PowerShell Lecture Notes - 5

Topic: Active Directory

Course: Hands-On Penetration Testing With Powershell
Date: 19-03-2024
Professor/Speaker:

Questions	Notes
Exploitation	-> Data Infiltration -> Get-ScheduledTask : Shows the list of scheduled tasks. -> Get-ScheduledTask | where {$_.TaskPath -notlike "\Microsoft"} | ft TaskName, TaskPath, State
Privilege Escalation	-> When attacker exploits rights and permissions of targeted account for the purpose of gaining further important permissions. -> (get-acl c:\).access | ft IdentityReference, FileSystemRights, AccessControlType, Inherited, InheritanceFlags -auto : To retrieve Admin control list of C: drive. -> Get-ADGroupMember -Identity Administrator : List Administrators in the active directory group.
Payloads	-> Modify and Configure payloads according to your needs. -> Payloads may contain Trojans, malwares, keyloggers,etc.