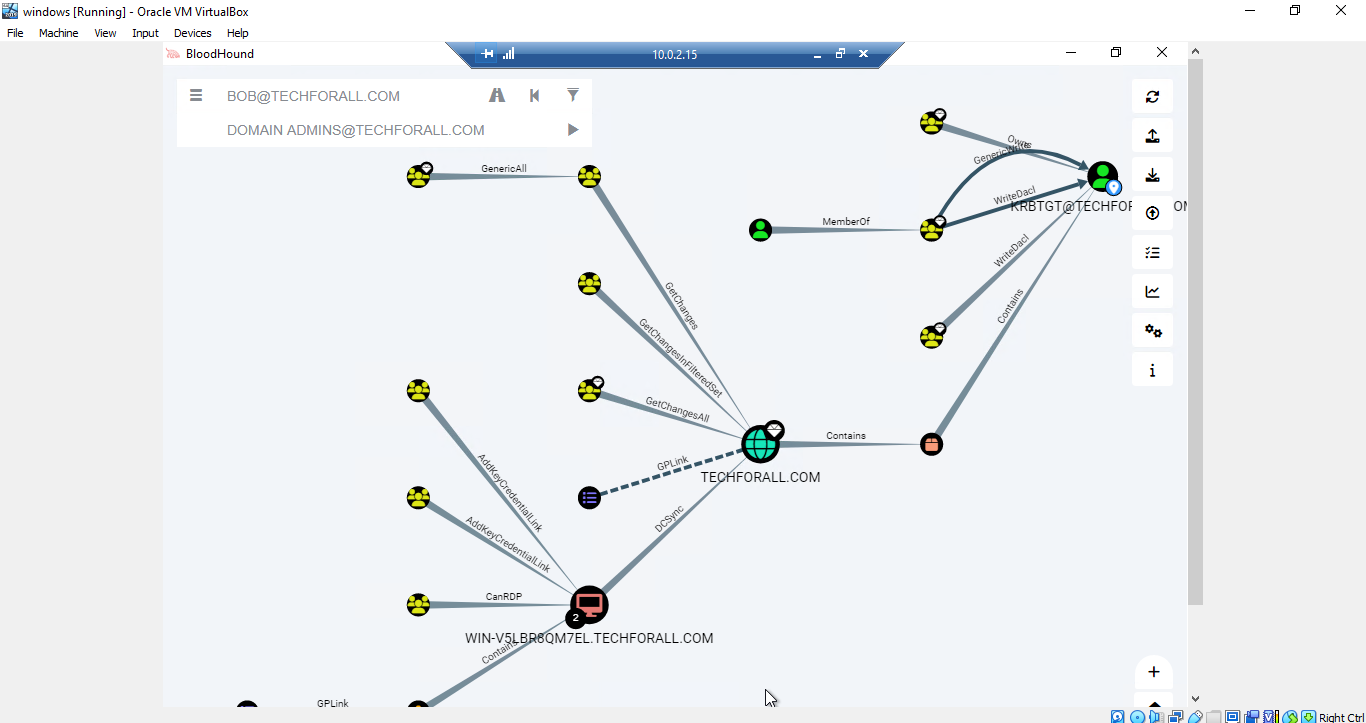












**Mimikatz**

